

Контроль каналов утечки конфиденциальных данных и наиболее типичные проблемы обеспечения информационной безопасности предприятий

1. КАНАЛЫ УТЕЧКИ ДАННЫХ	2
2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДОЛЖНА СПОСОБСТВОВАТЬ БИЗНЕСУ, А НЕ ПРЕПЯТСТВОВАТЬ ЕМУ. ВСЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ ДОЛЖНЫ БЫТЬ ОТКРЫТЫ	2
3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ЭТО КОНТРОЛЬ ВСЕХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ	3
4. ДЛЯ ЧЕГО НУЖЕН ПОИСК, И КАКИМ ОН ДОЛЖЕН БЫТЬ	3
4.1. Поиск по словам с учетом морфологии	3
4.2. Поиск по фразам с учетом порядка слов и расстояния между ними	3
4.3. Поиск по регулярным выражениям.	3
4.4. Поиск по цифровым отпечаткам.	4
4.5. Поиск документов похожих по содержанию.	4
4.6. Поиск с использованием синонимов.	4
5. КОГО НАДО БОЯТЬСЯ	5
6. ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ	5
7. РАСПОЗНАВАНИЕ УХИЩРЕНИЙ ИНСАЙДЕРОВ.	6
8. ОТСЛЕЖИВАНИЕ НАСТРОЕНИЙ В КОЛЛЕКТИВЕ	6
9. СОЗДАНИЕ И ОТСЛЕЖИВАНИЕ ГРУППЫ РИСКА.	6
10. ПРОВЕДЕНИЕ СЛУЖЕБНЫХ РАССЛЕДОВАНИЙ.	7
11. КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОНКРЕТНЫХ ПРИМЕРАХ	7
11.1. Утечка информации по электронной почте (строительная компания)	7
11.2. Утечка информации по SKYPE (финансовый сектор).....	7
11.3. РАСПЕЧАТКА ЦЕННОЙ ИНФОРМАЦИИ НА ПРИНТЕРЕ (ПРОИЗВОДСТВО И ТОРГОВЛЯ).....	8
11.4. Передача ценной информации по ICQ и обнаружение ее на рабочих станциях (ТЕЛЕКОММУНИКАЦИИ)	8
11.5. Передача файла с конфиденциальной информацией по SKYPE (банковский сектор)	8
11.6. Комплексный анализ всех каналов (дистрибуция и логистика)	8
12. ИТОГ	8



1. Каналы утечки данных

Была раньше в ходу такая поговорка: болтун – находка для шпиона. Стоит какой-либо информации, не предназначенной для широкого распространения, уйти на сторону, и любого руководителя могут ждать большие проблемы. Как их избежать

Пути утечки конфиденциальных данных из организации могут быть самыми разнообразными:

- Письмо с ценной информацией может быть отослано по электронной почте.
- 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.
- Ценные данные могут быть переписаны на съёмный носитель (USB-флешку или CD/DVD диски).
- Информация может быть распечатана на принтере.

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

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

Удобство использования того же скайпа например для проведения конференций, общения с клиентами и быстрого решения мелких вопросов неоспоримо. Также и сменные носители давно стали привычным средством обмена информации. Например, многие налоговые службы давно принимают документы от бухгалтеров на флэшках.

Перегнуть палку очень легко: можно запретить и заблокировать все, но следуя этой логике можно и вообще отказаться от использования компьютеров и вернуться к бумажной почте.

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

3. 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. Однако сама 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.

4. Для чего нужен поиск, и каким он должен быть

Комплексная система безопасности позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и резко сократить трудозатраты на их анализ. Это очень актуально в свете повсеместной информатизации бизнеса и быстрого накопления колоссальных объемов электронных документов. Критичной становится функция поиска в больших объемах данных, которые, как свидетельствует практика, зачастую на 90% состоят из «информационного мусора».

Наиболее важным компонентом любой системы информационной безопасности является аналитический модуль. Именно он позволяет сотрудникам службы информационной безопасности оперативно и точно принимать решения о степени конфиденциальности перехваченных данных. Поисковые механизмы позволяют эффективно работать со всеми видами конфиденциальной информации, содержащейся в перехваченных данных.

В системах информационной безопасности применяются следующие виды поиска:

4.1. Поиск по словам с учетом морфологии

Это простейший вид поиска, позволяющий находить документы, содержащие заданные слова и различные их формы.

4.2. Поиск по фразам с учетом порядка слов и расстояния между ними

Позволяет анализировать документ не по отдельным словам, а по словосочетаниям (например, фамилии и имени) или устойчивым определениям.

