ЛАБОРАТОРНАЯ РАБОТА №4
«SearchInform»
Вариант 5

Плотников Антон, А3401

Санкт-Петербург, 2017

1. Подготовка окружения

1.1. Ход работы

1.1.1. Подготовка окружения для виртуализации

В данной работе используется программа *VMPlayer* для виртуализации и образ виртуальной машины, предоставляемый компанией *SearchInform* в учебных целях. Конфигурация тривиальна и не использует дополнительных настроек, в качестве хоста используется операционная система на базе ядра *linux 4.11*.

1.1.2. Смена пароля

Для смены пароля необходимо зайти в панель управления компьютером → администрирование → управление компьютером → служебные программы → пользователи → Администратор.

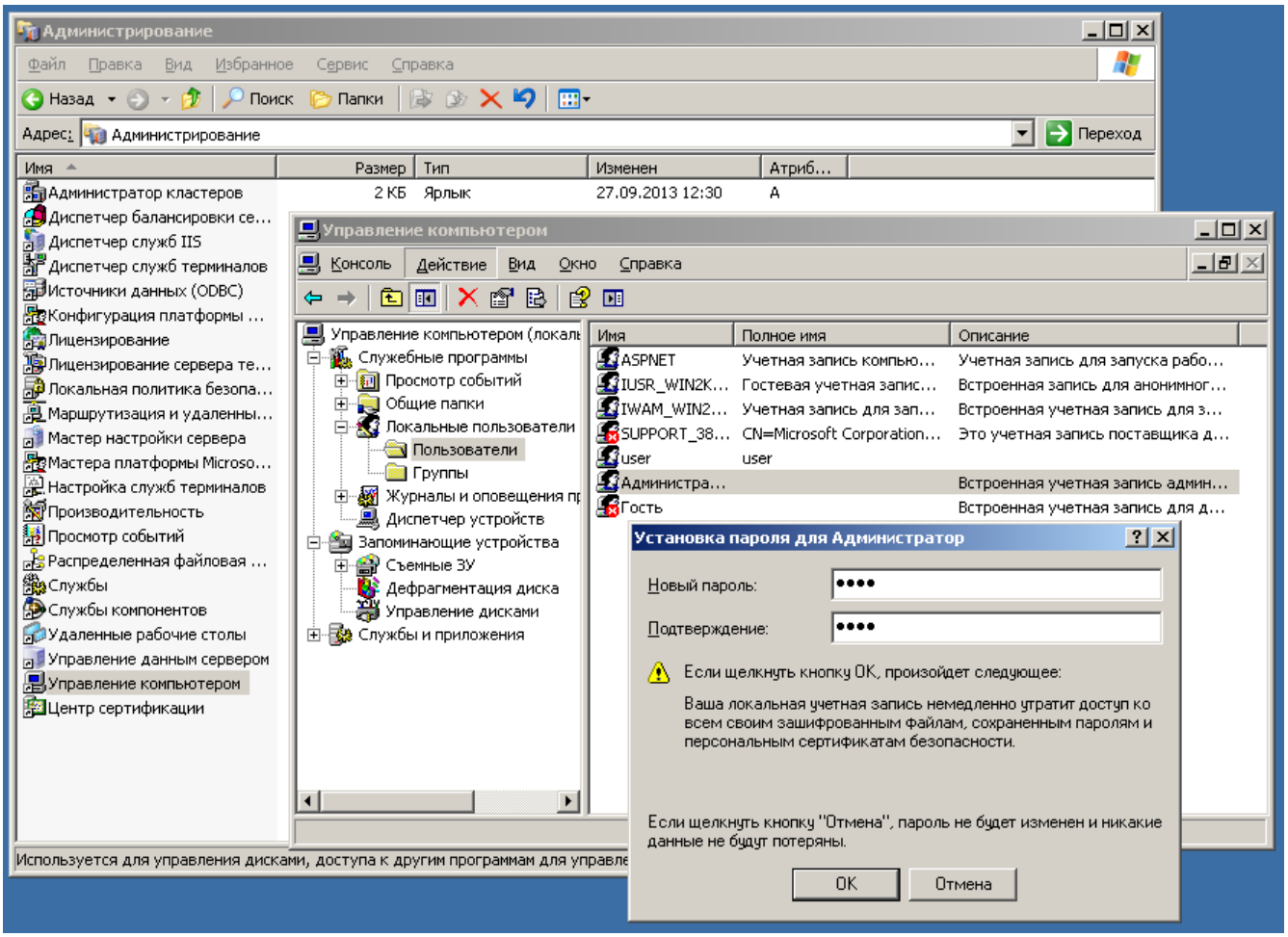


Рис. 1: Изменение пароля администратора.

1.1.3. Изменение пароля доступа к консолям основных серверов

Изменить пароли можно с помощью программ *Search Server Console*, *SearchInform DataCenter*, *SearchInform EndpointSniffer*, *SearchInform NetworkSniffer*, *SearchInform ReportCenter Console*, *SearchInform AlertCenter Client* как показано на рис. 2 - 7.

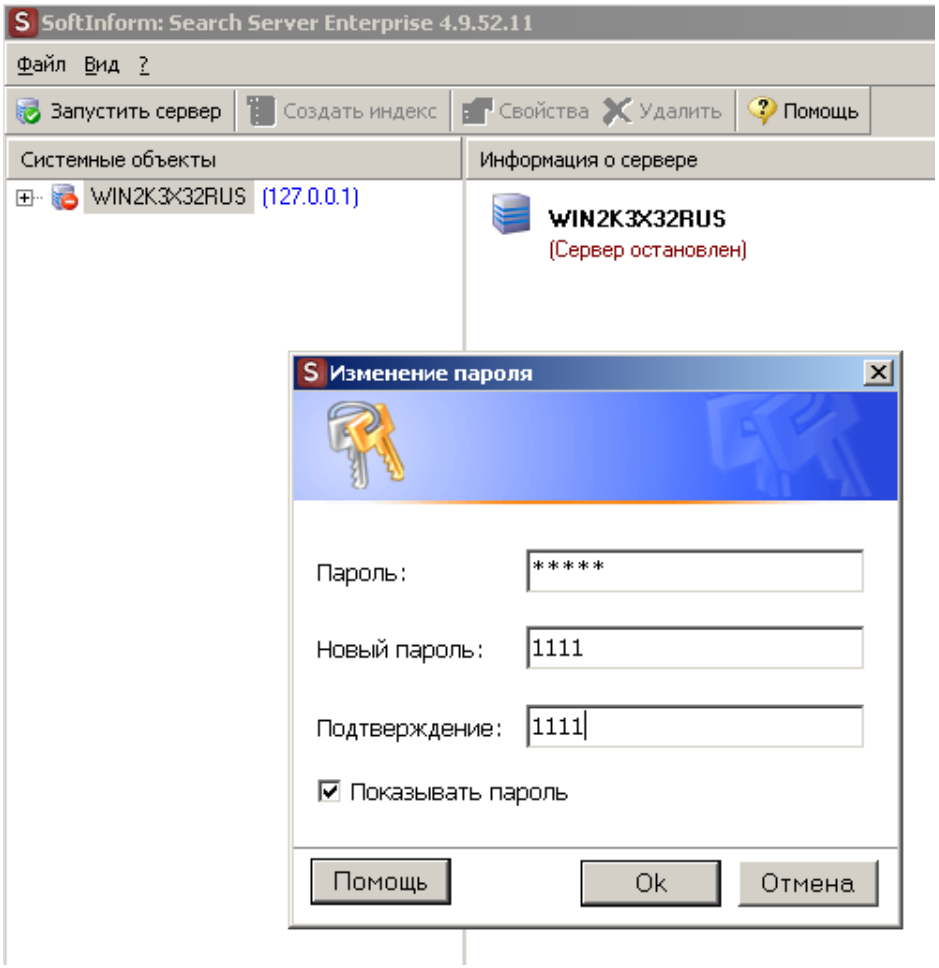


Рис. 2: Изменение пароля сервера.

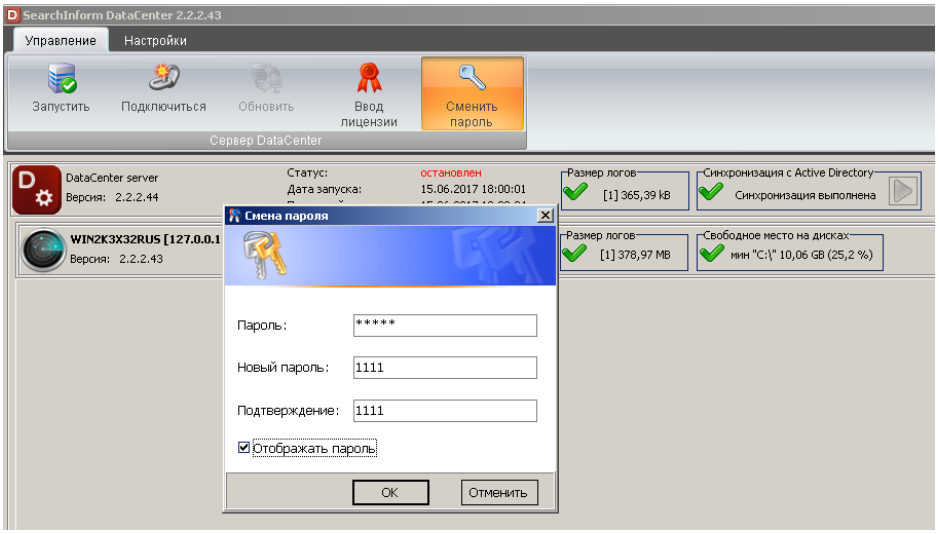


Рис. 3: Изменение пароля DataCenter.

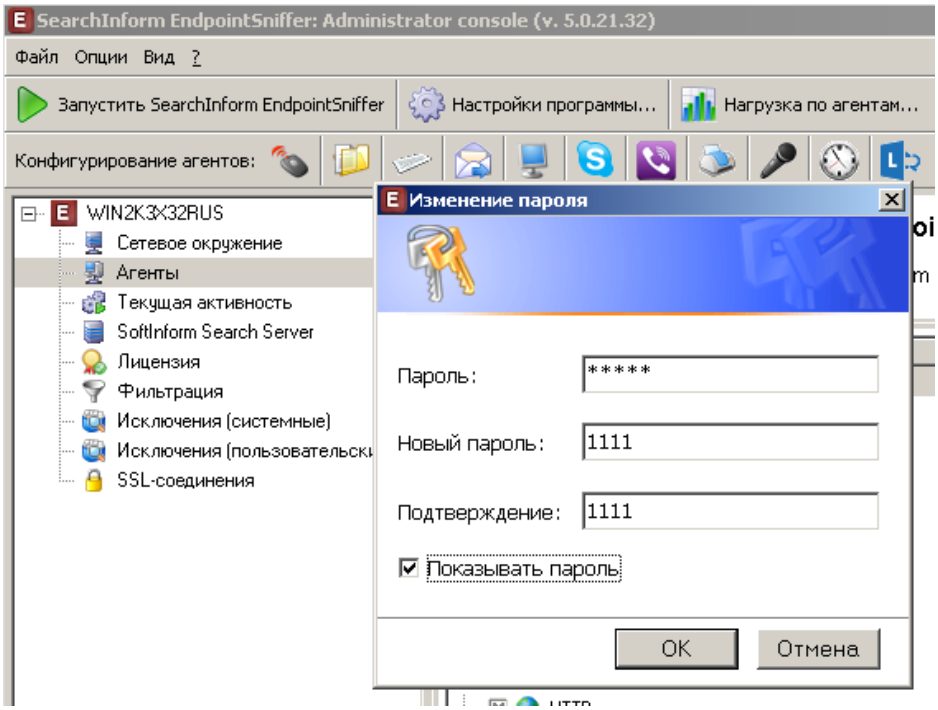


Рис. 4: Изменение пароля EndpointSniffer.

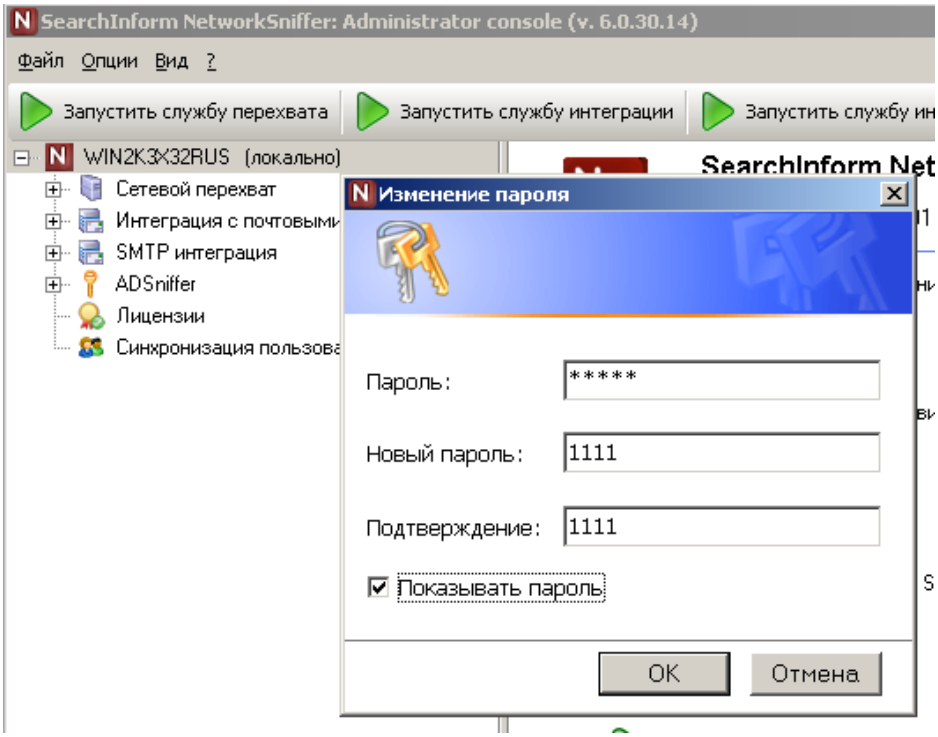


Рис. 5: Изменение пароля NetworkSniffer.

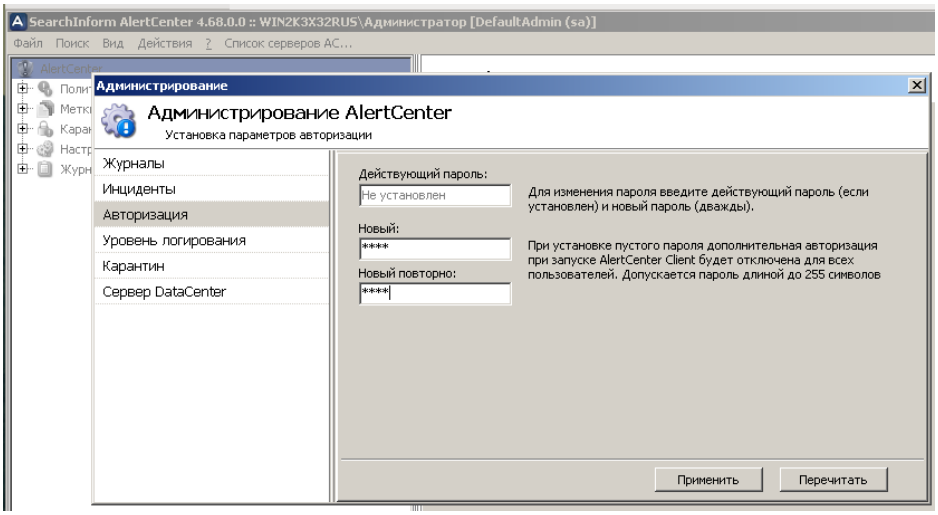


Рис. 6: Изменение пароля AlertCenter.

