**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт компьютерных технологий и защиты информации

### КАФЕДРА СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### к выполнению лабораторной работы № 1

на тему

**«**Настройка средств предотвращения утечки конфиденциальной информации**»**

Казань 2021

## Методические указания к выполнению лабораторной работы по изучению программных средств предотвращения утечки конфиденциальной информации

**Тема:**

Программные средства предотвращения утечки конфиденциальной информации.

**Цель:**

Получить навык работы со средствами предотвращения утечки конфиденциальной информации.

**Программно-аппаратные средства:**

Компьютерная лаборатория с установленным ПО виртуализации VMware Player. На платформе виртуализации развернут Windows Server 2003 R2 Enterprise Edition. На сервере установлены модули DLP-системы Контур информационной безопасности от SearchInform (SearchInform AlertCenter; SearchInform ReportCenter; SearchInform DataCenter).

### 3.2.1 Теоретическая часть

DLP-система представляет собой комплекс программно-аппаратных средств, обеспечивающих защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика.

Работа DLP-систем строится на перехвате и последующем анализе потоков данных, пересекающих периметр в направлении «вовне» либо циркулирующих внутри защищаемой корпоративной сети. Перехваченная информация анализируется с помощью различных поисковых алгоритмов, а при обнаружении данных, соответствующих выбранным критериям, срабатывает активная компонента системы, оповещая об инциденте сотрудника службы информационной безопасности (рисунок 3.1). При этом в ряде случаев передача сообщения (пакета, потока, сессии) может блокироваться. Существующие на данный момент DLP-системы обладают широкими функциональными возможностями и демонстрируют достаточно высокую эффективность при условии их грамотного применения.

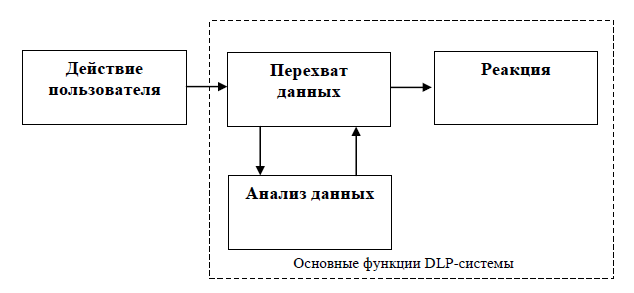


Рис. 3.1. Принцип функционирования DLP-системы

DLP-системы можно условно разделить на три типа: системные (уровня хоста), сетевые и прикладные (как правило, уровня СУБД). Независимо от типов DLP-систем применяемые методы анализа данных бывают атрибутные (например, использующие свойства объектов системы) и семантические (основанные на смысловом анализе информации, как правило, путем выявления сочетаний ключевых данных).

С технической точки зрения существует несколько возможностей получения информации об активности работников. К ним относятся:

* системы идентификации и аутентификации;
* логирование (журналирование);
* перехват, мониторинг и анализ трафика.

**Системы идентификации и аутентификации** позволяют с высокой степенью вероятности определить подлинность пользователя, либо удаленного узла. Данные системы предназначены для однозначного определения субъекта доступа и его полномочий по отношению к конкретному ресурсу.

**Логирование (журналирование).** Файл регистрации, протокол, журнал или лог – файл с записями о событиях в хронологическом порядке. Анализ различных логов позволяет получить более полную картину поведения работника. К примеру, анализ логов прокси-сервера покажет, какие ресурсы посещал сотрудник. Тем не менее, у анализа логов тот же недостаток: сами по себе записи в логах являются лишь косвенным подтверждением предполагаемой активности работника.

**Перехват, мониторинг и анализ трафика** осуществляется при помощи т.н. снифферов. Сниффер — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, направляемого на другие узлы. Поскольку первоначально при использовании снифферов анализ трафика осуществлялся вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), это делало возможным анализ лишь небольших его объёмов. Сегодня снифферы, как правило, включаются в состав более сложных систем, обладающих развитыми аналитическими функциями. Именно к таким и относятся рассматриваемые DLP-системы. Перехват трафика позволяет максимально полно контролировать работника, так как в этом случае помимо анализа косвенных признаков (посещённые ресурсы, действия с файлами и т.д.) появляется и прямая информация о действиях человека (содержание переписки по электронной почте, переписки при помощи IM, снимки рабочего стола и др. сведения).

Наиболее распространены следующие способы перехвата информации:

* перехват в разрыв;
* сетевой перехват;
* перехват путем интеграции со сторонними продуктами;
* агентский перехват.

**Перехват в разрыв.** В этом случае весь трафик компании пропускается через специальное физическое устройство. На сегодняшний день от такого вида перехвата отказались практически все производители DLP-систем, так как при использовании данного способа слишком велики угрозы бизнесу. В случае отказа, «падения» этого устройства в компании автоматически останавливается практически всё.

**Сетевой перехват.** Данный подход основан на том, что большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов на отдельно взятый порт. В основном это применяется для мониторинга всего трафика в целях безопасности, либо оценки производительности\загрузки сетевого оборудования с применением аппаратных средств, но также может быть использовано и для работы DLP-системы. В этом случае весь сетевой трафик направляется на коммутатор с поддержкой функции зеркалирования портов, который, снимает с трафика копию, которая, в свою очередь, затем анализируется.

Плюсы сетевого перехвата:

* независимость от операционной системы на машине работника;
* отсутствие дополнительной нагрузки на сеть;
* незаметность для работников и антивирусного программного обеспечения.

Минусы сетевого перехвата:

* проблемы с перехватом шифрованного трафика;
* малое количество контролируемых каналов.

**Перехват путем интеграции со сторонними продуктами.** Этот вид перехвата ориентирован на работу с прокси-серверами и почтовыми серверами. По принципу работы схож с сетевым перехватом. Главное из них заключается в том, что вместо адреса сетевого адаптера, с которого будет «сниматься» трафик, указываются сервер и порт подключения к нему.

Главный плюс перехвата путем интеграции со сторонними продуктами заключается в возможности перехвата почтовых сообщений, передаваемых по шифрованному каналу. Главный минус – еще меньшее количество контролируемых каналов в сравнении с сетевым перехватом.

**Агентский перехват.** В общем случае агенты представляют собой сервисы/программы, устанавливаемые непосредственно на компьютер или планшет пользователя и предназначенные для перехвата информации, а также её дальнейшей отсылки на сервер для анализа.

Этот вид перехвата на сегодняшний день пользуется наибольшим вниманием производителей DLP-систем и обладает рядом несомненных достоинств.

Плюсы агентского перехвата:

* позволяет контролировать все каналы информации;
* позволяет осуществлять перехват шифрованного трафика;
* позволяет в случае необходимости блокировать передачу информации.

Минусы агентского перехвата:

* создает дополнительную нагрузку на сеть;
* реализация связана с необходимостью присутствия агента непосредственно на компьютере работника;
* потребность в отдельных агентах для каждой операционной системы.

В данной лабораторной работе рассмотрены некоторые виды перехвата информации на базе Контура информационной безопасности SearchInform. Архитектура данной DLP-системы представлена на рисунке 3.2.

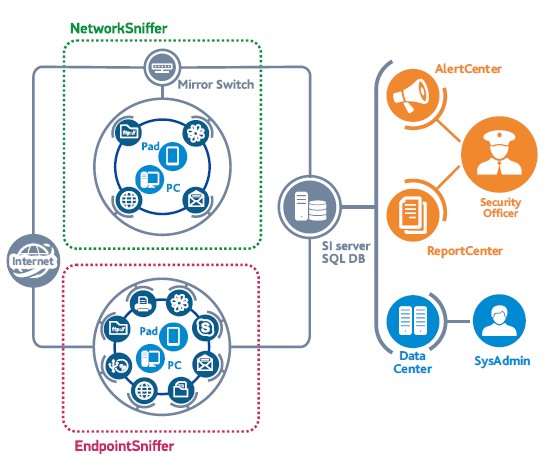


Рис. 3.2. Архитектура DLP-системы Контур информационной безопасности SearchInform

**SearchInform AlertCenter** предназначен для автоматического мониторинга информационных потоков с возможностью уведомления сотрудника службы безопасности о случаях нарушения политик информационной безопасности в отношении передаваемых данных.

