



ности в защите периметра сети, утечки информации через сотрудников, допущенных к ней, забираются все выше в «хит-параде» наиболее опасных инцидентов в информационной сфере. Также на этот риск оказывает влияние то огромное количество персональных данных, которые накопили правительственные организации, финансовые институты, телекоммуникационные компании, и которые время от времени похищаются. Именно утечки таких данных становятся (а в некоторых странах – обязаны становиться) гласными. Большинство же утечек данных через сотрудников, имеющих к ним доступ, остаются либо скрытыми от общественности, либо даже нераскрытыми. Именно благодаря тому, что факты утечек и их размеры неохотно раскрываются руководством компаний, исследования в этой области пока носят весьма субъективный характер, сдерживая оценку эффективности различных средств борьбы с утечками.

Большинство опрошенных сходятся в одном - внутренние угрозы - наиболее беспокоящий компании класс угроз. И при этом – наименее исследованный. Даже терминология, что именно считать внутренними угрозами, а что – внешними, до сих пор не устоялась. Например, ФБР США под термином «внутренние угрозы», подразумевается, в числе прочих, несанкционированный доступ к документам и приложениям со стороны сотрудников компании. Все типы инцидентов, связанные с использованием информации или компьютера, к которым у сотрудника нет доступа, американская терминология относит к внутренним угрозам. С точки зрения же российской терминологии, эта угроза считается внешней, поскольку решения по ее предотвращению те же, что и решения по предотвращению доступа к корпоративной информации любых других посетителей офиса компании – разделением физического и информационного доступа. В дальнейшем под внутренними угрозами мы будем подразумевать угрозы утечки информации в ходе доступа к ней пользователей, имеющих этот доступ ввиду служебных обязанностей. Причем утечки только в электронном виде или в виде печатных копий – такие типы утечек, как фотографирование экрана и переписывание данных от руки не рассматривается.

Приведем несколько примеров, иллюстрирующих разницу в подходах к классификации. Предположим, сотрудник, работающий с конфиденциальной информацией, отошел на время от компьютера, не заблокировав его, в это время сосед по кабинету сбросил на флеш-диск данные, с которыми работал сотрудник. По классификации ФБР, это реализация внутренней угрозы, так как злоумышленник находился внутри компании. С точки зрения российской классификации – реализовалась угроза внешняя, так как злоумышленник не имел служебного доступа к данным, и нарушил не правила хранения информации, а правила разделения доступа к информации.

## Определение конфиденциальной информации

Определив, от кого мы защищаем конфиденциальную информацию, хранящуюся в корпоративной информационной сети, неплохо теперь определить, что мы защищаем. Прежде всего, в компании необходимо дать определение конфиденциальной информации и определить разрешенные действия с не для разных групп пользователей. В каждой компании существует (или, по крайней мере, должно существовать) «Положение о конфиденциальной информации», описывающее порядок работы с конфиденциальной информацией, находящейся в бумажных документах. Прежде всего, необходимо адаптировать его к документам, содержащим конфиденциальную информацию в электронном виде. В реальности эта адаптация занимает несколько недель и сводится к адаптации Положения к таким отсутствующим в бумажных документах понятиям, как копия документа, часть документа и т.д. Регламенты работы с конфиденциальной информацией в электронном виде также с небольшими изменениями приходят из регламентов обращения с документами в бумажном виде. Т.е. определяется цикл жизни документа – где он создается, как и кем используются, кто и в каких условиях может вносить в него изменения, сколько он хранится и как уничтожается.

С документами более или менее понятно, по большому счету, нет разницы электронный он или бумажный. Есть нюансы, касающиеся например, переписки по электронной почте. Регламенты обращения с электронной почтой, конечно, строго регламентируют отправку по электронной почте документов, содержащих конфиденциальную информацию. Однако в процессе адаптации «Положения о конфиденциальной информации» к информации в электронном виде, необходимо особо оговорить запрещенные виды информации, которые могут исходить из компании в виде электронной почты. Почти во всех компаниях есть стандартный набор информации, которую может отправлять с корпоративной почты одно подразделение и не может другое. Так, посылать письма, в которых содержится упоминания первых лиц компании может лишь служба PR, банковские реквизиты – бухгалтерия, цены на продукцию – служба сбыта, тендерную документацию – отдел закупок т.д.. Конечно, в каждой компании есть свои нюансы. О технических методах реализации этих регламентов поговорим в этой статье попозже