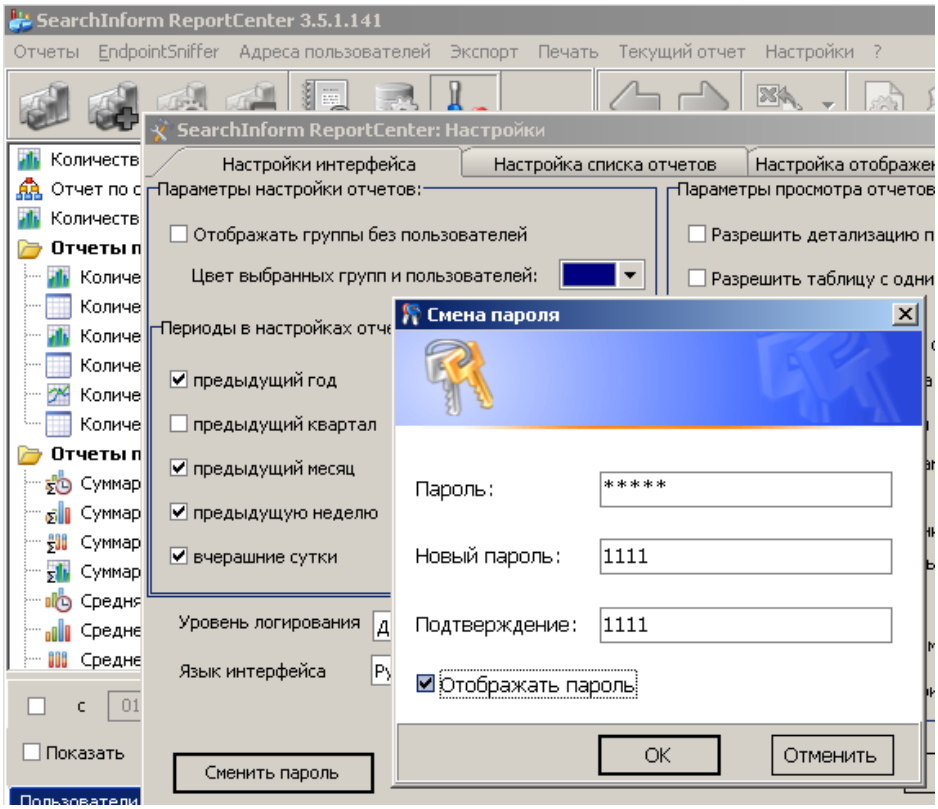


Рис. 7: Изменение пароля ReprotCenter.

1.1.4. Ограничить права доступа пользователей к индексам Search Server

Это можно сделать с помощью *SearchIorm Server Console*, см. рис. 8.

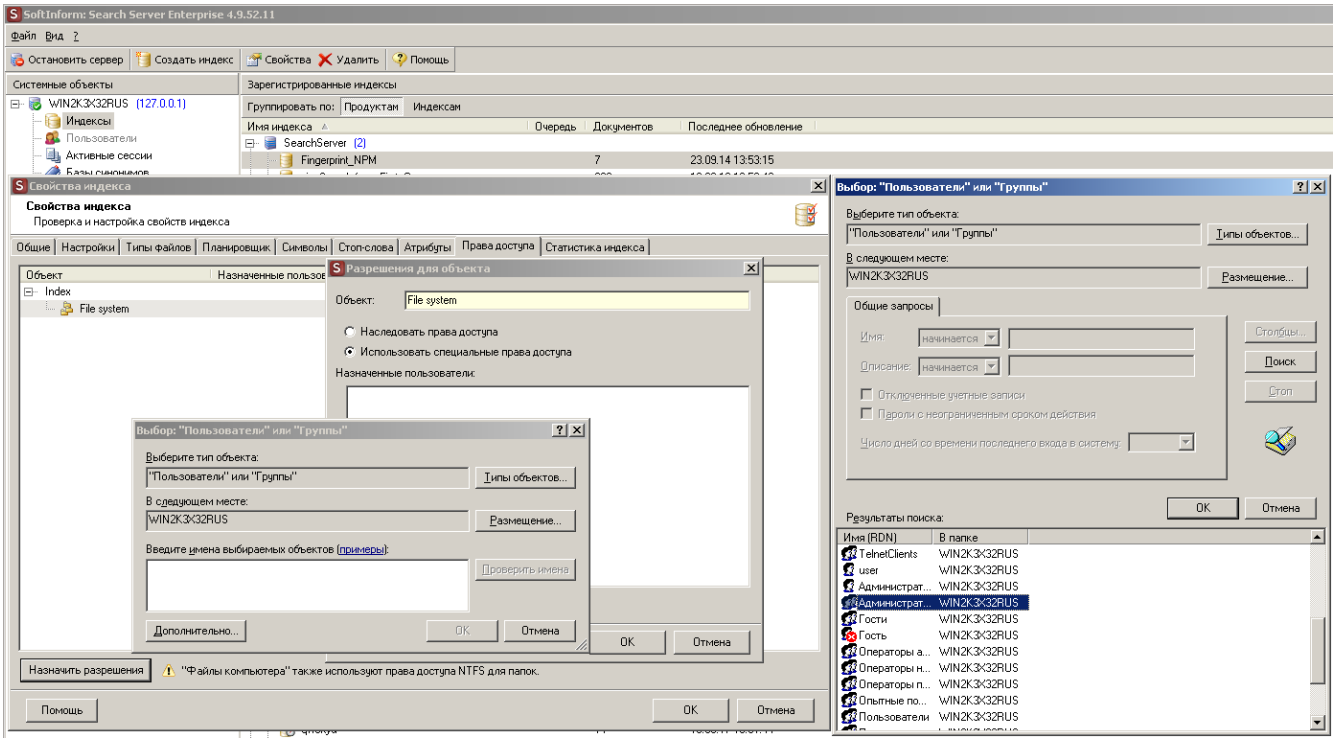


Рис. 8: Изменение пароля ReprotCenter.

1.1.5. Управление пользователями системных служб SearchInform

Установим в качестве пользователя, от имени которого работает сервас *SearchInform AlertCenter server* Администартора, рис. 9.

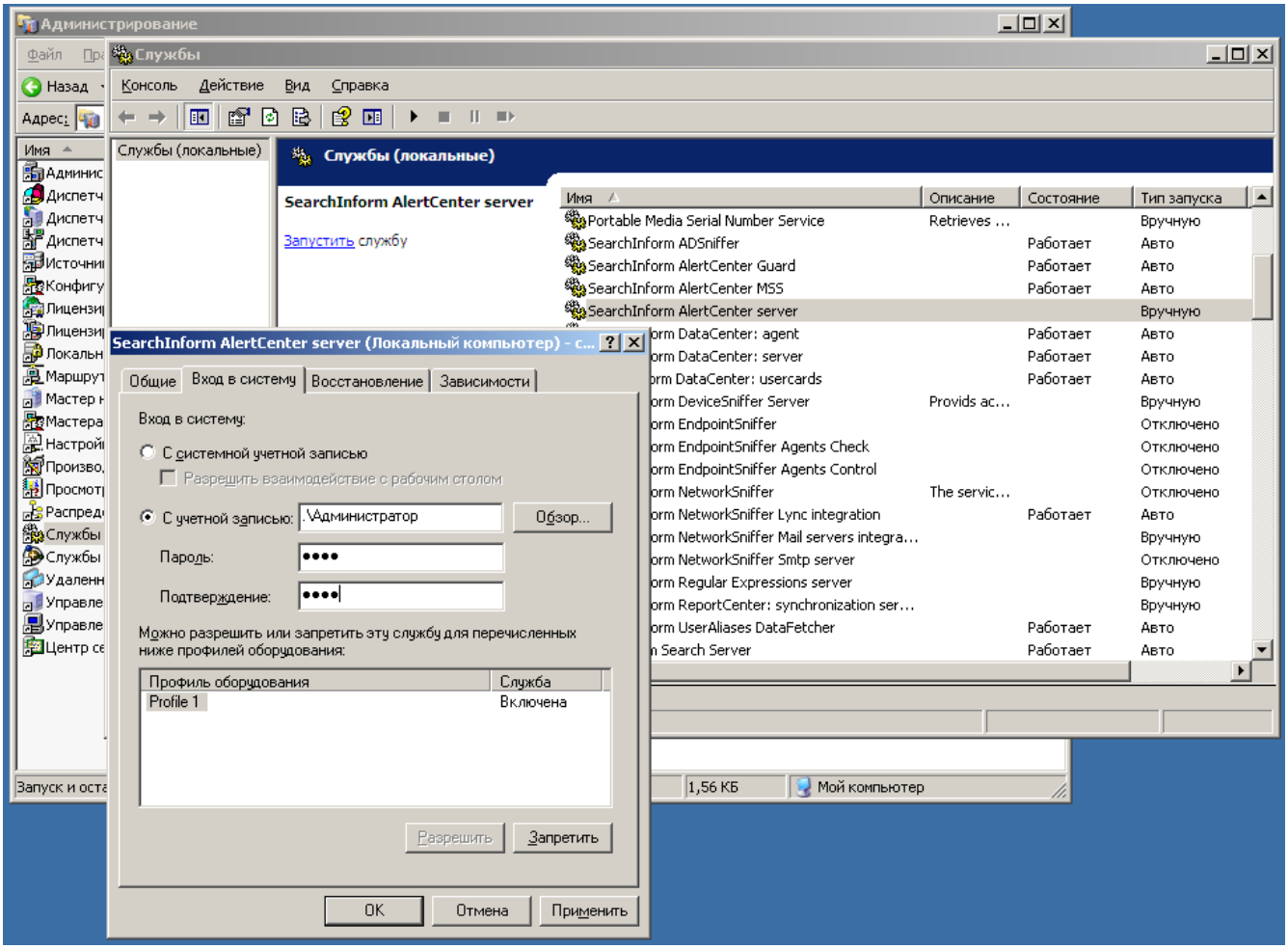


Рис. 9: Установка администратора в качестве пользователя для AlertCenter server.

1.1.6. Настройка параметров функционирования SearchInform AlertCenter

Настроим *AlertCenter*, как на рис. 10.

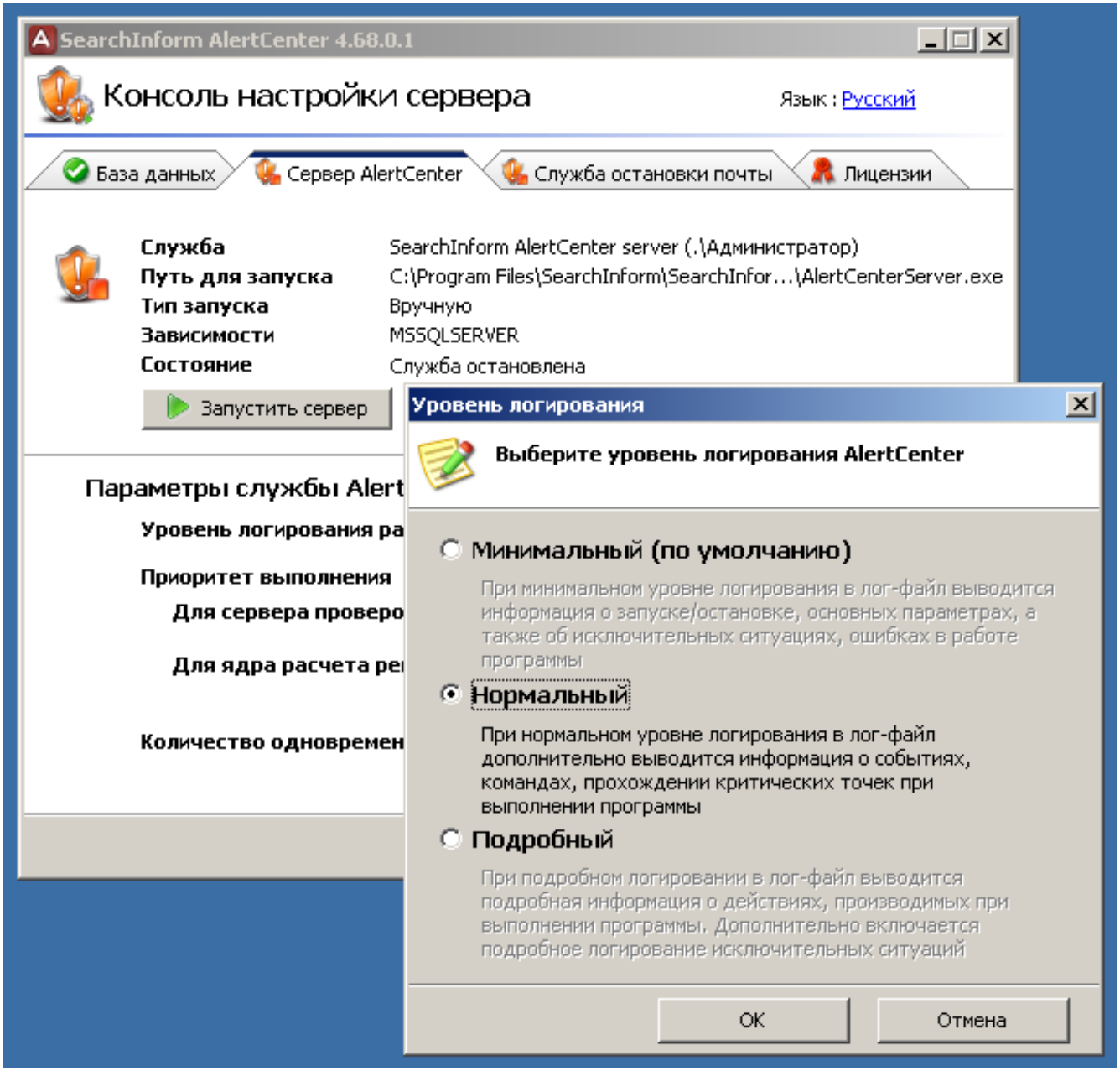


Рис. 10: Настройка AlertCenter.

1.1.7. Настройка системной службы SearchInform DataCenter : agent

Настроим автоматический запуск этой службы, как на рис. 11.

