SearchInform

Контур Информационной Безопасности Предприятия

В последнее время очень актуальной проблемой для многих компаний является деятельность инсайдеров, которые занимаются хищением конфиденциальной информации. Комплексные системы безопасности, просто перехватывающие информацию, не дают возможности качественно проанализировать её. Анализ информации включает в себя множество составляющих: сбор полной статистики, прослеживание тенденций, поиск информации в перехваченных данных.

SearchInform

Кто может пострадать от утечки информации?

Утечки информации наносят ущерб компаниям во всех отраслях. Даже очень крупные и успешные компании не застрахованы от деятельности инсайдеров, что подтверждается периодически появляющимися в прессе сообщениями об утечках:

- 2007-м году корейский автогигант Kia Motors потерял несколько миллиардов долларов из-за продажи инсайдерами разработок компании её конкурентам из Китая;
- 2008-м Bank of New York допустил утечку информации о своих клиентах, обошедшуюся ему в $866 млн.;
- 2009-м три подразделения британской группы компаний HSBC были оштрафованы на сумму более £3 млн. за неспособность обеспечить адекватную защиту данных своих клиентов от утечки и кражи.

Проблема защиты информации от утечек в России стоит не менее остро, чем в целом по миру. Согласно исследованию, проведённому в мае 2009 кадровым холдингом АНКОР, 22% россиян пользуются служебной информацией для стороннего приработка.

SearchInform

Возможные пути утечки информации

Информация может быть переписана на локальный компьютер, где может подвергаться несанкционированным правкам.

Это может быть отосланное по почтовым протоколам (SMTP, POP3, IMAP,MAPI) электронное письмо.

Посты размещенные в форумах, блогах, социальных сетях.

Сообщение, отправленное посредством клиентов для мгновенного обмена сообщениями (ICQ, JABBER, MSN Messenger, Mail.ru Агент и другие).

Голосовые или текстовые сообщения отправленные через Skype.

Также данные могут быть переписаны на съёмный носитель (например USB-носитель или CD/DVD диски).

Информация может быть распечатаны на принтере.

Альтернатива блокировке каналов утечки информации

Существует распространённое решение проблемы утечки информации за пределы компании – блокировка каналов возможного хищения. Однако этот вариант не является оптимальным. Можно блокировать возможность доступа к локальным дискам компьютера и к электронной почте, однако, сделав это, вы скорее всего лишите сотрудника возможности работать вовсе. А также блокировка ICQ, USB-портов или доступа к записывающим CD/DVD устройствам и принтеру неблаготворно влияет на сотрудника, а зачастую также не даёт работать полноценно.

Современная система должна позволять сотруднику использовать все каналы для передачи информации, однако перехватывать и анализировать информационные потоки, идущие по этим каналам.

SearchInform

Контур информационной безопасности

«Контур информационной безопасности SearchInform» позволяет отслеживать утечки конфиденциальной информации через e-mail, ICQ, Skype, посты на форумах или комментарии в блогах, внешние устройства (USB/CD), документы отправляемые на печать и выявлять её появление на компьютерах пользователей.

В первую очередь качество отслеживания утечек конфиденциальной информации определяется возможностями полнотекстового поиска.

Полнотекстовый поиск – инструмент для обеспечения информационной безопасности

Современные средства предотвращения утечек информации генерируют огромный объём данных, с которым невозможно разобраться вручную. Поэтому на первый план выходят возможности системы по анализу перехваченных данных.

Наш продукт поддерживает поиск по фразам с учётом расстояний между нужными словами, поиск документов где есть похожие на заданный абзацы или фрагменты текста, позволяет гораздо более эффективно выявлять утечки конфиденциальной информации по открытым каналам даже при её переписывании другими словами.

Интеллектуальные виды полнотекстового поиска

В качестве примера возьмём ситуацию, когда службе информационной безопасности поручено контролировать факты поиска сотрудниками компании другого места работы. Одним из вариантов это выяснить будет установление факта рассылки резюме.

Первым делом необходимо составить список слов и фраз, характерных именно для резюме:

Год рождения	Электронная почта	Опыт работы	Владение иностранным языком
Адрес проживания	Образование	Заработная плата	Личные и деловые качества
Телефон	Должность	Резюме	.....