Регламенты использования документов, содержащих конфиденциальную информацию должны включать описание системы хранения документов и организацию доступа к ним. Здесь тоже нет ничего принципиально нового – опыт работы с бумажными документами накоплен огромный. Те же нехитрые правила – перед получением доступа к документам для чтения или внесения изменений сотрудник указывает, на каком основании и для чего он собирается получить доступ к документу, что собирается с ним делать, когда он закончит работать с документом и т.д. Этот «журнал» работы с документом в случае с электронными документами вести даже проще, чем с бумажными документами, т.к. большая часть операций (например, проверка прав доступа или прав на изменение содержания, учет времени работы и контроль изменений) может идти в автоматическом режиме. Термин «журналирование», обозначающий процесс ведения журнала доступа к документу, встречается в источниках наряду с термином «логирование».

Также в положении должно быть отмечено, что никакой администратор не может изменять информацию в журнале своей работы, чтобы возможность скрыть следы своей работы не подвигла его на неправомерные действия.

После построения документарной базы можно переходить к следующей процедуре: классификации имеющейся информации. Необходимо определить, какие документы являются конфиденциальными, какие сотрудники имеют доступ какого уровня к каким документам. Так создается так называемый реестр конфиденциальных документов, содержащий помимо описания документов и прав доступа, еще и правила внесения в него документов и правила их изъятия (уничтожения). Поскольку в каждой компании каждый день создается множество новых документов, часть из них – конфиденциальные, то без создания механизма их автоматической или полуавтоматической классификации реестр уже через несколько месяцев потеряет актуальность.

Особо следует обратить внимание на организацию процесса пометки конфиденциальных документов. Каждый конфиденциальный документ должен содержать метку, по которой следящие программы могли бы определить степень его конфиденциальности. Здесь выбор за заказчиком. Если защищаемые документы исключительно формата MS Office, то в качестве метки может использоваться запись конфиденциально в соответствующих полях «Свойств» документов. Автор сталкивался и с программными метками, но наиболее распространенный способ – принудительное добавление в имя файла идентификатора «conf». Это удобно и визуально – даже в очереди на печать можно сразу увидеть конфиденциальные документы. К тому же нелишне еще раз напомнить пользователю при открытии файла, что документ конфиденциален.

После создания реестра конфиденциальных документов можно приступать к реорганизации их хранения. В крупных компаниях организационными и техническими мерами запрещается хранение конфиденциальной информации локально – на рабочих станциях. Обычно конфиденциальная ин-

формация хранится в специальных клиент-серверных или web-приложениях (корпоративных интранет-порталах, документных хранилищах, бизнес-приложениях, справочно-нормативных базах, системах документооборота, ERP и т.д.) которые разделяют права доступа пользователей и защищают информацию от сохранения в несанкционированном месте. Защита таких данных на сервере имеет многоуровневую защиту (на уровнях аппаратной платформы, операционной системы, СУБД и приложения). Однако риски утечки этой информации с рабочих станций, тем не менее, существуют.

## Способы хранения конфиденциальной информации

Компания должна защищать от утечки информацию трех основных типов – сводная информация, конфиденциальные документы и интеллектуальная собственность.

К сводной информации обычно относят разнообразные структурированные данные в формате базы данных или электронных таблиц. Это может быть не только информация о продуктах и ценах, финансовая информация и т.д., которая представляет ценность для конкурентов, но и персональная информация о клиентах, которую компания должна охранять по закону. При их похищении информации такого типа, похитителю важно сохранить полноту, достоверность и структуру информации – ценность неполной информации в общем случае резко уменьшается. Отдельным случаем рассматривается «заказ» на похищение конкретной информации из базы данных, а не всей базы данных. Однако, большинство инсайдеров допускают утечки информации, не имея конкретных заказчиков на нее, поэтому второй случай встречается гораздо реже. В любом случае, здесь и далее рассматривается утечка данных такого объема, чтобы вынос ее «в оперативной памяти человеческого мозга» или «переписанными на бумажку» не представлялся возможным.

Интеллектуальная собственность – любая информация в электронном виде, которая обеспечивают компании конкурентные преимущества. Это могут быть любые внутренние материалы – шаблоны документов, должностные инструкции, описание бизнес-процессов, справочно-нормативная информация, документы, содержащие информацию об изобретениях, патентах, перспективных разработках и другие, охраняемые законом. Эта информация может храниться в любом месте – в документном хранилище, базе данных, в специальных папках на серверах, на локальных рабочих станциях. Форматы хранения – любые форматы приложений, в том числе и отсканированные образы документов, чертежей. В отличие от предыдущей группы информации, ценными являются не только сами документы, но и их фрагменты, черновики и т.д.