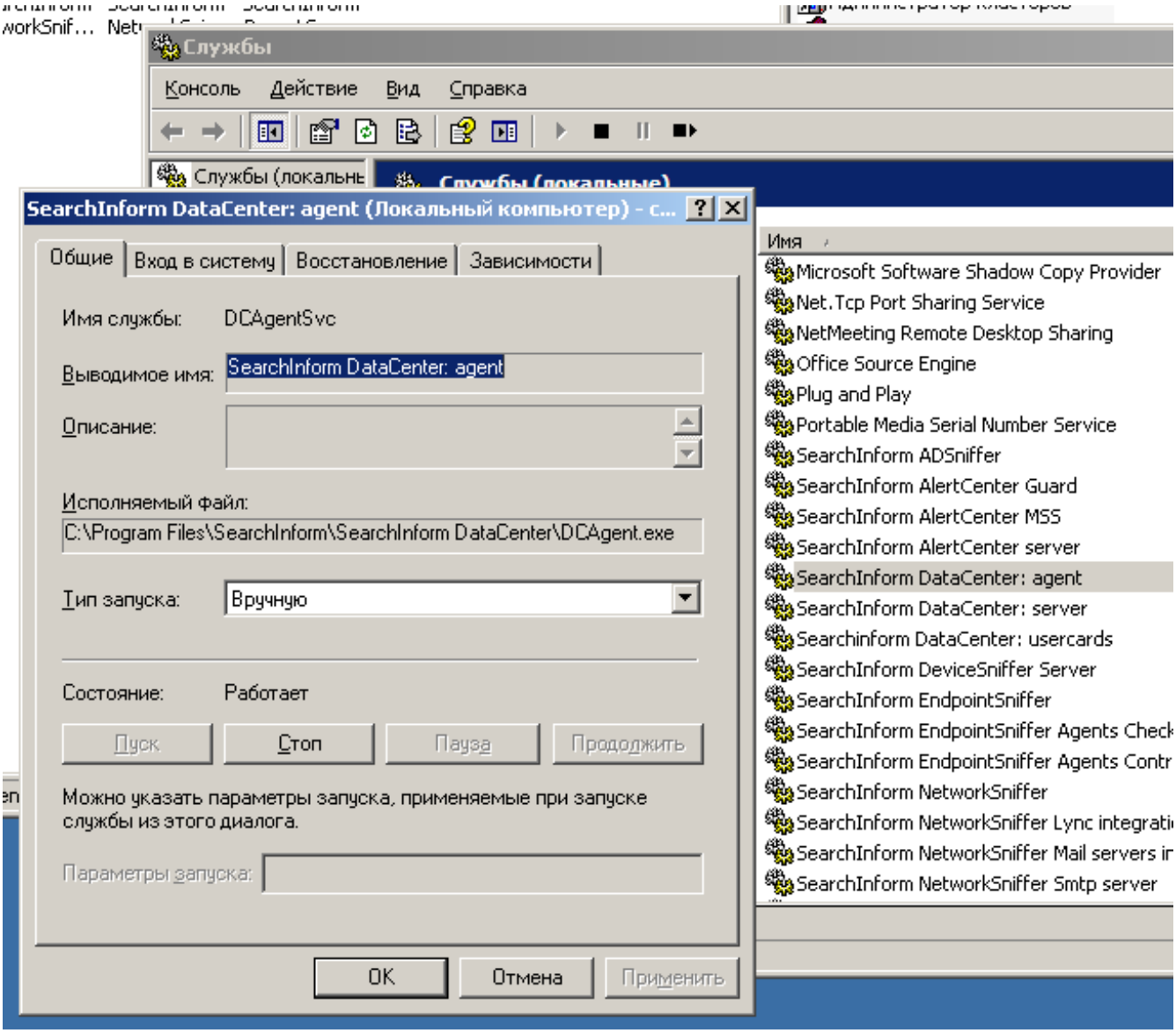


Рис. 11: Настройка Автозапуска DataCenter: agent.

1.1.8. Настройка параметров функционирования SearchInform EndpointSniffer

Аналогично настроим автозапуск *EndpointSniffer*, см рис. esAutorun.

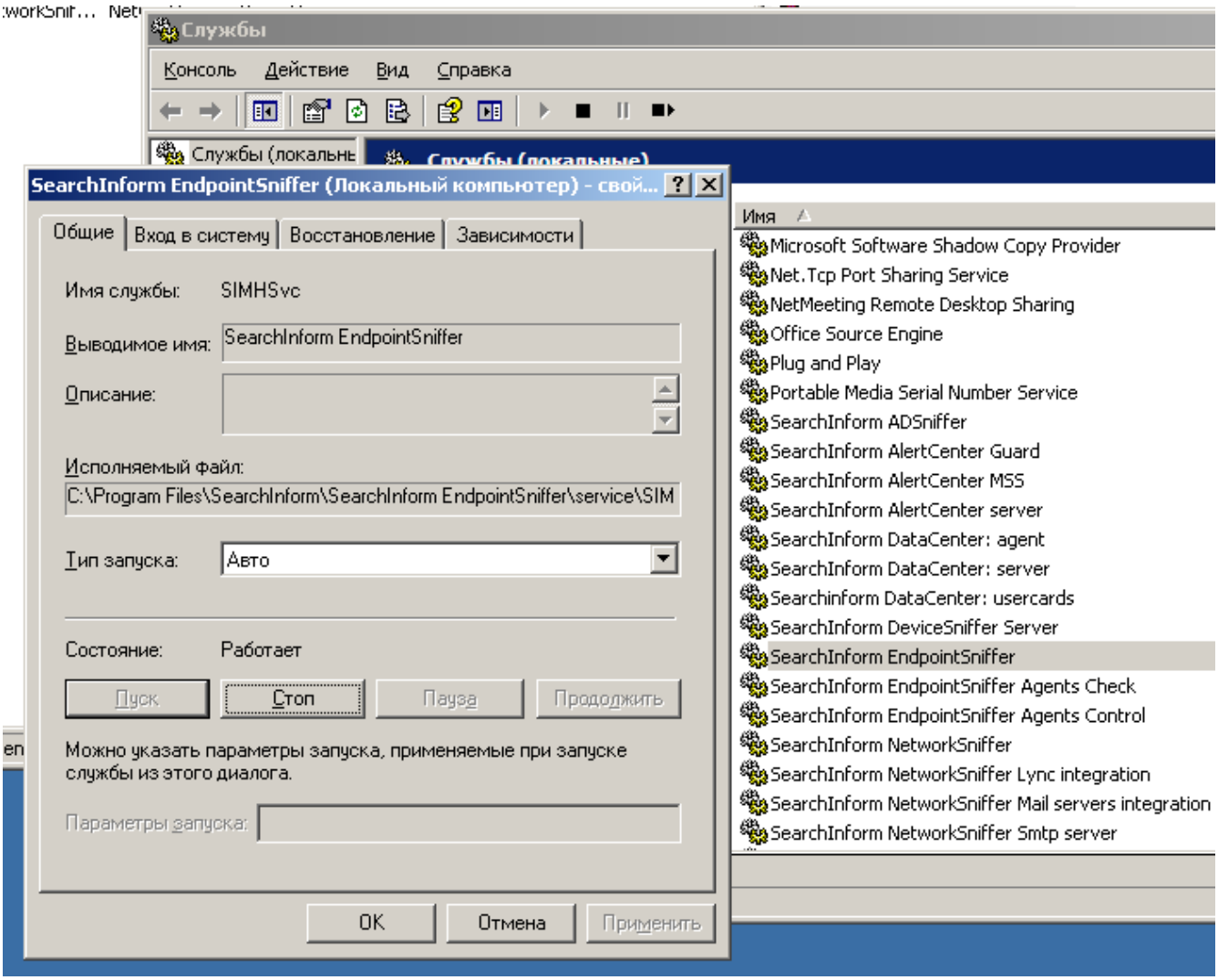


Рис. 12: Настройка Автозапуска EndpointSniffer.

1.2. Контрольные вопросы

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

  Для контроля пользователей, обладающей информацией, содержащейся в документах. Для контроля местонахождения документов (в случае физических носителей).

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

  Требуется для оперативной настройки специфических средств для обеспечения информационной безопасности. Также для оперативного добавления и прав доступа пользователей.

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

- Какая из схем подключения наиболее оптимальна при наличии технической возможности?

- Перечислите основные аппаратные требования для штатного функционирования операционной системы Windows Server 2003?

  Процессор с тактовой частотой 400 МГц; минимум 512 МБ ОЗУ; для сетевой установки: 1,2 ГБ; для установки с компакт-диска: 2,9 ГБ;

- Что такое индекс?

  Ассоциативный массив значения какой-либо функции от данных, на соответствующие данные.

2. Принципы использования программного комплекса SearchInform для мониторинга утечек конфиденциальной информации

2.1. Ход работы

2.1.1. Определение списка пользователей, данные которых будут перехватываться системой

Запустим SearchInform NetworkSniffer Administrator Console и настроим фильтр перехвата так, что после редактирования будут перехватываться данные пользователей ivanov и bublik для всех контролируемых протоколов. Результат настройки см. рис. 13.

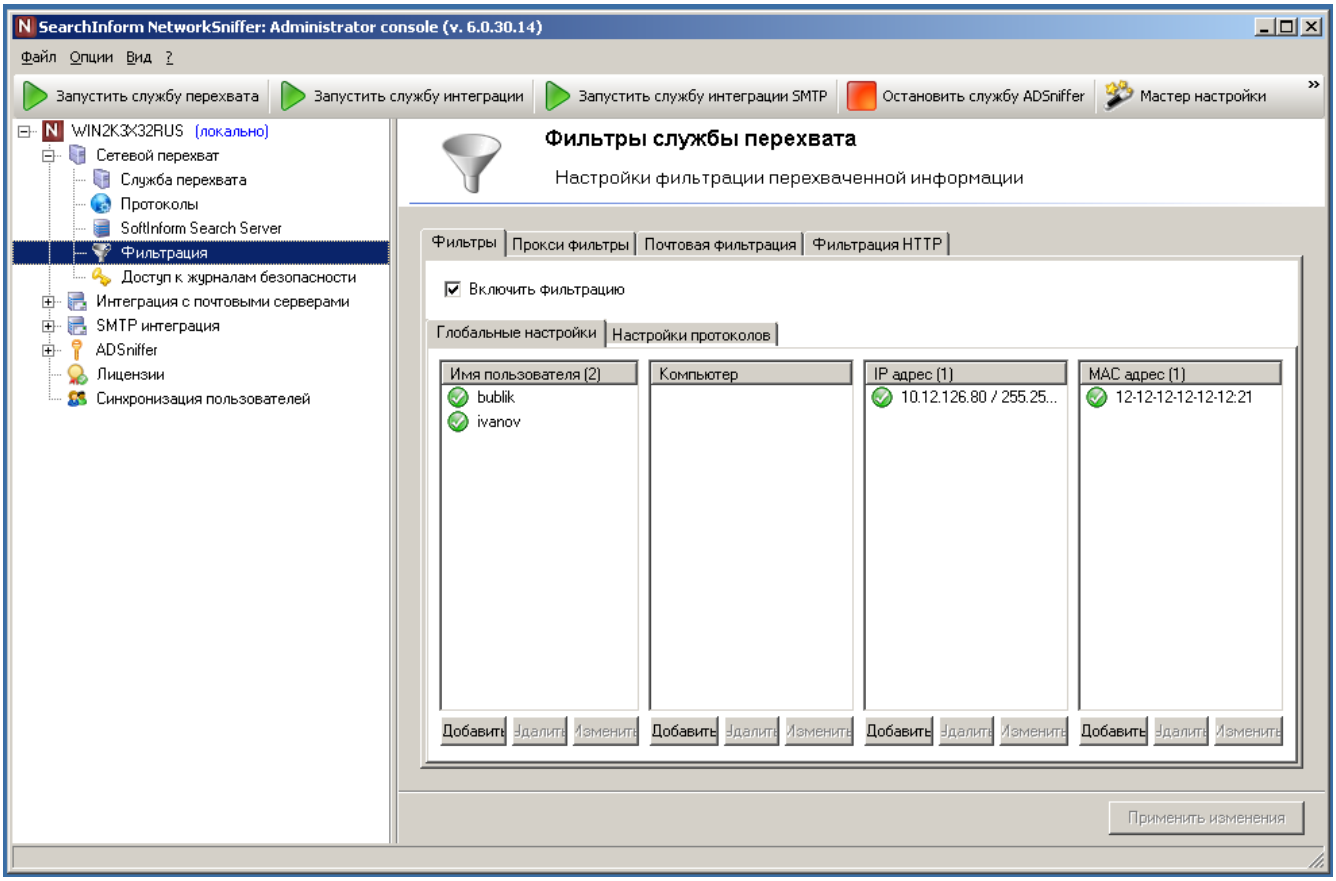
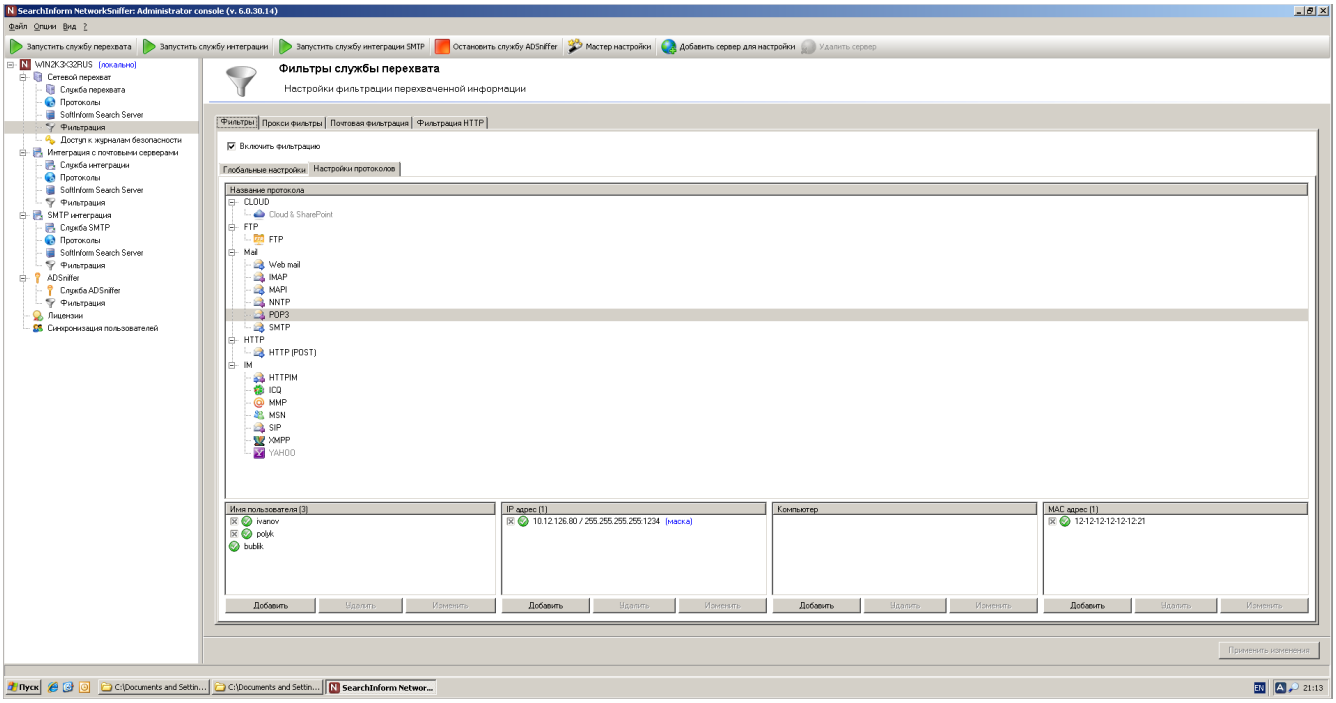
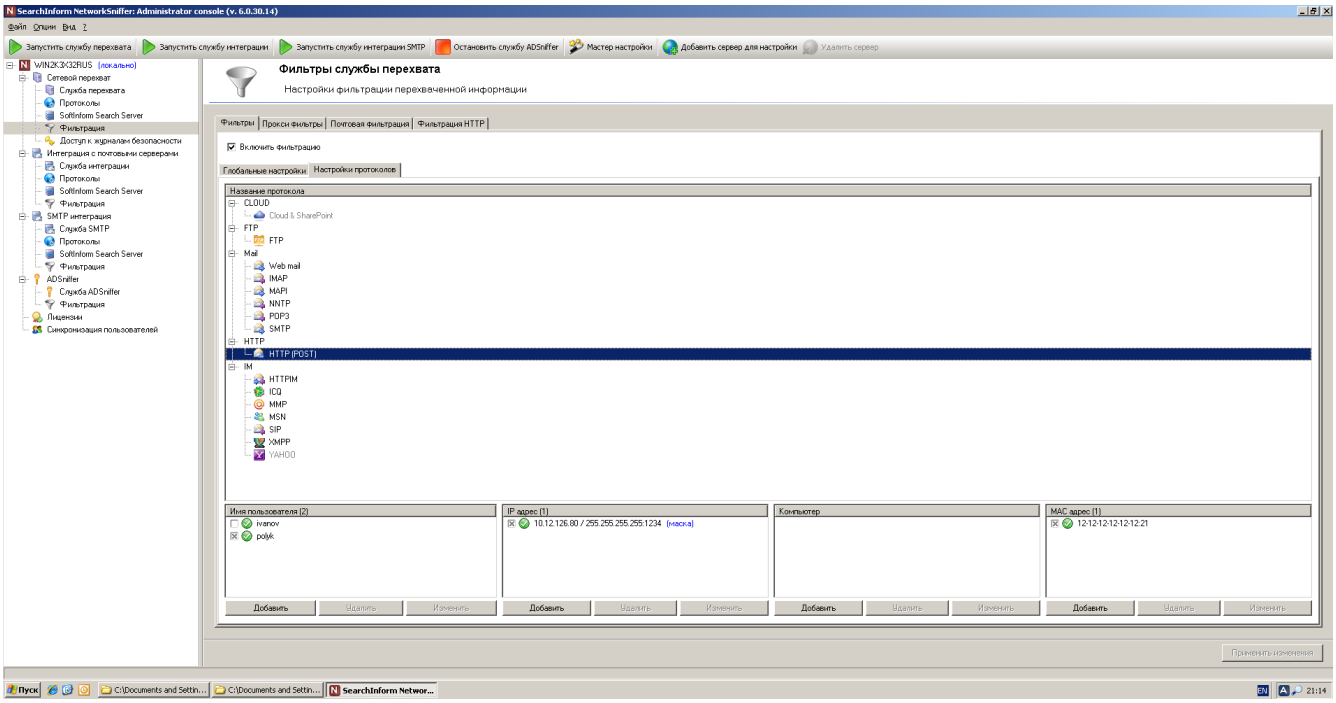
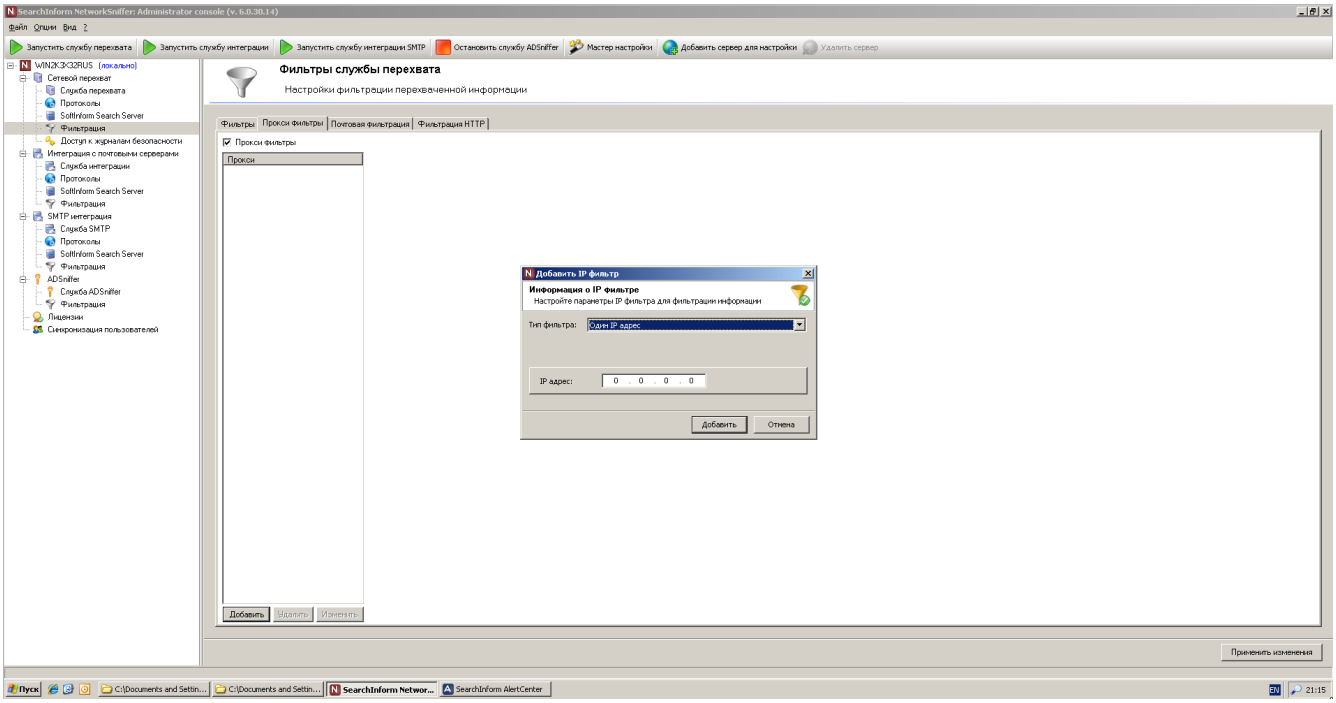