Оба названных вида поиска – наиболее простые, и могут использоваться лишь как вспомогательные в комплексе с более сложными:

4.3. Поиск по регулярным выражениям.

Он 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.

Напомним, что обеспечение конфиденциальности персональных данных, которыми располагает компания – обязанность, закрепленная Федеральным законом №152 «О персональных данных».

4.4. Поиск по цифровым отпечаткам.

Этот вид поиска предполагает определение группы конфиденциальных документов и снятие с них цифровых отпечатков, по которым в дальнейшем и будет осуществляться поиск. С помощью данного метода можно быстро выявлять в информационных потоках документы, содержащие большие фрагменты текста из документов, относящихся к конфиденциальным.

Основным достоинством метода является высокая скорость работы, а к недостаткам можно отнести его неэффективность при внесении в документ значимых изменений и необходимость оперативного создания цифровых отпечатков всех новых документов для возможности их поиска.

4.5. Поиск документов похожих по содержанию.

Интеллектуальные возможности этого типа поиска позволяют отслеживать отсылку конфиденциальных документов даже в том случае, если они были предварительно отредактированы. В качестве поискового запроса используются как фрагменты документов, так и документы целиком, а результатом поиска являются документы, не только содержащие весь поисковый запрос, но и похожие на него по смыслу.

Поиск документов, похожих по содержанию, позволяет существенно экономить время сотрудника по безопасности. Так, одной из задач службы информационной безопасности является контроль поиска сотрудниками компании другого места работы. Для этого порой вполне достаточно установить факты рассылки резюме.

В единый поисковый запрос включается список слов и фраз, характерных именно для резюме: год рождения; адрес проживания; телефон; электронная почта; образование; должность; опыт работы; заработная плата; резюме; владение иностранным языком; и пр.

В результате поиска обнаружен ряд отправленных сотрудниками резюме. Если бы поиск осуществлялся по каждому слову из списка, то понадобилось бы просмотреть сотни результатов, в которых содержится искомое слово, но которые не являются резюме. Таким образом, сотрудник по информационной безопасности затрачивает на поиск резюме меньше времени, его работа более эффективна.

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.

4.6. Поиск с использованием синонимов.

Он дает возможность оперативно находить среди диалогов, например, ведущихся через интернет-мессенджеры, именно те, которые соответствуют определенным тематикам, скажем, 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.
- Так вроде все как всегда.
- Он ни разу в таких **вопросах** мне **содействия** не оказывал. Вполне возможно не в теме.

Именно совместное использование всех типов поиска позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и резко сократить трудозатраты на их анализ.

5. Кого надо бояться

Общепризнанный факт: в наши дни одной из главных угроз информационной безопасности любой компании стали инсайдеры – остальные угрозы (хакеры, вирусы и т.п.) более-менее успешно нейтрализуются специализированным софтом и сотрудниками IT-отделов. Именно на совести инсайдеров большинство громких утечек конфиденциальной информации, зафиксированных по всему миру в последние годы.

Чаще всего к инсайдерам относят:

- сотрудников, сознательно работающих на конкурентов;
- сотрудников, прямо или косвенно связанных с криминальными структурами;
- просто недобросовестных сотрудников, ставящих свои интересы заведомо выше интересов фирмы;
- сотрудников, обиженных на начальство и по этой причине скрытно вредящих, не получая от этого какой-либо выгоды.

Как показывает практика работы отделов по информационной безопасности, более 80% утечек данных, повлекших негативные последствия – результат действия инсайдеров. При этом, конечно, далеко не всегда сотрудники выдают корпоративные секреты сознательно, выступая в роли инсайдеров. Работники могут совершенно случайно разгласить сведения (логины, пароли), с помощью которых можно получить доступ к серверу фирмы и конфиденциальным данным.

6. Идентификация пользователей

Доменные имена. Интеграция с доменной системой Windows даёт 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 вымышленным именем (ник-неймом) или вошел в сеть с чужого компьютера. Доменное имя – часто единственная зацепка, по которой сотрудник по безопасности может вычислить того, кто виновен в утечке ценной информации из компании.

К примеру, если сотрудник переслал файл с конфиденциальной информацией через бесплатный почтовый ящик rupsik82@mail.ru, то доменное имя, под которым сотрудник вошел в корпоративную компьютерную сеть компании и которое известно службе безопасности – это единственный способ выяснить, кто действительно скрывается за логином rupsik82.

7. Распознавание ухищрений инсайдеров.