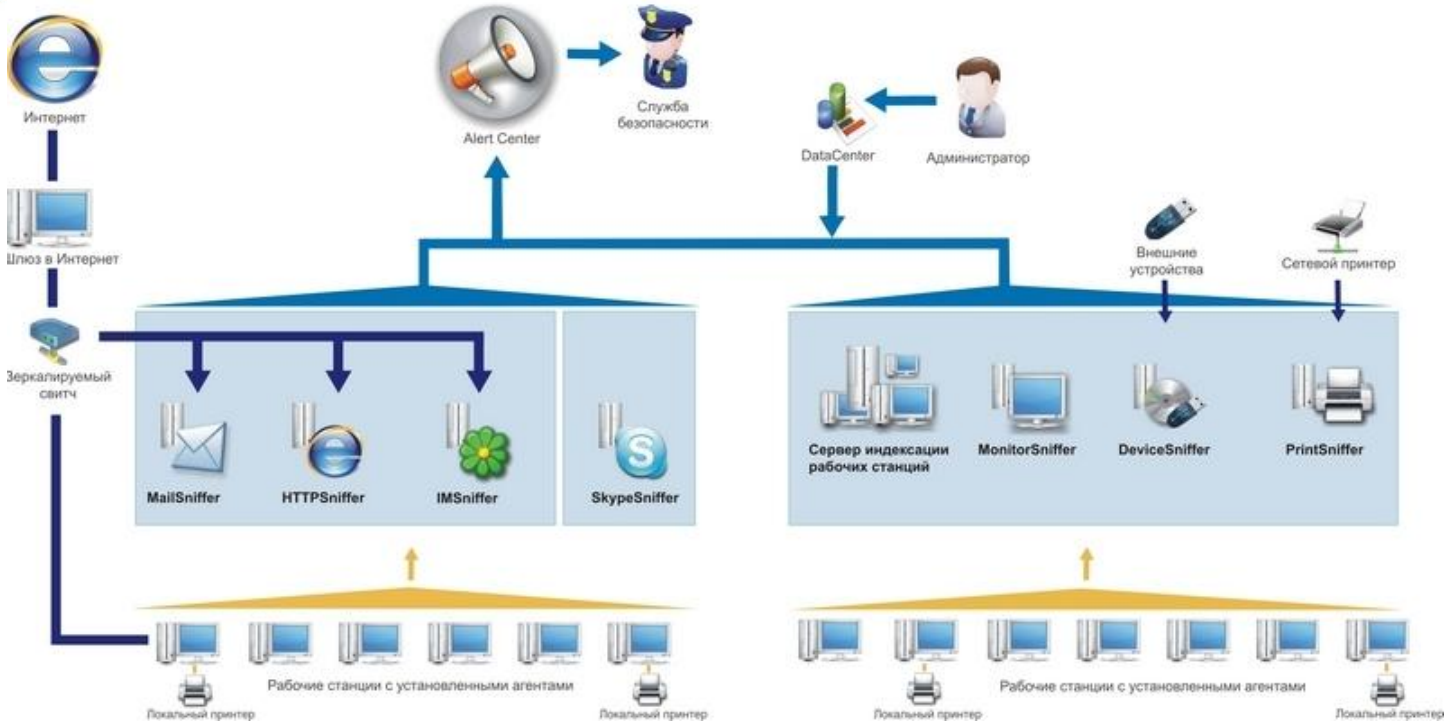
Вся эта информация оформляется в единый поисковый запрос. В результате поиска мы получаем список резюме с минимальным содержанием ненужных вариантов.

С помощью обычного фразового поиска также можно найти нужную информацию, используя в запросе одну поисковую фразу (например, «год рождения»), однако количество ненужных документов, попавших в выдачу будет огромным. Вследствие этого, для поиска нужной информации придется затратить куда больше времени на подбор дополнительных ключевых фраз и изучение нецелевых документов, содержащих эти ключевые фразы.

Поиск по шаблонам

Поиск по регулярным выражениям позволяет найти специфические данные (номера телефонов, номера кредиток, слова и их сокращения и т. д.) тогда, когда полнотекстовый поиск не справляется с этой задачей.

Компоненты контура



Разрабатывая «Контур информационной безопасности SearchInform», мы сфокусировались на предоставлении специалистам, отвечающим за информационную безопасность организации, не только полного охвата всех возможных каналов утечки информации, но и мощных средств анализа перехваченной информации. Давайте ознакомимся подробнее с программами, которые входят в него.

Индексация рабочих станций

SearchInform Server позволяет проиндексировать всю доступную информацию со всех компьютеров в локальной сети предприятия. Администратор может выбрать как любой диск, так и любой компьютер в сети для последующей индексации.

Перехват интернет-трафика

SearchInform NetworkSniffer позволяет осуществлять перехват информации, которую пользователь передаёт через интернет. При этом поддерживаются все распространённые протоколы, которые могут использоваться инсайдерами.