Все остальные документы, содержащие неструктурированную конфиденциальную информацию, можно отнести к оперативному документообороту. Это приказы по компании, электронная переписка внутри компании. Информация, находящаяся в них, имеет оперативный интерес для конкурентов и партнеров компании, и, будучи похищена, также может привести к моральным и материальным потерям. В 2000 году по компьютерной прессе гуляла копия приказа по одной из компаний «программистам принимать душ не реже двух раз в неделю». Вряд ли она привела к материальным потерям, но пятно на репутацию компании бросила. А вот утечка документа, содержащего себестоимость коммерческого предложения, попавшая к заказчику, может привести к конкретным убыткам – заказчик будет знать, до какой суммы компания готова уступить. Поскольку такая информация разрознена, хранение ее никак обычно не регламентировано, защита ее от утечек особо затрундена.

Один из путей утечки информации через санкционированный доступ – клиентские приложения. Большинство рабочих станций в офисах крупных компаний – компьютеры на платформе Wintel. Архитектура таких рабочих мест делают информацию, открытую с помощью клиентских приложений практически беззащитной. Хранение информации в незашифрованных временных файлах, встроенная в операционную систему возможность копирования информации в буфер (операции Copy и

PrintScreen), наличие многих каналов ввода-вывода (дискеты, CD-R, USB, WiFi, Bluetooth и т.д.) делают рабочую станцию весьма опасным устройством для реализации внутренних угроз. Заметим, что таких угроз нет при доступе к информационной системе через тонкие клиенты или системы мейнфрейм-терминал.

Другой потенциальный источник утечек – копии информации на мобильных рабочих местах. Требования бизнеса сегодня привели к тому, что часть сотрудников проводит большую часть времени вне офиса. Есть виды бизнеса, практически невозможные без мобильных рабочих мест, такие как консалтинг, аудит и другие. Для эффективной работы вне доступа к корпоративной сети им необходимы копии служебных документов, в том числе и конфиденциальных. Простой запрет на хранение информации на мобильных рабочих местах приведет к невозможности выполнять служебные обязанности вне офиса, что непременно скажется на эффективности бизнеса компании. Поэтому практически все мобильные сотрудники имеют копии конфиденциальной информации продуктов. Закрытие всех портов ввода-вывода на ноутбуках во-первых, достаточно сложно технически, а во вторых – затруднит выполнение служебных обязанностей мобильных пользователей, т.к. мобильные пользователи по своим служебным обязанностям должны использовать как сменные носители, так и коммуникационные порты.

## От кого защищаем информацию

Сотрудники, допускающие утечку конфиденциальной информации, будучи допущенными к ней, классифицируются по нескольким критериям – злонамеренные или халатные, ставящие цели себе сами или действующие по заказу, охотящиеся за конкретной информацией или выносящие все, к чему имеют доступ. Правильно классифицировав потенциального нарушителя, сотрудники подразделения информационной безопасности компании могут спрогнозировать поведение нарушителя при невозможности осуществления попытки утечки информации. Кроме того, рассматривая средства защиты, всегда надо иметь в виду, против каких нарушителей эти средства действенны, а против каких – нет.

Мы разделяем нарушителей на пять основных видов – неосторожные, манипулируемые, саботажники, нелояльные и мотивируемые извне. Рассмотрим каждый вид и их подвиды подробнее.

### Неосторожные

В других источниках также встречается название «халатные». Эти сотрудники создают незлонамеренные ненаправленные угрозы, т.е. они нарушают правила хранения конфиденциальной информации, действуя из лучших побуждений. Самые частые инциденты с такими нарушителями – вынос информации из офиса для работы с ней дома, в командировке и т.д., с дальнейшей утерей носителя или доступом членов семьи к этой информации. Несмотря на добрые намерения, ущерб от таких утечек может быть ничуть не меньше, чем от промышленных шпионов. Столкнувшись с невозможностью осуществить копирование информации, этот тип нарушителей будет действовать по инструкции – обратится за помощью к коллегам или системному администратору, которые объяснят ему, что вынос этой информации за пределы офиса запрещен. Поэтому против таких нарушителей действенными являются простые технические средства предотвращения каналов утечек – контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода-вывода.