AlertCenter имеет клиент-серверную архитектуру. Сервер AlertCenter обычно устанавливается на выделенный сервер, обеспечивая проверку перехваченных документов и отправку уведомлений в случае совпадений по введенным запросам. Клиентская часть, как правило, устанавливается на рабочую станцию сотрудника службы безопасности для настройки политик проверки перехваченных документов.

Благодаря поддержке и взаимодействию всех приложений КИБ AlertCenter обеспечивает мониторинг:

* документов, хранящихся на жестких дисках рабочих станций домена;
* данных, передаваемых на внешние устройства, такие как USB-флеш-накопители, CD/DVD диски, внешние винчестеры, Bluetooth-адаптеры и т.д.;
* входящего и исходящего трафика по FTP-соединению;
* сообщений, отправленных в форумы, блогов и иных сервисов при помощи веб-форм, поддерживающих GET- и POST-методы;
* сообщений IM-клиентов (ICQ, MSN, QIP и др.), а также сообщений в социальных сетях (Facebook, LinkedIn, В Контакте и др.);
* сообщений электронной почты, отправленных при помощи клиентов или при помощи почтовых веб-сервисов;
* документов, распечатанных на локальных и сетевых принтерах;
* сеансов текстовой и голосовой связи скайпа, файлов и SMS-сообщений, отправленных при помощи Skype.

Программный продукт **SearchInform ReportCenter** входит в состав предназначен для подключения к базам и индексам компонентов системы безопасности, обработки информации по статистике инцидентов, активности пользователей и генерации отчетов в удобной для сотрудников службы безопасности форме.

Для получения необходимых данных ReportCenter подключается к базе инцидентов компонента AlertCenter, а также к индексам, созданным для DeviceSniffer, FTPSniffer, HTTPSniffer, IMSniffer, MailSniffer, PrintSniffer, SkypeSniffer.

Благодаря поддержке вышеуказанных компонентов Searchinform ReportCenter обеспечивает построение отчетов по следующим классам переданной пользователями информации:

* документы, записанные на USB-носители, CD/DVD-матрицы и другие накопители;
* файлы, отправленные и полученные по FTP-cоединению;
* сообщения, отправленные в форумы, блоги и иные сервисы при помощи веб-форм, поддерживающих POST-метод;
* сообщения IM-клиентов (ICQ, MSN, QIP и др.);
* сообщения электронной почты, отправленные при помощи клиентов или при помощи почтовых веб-сервисов;
* документы, распечатанные на сетевых принтерах;
* сеансы текстовой и голосовой связи Skype, файлы и SMS-сообщения, переданные при помощи Skype.

Сгенерированные отчеты могут быть представлены как в табличной форме, так и виде диаграмм, в виде временного графика, а также в виде графа отношений, представляющего собой регулируемую визуализацию связей между пользователями, находящимися в контакте.

Программный продукт **SearchInform DataCenter** предназначен для автоматизированного и ручного управления различными аспектами работы КИБ.

Перечень ключевых функций Searchinform DataCenter:

* управление индексами и базами данных продуктов;
* контроль работоспособности КИБ;
* управление службами компонентов КИБ;
* мониторинг дискового пространства на серверах КИБ;
* автоматическое оповещение о важных событиях;
* синхронизация с одним или более доменом Active Directory;
* разграничение прав доступа сотрудников службы безопасности к информации определенных пользователей или групп пользователей;
* задание настроек для подключения к базам данных по умолчанию;
* управление настройками компонентов КИБ.

### 3.2.2 Задание

1. Изучить теоретическую часть (45 минут);
2. Внедрить политику информационной безопасности в SearchInform AlertCenter (20 минут);
3. Проанализировать события, попавшие в журнал карантина в SearchInform AlertCenter (10 минут);
4. Добавить пользователей в консоли SearchInform AlertCenter и наделить их правами в соответствии занимаемым должностям (10 минут);
5. Сформировать отчет по активности выбранных пользователей в SearchInform ReportCenter (20 минут);
6. Создание персонального отчета по выбранным атрибутам в SearchInform ReportCenter (15 минут);
7. Подготовить отчет о выполненной работе (30 минут);
8. Ответить на контрольные вопросы (30 минут).

### 3.2.3 Инструкция к выполнению заданий

**Внедрение политики ИБ в SearchInform AlertCenter**

1. Запустите средство виртуализации VMware Player и откройте клиент SearchInform AlertCenter (рисунок 3.3). Пароль ко всем компонентам системы - Admin;

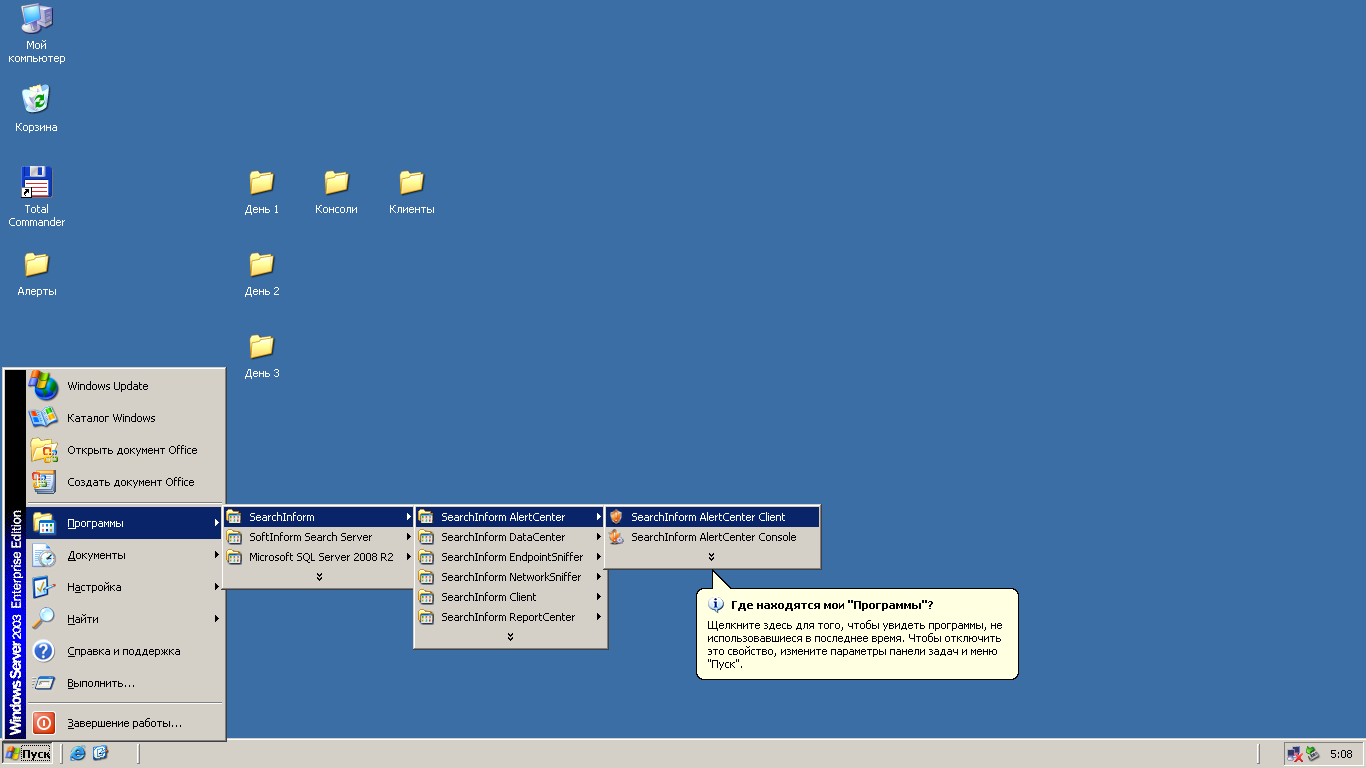


Рис. 3.3. Запуск клиента SearchInform AlertCenter на виртуальной машине

1. Откройте вкладку «Политики безопасности» и добавьте новую политику, вписав название в появившееся окно (рисунок 3.4).