Электронная почта

Один из наиболее опасных каналов утечек, так как поддерживается пересылка больших объёмов данных.

HTTP

Возможны утечки информации в социальные сети, блоги, на форумы, а также через Web-приложения для отправки электронной почты и SMS, Web-чаты.

Skype

«Контур информационной безопасности SearchInform» является первым решений в области информационной безопасности, обеспечившим перехват как голосовых, так и текстовых сообщений, передаваемых через Skype.

Службы мгновенного обмена сообщениями (IM)

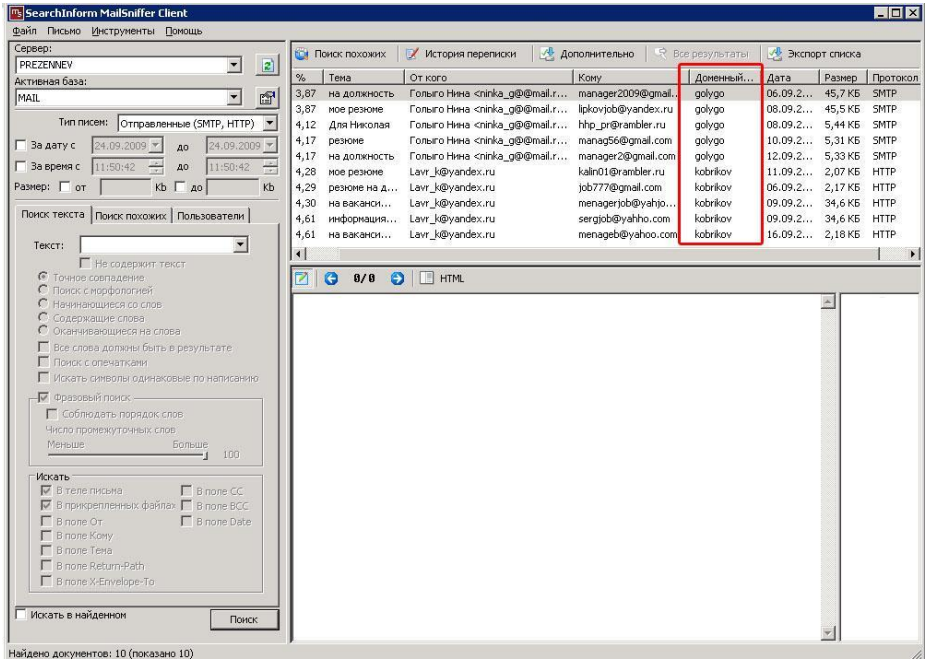
Поддерживаются протоколы ICQ, MSN, Mail.ru Агент, JABBER, активно используемые офисными работниками.

SearchInform

Интеграция с доменной системой Windows

Интеграция с доменной системой Windows даёт возможность достоверно идентифицировать пользователя, отправившего сообщение по электронной почте, Skype, ICQ, MSN, JABBER оставившего его на форуме или в блоге, даже если сотрудник воспользовался для этого почтовым ящиком на бесплатном сервере и подписался чужим именем.

С доменной системой Windows интегрированы все продукты, входящие в состав «Контура информационной безопасности SearchInform», и вы можете так же легко узнать, кто распечатал конфиденциальную информацию или переписал её на внешний носитель.



Перехват информации выводимой на печать и записываемой на внешние носители

PrintSniffer – программа, которая контролирует содержимое документов, отправленных на печать. Все данные перехватываются, содержимое файлов индексируется и хранится в базе заданный промежуток времени.
Отслеживая документы, напечатанные на принтере, можно не только предотвращать попытки хищения информации, но также оценить целесообразность использования принтера каждым сотрудником и избежать перерасхода бумаги и тонера.

DeviceSniffer – программа, с помощью которой можно перехватывать файлы, записываемые пользователем на внешние носители (флэшки, компакт-диски, внешние винчестеры). С помощью этой программы вы можете избежать утечки больших объёмов данных, которые инсайдер переписывает на внешние носители из-за невозможности их передачи по интернету.

Распознавание ухищрений инсайдеров

Зачастую недобросовестные сотрудники, пытаясь обмануть службу безопасности, передают информацию в графическом виде или, например, в зашифрованном архиве.

«Контур информационной безопасности SearchInform» позволяет:

- Обнаруживать передачу зашифрованных архивов по всем каналам утечки информации.
- Определять пересылку файлов с измененным типом.
- Распознавать текст в графических файлах.

