SearchInform

Необходимость контроля каналов утечки конфиденциальной информации для защиты персональных данных

Галина Сытник, Июнь 2012

Работа с персональными данными

Выдержки из ФЗ 152 «О персональных данных»

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке.

1. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, **копирования, распространения персональных данных**, а также от иных неправомерных действий.

2. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только **на таких материальных носителях информации** и с применением такой технологии ее хранения, **которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним**, уничтожения, изменения, блокирования, копирования, распространения.

SearchInform

Работа с персональными данными

Для осуществления защиты персональных данных оператором должны быть приняты следующие меры:

1. **Шифрование баз данных**. Оно позволит защитить информацию от сотрудников, которые по долгу службы имеют доступ к серверам, на которых хранится информация (например, системный администратор).
2. **Шифрование каналов связи**, по которым ведется работа операторов с базами данных. Это позволит избежать перехвата информации в процессе ее передачи.
3. **Разграничение прав доступа** к базам данных, содержащих персональные данные. Каждый сотрудник должен иметь доступ только к тем данным, которые необходимы ему для выполнения служебных обязанностей.

Перечисленные меры позволяют защититься только от случайного или преднамеренного попадания данных к сотрудникам, не имеющим права с этими данными знакомиться.

SearchInform

Работа с персональными данными

Сотрудники, которые работают с персональными данными по долгу службы, будут всегда иметь доступ к ним в незашифрованном виде.

Для полноценной защиты данных от утечек необходимо исключить возможность пересылки ими информации, не регламентированной установленными правилами работы.

Для этого необходимо принятие еще одной обязательной меры для защиты персональных данных от утечек - **организации контроля за всеми информационными потоками**.

Такой контроль должен позволять оперативно обнаруживать все факты передачи персональных данных по всем возможным каналам утечки.

SearchInform

Возможные пути утечки конфиденциальной информации

Электронное письмо с ценной информацией может быть отослано по почтовым протоколам.

Информация может быть отправлена посредством клиентов для мгновенного обмена сообщениями (ICQ, MSN Messenger, QIP, Jabber).

Голосовые или текстовые сообщения, отправленные через Skype, также могут содержать важную корпоративную информацию.

Информация может быть размещена на форумах, блогах, передана по социальным сетям. Передана по FTP-протоколу.

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

Информация может быть распечатана на принтере.

SearchInform

Информационная безопасность должна способствовать бизнесу, а не препятствовать ему. Все каналы передачи информации должны быть открытыми

Зачастую, для предотвращения утечек информации, компании запрещают сотрудникам использовать удобные и популярные каналы ее передачи и общения с внешним миром.

Например, для безопасности обычно разрешено использовать только корпоративную электронную почту, а такие средства как ICQ, Skype запрещены, несмотря на то, что они во многих случаях могли бы существенно увеличить эффективность работы.

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

SearchInform

Информационная безопасность – это контроль всех каналов передачи информации

В мультфильме «Волшебник Изумрудного города» на границе страны стояли ворота, которые охранял большой страшный волк – никто не мог пройти. Вот только вся остальная граница была лишь нарисована.

Так и с информационной безопасностью: если, например, запретить только запись информации на флешки, диски и другие носители, то данные будут благополучно уходить через электронную почту или интернет-пейджеры.

Или, например, бытует мнение, что перехватить информацию, передаваемую в Skype, нельзя. Именно поэтому пользователи намного свободнее общаются в Skype на рабочем месте, чем в других интернет-мессенджерах. В связи с этим непременно следует контролировать текстовые и голосовые сообщения, а также файлы, передаваемые в Skype.

Реализация комплексной политики информационной безопасности невозможна при наличии хотя бы одного неконтролируемого службой безопасности канала потенциальных утечек.

SearchInform

Аналитические инструменты в системе информационной безопасности

Наиболее важным компонентом любой системы информационной безопасности является аналитический модуль. Совместное использование всех типов поиска позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и резко сократить трудозатраты на их анализ.