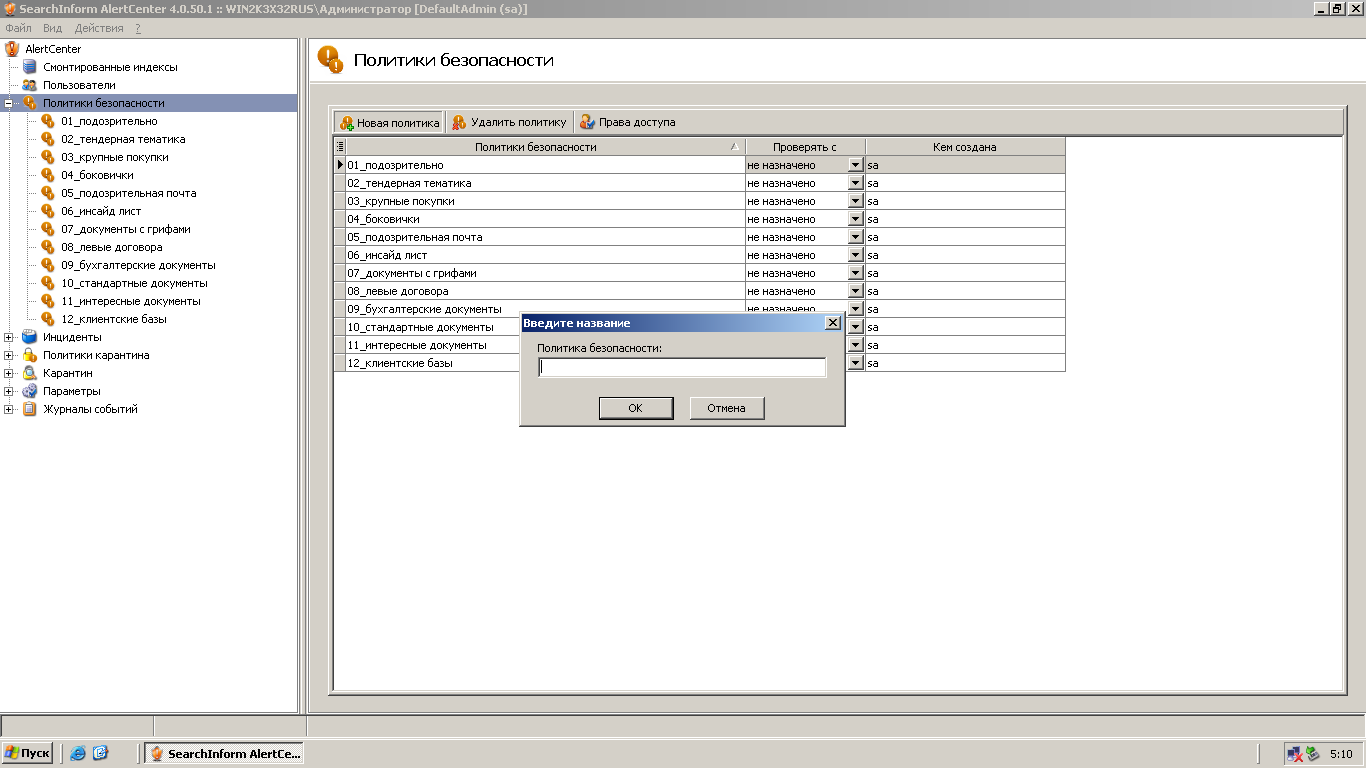


Рис. 3.4. Добавление новой политики безопасности

1. Найдите в списке созданную политику и задайте произвольные критерии поиска инцидентов (рисунки 3.5-3.6);