Частую 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;
- обнаруживать передачу зашифрованных архивов по всем каналам утечки информации;
- определять пересылку файлов с измененным типом.

8. Отслеживание настроений в коллективе.

Чтобы препятствовать созданию негативного имиджа организации и предугадать возможные утечки ценной для компании информации, важно знать настроения в коллективе. Мнения сотрудников о компании и руководстве часто отражаются в их общении в ICQ и Skype, на форумах, блогах, в социальных сетях.

Важно обращать внимание и на «всплески» активности сотрудников. Если, к примеру, ключевой сотрудник за что-то обиделся на руководство, он может довольно долго «злопыхать» об этом в ICQ – система информационной безопасности сигнализирует о том, что количество сообщений, отправленных сотрудником в этот день, резко возросло. На настроения сотрудника стоит обратить внимание, ведь затаенная обида может иметь более серьезные последствия – например, передачу ценных документов компании конкурентам в отместку начальству.

С помощью системы информационной безопасности также можно отследить связи сотрудников между собой и с лицами вне организации: кто с кем регулярно общается, кто с кем дружит. Отслеживание цепочек этих связей впоследствии может помочь при проведении служебных расследований: кто кому передал ценную информацию внутри организации, и с чьей помощью информация покинула стены компании, т.е. отследить весь путь передачи информации от сотрудника к сотруднику и лицам извне.

9. Создание и отслеживание группы риска.

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

В группу риска имеет смысл включать:

- Сотрудников с которыми связаны инциденты по нарушению политик информационной безопасности
- Сотрудников использующих различные трюки (пересылающих защищенные паролем архивы, переименованные файлы, большое количество отсканированных документов)
- Недовольных сотрудников (негативные отзывы о руководстве, о компании и т..д.)
- Сотрудников которые по каким то причинам начали намного менее эффективно работать.
- Сотрудников имеющих отношение к движениям финансов и товаров, а также часть менеджеров среднего звена (руководители департаментов)

10. Проведение служебных расследований.

В случае возникновения инцидента с утечкой конфиденциальной информации с помощью систем информационной безопасности можно проводить служебные расследования. Например, специалистом по безопасности была обнаружена пересылка сотрудником запароленного архива по электронной почте. В этой ситуации, с одной стороны, стоит поискать, не передал ли сотрудник пароль к архиву по другому каналу, например, в разговоре по ICQ или Skype. С другой стороны, стоит проанализировать активность сотрудника (его контакты, общение, пересылаемые документы), скажем, за последний месяц.

Проведение подобного расследования возможно, если система информационной безопасности обладает:

- архивом перехваченной информации;
- возможностью получить срез по активностям сотрудника по всем каналам передачи информации;
- способностью контролировать содержимое 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, иначе говоря, в группу риска.

11. Контур информационной безопасности на конкретных примерах

«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, голосовые и текстовые сообщения Skype, социальные сети, форумы и блоги, внешние устройства (USB/CD/DVD), документы, отправляемые на печать, а также появление конфиденциальной информации на компьютерах пользователей.

Давайте рассмотрим работу «Контура информационной безопасности» на конкретных примерах.

11.1. Утечка информации по электронной почте (строительная компания)

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.

11.2. Утечка информации по Skype (финансовый сектор)

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 перехват был осуществлен благодаря SearchInform SkypeSniffer.

11.3. Распечатка ценной информации на принтере (производство и торговля)

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.

11.4. Передача ценной информации по ICQ и обнаружение ее на рабочих станциях (телекоммуникации)

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.

11.5. Передача файла с конфиденциальной информацией по Skype (банковский сектор)

Финансовое учреждение подготовило к запуску новый проект, связанный с розничным кредитованием. Однако руководительница одного из отделов учреждения, в переписке по Skype, выдала все подробности запуска проекта подруге, которая являлась сотрудницей фирмы-конкурента. В частности, она передала по Skype файл, содержащий персональные данные – ФИО клиентов и номера кредитных договоров. Их пересылку с помощью поиска по регулярным выражениям и обнаружил «Контур информационной безопасности».

11.6. Комплексный анализ всех каналов (дистрибуция и логистика)

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.

12.Итог

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

На наш взгляд, в плане всех описанных функциональных возможностей, наилучшим выбором для российских корпоративных пользователей станет разработанный компанией SearchInform «Контур информационной безопасности». В нем реализованы все необходимые функции информационного контроля. Данная система идеально подходит для крупных и стратегически важных предприятий, она отвечает всем современным требованиям и способна адекватно отвечать на любые угрозы информбезопасности.