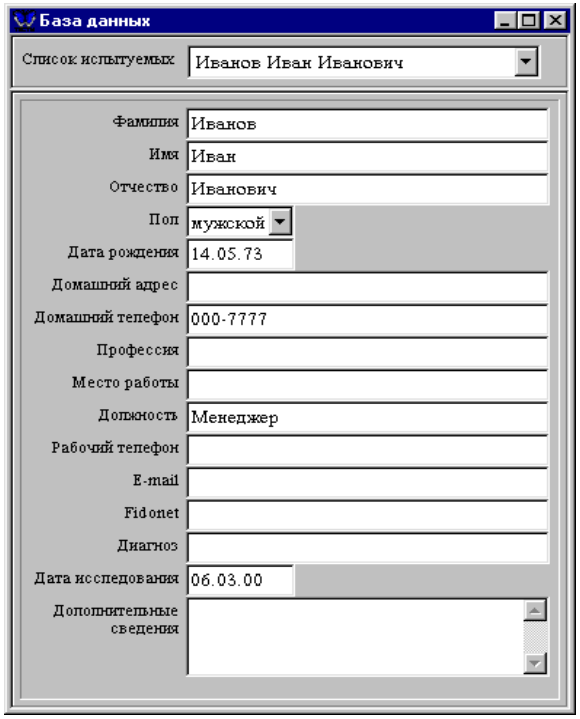
SearchInform

Что такое персональные данные?

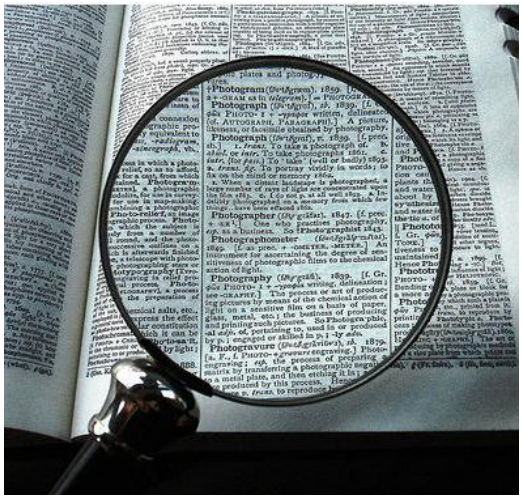
Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Как правило, это жестко структурированные данные, которые хранятся в базах данных.

Примеры:
Фамилия, имя, отчество, год, месяц, дата и место рождения, адрес; семейное, социальное, имущественное положение; образование, профессия, доходы, другая информация.



Поиск по словам, фразам и словарям



Поиск по словам и фразам с учетом морфологии – простейшие виды поиска и могут использоваться лишь как вспомогательные в комплексе с более сложными.

Поиск по словарям позволяет выделить из общего потока документы заданной тематики.