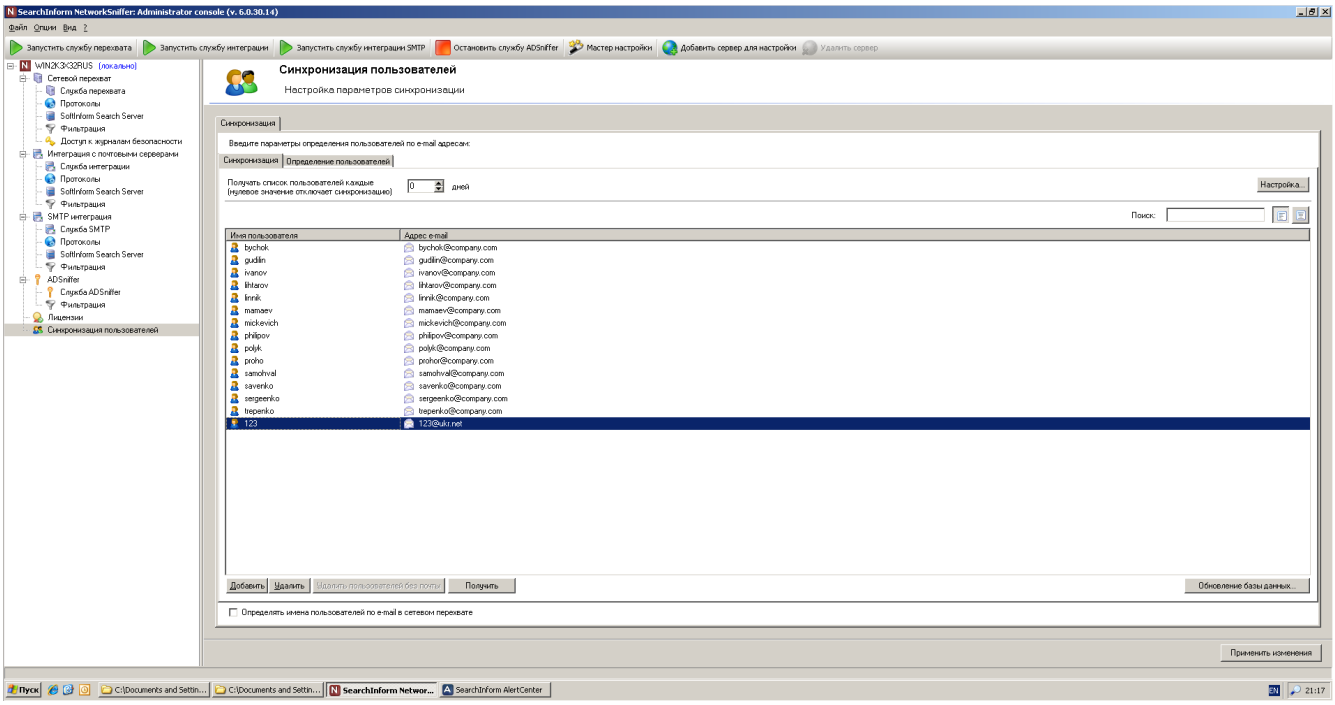
Рис. 13: Результат настройки NetworkSniffer.

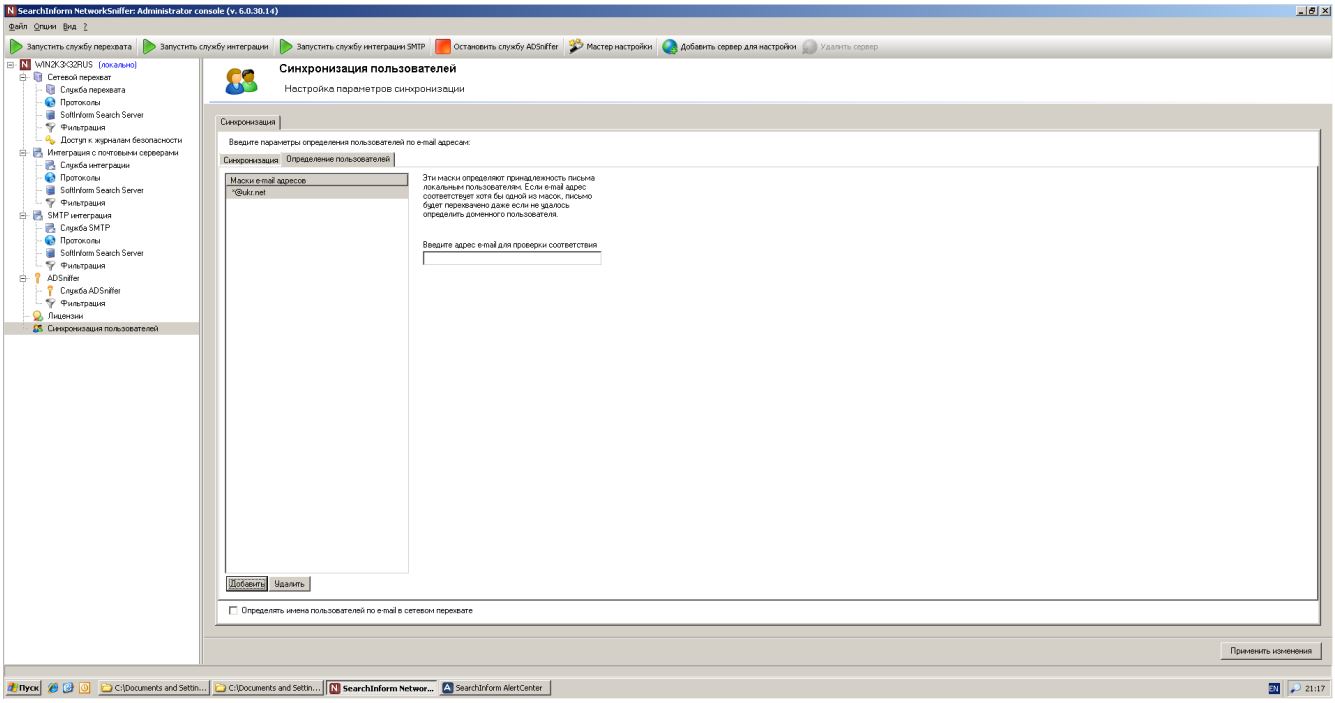
Скриншоты хода работы:

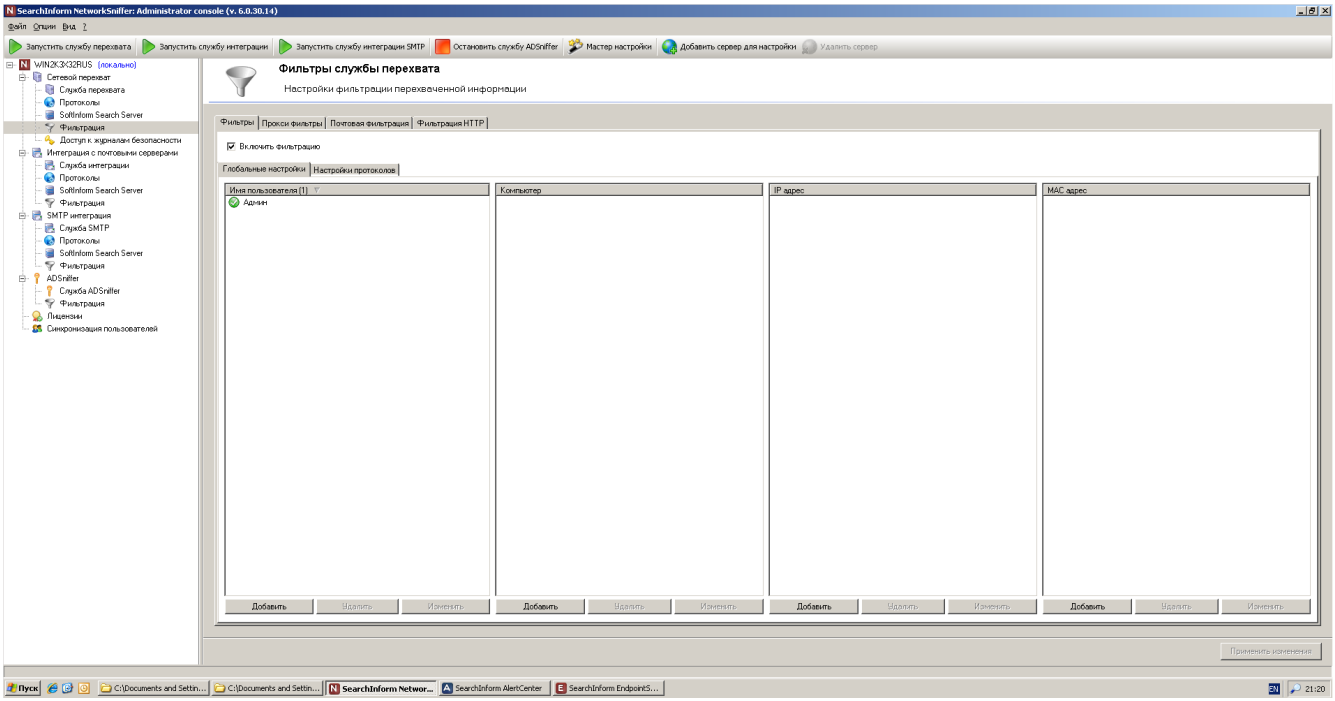

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Фильтры службы перехвата
Настройки фильтрации перехваченной информации
Фильтры
Прокси фильтры
Почтовая фильтрация
Фильтрация HTTP
Включить фильтрацию
Глобальные настройки
Настройки протоколов
Название протокола
CLOUD
Cloud & SharePoint
FTP
FTP
Mail
Web mail
IMAP
MAPI
NNTP
POP3
SMTP
HTTP
HTTP (POST)
IM
HTTPIM
ICQ
MMP
MSN
SIP
XMPP
YAHOO
Имя пользователя (3)
ivanov
polyk
bublik
IP адрес (1)
10.12.126.80 / 255.255.255.255:1234
MAC адрес (1)
12-12-12-12-12-12-21
Добавить
Удалить
Изменить
Применить изменения