### Манипулируемые

Последние годы термин «социальная инженерия» чаще всего используется для описания различных типов мошенничества в Сети. Однако манипуляции используются не только для получения обманным путем персональной информации пользователей – паролей, пин-кодов, номеров кредитных карт и адресов. Известный экс-хакер Кевин Митник считает, что именно социальная инженерия сегодня

является «бичом» информационных систем. Примеры, которые приводит Митник в своей книге «...», показывают, например, что «добросовестная» секретарша может по просьбе злоумышленника «для надежности» продублировать почтовое сообщение, содержащее конфиденциальную информацию, на открытый почтовый ящик. Таким образом может быть осуществлена утечка конфиденциальной информации.

Поскольку манипулируемые и неосторожные сотрудники действуют из своего понимания «блага» компании (оправдываясь тем, что иногда ради этого блага нужно нарушить дурацкие инструкции, которые только мешают эффективно работать), два этих типа нарушителей иногда объединяют в тип «незлонамеренных». Как уже говорилось выше, ущерб не зависит от намерений, зато от намерений зависит поведение нарушителя в случае невозможности осуществить свое действие. Как лояльные сотрудники, эти нарушители, столкнувшись с техническим блокированием их попыток нарушить регламенты хранения и движения информации, обратятся за помощью к коллегам, техническому персоналу или руководству, которые могут указать им на депустимость планируемых действий.

Следующая группа нарушителей – злонамеренные, т.е. в отличие от сотрудников, описанных выше, осознающие, что своими действиями они наносят вред компании, в которой они работают. По мотивам враждебных действий, которые позволяют прогнозировать их поведение, они подразделяются на три типа – саботажники, нелояльные и мотивируемые извне.

### Саботажники

Саботажники (в других источниках – обиженные сотрудники) – это сотрудники, стремящиеся нанести вред компании из-за личных мотивов. Чаще всего мотивом такого поведения может быть обида из-за недостаточной оценки их роли в компании – недостаточный размер материальной компенсации, неподобающее место в корпоративной иерархии, отсутствие элементов моральной мотивации или отказ в выделении корпоративных статусных атрибутов (ноутбука, автомобиля, секретаря). Для оценки моделей поведения нарушителя отметим два ключевых отличия от других типов нарушителей – во-первых, сотрудник не собирается покинуть компанию и, во-вторых, сотрудник стремится нанести вред, а не похитить информацию. То есть, он стремится, чтобы руководство не узнало, что утечка произошла из-за него и, столкнувшись с технической невозможностью похитить какую-либо информацию, он может направить свою разрушительную энергию на что-нибудь другое, например, на уничтожение или фальсификацию доступной информации, или похищения материальных ценностей. При этом сотрудник, исходя из собственных представлений о ценности информации и нанесенном вреде, определяет, какую информацию имеет смысл похитить и кому ее передать. Чаще всего это пресса или теневые структуры, для соответственно оглашения или шантажа. Примером реализации такой угрозы может служить передача экологической прессе данных о состоянии затопленных ядерных подводных лодок одним из сотрудников предприятия, ответственного за мониторинг этого состояния.

### Нелояльные

Следующий тип нарушителей – нелояльные сотрудники. Прежде всего, это сотрудники, принявшие решение сменить место работы или миноритарные акционеры, решившие открыть собственный бизнес. Именно о них в первую очередь думают руководители компании, когда речь заходит о внутренних угрозах – стало привычным, что увольняющийся сотрудник коммерческого отдела уносит с собой копию базы клиентов, а финансового – копию финансовой базы. В последнее время также увеличилось количество инцидентов, связанных с похищением интеллектуальной собственности высокотехнологичных европейских и американских компаний стажерами из развивающихся стран, поэтому временных сотрудников иногда также относят к этому типу. По направленности угроза, исходящая от таких нарушителей является ненаправленной – нарушители стараются унести максимально возможное количество доступной информации, часто даже не подозревая о ее ценности и не имея представления, как они ее будут использовать. Самый частый способ получения доступа к информации или возможности ее скопировать – это имитация производственной необходимости. Именно на

этом их чаще всего и ловят. От предыдущего типа нарушителей нелояльные отличаются в основном тем, что, похитив информацию, они не скрывают факта похищения. Более того, иногда похищенная информация используется, как гарант для обеспечения комфортного увольнения – с компенсацией и рекомендациями.