Мониторинг всех каналов утечки

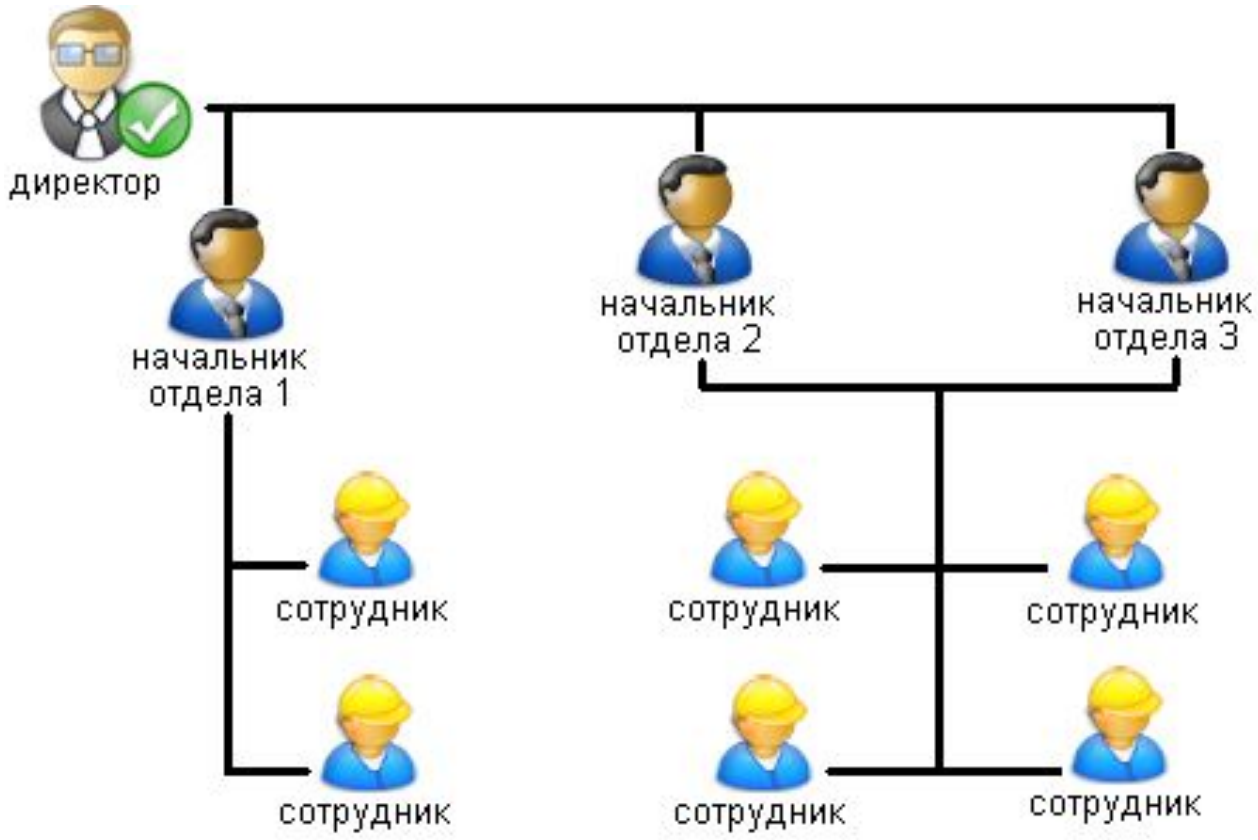
Контроль над всеми каналами, по которым возможна утечка информации, даёт специалистам по информационной безопасности возможность строить срез по активностям пользователей и отслеживать информацию, передаваемую ими по каждому из каналов, в случае возникновения подозрений, что кто-то из них ведёт инсайдерскую деятельность.

Многие сотрудники используют Skype для инсайдерской деятельности так как считают, что невозможно перехватить. «Контуром информационной безопасности» позволяет выявить тех, кто использует на рабочем месте Skype для отправки конфиденциальных данных

Отметим, что в профилактических целях полезно проводить мониторинг активности 1 - 2% персонала организации каждый месяц. В случае выявления каких-либо инцидентов, связанных с нарушением политик информационной безопасности организации, сотрудник должен быть добавлен в список активного мониторинга.