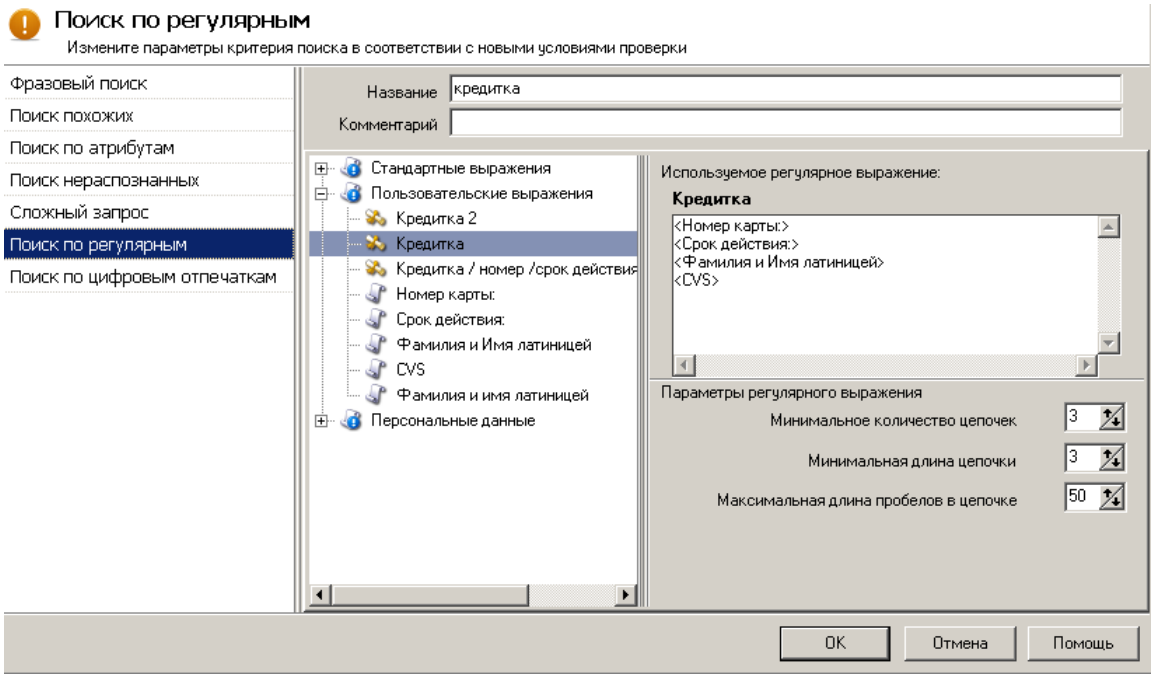
Поиск по регулярным выражениям

Такой поиск позволяет отследить последовательности символов, характерные для различных форм персональных данных: содержащихся в финансовых документах, структурированных записях в базах данных и т.п.

С его помощью система оперативно отреагирует на попытку отправки записи с такими персональными данными, как фамилия человека, дата его рождения, номера кредитных карт, телефоны и т.д.

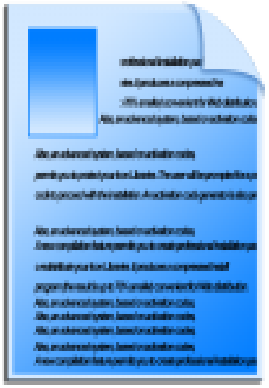
Поиск по регулярным выражениям

- Учитываются несколько атрибутов для описания данных
- Используется валидация данных
- Определяется, сколько атрибутов одновременно должны сработать
- Определяется, какое количество записей является критичным

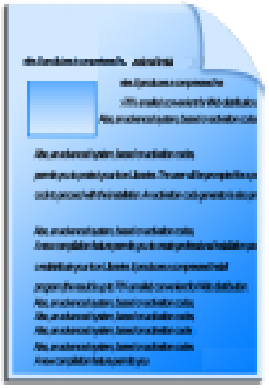


Поиск документов, похожих по содержанию

Поиск похожих позволяет задать конфиденциальные документы целиком в поисковый запрос. Контур информационной безопасности обнаружит эти документы даже в том случае, если они были серьезно отредактированы инсайдером перед пересылкой, записью на флэшку или распечаткой.



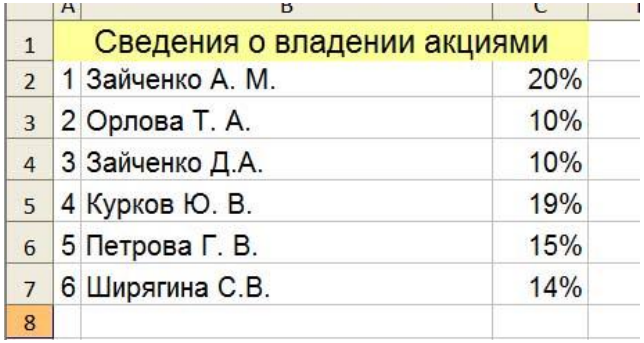
СХОДСТВО
95 %



Поиск документов, похожих по содержанию, на практике

Поиск похожих может дать неожиданные результаты. Например, по списку месяцев или списку сотрудников/клиентов/партнеров можно обнаружить отчеты о финансовой деятельности, зарплатные ведомости, информацию о сделках с клиентами и пр.