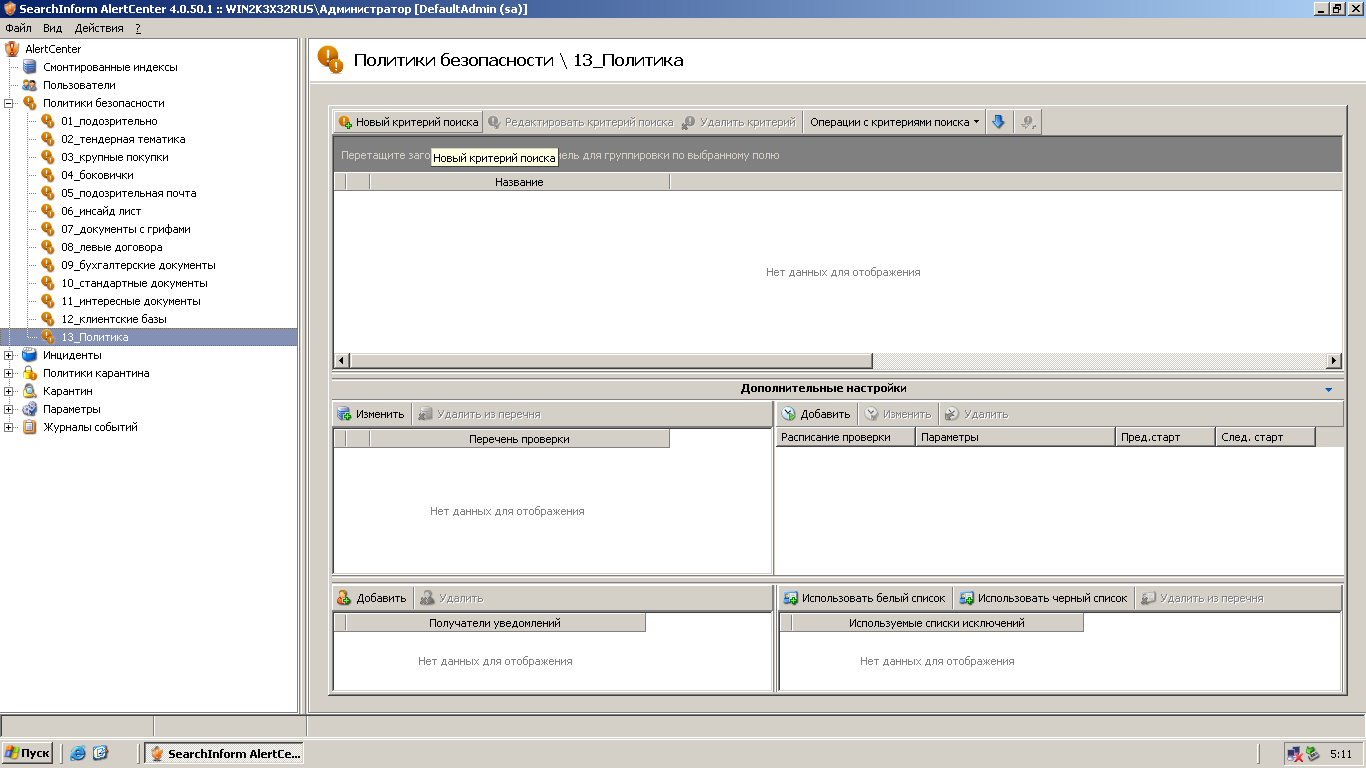


Рис. 3.5. Создание критерия поиска инцидентов

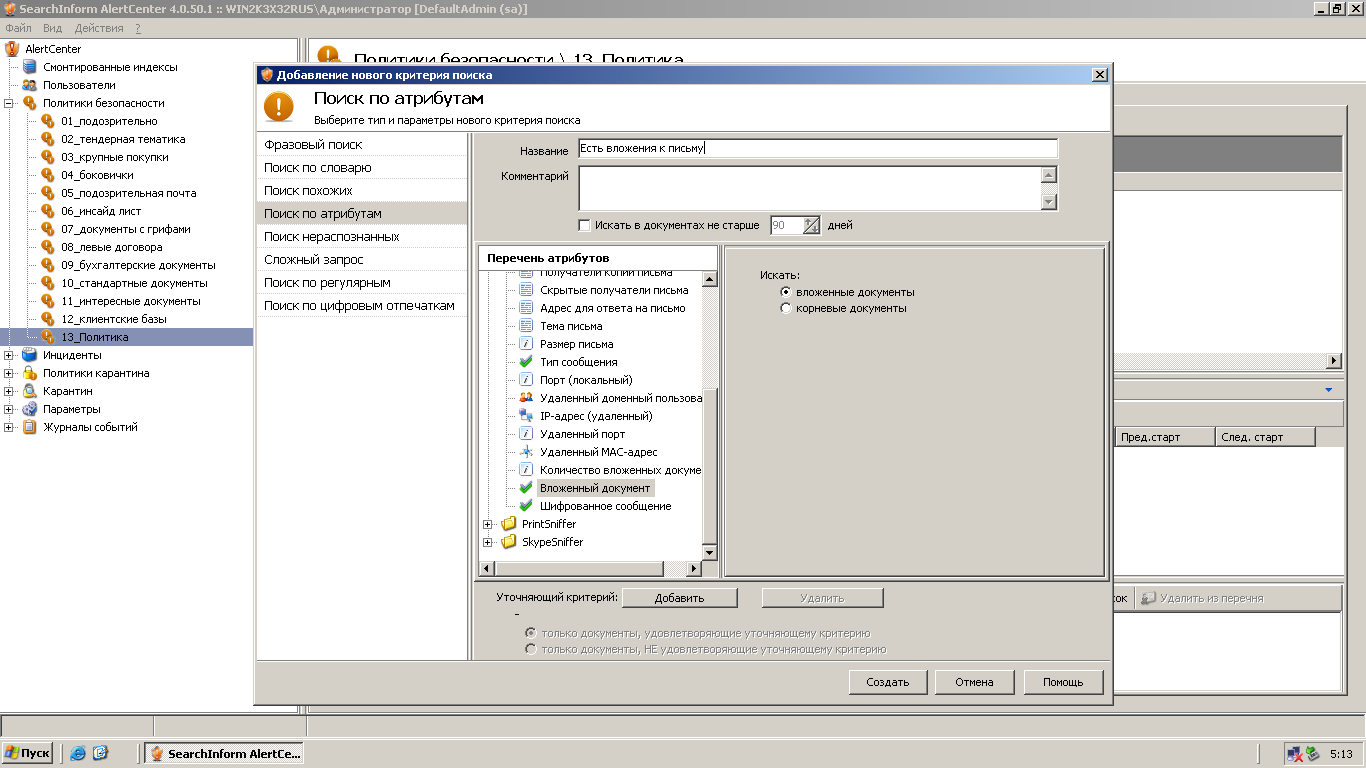


Рис. 3.6. Выбор типа и параметров нового критерия поиска инцидентов

1. Запустите созданную политику и проверьте во вкладке «Инциденты», найден ли инцидент, соответствующий вашей политике;
2. Попробуйте задать такие критерии поиска в политике, чтобы система нашла хотя бы один произошедший инцидент.

**Анализ журнала карантина в SearchInform AlertCenter**

1. Откройте вкладку «Проверки карантина» и проанализируйте находящиеся там объекты (рисунок 3.7);

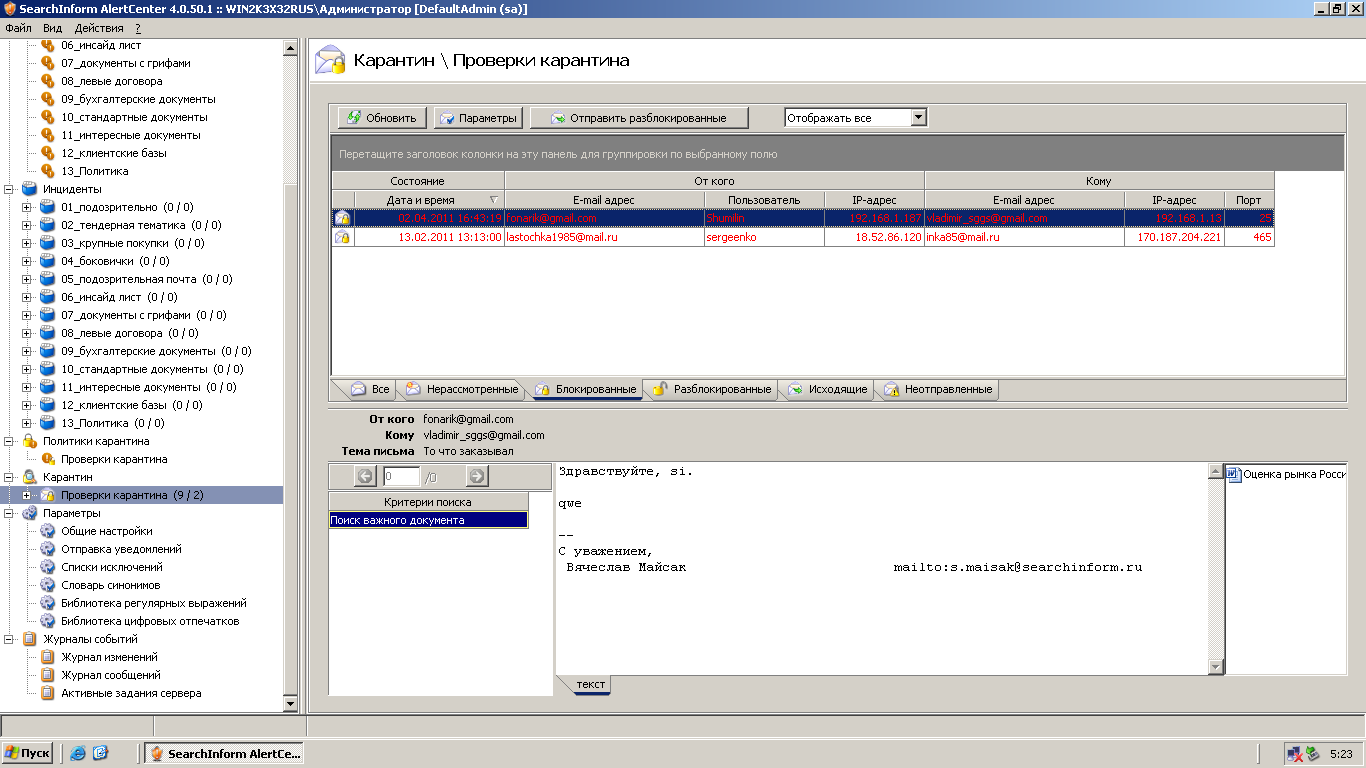


Рис. 3.7. Журнал карантина

1. Отразите в отчете причины попадания 1-2 выбранных объектов в данный журнал.

**Добавление пользователей в консоли SearchInform AlertCenter**

1. Откройте вкладку «Пользователи» в консоли SearchInform AlertCenter и нажмите «Добавить пользователей» (рисунок 3.8);