SearchInform

Разграничение прав доступа

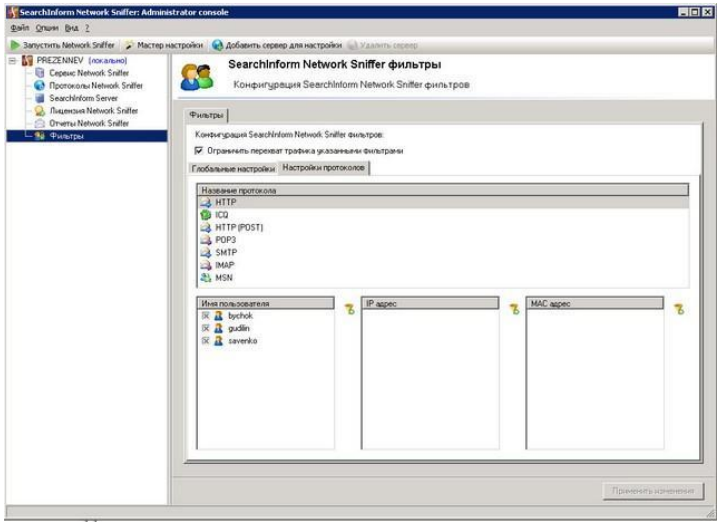


Каждый из компонентов контура информационной безопасности предприятия согласуется с единой системой разграничения прав доступа. Система обладает рядом гибких настроек и позволяет выстроить иерархию доступа к конфиденциальной информации любым образом.

SearchInform

Фильтры

В организации зачастую бывает необходимым исключить из числа контролируемых ряд сотрудников – например, руководство компании. «Контур информационной безопасности SearchInform» поддерживает специальные фильтры, которые позволяют настроить, какую информацию перехватывать для каждого из компьютеров. Вы легко можете настроить фильтры, к примеру, таким образом, что у руководителя компании, его заместителя и бухгалтера будет осуществляться перехват только почты, а мониторинг ICQ и HTTP не будет вестись.



Одинаковый интерфейс для всех серверных консолей в рамках «Контура информационной безопасности SearchInform» позволяет специалистам по информационной безопасности быстро освоиться с использованием всех компонентов, изучив работу только одного из них.

DataCenter

DataCenter – это центр управления всеми индексами, созданными компонентами контура информационной безопасности.

DataCenter позволяет:

- Разбивать индексы на части, увеличивая производительность поиска информации.
- Задавать определенные параметры (размер, количество документов, время) при создании каждого нового индекса.
- Следить за состоянием работы всех компонентов контура информационной безопасности и отсылать уведомление на e-mail о каких либо неисправностях.