	A	B	C
1	Зарплата за декабрь		
2	1	Иванов	30000
3	2	Петров	40000
4	3	Сидоров	50000
5	4	Крюков	16000
6	5	Малинин	30000
7	6	Филипов	40000
8	7	Медведев	50000
9	8	Хайкин	16000
10	9	Петров	30000
11	10	Сидоров	40000
12	11	Крюков	50000
13	12	Малинин	16000
14	13	Филипов	
15	14	Медведев	



1	Сведения о владении акциями		
2	1	Зайченко А. М.	20%
3	2	Орлова Т. А.	10%
4	3	Зайченко Д.А.	10%
5	4	Курков Ю. В.	19%
6	5	Петрова Г. В.	15%
7	6	Ширягина С.В.	14%
8			

Синонимы

Отдельно стоит задача поиска разговоров в ICQ или Skype на определенную тематику, например, о получении «откатов».

Для решения этой задачи недостаточно просто подобрать ключевые слова, необходимо также учитывать все возможные их варианты (синонимы). Причем синонимы не в обычном их понимании, а именно пользовательские синонимы, например:

*- **Вопрос**, проблема, задача, дело, трудность, заморочка…*
*- Деньги, оплата, капуста, **президенты**, благодарность, посул…*
*- Услуга, помощь, отдолжение, поддержка, **содействие…***

При поиске по словам «проблема» и «помощь» мы обнаружили фразы из диалога:

*- Да, но человек, который будет **вопрос** решать количеством **президентов** не доволен.*
*- Да, он ни разу в таких **вопросах** мне **содействия** не оказывал. Вполне возможно не в теме.*

SearchInform

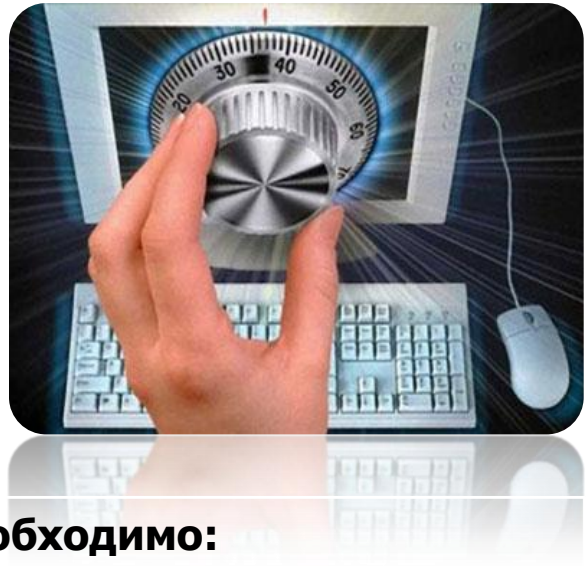
Доменные имена

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

SearchInform

Распознавание ухищрений инсайдеров

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



Для полноценного контроля необходимо:

- распознавать текст в графических файлах и осуществлять поиск по нему
- обнаруживать передачу зашифрованных архивов по всем каналам возможной утечки информации
- выявлять пересылку файлов с измененным типом

SearchInform

Создание и отслеживание группы риска

Сотрудников, по той или иной причине попавших под подозрение, нужно пристально контролировать. Для этого необходимо анализировать всю информацию, которая уходит во внешний мир под их учетной записью.

В группу риска имеет смысл включать:

1. Сотрудников, которые замечены в нарушении политик информационной безопасности
2. Сотрудников, использующих различные трюки (переименованные файлы, запароленные архивы и т.д.)
3. Недовольных сотрудников (негативные отзывы о руководстве, о компании и т.д.)
4. Сотрудников, которые по каким-то причинам начали менее эффективно работать
5. Сотрудников, имеющих отношение к движениям финансов и товаров, а также часть менеджеров среднего звена (руководители департаментов)

SearchInform

Проведение служебных расследований

В случае утечки конфиденциальной информации с помощью систем информационной безопасности можно проводить служебные расследования. Для этого необходимо:

- наличие архива перехваченной информации;
- возможность получить срез по активностям сотрудника по всем каналам передачи информации;
- контроль содержимого рабочих станций и общедоступных сетевых ресурсов;

В профилактических целях полезно проводить ретроспективный мониторинг активности 1-2% персонала организации за прошедший месяц. В случае выявления каких-либо инцидентов, связанных с нарушением политик информационной безопасности организации, сотрудник должен быть добавлен в список активного мониторинга (т.е. в группу риска).