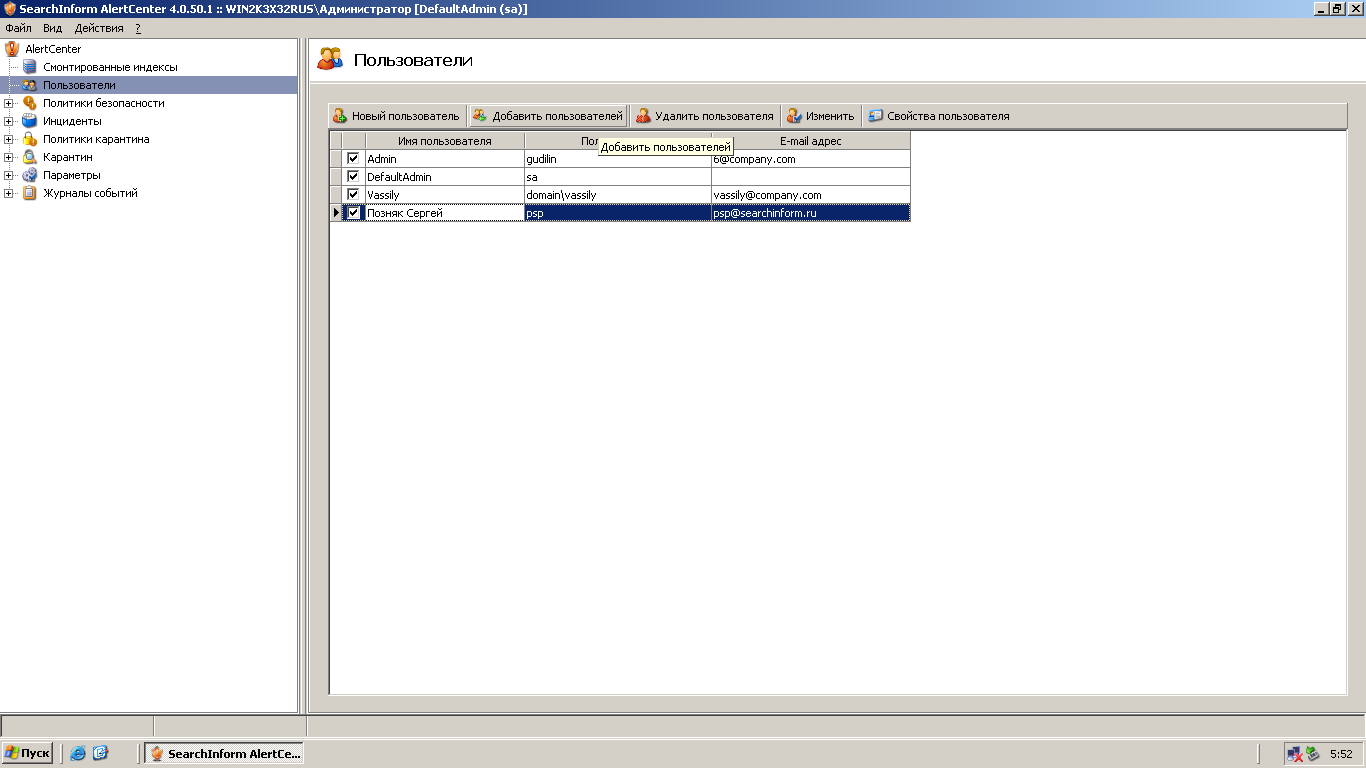


Рис. 3.8. Добавление пользователей в консоль SearchInform AlertCenter

1. Из появившегося списка выберите произвольного пользователя модуля DataCenter. Нажмите внизу окна клавишу «Добавить» (рисунок 3.9);

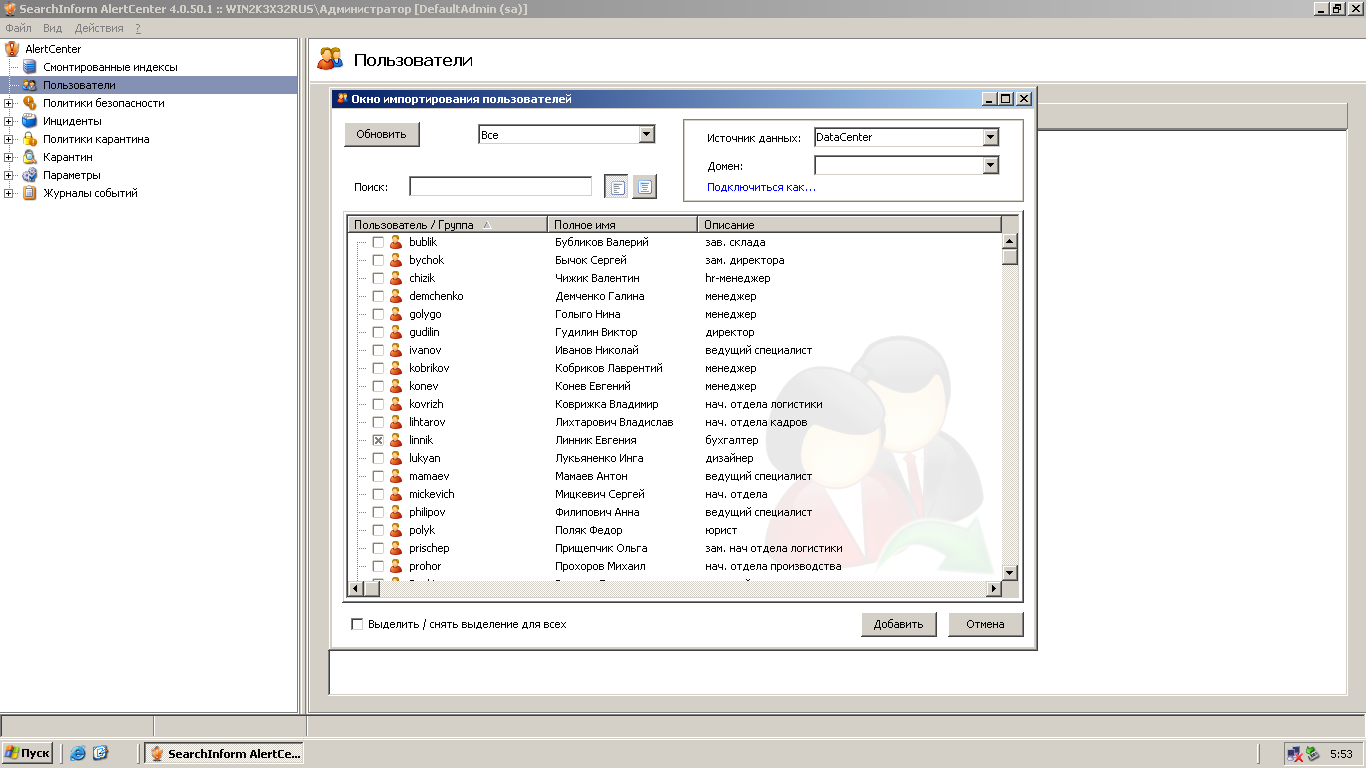


Рис. 3.9. Выбор пользователя из модуля DataCenter в консоли SearchInform AlertCenter

1. После того как пользователь был добавлен, выделите строку списка, соответствующую добавленному пользователю, и нажмите «Изменить». Предоставьте пользователю права для работы с политиками в соответствии с его должностью (рисунок 3.10).

На вкладке «Политики безопасности» для каждой из политик индивидуально можно задать права доступа:

* «Запрещено» – пользователю не доступны как сама политика, так и результаты проверки по ней;
* «Только просмотр» – пользователь имеет доступ к политике, но без права ее изменения;
* «Изменить» – доступ с правом редактирования.