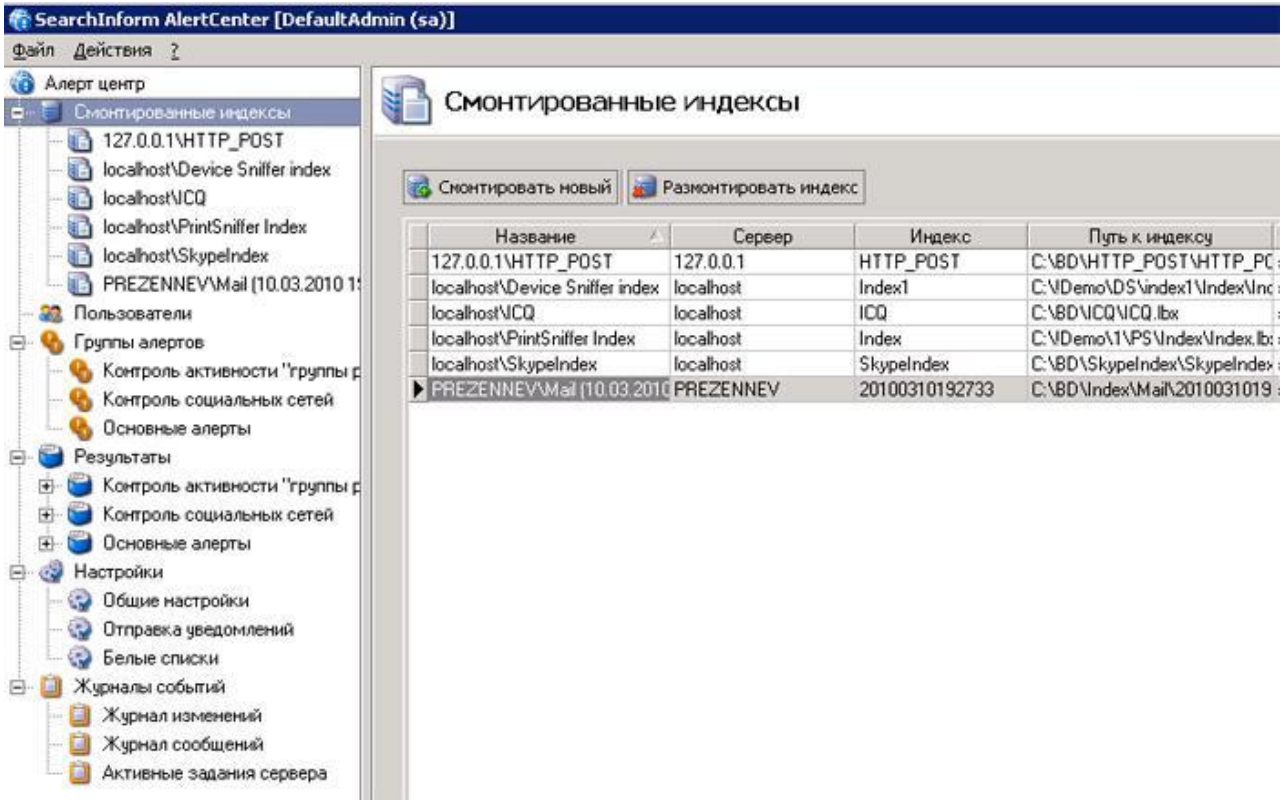
Центр оповещения

AlertCenter является звеном, связывающим между собой все компоненты в единый контур информационной безопасности компании. AlertCenter опрашивает все компоненты и, при наличии определённых ключевых слов, фраз или даже фрагментов текста в перехваченной любой из программ информации, немедленно даёт об этом знать лицу, ответственному за информационную безопасность.

Приложение включает в себя консоль сервера и клиент AlertCenter, что позволяет разграничить доступ к оповещениям и настройкам между ответственными за информационную безопасность сотрудниками.