SearchInform

Контур информационной безопасности

«Контур информационной безопасности SearchInform» позволяет решать все вышеперечисленные задачи на практике. С его помощью можно выявить утечки конфиденциальной информации и персональных данных через электронную почту, ICQ и другие интернет-мессенджеры, Skype, социальные сети, форумы и блоги, внешние устройства (USB/CD/ DVD), документы, отправляемые на печать.

SearchInform

Элементы Контура информационной безопасности

Перехват интернет-трафика

SearchInform NetworkSniffer позволяет осуществлять перехват информации, передаваемую через интернет. Поддерживаются все распространенные протоколы, которые могут использоваться инсайдерами. Предлагается поддержка прокси-серверов - как программных (Kerio, Squid и т.д.), так и аппаратных (BlueCoat, IronPort и т.д.) - через стандартный протокол ICAP.

Электронная почта

Один из наиболее опасных каналов утечек, так как поддерживается пересылка больших объемов данных. Поддерживаются протоколы SMTP, POP3, MAPI, IMAP.

HTTP

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

FTP

Этот протокол - важнейшее средство передачи больших объемов данных, и может использоваться недобросовестными сотрудниками для передачи целых баз данных, детализированных чертежей, пакетов отсканированных документов и пр.

SearchInform

Элементы Контура информационной безопасности

Skype

«Контур информационной безопасности SearchInform» является первым решений в области информационной безопасности, обеспечившим перехват не только голосовых и текстовых сообщений, но и файлов, передаваемых через Skype.

Службы мгновенного обмена сообщениями (IM)

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

PrintSniffer

Это 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.

SearchInform

Элементы Контура информационной безопасности

DeviceSniffer – программа, выполняющая аудит внешних носителей, подключенных к компьютеру (флэшки, компакт-диски, внешние винчестеры), а также перехват записываемых на них файлов благодаря функции «теневого копирования». С помощью этой программы вы можете избежать утечки больших объемов данных, которые инсайдер переписывает на внешние носители из-за невозможности их передачи по интернету.

MonitorSniffer предназначен для перехвата информации, отображаемой на мониторах пользователей и сохранения полученных снимков экрана в базе данных. Поддерживается контроль экрана одного или нескольких пользователей в режиме реального времени, можно отслеживать состояние экранов пользователей терминальных серверов, работающих по RDP-соединению (протоколу удаленного рабочего стола).

SearchInform

Элементы Контура информационной безопасности

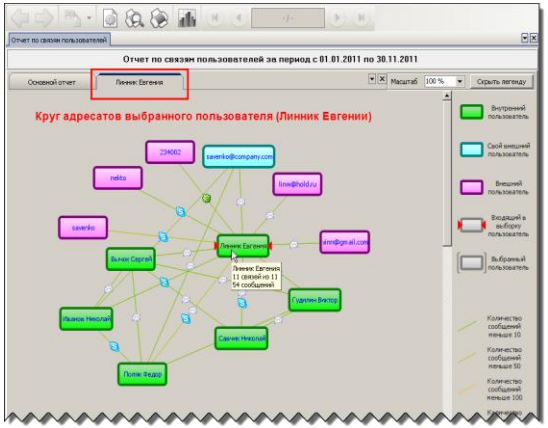
FileSniffer контролирует работу пользователей на общих сетевых ресурсах, которые содержат большие объемы конфиденциальных данных, не предназначенных для распространения за пределами компании. Копируя документы с этих ресурсов, сотрудники могут торговать корпоративными секретами. SearchInform FileSniffer позволяет контролировать все операции с файлами на общедоступных сетевых ресурсах, защищая информацию, находящуюся на них.

Индексация рабочих станций позволяет реального времени отслеживать появление, копирование, перемещение и удаление конфиденциальной информации на рабочих станциях пользователей. Подобный аудит пользовательских компьютеров во всей локальной сети предприятия позволит вовремя обнаружить сотрудника, собирающегося передать закрытые корпоративные документы третьим лицам.