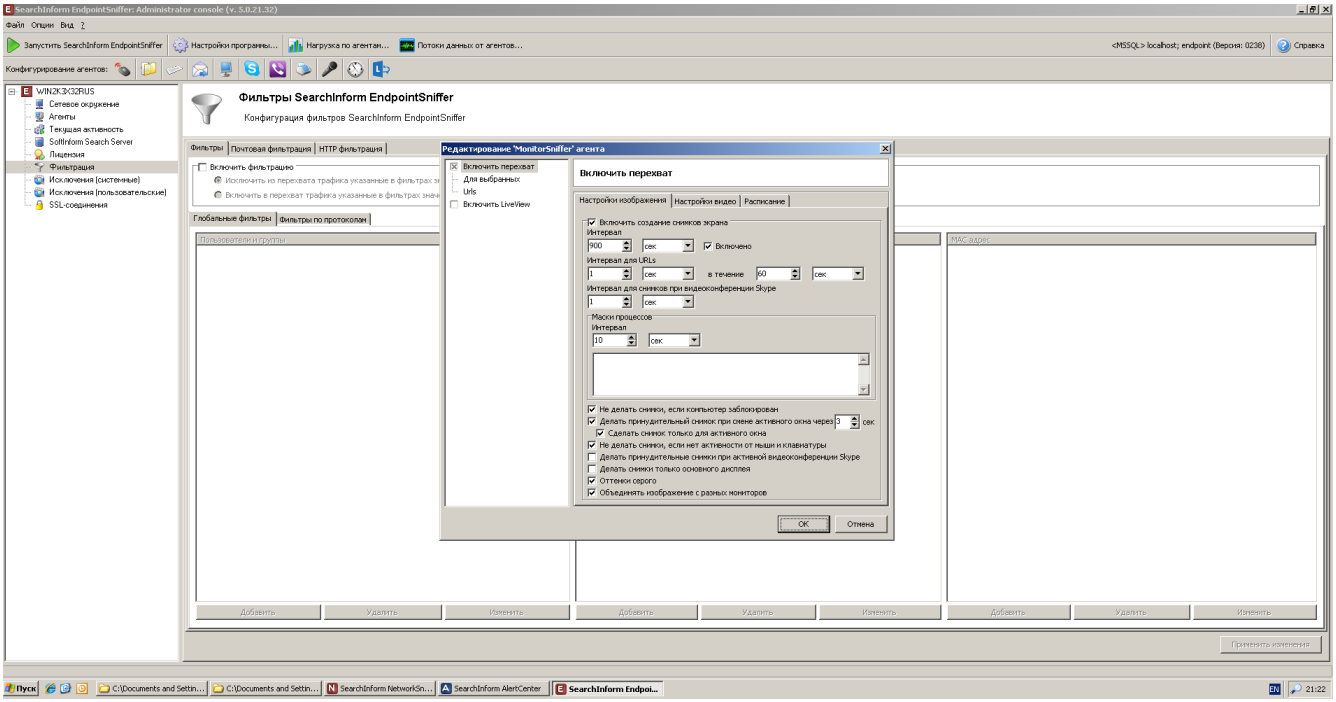

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Фильтры службы перехвата
Настройки фильтрации перехваченной информации
Фильтры
Прокси фильтры
Почтовая фильтрация
Фильтрация HTTP
Включить фильтрацию
Глобальные настройки
Настройки протоколов
Название протокола
CLOUD
Cloud & SharePoint
FTP
FTP
Mail
Web mail
IMAP
MAPI
NNTP
POP3
SMTP
HTTP
HTTP (POST)
IM
HTTPIM
ICQ
MMP
MSN
SIP
XMPP
YAHOO
Имя пользователя (2)
ivanov
polyk
IP адрес (1)
10.12.126.80 / 255.255.255.255:1234
MAC адрес (1)
12-12-12-12-12-12-21
Добавить
Удалить
Изменить
Применить изменения

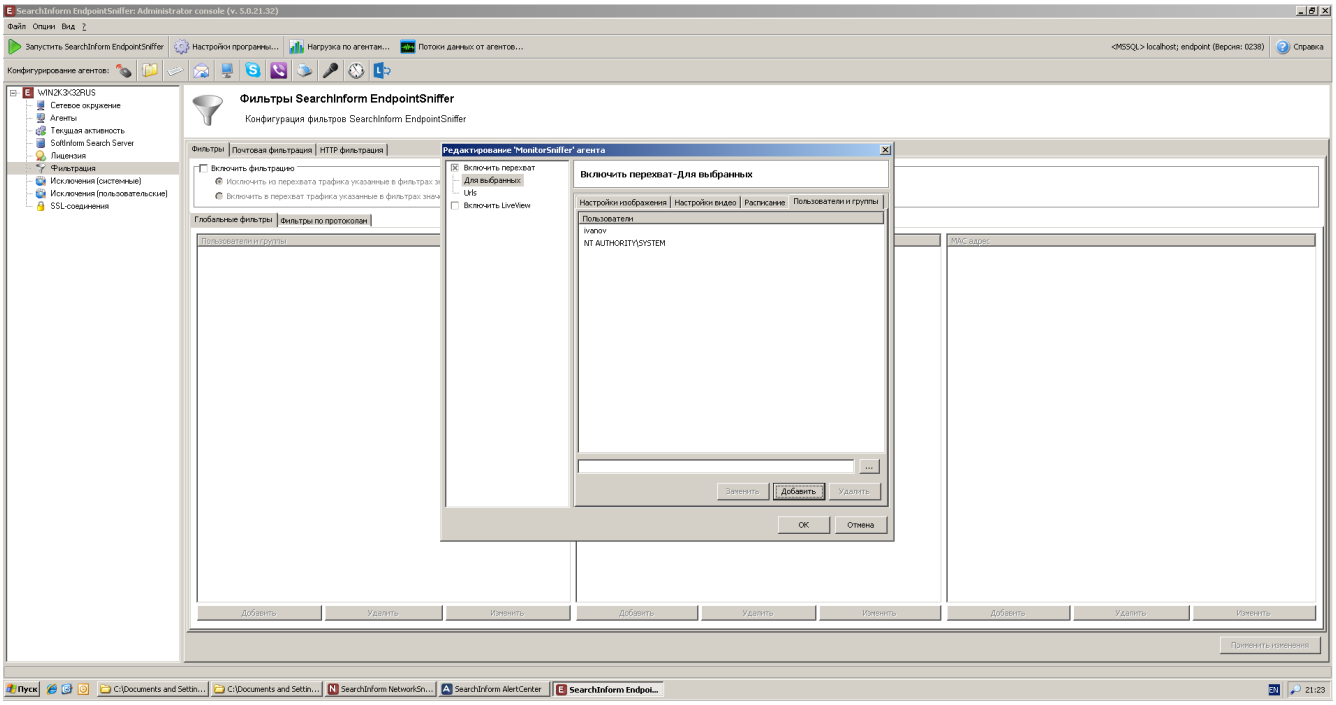

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Файл Опции Вид ?
Запустить службу перехвата
Запустить службу интеграции
Запустить службу интеграции SMTP
Остановить службу ADSniffer
Мастер настройки
Добавить сервер для настройки
Удалить сервер
WIN2K3X32RUS (локально)
Сетевой перехват
Служба перехвата
Протоколы
SoftInform Search Server
Фильтрация
Доступ к журналам безопасности
Интеграция с почтовыми серверами
Служба интеграции
Протоколы
SoftInform Search Server
Фильтрация
SMTP интеграция
Служба SMTP
Протоколы
SoftInform Search Server
Фильтрация
ADSniffer
Служба ADSniffer
Фильтрация
Лицензии
Синхронизация пользователей
Фильтры службы перехвата
Настройки фильтрации перехваченной информации
Фильтры
Прокси фильтры
Почтовая фильтрация
Фильтрация HTTP
Прокси фильтры
Прокси
Добавить
Удалить
Изменить
Добавить IP фильтр
Информация о IP фильтре
Настройте параметры IP фильтра для фильтрации информации
Тип фильтра:
Один IP адрес
IP адрес:
0 . 0 . 0 . 0
Добавить
Отмена
Применить изменения
Пуск
C:\Documents and Settin...
C:\Documents and Settin...
SearchInform Networ...
SearchInform AlertCenter
EN
21:15

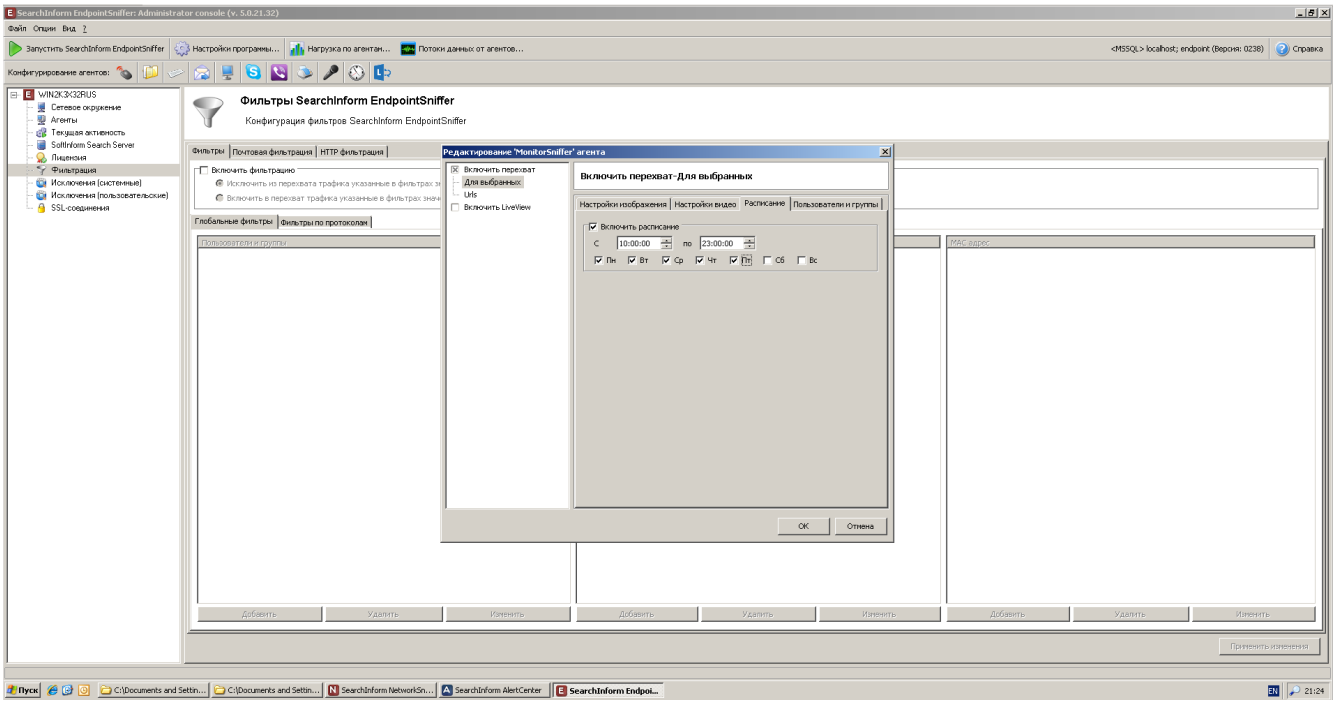

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Файл Опции Вид ?
Запустить службу перехвата
Запустить службу интеграции
Запустить службу интеграции SMTP
Остановить службу ADSniffer
Мастер настройки
Добавить сервер для настройки
Удалить сервер
WIN2K3X32RUS (локально)
Сетевой перехват
Служба перехвата
Протоколы
SoftInform Search Server
Фильтрация
Доступ к журналам безопасности
Интеграция с почтовыми серверами
Служба интеграции
Протоколы
SoftInform Search Server
Фильтрация
SMTP интеграция
Служба SMTP
Протоколы
SoftInform Search Server
Фильтрация
ADSniffer
Служба ADSniffer
Фильтрация
Лицензии
Синхронизация пользователей
Синхронизация пользователей
Настройка параметров синхронизации
Синхронизация
Введите параметры определения пользователей по e-mail адресам:
Синхронизация
Определение пользователей
Получать список пользователей каждые (нулевое значение отключает синхронизацию)
0
дней
Настройка...
Поиск:
Имя пользователя
Адрес e-mail
bychok bychok@company.com
gudilin gudilin@company.com
ivanov ivanov@company.com
lihtarov lihtarov@company.com
linnik linnik@company.com
mamaev mamaev@company.com
mickevich mickevich@company.com
philipov philipov@company.com
polyk polyk@company.com
prohor prohor@company.com
samohval samohval@company.com
savenko savenko@company.com
sergeenko sergeenko@company.com
trepenko trepenko@company.com
123 123@ukl.net
Добавить
Удалить
Удалить пользователей без почты
Получить
Обновление базы данных...
Определять имена пользователей по e-mail в сетевом перехвате
Применить изменения
Пуск
C:\Documents and Settin...
C:\Documents and Settin...
SearchInform Networ...
SearchInform AlertCenter
EN
21:17