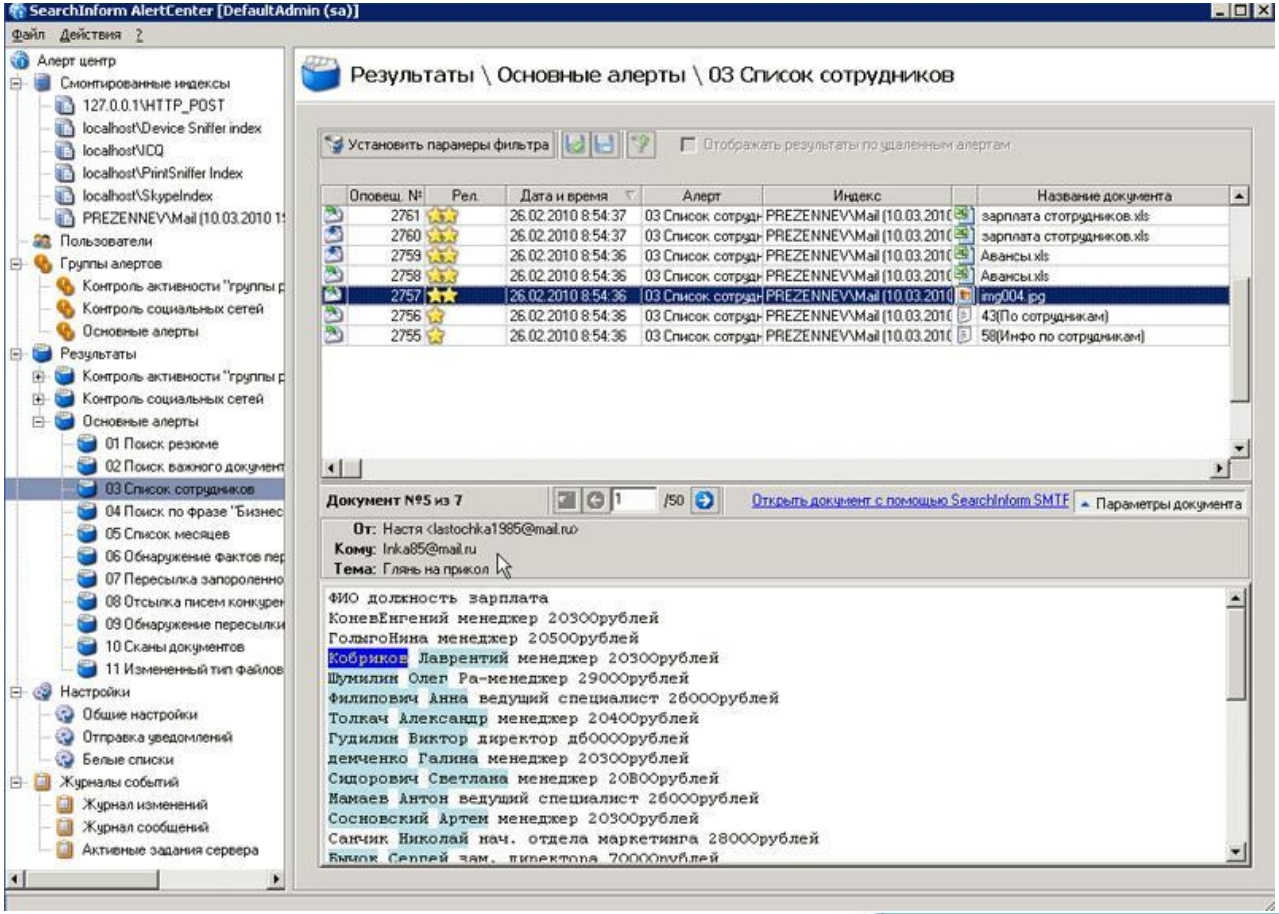
Центр оповещения

AlertCenter является самостоятельным приложением, которое можно подключить к любому индексу, созданному с помощью продуктов «SearchInform», и с заданной периодичностью проверять поисковый индекс на наличие определённых пользователем ключевых слов.



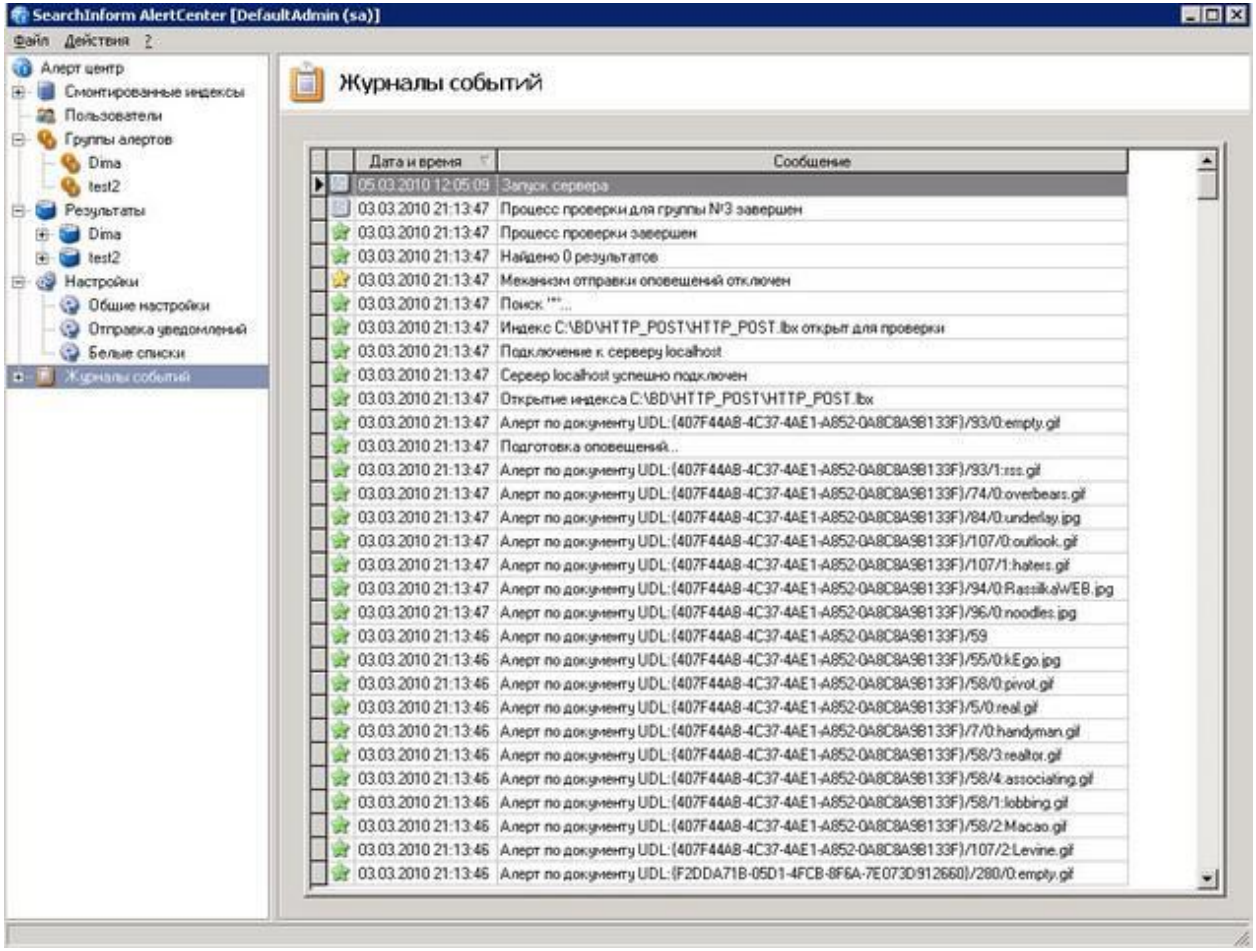
Центр оповещения

Открытие документов, по которым сработали уведомления, в клиентах приложений «Контура информационной безопасности SearchInform» и в сопоставленных приложениях позволит специалистам по безопасности быстро изучать подробности, касающиеся каждого инцидента.