SearchInform

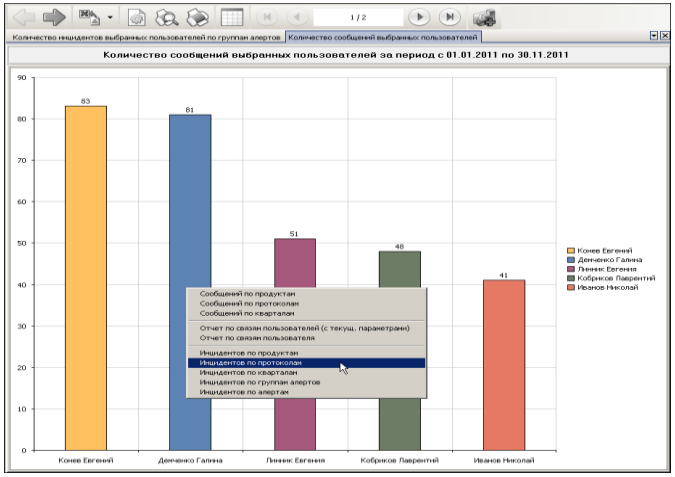
Элементы Контура информационной безопасности

SearchInform ReportCenter - инструмент, позволяющий узнать, с кем общаются сотрудники в течение заданного периода времени по каждому из каналов обмена информацией как внутри компании, так и за ее пределами.



Построение графа позволяет визуализировать как связи всех сотрудников в целом, так и круг общения конкретного пользователя. Так можно выявить тех, кто наиболее интенсивно переписывается с нежелательными адресатами, нерационально расходуя рабочее время.

В приложении также предусмотрена дифференциация связей по цвету в зависимости от количества переданных сотрудниками сообщений, что упрощает визуальную идентификацию «аномально» общительных пользователей. Кроме того, на каждой связи размещается пиктограмма канала, по которому осуществлялось общение.



SearchInform

Элементы «Контура информационной безопасности»

Контроль ноутбуков

Лэптоп - это не только удобный рабочий инструмент, который все больше сотрудников использует в офисе, в командировках и дома, но и серьезная угроза для ИБ организаций.

Находясь за пределами контролируемой работодателем сети, сотрудник может передать конфиденциальные данные с ноутбука третьим лицам. SearchInform **EndpointSniffer** позволяет это контролировать. Он собирает отправленные данные, которые будут переданы для анализа отделу ИБ сразу же, как только лэптоп снова окажется в корпоративной сети. Поддерживается работа с данными, отправленными через электронную почту (IMAP/MAPI, а через SMTP/POP3 - с шифрованием), web-формы (HTTP/HTTPS), системы мгновенного обмена сообщениями (ICQ, Jabber, MSN Messenger), FTP, Skype, переданными на печать. Кроме того, возможно контролировать активность сотрудника в режиме реального времени с помощью периодического снятия скриншотов рабочего стола.

Агент EndpointSniffer тщательно скрывает свое присутствие на лэптопе, и обнаружить его непросто даже квалифицированному специалисту.

SearchInform

Архитектура системы

Все компоненты системы имеют клиент-серверную структуру. Серверная – это одна из платформ для перехвата данных – **SearchInform NetworkSniffer** либо **SearchInform Endpoint-Sniffer** и клиентские приложения, предназначенные для работы с базой перехваченных данных и проведения служебных расследований. Использование единого поискового аналитического движка позволяет в полной мере использовать все перечисленные поисковые возможности.