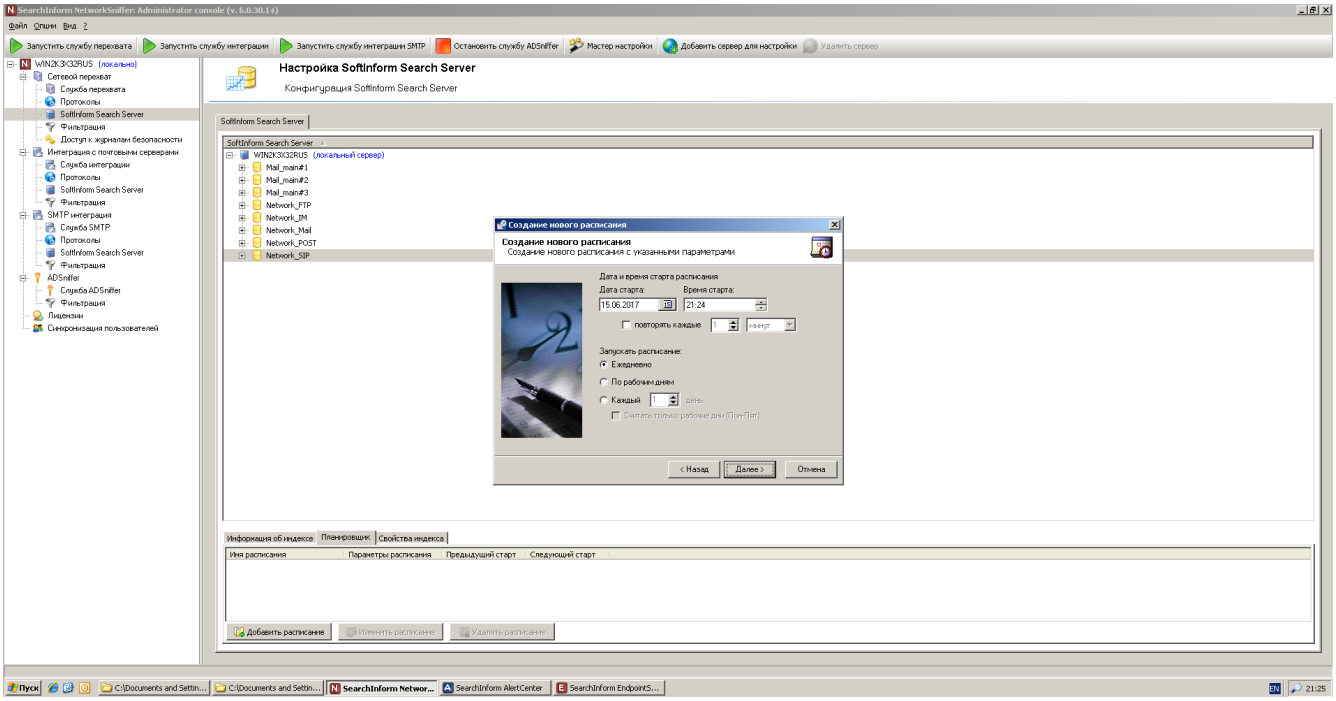

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Файл Опции Вид ?
Запустить службу перехвата
Запустить службу интеграции
Запустить службу интеграции SMTP
Остановить службу ADSniffer
Мастер настройки
Добавить сервер для настройки
Удалить сервер
WIN2K3X32RUS (локально)
Сетевой перехват
Служба перехвата
Протоколы
SoftInform Search Server
Фильтрация
Доступ к журналам безопасности
Интеграция с почтовыми серверами
Служба интеграции
Протоколы
SoftInform Search Server
Фильтрация
SMTP интеграция
Служба SMTP
Протоколы
SoftInform Search Server
Фильтрация
ADSniffer
Служба ADSniffer
Фильтрация
Лицензии
Синхронизация пользователей
Синхронизация пользователей
Настройка параметров синхронизации
Синхронизация
Введите параметры определения пользователей по e-mail адресам:
Синхронизация
Определение пользователей
Маски e-mail адресов
*@ukr.net
Эти маски определяют принадлежность письма локальным пользователям. Если e-mail адрес соответствует хотя бы одной из масок, письмо будет перехвачено даже если не удалось определить доменного пользователя.
Введите адрес e-mail для проверки соответствия
Добавить
Удалить
Определять имена пользователей по e-mail в сетевом перехвате
Применить изменения
Пуск
C:\Documents and Settin...
C:\Documents and Settin...
SearchInform Networ...
SearchInform AlertCenter
EN
21:17

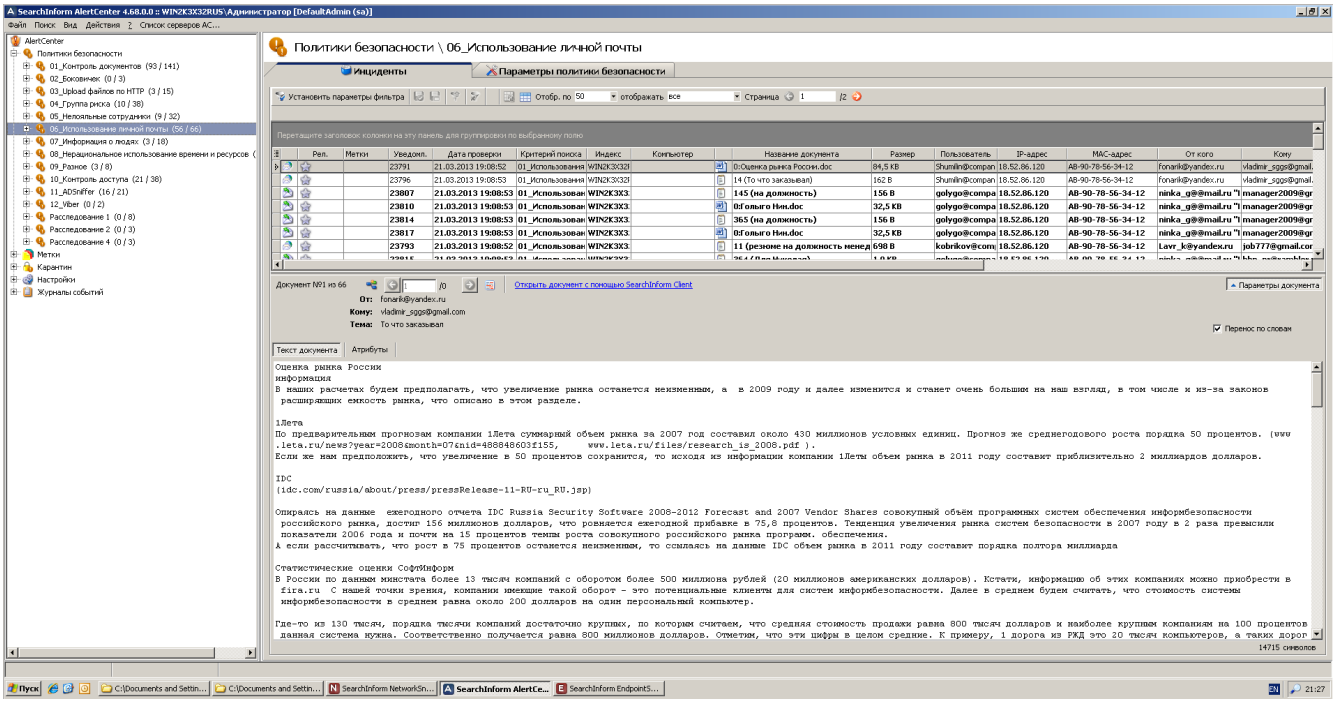

SearchInform NetworkSniffer: Administrator console (v. 6.0.30.14)
Файл Опции Вид ?
Запустить службу перехвата
Запустить службу интеграции
Запустить службу интеграции SMTP
Остановить службу ADSniffer
Мастер настройки
Добавить сервер для настройки
Удалить сервер
WIN2K3X32RUS (локально)
Сетевой перехват
Служба перехвата
Протоколы
SoftInform Search Server
Фильтрация
Доступ к журналам безопасности
Интеграция с почтовыми серверами
Служба интеграции
Протоколы
SoftInform Search Server
Фильтрация
SMTP интеграция
Служба SMTP
Протоколы
SoftInform Search Server
Фильтрация
ADSniffer
Служба ADSniffer
Фильтрация
Лицензии
Синхронизация пользователей
Фильтры службы перехвата
Настройки фильтрации перехваченной информации
Фильтры
Прокси фильтры
Почтовая фильтрация
Фильтрация HTTP
Включить фильтрацию
Глобальные настройки
Настройки протоколов
Имя пользователя (1)
Компьютер
IP адрес
MAC адрес
Админ
Добавить
Удалить
Изменить
Применить изменения
Пуск
C:\Documents and Settin...
C:\Documents and Settin...
SearchInform Networ...
SearchInform AlertCenter
SearchInform EndpointS...
EN
21:20


Фильтры SearchInform EndpointSniffer
Конфигурация фильтров SearchInform EndpointSniffer
Редактирование 'MonitorSniffer' агента
Включить перехват
Настройки изображения
Настройки видео
Расписание
OK
Отмена


Фильтры SearchInform EndpointSniffer
Конфигурация фильтров SearchInform EndpointSniffer
Редактирование 'MonitorSniffer' агента
Включить перехват-Для выбранных
Настройки изображения
Настройки видео
Расписание
Пользователи и группы
ivanov
NT AUTHORITY\SYSTEM
Заменить
Добавить
Удалить
OK
Отмена


Фильтры SearchInform EndpointSniffer
Конфигурация фильтров SearchInform EndpointSniffer
Редактирование 'MonitorSniffer' агента
Включить перехват-Для выбранных
OK
Отмена


Настройка SoftInform Search Server
Конфигурация SoftInform Search Server
Создание нового расписания
Создание нового расписания с указанными параметрами
< Назад
Далее >
Отмена