Центр оповещения

Ведение журнала событий и журнала результатов позволяет оценить эффективность борьбы с утечками информации и работу отдела информационной безопасности.



Преимущества Контура информационной безопасности SearchInform

- **Простота внедрения**

Программный комплекс «SearchInform» можно проинсталлировать всего за несколько часов. Клиент может обойтись силами своих IT-специалистов. В этой ситуации отпадает необходимость предоставлять внутренние документы компании сотрудникам компании-разработчика.

- **Сохранение существующей структуры локальной сети**

Внедрение системы не влияет на функционирование существующих информационных систем внутри компании.

- **Комплексность решения**

Позволяет контролировать все каналы утечки информации, а многокомпонентная структура позволяет выбрать только необходимые модули.

- **Единственное решение, которое позволяет контролировать программу Skype**
- **Полная интеграция с доменной структурой Windows**
- **Функция «поиск похожих»**

Позволяет собственными силами быстро и гибко настроить систему оповещения, не привлекая для этого сторонних специалистов. При этом для эффективной защиты конфиденциальных данных необходимы минимальные трудозатраты на анализ информационных потоков.

Преимущества Контура информационной безопасности SearchInform

- **Разграничение прав доступа к информации**

Дает возможность настройки прав доступа к перехваченной информации.

- **Контроль содержимого рабочих станций и общедоступных сетевых ресурсов**

Позволяет отслеживать появление конфиденциальной информации в местах, для этого не предназначенных.

- **Срез по активностям сотрудника для оперативной работы**

Отследив факт утечки информации по одному каналу, есть возможность просмотреть все активности пользователя по всем каналам.

- **Создание архива перехваченной информации**

Позволяет восстановить последовательность событий в прошлом.

- **Прозрачность ценовой политики и стоимости финального**
- **внедрения**
- **Бесплатная техническая поддержка на 1 год и бесплатная пробная версия**

Предоставляется на 30 дней для проведения полномасштабного тестирования программ в реальных условиях.

Сертификаты

«Контур информационной безопасности SearchInform» имеет ряд сертификатов:

- «Газпром»
- ФСТЭК России
- Сертифицирующих органов Республики Беларусь
- Сертифицирующих органов Республики Казахстан

Итоги

Программные продукты «SearchInform» успешно решают поставленные задачи в банках и финансовых компаниях, государственных структурах и в крупных промышленных, сырьевых, телекоммуникационных и IT-компаниях России и стран СНГ.

Законы, регулирующие работу с конфиденциальной информацией

Федеральный закон О персональных данных.

Данный закон, в частности, определяет требования к информационным системам персональных данных и регламентирует необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним.

Федеральный закон о коммерческой тайне.

Этот закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности.

Федеральный закон Об архивном деле.

Этот закон регулирует отношения в сфере организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов независимо от их форм собственности.

Стандарт Банка России.

«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
Данный документ, в частности, регламентирует порядок работы с конфиденциальной информацией внутри банка.

Законы, регулирующие работу с конфиденциальной информацией

Закон HIPAA

(Health Insurance Portability and Accountability Act of 1996) гласит, что: «Все медицинские, страховые и финансовые организации, работающие с чувствительной медицинской информацией должны хранить не менее 6 лет всю свою электронную документацию».

Соглашение Basel II

(«Международная конвергенция измерения капитала и стандартов капитала: новые подходы»). Все банки Европы, а также крупнейшие банки США должны иметь архивы электронной корреспонденции с возможностью проведения аналитических выборок и гарантией аутентичности сохраняемых сообщений.

Закон SOX

(Sarbanes-Oxley Act of 2002), §802 – Все публичные компании, представленные на фондовом рынке США, обязаны собирать, архивировать и хранить на протяжении минимум семи лет электронную корпоративную корреспонденцию.

Правило 17a-4 Комиссии по ценным бумагам США

(SEC Rule 17a-4). Все финансовые публичные компании, представленные на фондовом рынке США, должны хранить переписку с клиентами в виде отдельной базы данных.

SearchInform

Спасибо за внимание