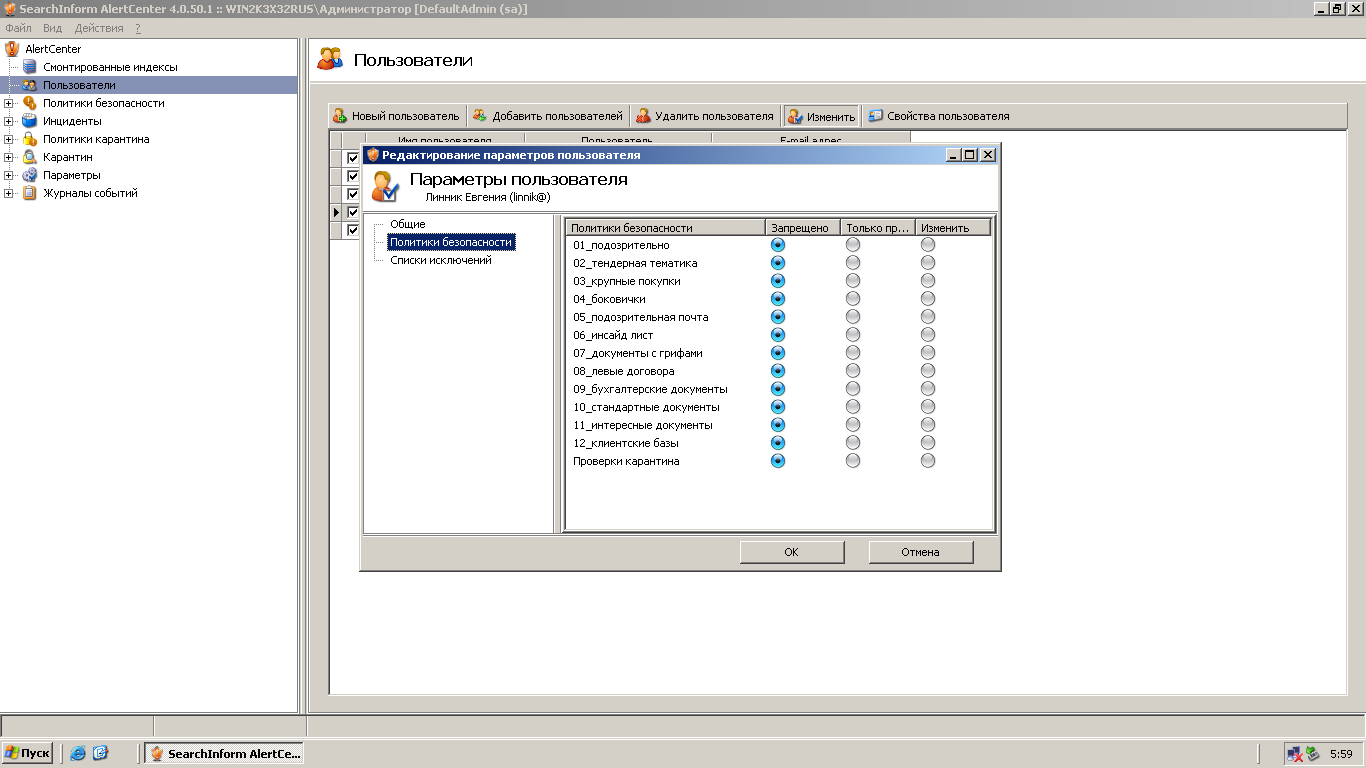


Рис. 3.10. Наделение пользователей правами в консоли SearchInform AlertCenter

**Формирование отчета об активности выбранных пользователей в SearInform ReportCenter**

1. Откройте SearchInform ReportCenter. В левом меню выберите форму отчета «Количество сообщений по пользователям» (рисунок 3.11);

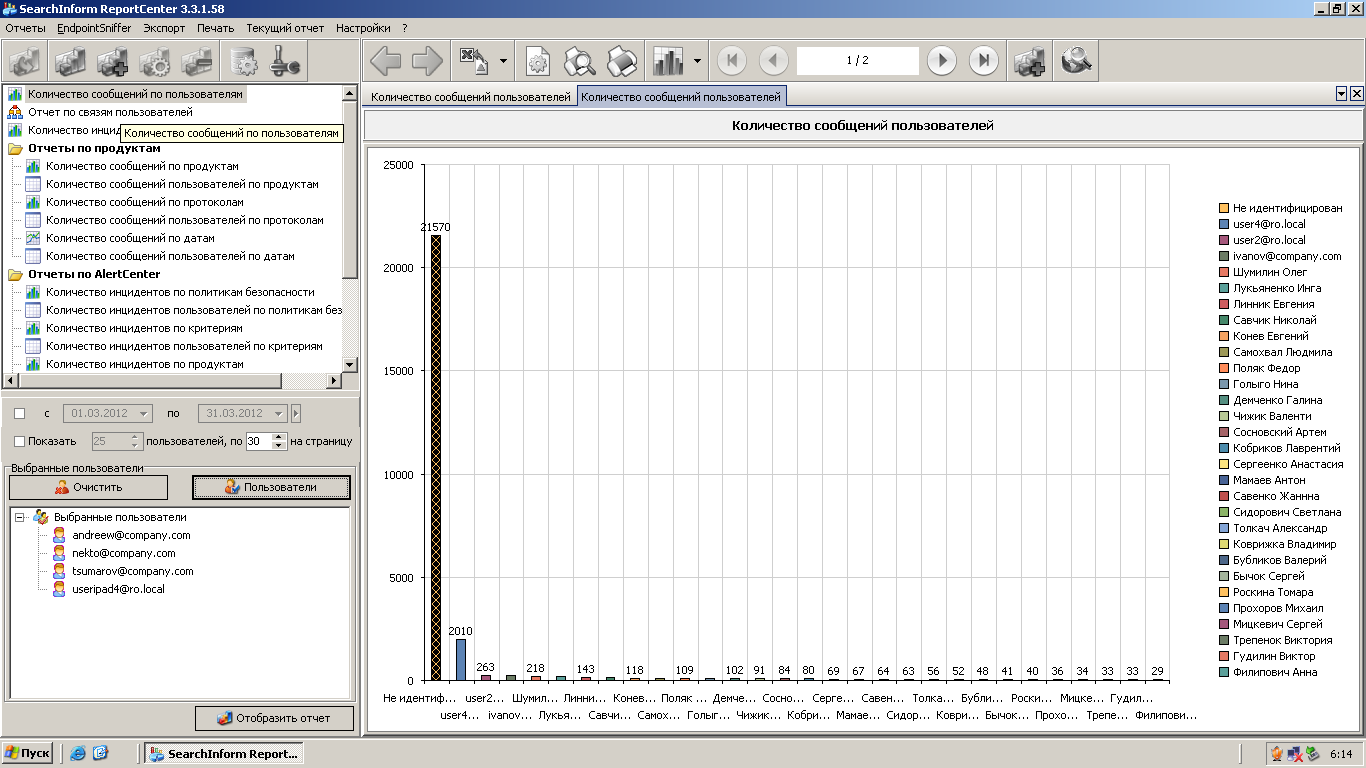


Рис. 3.11. Выбор формы отчета

1. Нажав клавишу «Пользователи», добавьте пользователей, по активности которых будет сформирован отчет. Добавьте интервал учета активности пользователей и нажмите «Отобразить отчет» (рисунок 3.12);

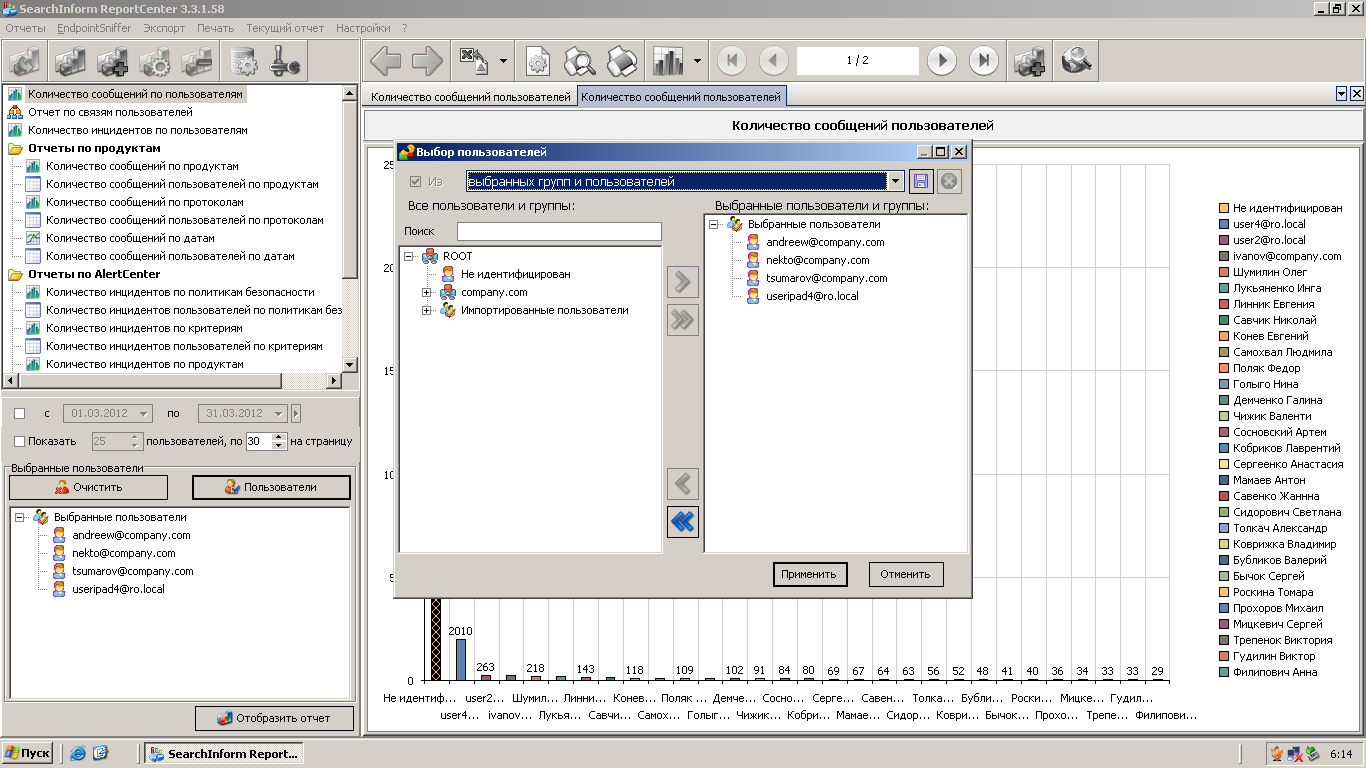


Рис. 3.12. Добавление пользователей, по которым будет сформирован отчет

1. Измените форму представления полученного отчета, нажав «Просмотр отчета в виде таблицы» (рисунок 3.13).