SearchInform NetworkSniffer - платформа для перехвата данных на уровне зеркалируемого трафика, т.е. NetworkSniffer обрабатывает трафик, не влияя на работу корпоративной сети. Перехватываются данные, пересылаемые пользователями по популярным сетевым протоколам и каналам (SMTP, POP3, IMAP, HTTP, HTTPs, MAPI, ICQ, JABBER, MSN) на уровне локальной сети, в том числе по FTP и SIP. Платформа включает в себя следующие продукты:


MailSniffer


IMSniffer


HTTPSniffer

FTPSniffer

SearchInform

Архитектура системы

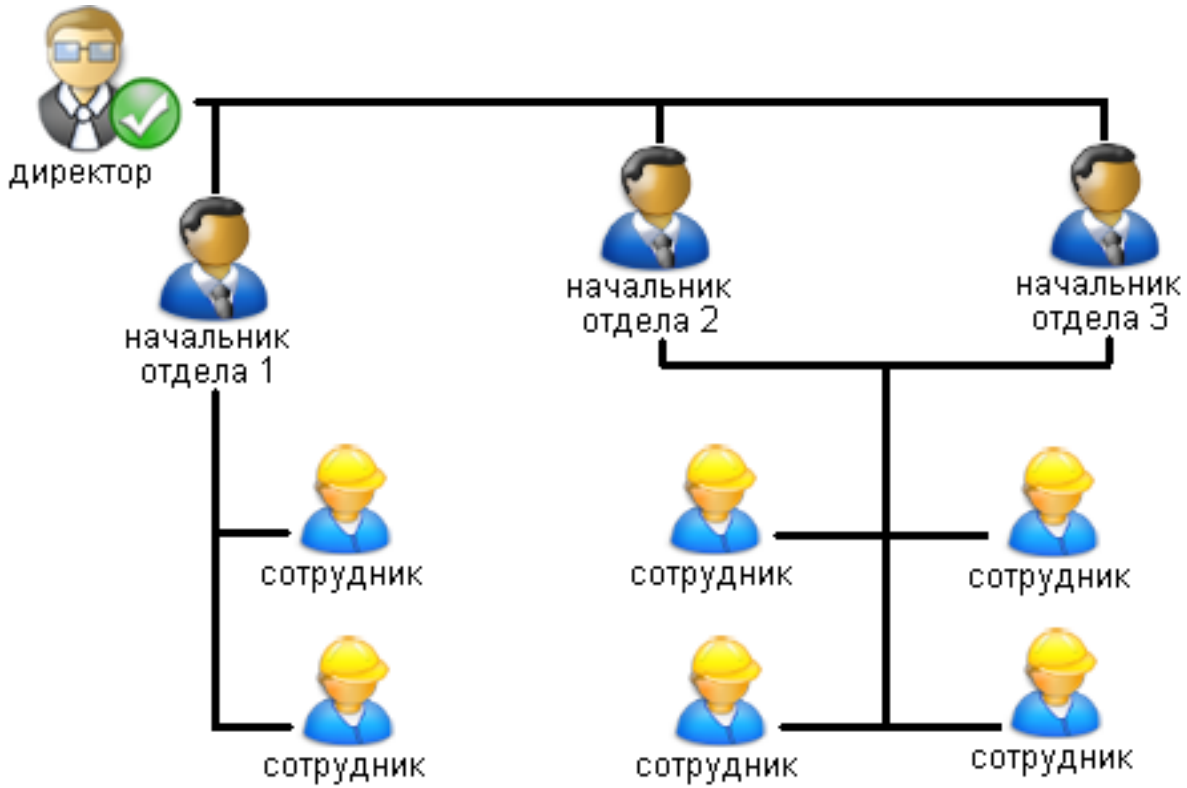
SearchInform EndpointSniffer - платформа для перехвата трафика посредством агентов.

Дополнительно позволяет контролировать сотрудников, находящихся за пределами корпоративной сети - они могут свободно передать конфиденциальные данные с ноутбука третьим лицам. SearchInform EndpointSniffer собирает отправленные данные и передает их для анализа отделу ИБ, как только лэптоп окажется в корпоративной сети. Преимущества работы агентов IMSniffer и MailSniffer на платформе SearchInform EndpointSniffer в том, что они обладают повышенной устойчивостью к различным сбоям (даже если сервера станут недоступными, перехват будет осуществляться), способны перехватывать и те данные, которые передаются по защищенным протоколам.

SearchInform EndpointSniffer-агенты:

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 выстраивать различную иерархию доступа к конфиденциальной информации.

Примеры утечек информации и способы их предотвращения

Электронная почта

Планы строительной компании о покупках земли под элитную застройку начали уходить на сторону. Владельцы участков, перед оговоренной продажей застройщику, уступали их риэлторам, которые выставляли за участки совсем другие суммы.

