

# 1. Безопасность – это не шутки

## 1.1. Какой должна быть правильная система информационной безопасности организации?

В любой сфере бизнеса не обойтись без секретов. Чего бы ни касалась секретная информация – технологий производства, доходов компании, списка её крупнейших клиентов, - в наше время электронных документов следить за её сохранностью нужно особенно тщательно.

### Почему это важно?

Информация – самый важный из ресурсов современного общества, вокруг которого крутятся деньги. Кто владеет информацией, тот владеет миром, как сказал однажды Натан Ротшильд. Этот человек, как никто другой, понимал важность информации – ведь он занимался биржевыми играми, а в них, как вы сами знаете, каждая крупица сведений может сделать бедняком даже самого богатого человека и наоборот.

Благодаря персональным компьютерам работать с информацией стало очень просто, и так же просто информацию стало передавать и принимать. У этой всесторонне положительной особенности электронных документов есть и отрицательные стороны: злоумышленникам намного проще похитить не предназначенную для чужих глаз информацию. Теперь не нужно красть толстые папки с документами – достаточно переписать данные на «флэшку», которая легко поместится в карман. Впрочем, для современного промышленного шпионажа часто даже нет нужды проникать на территорию конкурентов физически – это можно сделать виртуально, взломав через интернет корпоративный сервер и скачав с него без особой спешки всё нужное.

Или обзавестись в компании собственным агентом-инсайдером, который запросто отправит своим новым хозяевам всю необходимую информацию по электронной почте.

Потеря секретных документов оборачивается нередко баснословными убытками, однако, несмотря на это, как коммерческие, так и государственные организации продолжают пренебрегать вопросами информационной безопасности. Это характерно не только для России. Не так давно американский «Белый дом» оказался в центре большого скандала, связанного с утечкой секретных данных через старые ноутбуки, выставленные на продажу.

Лучше учиться на чужих ошибках, пусть даже и глупых. Впрочем, как показывает практика, чем глупее ошибка, тем большей прозорливостью надо обладать, чтобы не наступить от излишней самонадеянности на грабли. А для того, чтобы обезопасить себя от утечек информации, необходимо иметь представление о том, какими именно путями информация может быть похищена.

### Как утекает информация?

На самом деле, путей утечки информации из организации существует великое множество. Самый распространённый – это, увы, обычная халатность и невнимательность работников, как это случилось с выставленными на продажу



«Белым домом» ноутбуками. К сожалению, такие случаи действительно трудно проконтролировать, однако существуют возможности их предотвратить.

Гораздо хуже обстоят дела с теми, кто ворует информацию целенаправленно. К слову, ворами вовсе не обязательно должны быть люди – с этой задачей вполне может справиться и программа. Такие программы называют вредоносными, и бывают они самыми разными. Клавиатурные шпионы, называемые на компьютерном сленге кейлоггерами (фактически, это калька с английского названия подобных программ) следят за тем, какие клавиши нажимает пользователь на клавиатуре, и могут, таким образом, похищать пароли, которые он вводит. Заполучив пароли, злоумышленники могут не только похитить ценную информацию, но и заразить компьютер вирусами, что воспрепятствует нормальной работе пользователя. При грамотно организованной атаке можно нарушить работу всей организации, причём на долгое время.

Помимо клавиатурных шпионов, существуют и другие типы вредоносных программ. Например, трояны (происходит это название от словосочетания «троянский конь», которое самым лучшим образом отражает сущность этого вида компьютерной гадости) – они заводятся на компьютере, как правило, по вине самого пользователя, после чего маскируется под что-либо полезное и начинают делать что-то, вредное или не слишком приятное для пользователя – например, рассылать спам. Трояны часто служат для пересылки паролей, украденных клавиатурными шпионами, и для распространения последних.

Руткит – это, пожалуй, самый страшный вид вредоносного программного обеспечения. Они маскируются в системе специальным образом и позволяют нехорошим людям получить полный контроль над компьютером пользователя, помогают красть различные важные данные и взламывать системы защиты корпоративных сетей. Часто руткиты называют не вредоносными программами, а инструментом администрирования, но, сами понимаете, название зависит от того, для каких целей они применяются. В руках нечистоплотных конкурентов или просто недоброжелателей вашей организации руткиты имеют огромную разрушительную силу, и приводят они всё к тому же – к убыткам.

Впрочем, стоит отметить, что как бы много разных вредоносных программ не находилось на компьютере пользователя, всё равно, бороться с ними на порядок проще чем с теми сотрудниками, которые желают причинить вред родной компании. Не так важно, что именно ими движет – желание отомстить за реальные или мнимые обиды, или же жажда наживы (к сожалению, всегда находятся люди, готовые продать за тридцать серебрянников). Инсайдеры – именно так называют сотрудников, использующих свои служебные полномочия для доступа к информации в нежелательных для организации целях – могут не только красть, но и уничтожить информацию, что в ряде случаев ничуть не лучше её передачи во вражеские руки.