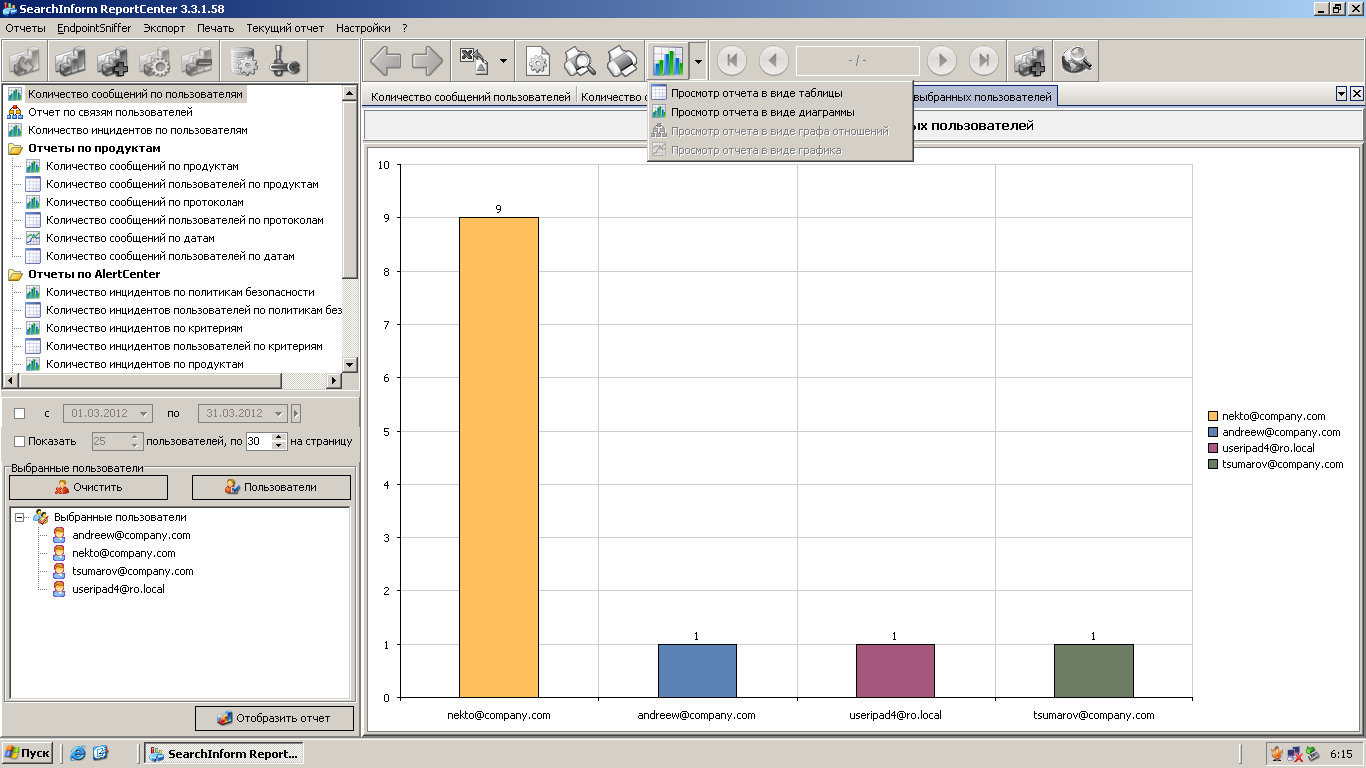


Рис. 3.13. Просмотр отчета в виде таблицы

**Создание персонального отчета в SearchInform ReportCenter**

1. Нажмите в меню вверху страницы «Отчеты» и создайте шаблон отчета (рисунок 3.14);

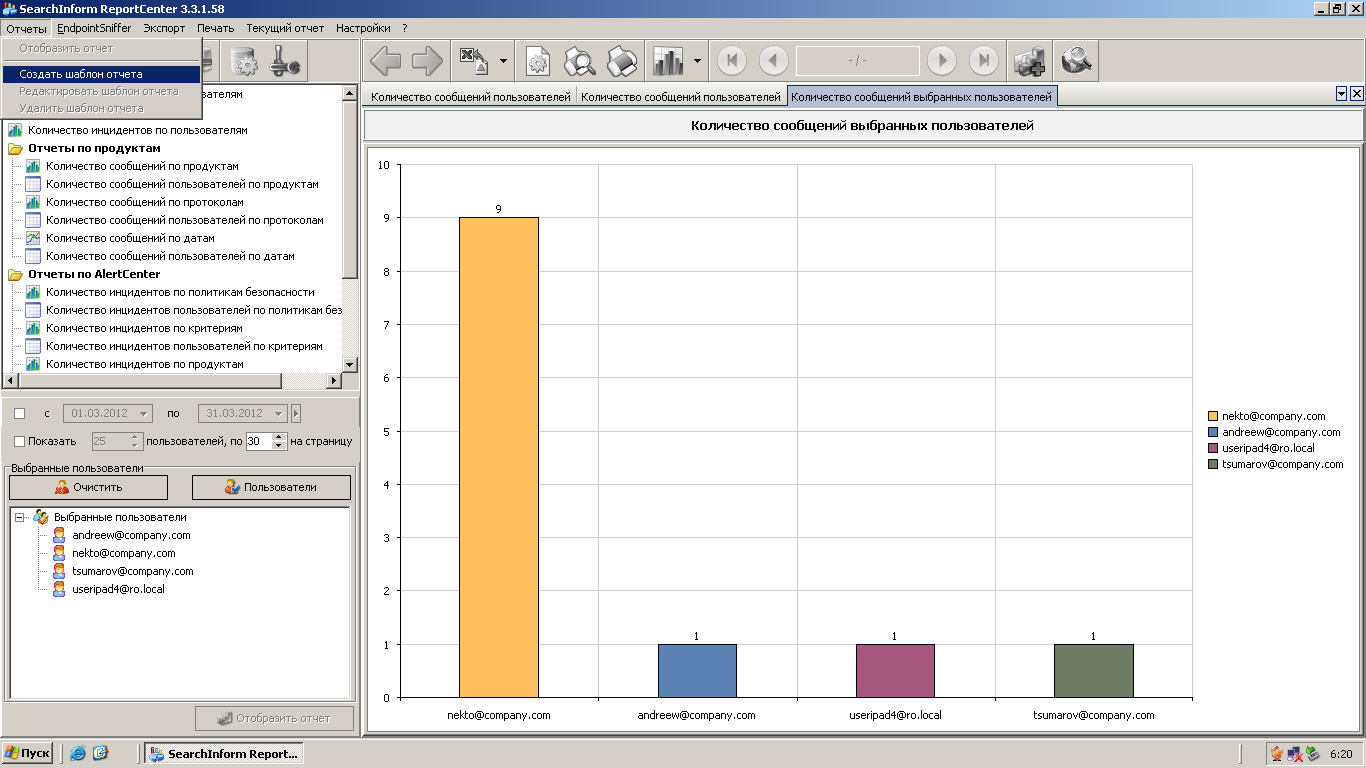


Рис. 3.14. Создание персонального шаблона отчета

1. Задайте атрибуты нового отчета в появившемся окне мастера отчетов (рисунок 3.15);