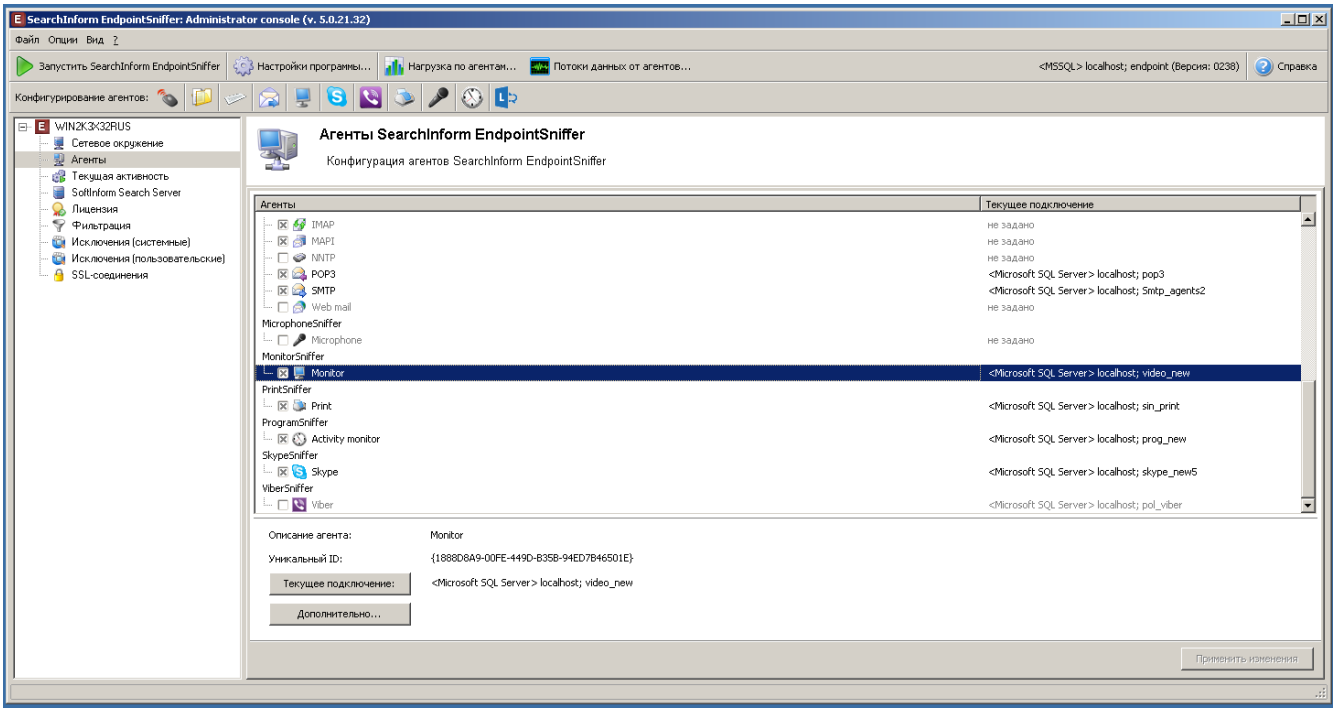


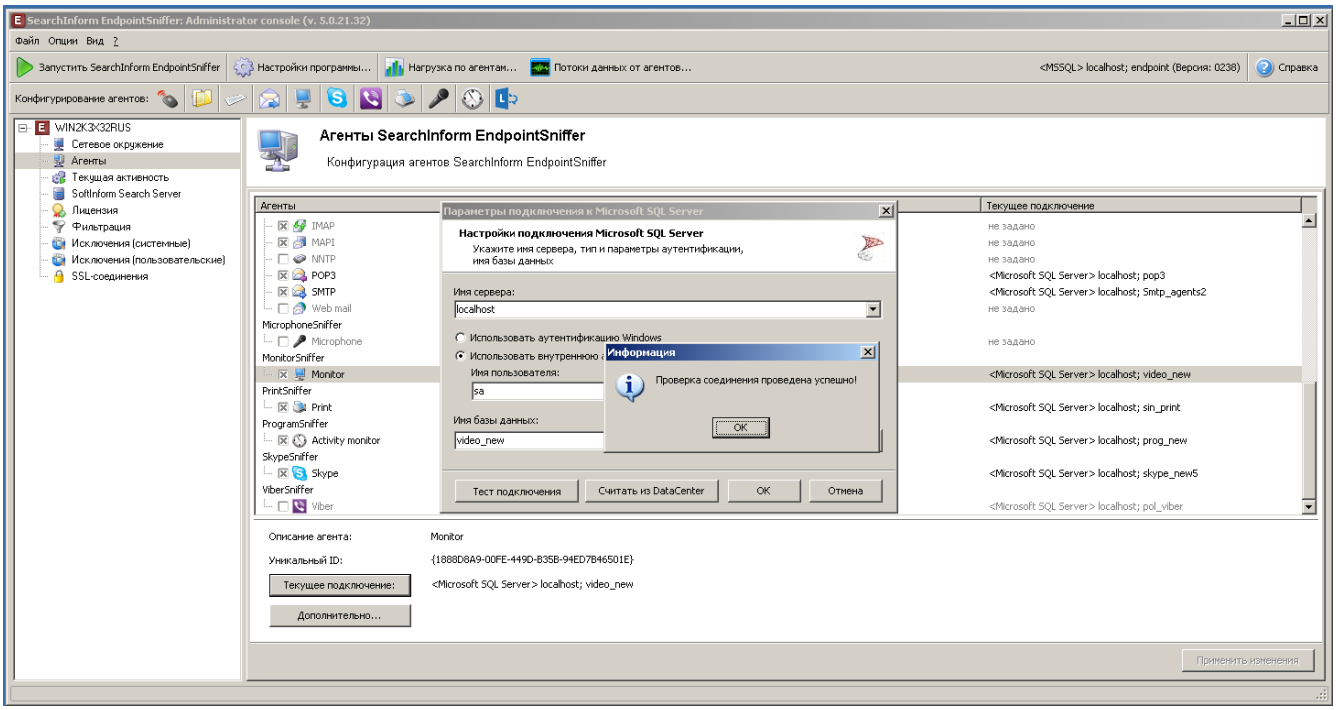
2.2. Контрольные вопросы

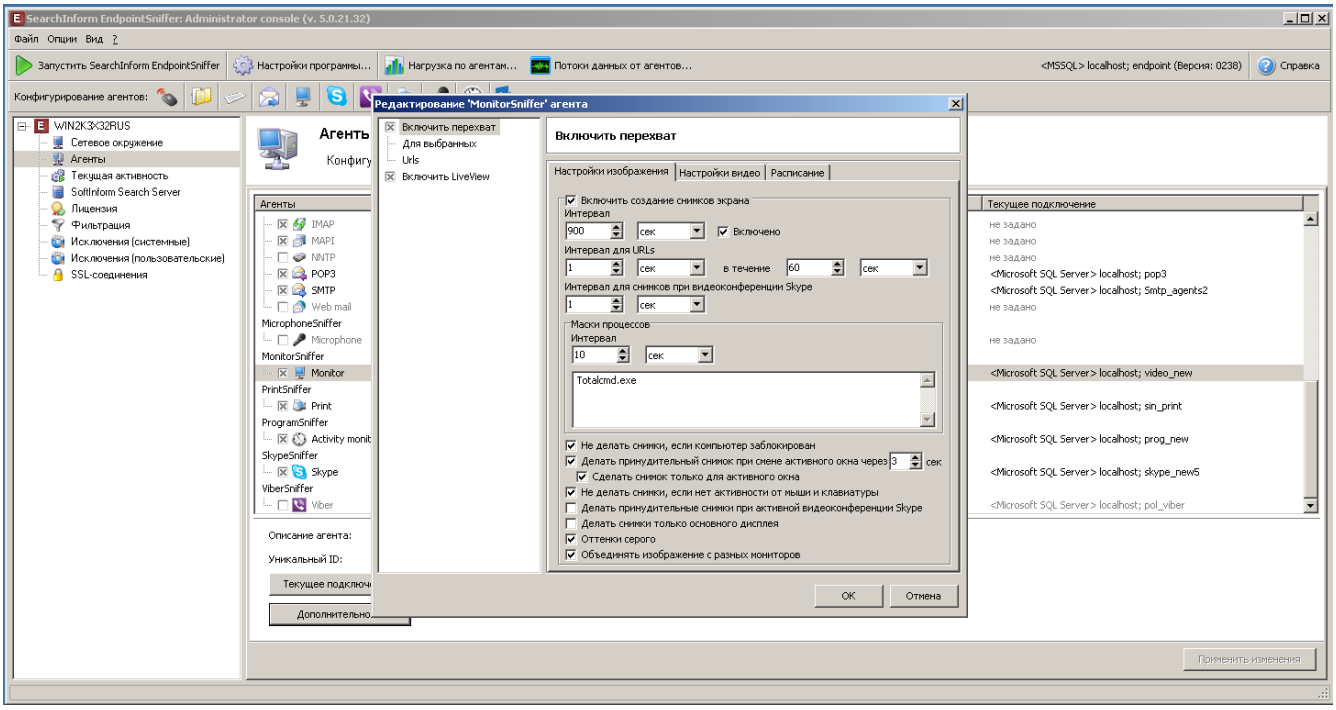
- Зачем нужна фильтрация по прокси-серверам?
  Для фильтрации трафика, направленного через конкретный прокси сервер.
- Зачем нужна фильтрация по почтовым серверам?
  Для фильтрации писем отправленных пользователями с конкретных почтовых серверов.
- Какие виды поиска рекомендуются для структурированных документов?
  Поиск по индексам.
- Какие виды поиска рекомендуются для не структурированных документов?
  Полнотекстовый поиск.
- Что такое «белый список»?
  Фильтр описывающий список разрешенных значений каких-либо атрибутов.
- Как используется «разрешающий белый список»?
  Перечисляются значения, которые должны пройти фильтрацию.
- Как используется «запрещающий белый список»?
  Перечисляются значения, которые не должны пройти фильтрацию.
- Чем отличается глобальный фильтр от фильтра по протоколам?
  Глобальный фильтр ГЛОБАЛЬНЫЙ, а фильтр по протоколам применяется к конкретным протоколам.
- Зачем подключать AlertCenter к индексам?
  Для ускорения поиска.
- Какой должен быть интервал обновления индексов?
  Зависит от ситуации.

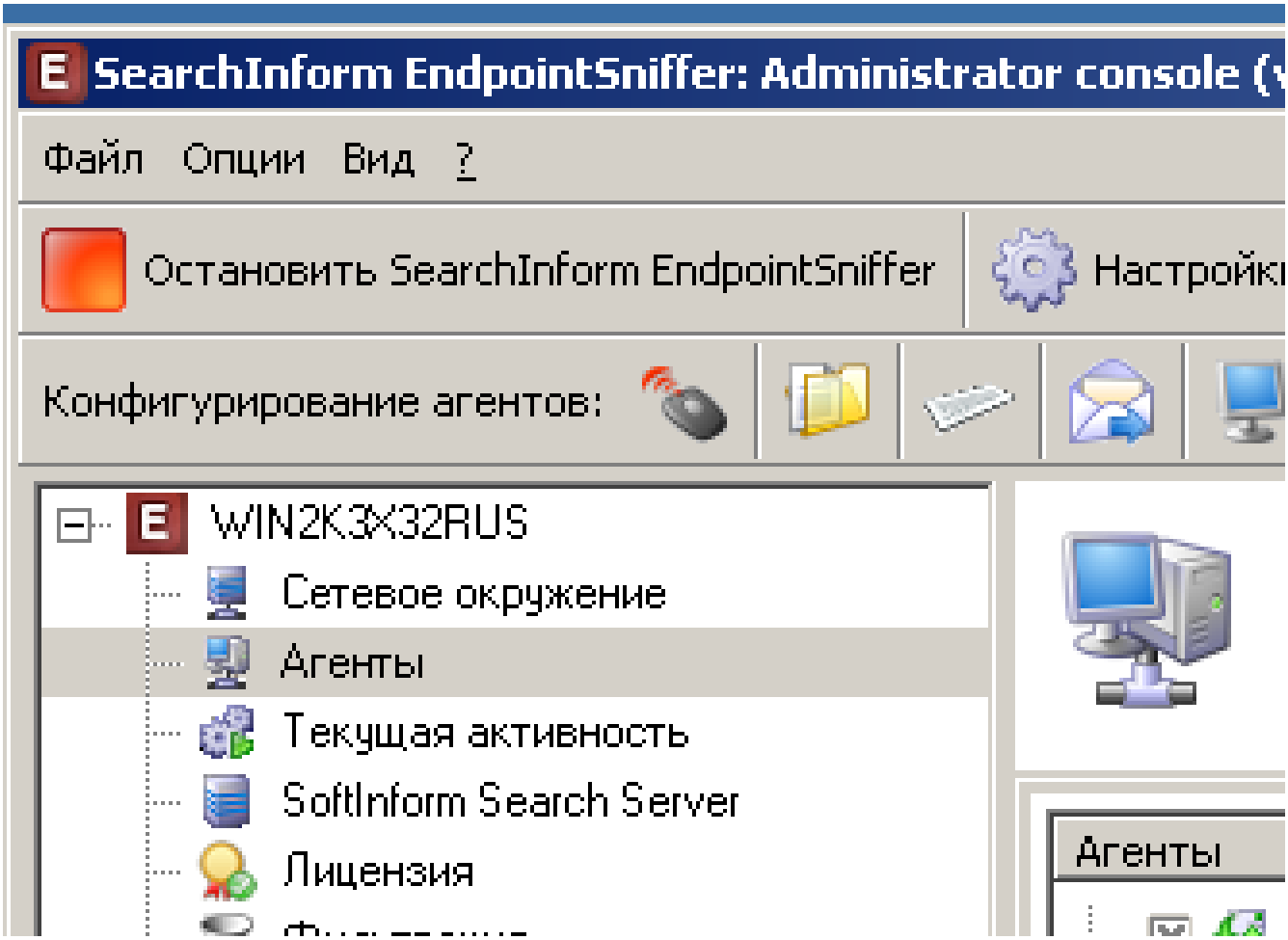
3. Настройка программного комплекса SearchInform для контроля содержимого экранов пользователей и поиска конфиденциальной информации без проведения синтаксического анализа

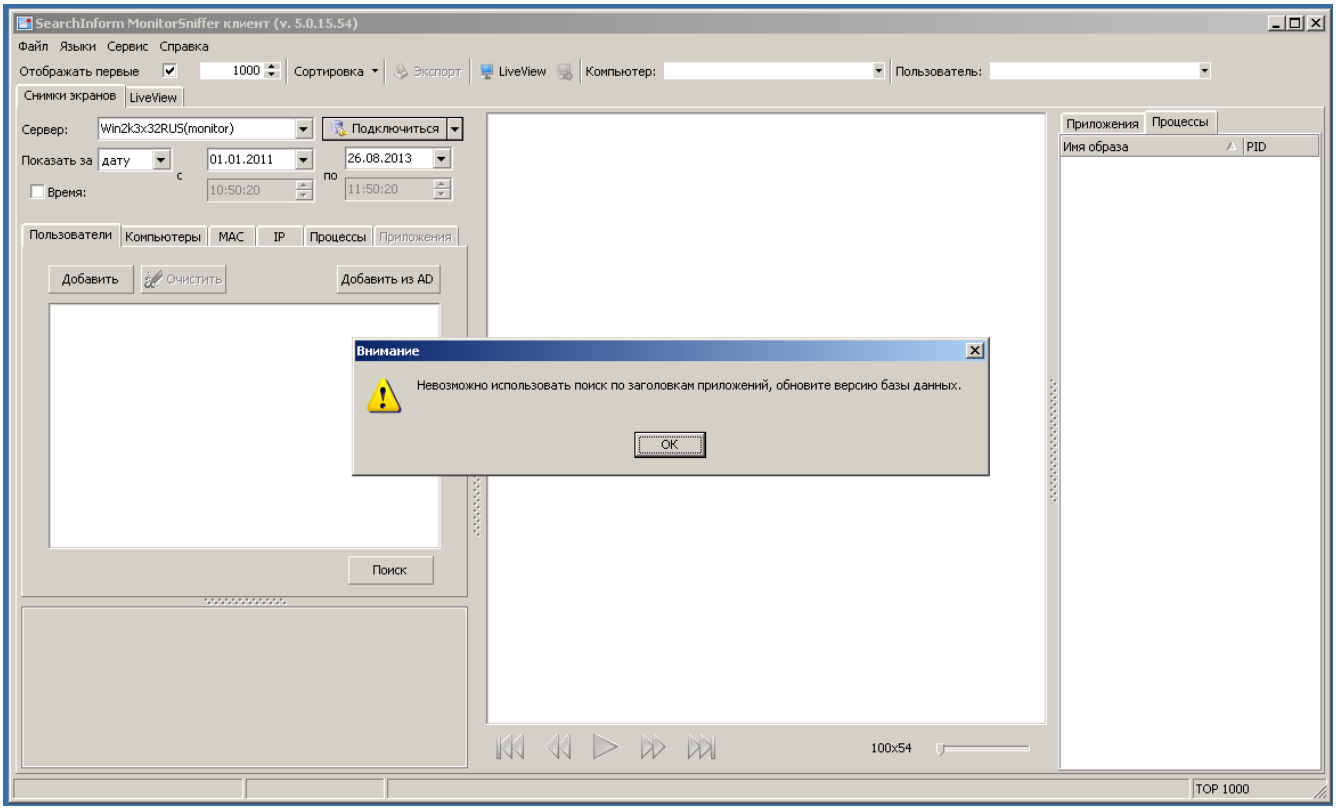
3.1. Контрольные вопросы






SearchInform EndpointSniffer: Administrator console (v. 5.0.21.32)
Файл Опции Вид ?
Запустить SearchInform EndpointSniffer
Настройки программы...
Нагрузка по агентам...
Потоки данных от агентов...
Справка
Конфигурирование агентов:
Редактирование 'MonitorSniffer' агента
WIN2K3X32RUS
Сетевое окружение
Агенты
Текущая активность
SoftInform Search Server
Лицензия
Фильтрация
Исключения (системные)
Исключения (пользовательские)
SSL-соединения
Включить перехват
Для выбранных
Urls
Включить LiveView
Настройки изображения
Настройки видео
Расписание
Включить создание снимков экрана
Интервал
Включено
Интервал для URLs
в течение
Интервал для снимков при видеоконференции Skype
Маски процессов
Totalcmd.exe
Не делать снимки, если компьютер заблокирован
Делать принудительный снимок при смене активного окна через
Сделать снимок только для активного окна
Не делать снимки, если нет активности от мыши и клавиатуры
Делать принудительные снимки при активной видеоконференции Skype
Делать снимки только основного дисплея
Оттенки серого
Объединять изображение с разных мониторов
OK
Отмена
Текущее подключение
Применить изменения


SearchInform EndpointSniffer: Administrator console (v
Файл Опции Вид ?
Остановить SearchInform EndpointSniffer
Настройки
Конфигурирование агентов:
WIN2K3X32RUS
Сетевое окружение
Агенты
Текущая активность
SoftInform Search Server
Лицензия
Агенты



К сожалению, в свежей версии образа не обновленная база данных.

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

  Несколько машин могут использовать один IP адрес.

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

  Пользователь может пользоваться не только одной машиной.

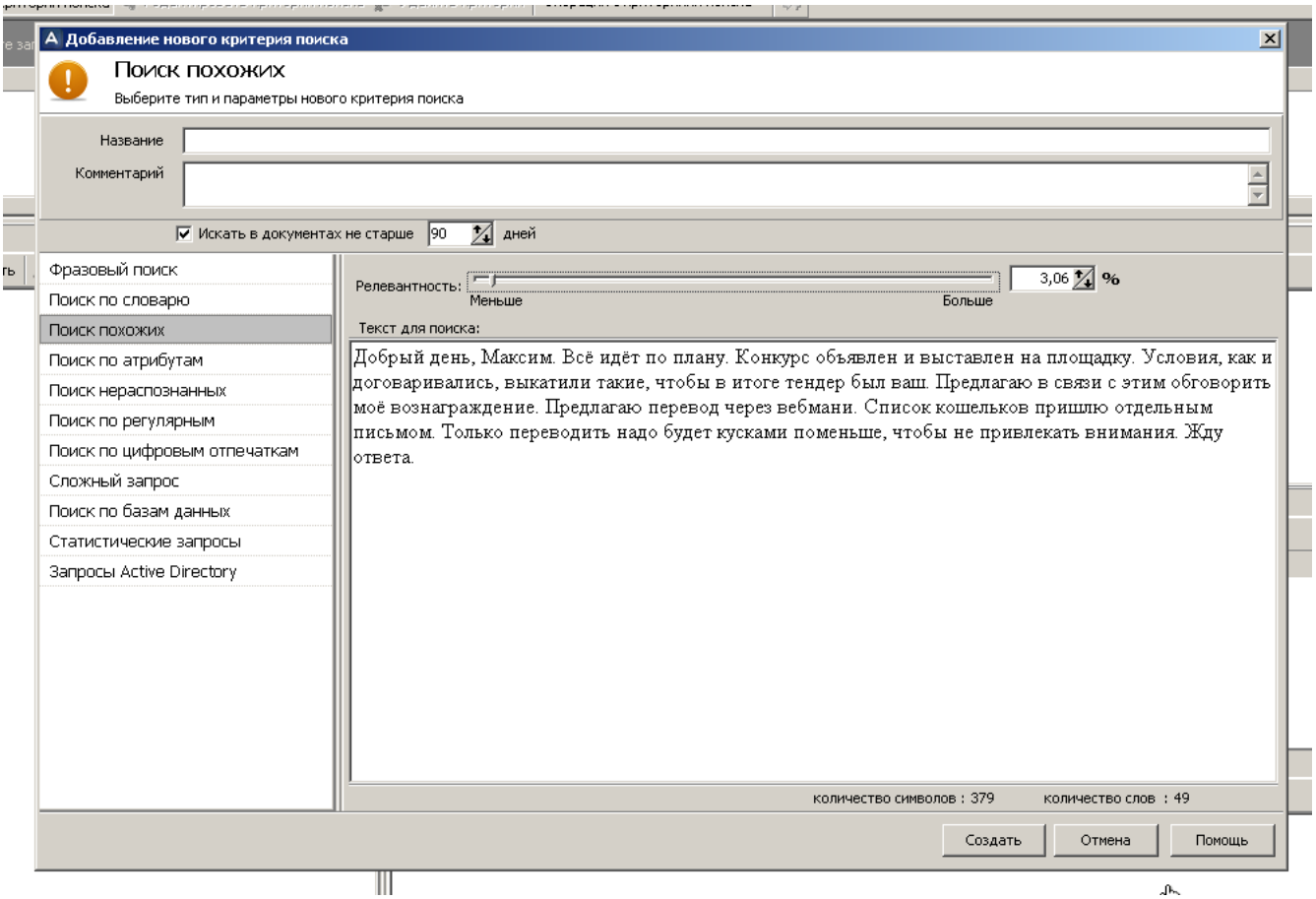
- Почему на данном виртуальном компьютере при текущей конфигурации программного комплекса SearchInform нельзя реализовать оперативный контроль за экраном пользователя?