По данным информационного агентства Snews, в 2007 году всего около 5% компаний смогли избежать утечек информации, остальные же зафиксировали неоднократные случаи кражи конфиденциальной информации: 19% опрошенных отмечали, что их компания подверглась краже конфиденциальной информации за 2007 год от 6 до 25 раз, а около 7% - более 25. Инсайдеры крадут всё: по данным того же исследования, наиболее интересны для них персональные данные сотрудников (57%), следом идут детали различных сделок (47%), финансовые отчеты (38%), интеллектуальная собственность же наименее популярна (25%).

Инсайдеры, в отличие от вредоносных программ, не ограничены рамками виртуального пространства, а потому информация, украденная ими, может



передаваться не только по электронной почте, ICQ или другим сетевым протоколам, но и на физических носителях. Инсайдер может использовать для своих целей «флэшки», корпоративные ноутбуки, компакт-диски. Причём кража информации с помощью удобных мобильных носителей даже более популярна, чем с помощью электронной почты: так, по исследованиям всё того же CNews, кража посредством мобильных накопителей наблюдается в 74% случаев. Помимо этого, они могут элементарно распечатывать электронные документы, после чего уносить их уже в бумажном виде.

### **Бороться? Обязательно!**

Как вытекает из того, что было сказано выше, борьба с утечками информации является суровой необходимостью современных условий ведения бизнеса. В случае, если не уделять никакого внимания утечкам информации, может случиться так, что несмотря на прекрасный маркетинг и менеджмент компания всё равно пойдёт ко дну. Каким образом бороться с утечками информации?

С теми утечками информации, которые происходят из-за имеющегося на корпоративных компьютерах вредоносного программного обеспечения, бороться сравнительно просто. Для защиты от вредоносных программ существуют специальные инструменты – антивирусы и брандмауэры. Антивирусы – это программы, которые умеют находить вредителей, уже проникших на компьютер, и уничтожать их, а брандмауэры (они же файрволы) – средства защиты системы от проникновения вредоносного программного обеспечения извне. Для обеспечения высокого уровня безопасности необходимо иметь и антивирус, и брандмауэр, причём и тот и другой необходимо регулярно обновлять, потому что в противном случае они не смогут эффективно бороться с самыми новыми версиями вредоносного программного обеспечения. Любой антивирус лучше, чем его полное отсутствие, то же относится и к брандмауэрам. Поскольку нередко трояны и руткиты рассылаются в письмах с рекламой (так называемый «спам»), то необходимо иметь также и хорошие средства борьбы со спамом.

А вот что касается защиты от утечки информации, которую организуют инсайдеры, то здесь всё гораздо сложнее, и установкой антивируса, брандмауэра и антиспама здесь обойтись не удастся.

Первым шагом в борьбе с инсайдерами должно стать грамотное разграничение прав доступа к информации среди сотрудников компании. Система разграничения прав доступа должна быть гибкой и настраиваться таким, например, образом, чтобы начальники смежных отделов могли изучать почту подчинённых, но рядовой сотрудник видел лишь свою почту в поисковой выдаче, при поиске информации. Документы, предназначенные для руководящего состава не должны быть доступны клеркам, бухгалтерия и вовсе должна быть закрыта для всех, кроме бухгалтеров. В идеале, сотруднику доступна лишь информация, необходимая для выполнения рабочих обязанностей. Как говорится в общих положениях стандарта банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организации банковской системы Российской Федерации», *«наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника(ов) внутри организации».*



Следующим этапом является контроль (в разумных, конечно же, пределах) электронной почты сотрудников. Сотрудники должны в рабочее время и с рабочих компьютеров использовать только корпоративный сервер электронной почты, в идеале использование личных почтовых ящиках на бесплатных серверах (Mail.ru, Yahoo.com, Yandex.ru) должно быть заблокировано из соображений информационной безопасности. Необходимым условием эффективной борьбы с утечками информации является создание архива электронной корреспонденции организации, который должен храниться определенный промежуток времени и быть доступен даже в том случае, когда сам пользователь уже удалил свои письма. Такой архив, среди всего прочего, позволит оценить добросовестность выполнения работником своих служебных обязанностей и использоваться в качестве резервной копии всей корреспонденции, находящейся на корпоративном почтовом сервере. Ограничивать доступ к архиву почты, само собой, тоже необходимо. Пункт 8.2.6.4 общего стандарта Банка России гласит: *«Электронная почта должна архивироваться. Архив должен быть доступен только подразделению (лицу) в организации, ответственному за обеспечение информационной безопасности (ИБ). Изменения в архиве не допускаются. Доступ к информации архива должен быть ограничен».*