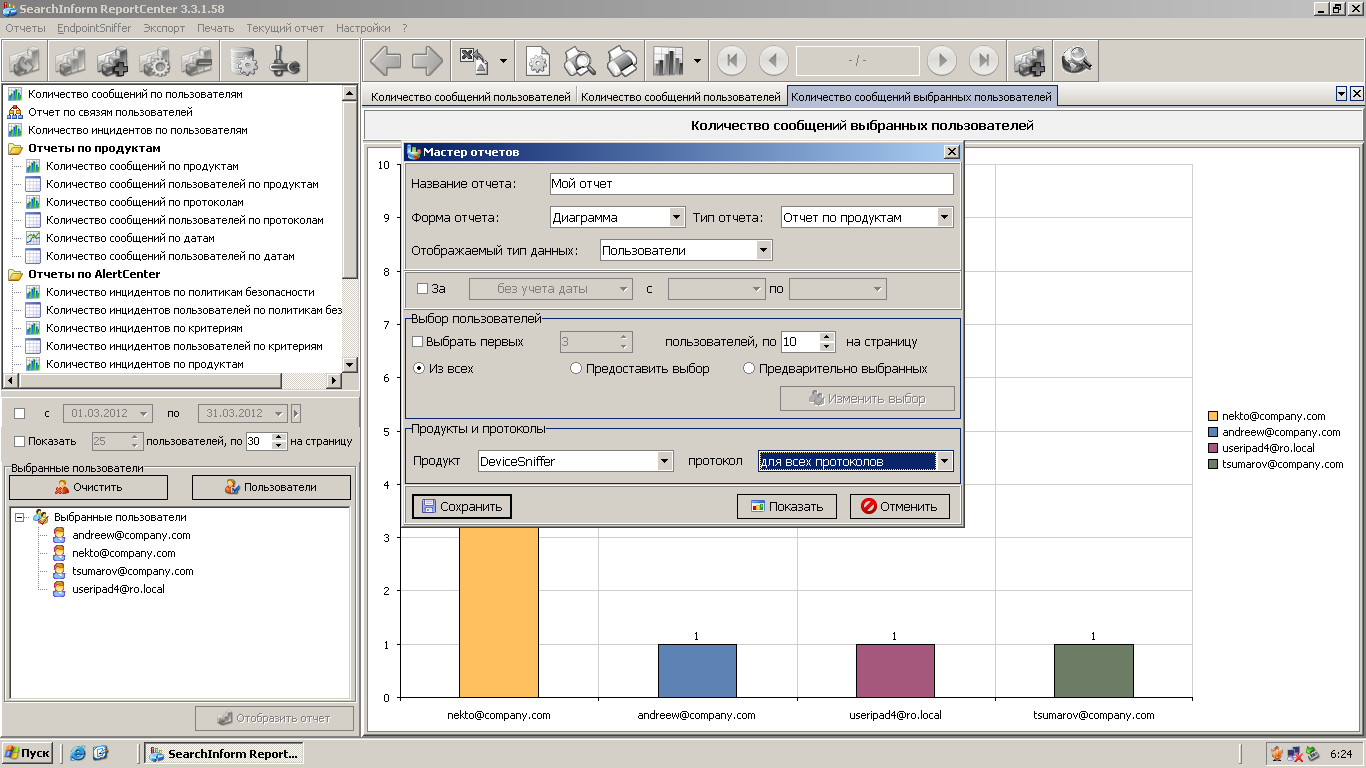


Рис. 3.15. Настройка шаблона персонального отчета

1. Для сохранения получившейся формы отчета в качестве шаблона щелкните кнопку «Сохранить», а для просмотра отчета без сохранения шаблона – щелкнуть кнопку «Показать» (рисунок 3.16).

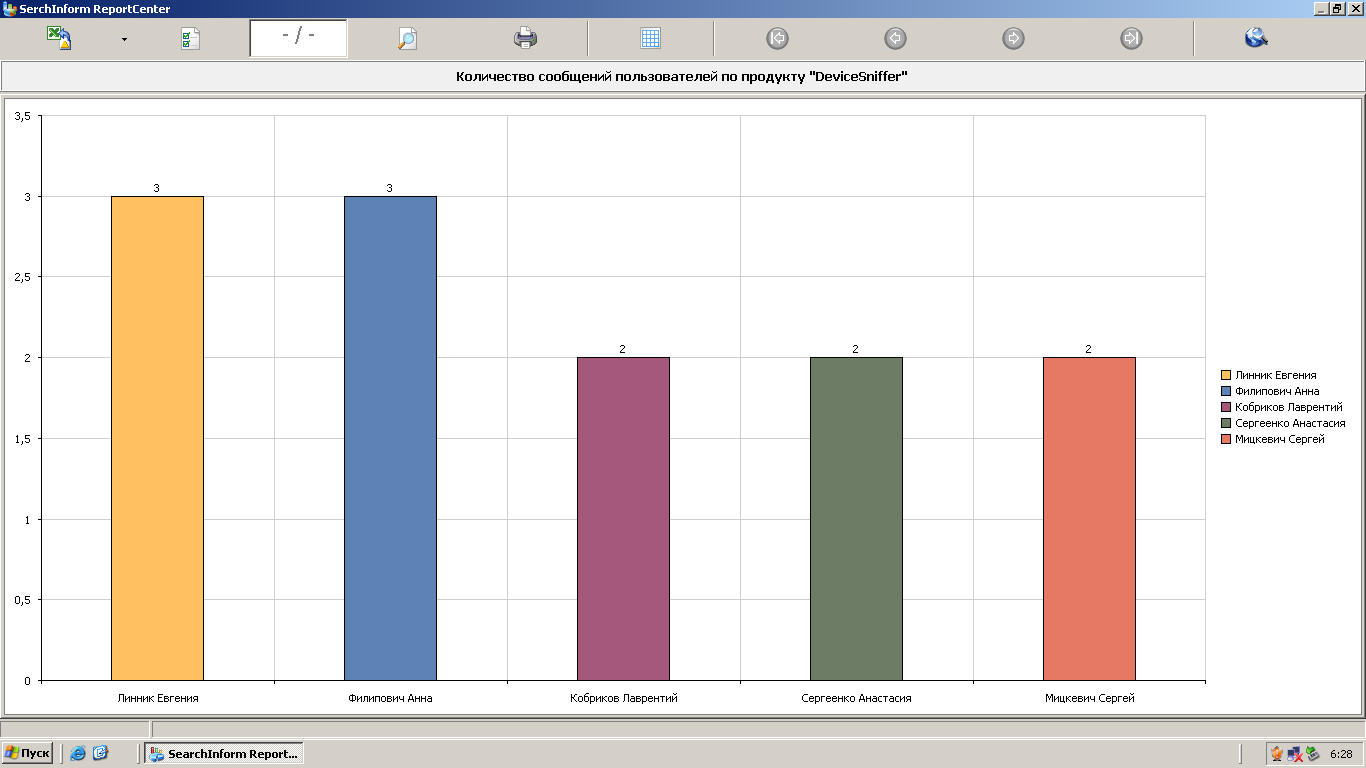


Рис. 3.16. Результат формирование персонального отчета

### 3.2.4 Пример отчета по лабораторной работе

**Тема:**

Программные средства предотвращения утечки конфиденциальной информации.

**Цель:**

Получить навык работы со средствами предотвращения утечки конфиденциальной информации.

**Выполнил**

Студент гр. № \_\_\_\_\_\_

ФИО

**Отчет**

**Внедрение политики ИБ в SearchInform AlertCenter**

Снимки экрана и результаты вывода программы, подтверждающие выполнение каждого пункта задания

**Анализ журнала карантина в SearchInform AlertCenter**

Снимки экрана и результаты вывода программы, подтверждающие выполнение каждого пункта задания

**Добавление пользователей в консоли SearchInform AlertCenter**

**Формирование отчета об активности выбранных пользователей в SearInform ReportCenter**

**Создание персонального отчета в SearchInform ReportCenter**

### 3.2.5 Контрольные вопросы

1. Охарактеризуйте назначение систем идентификации и аутентификации.
2. Охарактеризуйте назначение сетевых анализаторов трафика/снифферов.
3. Перечислите плюсы и минусы агентского перехвата информации в компьютерных сетях.
4. Зачем необходимо осуществлять настройку синхронизации с Active Directory?
5. Назовите назначение программного продукта Searchinform AlertCenter.
6. Как осуществляется настройка политик безопасности?
7. Сколько существует в Searchinform AlertCenter типов доступа пользователя к политике безопасности?
8. Назовите назначение программного продукта Searchinform ReportCenter.
9. Как осуществляется выбор временного периода, за который будет сгенерирован тот или иной отчет?
10. Как осуществляется выбор пользователей, по которым будет сгенерирован тот или иной отчет?
11. Какие формы используются для представления отчетов?
12. Опишите процедуру создания нового шаблона отчета.