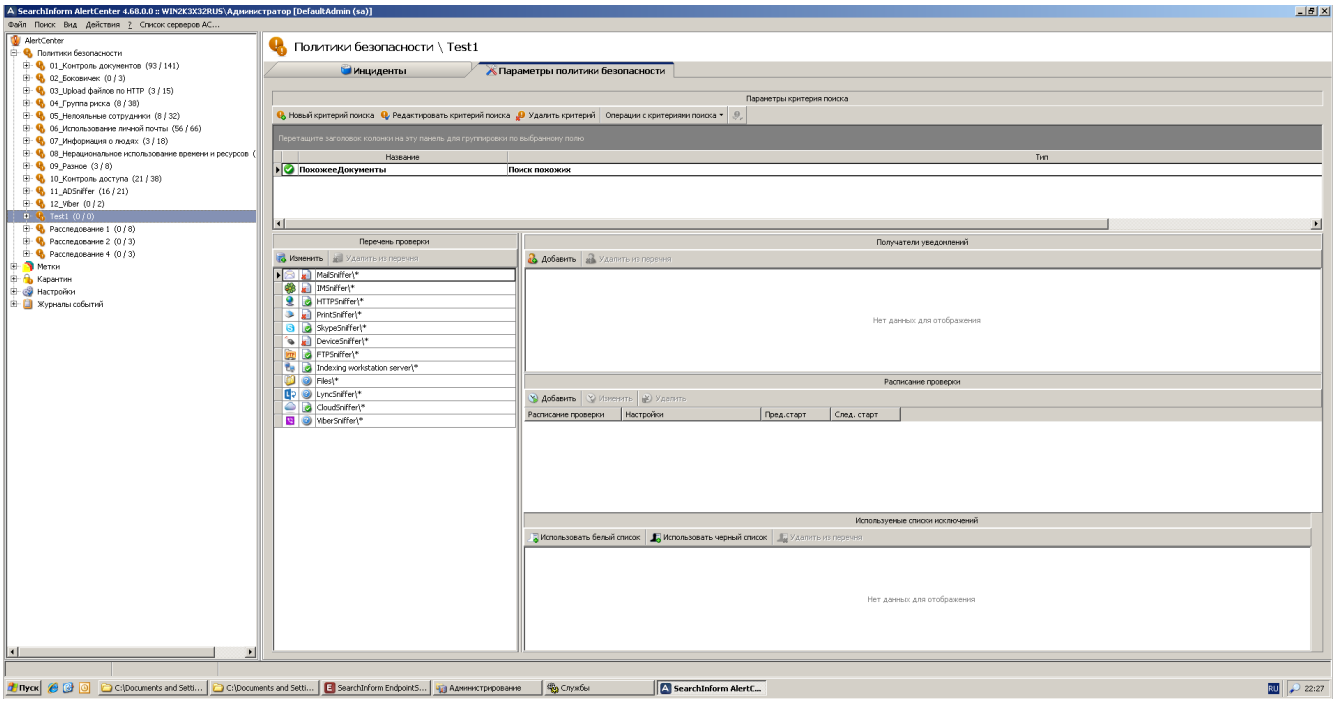
  Конфигурация не эмулирует только сервер с SearchInform.

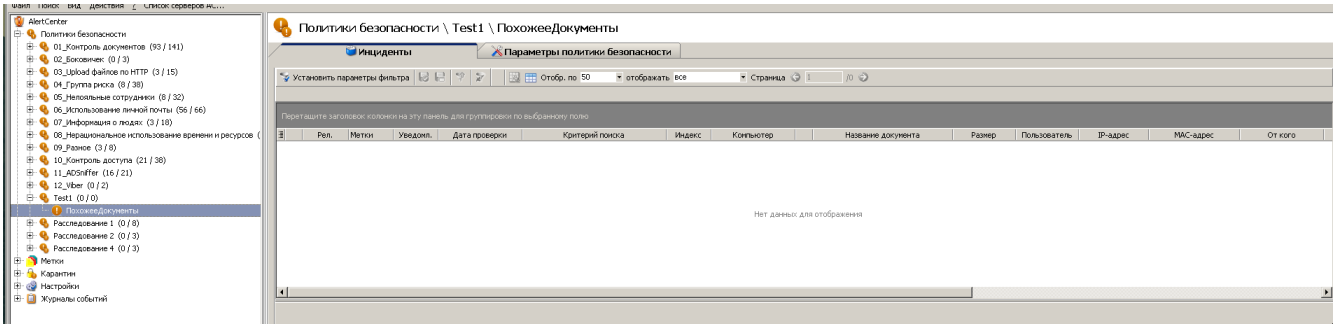
- Какое назначение опции LiveView агента MonitorSniffer?

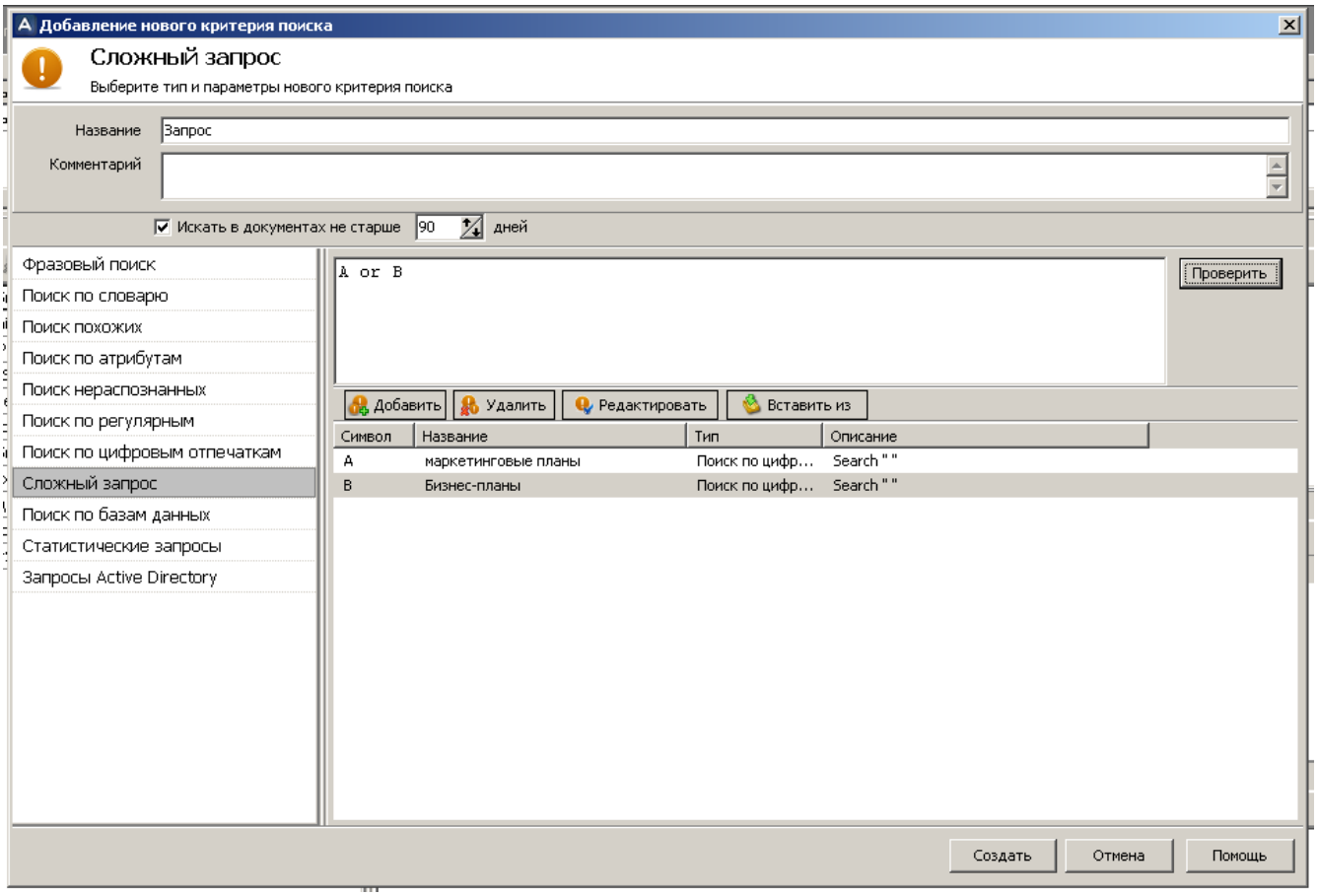
  Просмотр действий пользователя.

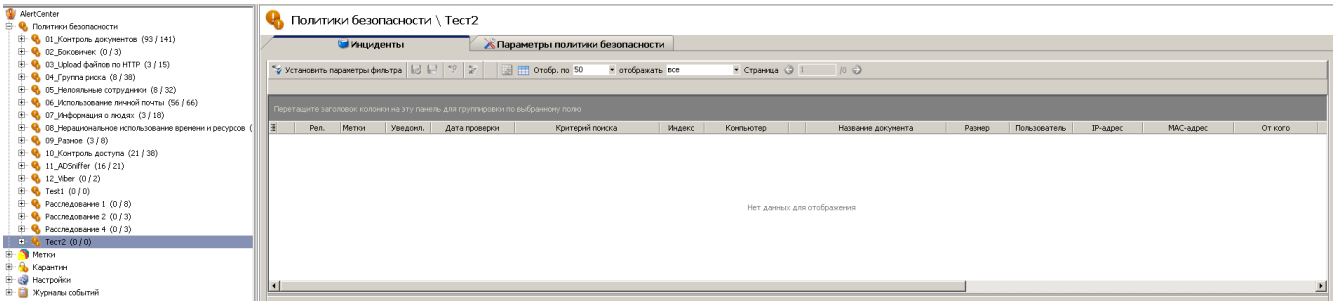
4. Настройка программного комплекса SearchInform для поиска конфиденциальной информации на основе подобия текстовых фрагментов

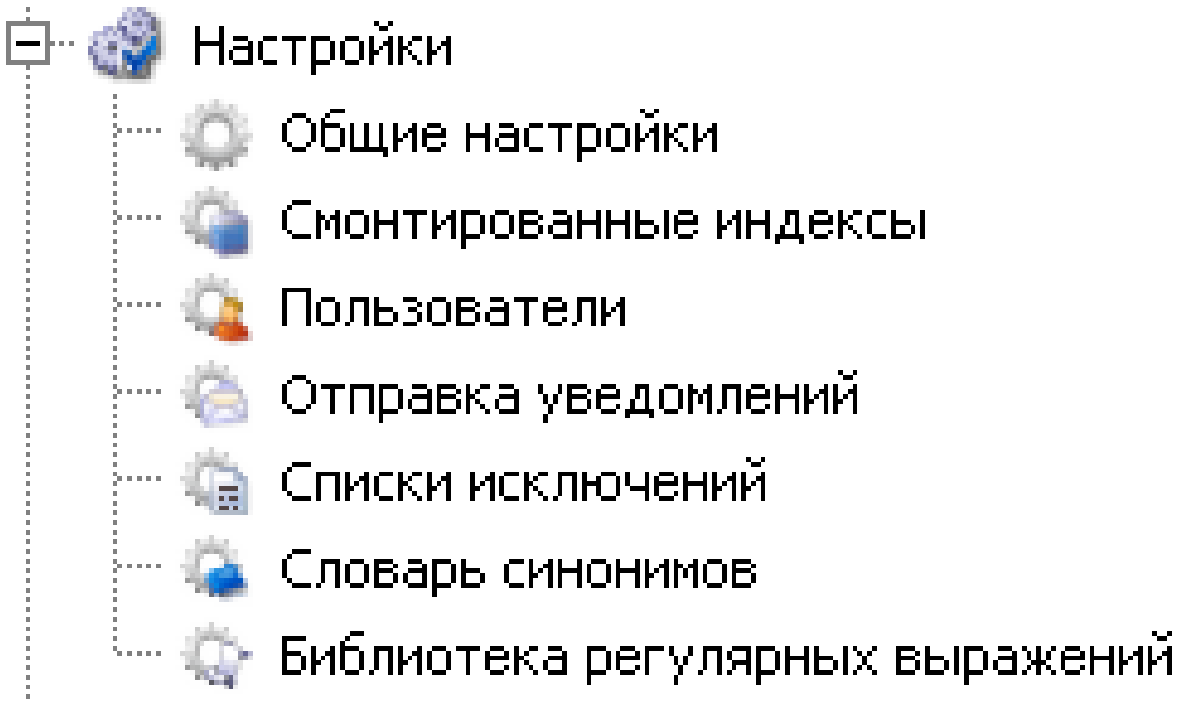





Политики безопасности \ Test1 \ ПохожееДокументы
Инциденты
Параметры политики безопасности
Нет данных для отображения


Добавление нового критерия поиска
Сложный запрос
Выберите тип и параметры нового критерия поиска
Название
Запрос
Комментарий
Искать в документах не старше
90
дней
Фразовый поиск
Поиск по словарю
Поиск похожих
Поиск по атрибутам
Поиск нераспознанных
Поиск по регулярным
Поиск по цифровым отпечаткам
Сложный запрос
Поиск по базам данных
Статистические запросы
Запросы Active Directory
A or B
Проверить
Добавить
Удалить
Редактировать
Вставить из
Символ
Название
Тип
Описание
A
маркетинговые планы
Поиск по цифр...
Search " "
B
Бизнес-планы
Поиск по цифр...
Search " "
Создать
Отмена
Помощь


Политики безопасности \ Тест2
Инциденты
Параметры политики безопасности
Нет данных для отображения



4.1. Контрольные вопросы

- Влияют ли пробелы между словами в запросе на результаты поиска по критерию «Поиск похожих»?

  Нет
- Какие документы целесообразно искать с помощью критерия «Поиск похожих»?

  Небольшие текстовые файлы
- Какие документы целесообразно искать с помощью критерия «По цифровым отпечаткам»?

  Большие текстовые файлы
- Что значит оператор and? И
- Что значит оператор or? Или
- Что значит оператор not? Не
- Что такое стоп-слова? Запрещенные подпоследовательности символов
- Как снять цифровой отпечаток из текста в графическом файле? Нужно как-либо факторизовать файл перед снятием отпечатка
- Можно ли снять цифровой отпечаток из pdf-файла?

  Нет, поскольку формат файла не содержит текст в явном виде, но можно распознать текст и работать отдельно с ним (потребует значительной вычислительной мощности)
- Можно ли снять цифровой отпечаток из java-файла?

  Да
- Какие документы нецелесообразно искать с помощью критерия «По цифровым отпечаткам»?

  Бинарные файлы
- Как объединяются простые запросы в сложные?

  С использованием логических конструкций
- Как проверить синтаксис сложного запроса?

  Кнопка ”Проверить”