Третьим пунктом в программе борьбы с утечками информации стоит необходимый контроль за действиями сотрудников организации. В общих положениях стандарта банка России сказано, что обязательна *«регистрация действий персонала и пользователей в специальном электронном журнале. Данный электронный журнал должен быть доступным для чтения, просмотра, анализа, хранения и резервного копирования только администратору ИБ».* Стоит заметить при этом, что администраторы информационной безопасности – тоже живые люди, и они, как и любые другие сотрудники, могут, к сожалению, оказаться инсайдерами. Потому их действия также необходимо контролировать. Идеальным вариантом будет создание двух взаимно контролирующих подразделений информационной безопасности.

### Практические решения

«Это всё, конечно, хорошо», - можете сказать вы, - «однако теория теорией, а как на практике реализовать защиту от утечек информации?». Действительно, создание качественной системы информационной безопасности «с нуля» собственными силами компании может оказаться почти неподъемной задачей. К счастью, существуют готовые решения, предлагаемые, ко всему прочему, российскими производителями, а потому доступные по своей стоимости.

Требования, предъявляемые к подобным решениям, как вы сами понимаете, довольно высоки. Они должны не только позволять контролировать входящий и исходящий трафик пользователя, но также и следить за тем, какие документы пользователь переписывает на «флэшку» и что печатает на принтере.

После длительного поиска на тематических форумах и сайтах по информбезопасности автор пришел к выводу, что наиболее интересным из программных продуктов для построения комплексного контура информационной безопасности предприятия является детище компании «СофтИнформ» (только не считите за рекламу).

Контур информационной безопасности «СофтИнформ» - комплексный продукт, способный обеспечить полноценную защиту от утечки информации всеми описанными выше путями. Он позволяет отслеживать утечки конфиденциальной

Это ваша власть  
над информацией



информации через e-mail, ICQ, внешние устройства, документы отправляемые на печать, а так же отслеживать появление конфиденциальной информации на компьютерах пользователей. Что немаловажно, информация, собранная в результате деятельности компонентов программы, доступна для анализа специалистами благодаря мощным механизмам поиска. Помимо полнотекстового поиска, контур информационной безопасности компании «СофтИнформ» предлагает фирменный «поиск похожих», когда в качестве поискового запроса будет использован целый документ (например, файл PDF или Microsoft Word), а в результате будут найдены документы, похожие на него по своему содержанию. Согласитесь, это сильно упрощает работу с большими объёмами информации. Также разработчики этого программного продукта утверждают, что он быстро устанавливается и легко интегрируется в информационную структуру предприятия.

В состав контура информационной безопасности входит несколько специализированных приложений для сбора информации и средство SearchInform AlertCenter, позволяющее собрать их все в единый контур защиты. SearchInform Server позволяет отследить появление конфиденциальной информации на компьютерах пользователей. При этом на компьютеры сотрудников устанавливаются программы-агенты, которые позволяют следить за появлением конфиденциальной информации в местах для этого не предназначенных. SearchInform MailSniffer предназначен для перехвата почтовых сообщений, что позволяет отследить утечку конфиденциальной информации по электронной почте. Кроме этого, с помощью MailSniffer можно наладить контроль над качеством работы сотрудников, посредством мониторинга переписки. Это является важным процессом в организации работы любого предприятия. SearchInform DeviceSniffer перехватывает информацию, записываемую на внешние устройства (через порты USB или, например, на CD/DVD диски), и таким образом предотвращается возможность утечки информации через сменные носители. Аналогичным образом действует и SearchInform IMSniffer, только эта программа перехватывает данные, отправляемые системами мгновенного обмена сообщениями (ICQ, QIP и т.д.). SearchInform PrintSniffer контролирует содержимое документов, отправленных на печать, что позволяет не только предотвращать попытки хищения информации, но также оценить целесообразность использования принтера каждым сотрудником. SearchInform AlertCenter обеспечивает единую систему разграничения прав доступа к данным, а при наличии признаков утечки информации любым из путей AlertCenter немедленно даёт об этом знать лицу, ответственному за информационную безопасность вашей организации.

Как видите, информационная безопасность предприятия – это действительно важно, и её не стоит пускать на самотёк. Купленная система информационной безопасности поможет сэкономить вам значительные деньги, которые могли бы украсть у вас инсайдеры. А потому информационная безопасность – не так статья расходов, на которой следует экономить.