Внедрение в компании SearchInform MailSniffer, помогло установить личность инсайдера, который пересылал сообщникам документы по электронной почте.

Примеры утечек информации и способы их предотвращения

Skype

Мониторинг чатов Skype работников компании, находящихся в «группе риска», позволил заранее узнать о том, что несколько сотрудников из одного отдела задумали одновременный переход в конкурирующую компанию. С учетом этого им был перекрыт доступ ко всей информации, которую они могли унести с собой, после чего компания-конкурент от них отказалась.

Свои планы сотрудники свободно обсуждали в Skype, так как были уверены, что их общение посредством этой программы перехватить нельзя. Однако это было сделано благодаря SearchInform SkypeSniffer.

Примеры утечек информации и способы их предотвращения

Принтер

На предприятии, производящем большой объем бакалейной продукции, в ходе аудиторской проверки выяснилось, что товаров на складах у реализаторов значительно больше, чем было отгружено.

SearchInform PrintSniffer позволил установить, что группа злоумышленников организовала на предприятии выпуск неучтенной продукции. Ее реализация через торговую сеть стала возможной за счет распечатки дубликатов накладных, в которых указывались нужные злоумышленникам цифры.

Примеры утечек информации и способы их предотвращения

ICQ и мониторинг рабочих станций

Посредством мониторинга ICQ были найдены стихотворения о руководстве компании не самого лестного содержания, наносящие серьезный ущерб деловому имиджу компании. Некоторые из них были опубликованы в Интернете.

Найти виновных помог анализ ICQ переписки, при помощи SearchInform IMSniffer. Было найдено самое первое сообщение со стихотворением, после чего были проверены рабочие станции виновных сотрудников, на которых и были найдены файлы со стихотворениями.

Примеры утечек информации и способы их предотвращения

Комплексный анализ всех каналов

У дистрибьюторской компании, работающей с большим количеством крупных торговых сетей, возникли серьезные сбои в логистике. Предварительное разбирательство показало, что причиной этого стали грубые ошибки одного из менеджеров.

Служба безопасности, используя базу, созданную «Контуром информационной безопасности», доказала, что менеджер действительно допустил ошибки, но лишь потому, что сам был злонамеренно введен в заблуждение работниками смежных подразделений.

SearchInform

Преимущества Контура информационной безопасности SearchInform

1. **Простота и скорость внедрения.** Процесс инсталяции занимает всего несколько часов и не влияет на функционирование существующих информационных систем внутри компании.

2. **Возможность контроля всех каналов передачи информации,** включая Skype, социальные сети, принтеры, а также работу пользователей на файл-серверах.

3. **Функция «поиск похожих».** Позволяет собственными силами быстро и гибко настроить систему оповещения, не привлекая сторонних специалистов. При этом для эффективной защиты конфиденциальных данных необходимы минимальные трудозатраты на анализ информационных потоков.

4. **Полная интеграция с доменной структурой Windows** позволяет достоверно идентифицировать пользователя.

5. **Расширенные поисковые возможности позволяют эффективно защищать конфиденциальные данные при минимальных трудозатратах на анализ информационных потоков** (достаточно 1 «безопасника» для контроля 1000 – 1500 рабочих станций в организации).

SearchInform

Компания **SearchInform** - лидер рынка СНГ в области решений по информационной безопасности

«Контур информационной безопасности SearchInform» используется в более чем 600 организациях России, Украины, Беларуси, Казахстана и Латвии. Только в 2011 году клиентами SearchInform стали более 200 компаний из разных отраслей – от банковского дела до машиностроения. Среди наших крупнейших клиентов – ВТБ 24, Газпромнефть, Лукойл-Информ, МТТ, Промсвязьбанк, Главгосэкспертиза России и многие другие.

SearchInform

Более подробную информацию
о компании SearchInform
и “Контуре информационной
безопасности”
Вы можете получить на нашем сайте:
www.searchinform.ru,
или позвонив нам по телефону:
(+7 495) 721-84-06