Два последних типа нарушителей все же не так опасны, как последний. Саботажники и нелояльные сотрудники все же сами определяют информацию для похищения и место ее «сбыта». Коммерческий директор, решивший уволиться, унесет с собой базу данных клиентов, но, возможно, он найдет работу в компании, напрямую не конкурирующей с нынешним работодателем. Переданная прессе саботажником информация может не оказаться сенсацией и не будет напечатана. Стажер, похитивший чертежи перспективной разработки, может не найти на нее покупателя. Во всех этих случаях информация не нанесет вред владельцу. Наткнувшись на невозможность похитить информацию, нарушители вряд ли будут искать техническую возможность обойти защиту, к тому же, скорее всего, они не обладают должной технической подготовкой для этого.

Однако, если еще до похищения информации, саботажник или нелояльный сотрудник выйдет на потенциального «покупателя» конкретной информации, будь то конкурент, пресса, криминальные структуры или спецслужбы, он становится самым опасным нарушителем – мотивированным извне. Теперь его дальнейшая судьба – работа, благосостояние, а иногда жизнь и здоровье напрямую зависят от полноты и актуальности информации, которую он сможет похитить.

### Нарушители, мотивируемые извне

Мотивированные извне – это сотрудники, цель которым определяет заказчик похищения информации. К этому типу сотрудников относят внедренных, т.е. специально устроенных на работу для похищения информации и завербованных, т.е. сотрудников, изначально лояльных, но впоследствии подкупленных или запуганных. Опасность этого типа нарушителей заключается в том, что в случае технических ограничений на вынос информации за пределы корпоративной информационной сети, «работодатели» могут снабдить его соответствующими устройствами или программами для обхода защиты.

## Другие типы нарушителей

В эту классификацию не случайно не включена такая распространенная группа экономических преступников, как инсайдеры – сотрудники, передающие с целью получения выгоды внутреннюю корпоративную информацию, которая может повлиять на стоимость акций. Дело в том, что техническими и организационными мерами пресечь утечку информации, влияющей на стоимость ценных бумаг, практически невозможно. Эта информация обычно очень невелика, часто всего несколько цифр или одно предложение, и может даже не существовать в электронном виде. Например, это прибыль компании какой-то период, разведанные запасы нефти, информация о предстоящем поглощении компании и т.п. В отличие от прессы, проверяющих органов и т.п., клиентам инсайдеров не нужны подтверждения в электронном виде. С технической точки зрения пресечь вынос такой информации (названия компании и дату запуска) за пределы компании «в оперативной памяти человеческого мозга» невозможно, для предотвращения таких утечек действует законодательно закрепленный запрет на использование инсайдерской информации при торговле ценными бумагами. Поэтому этот тип нарушителей не принимается в предложенной классификации во внимание.

## Основные направления защиты

Поскольку потенциальными похитителями информации являются все сотрудники, имеющие к ней до-

ступ, методы защиты планируются таким образом, чтобы соблюсти баланс доступности информации для легального использования и защищенности ее утечки. Традиционный выбор информационной безопасности между доступностью и безопасностью каждой компанией решается в зависимости от уровня паранойи в корпорации.

### Защита документов

Это самая разработанная область защиты электронной информации от внутренних угроз. За образец бизнес-процесса защиты электронного документа взяты методы работы с бумажными документами, описывающие как создается документ, как изменяется, как хранится и как уничтожается. Часть функций контроля жизненного цикла электронного документа автоматизированы, часть осталась неизменной с прошлых веков.

### Защита каналов утечки

Этот вид защиты электронных документов также имеет аналог в прошлом. Во всяком случае, пока не научились копировать информацию непосредственно в мозг человека, контроль выноса с территории компании физических носителей остается одним из самых эффективных. Во многих компаниях уже нельзя входить на территорию с сотовыми телефонами и фотокамерами. Миниатюризация носителей информации и встраивание Flash-памяти в часы, медиа-плееры делают такой контроль все менее эффективным. Поэтому наиболее эффективная защита документов этим способом – контроль копируемой информации «до» того, как она будет скопирована.

### Мониторинг (аудит) действий пользователя

Эта часть действий, направленных на обеспечение защиты от внутренних угроз, в руководящих документах Гостехкомиссии (ныне ФСТЭК) называется аудитом действий пользователя. Что делает с документом пользователь, получив к нему доступ, также интересует специалистов по безопасности. Иногда наблюдатель – офицер безопасности, иногда – видеокамеры, в последнее время – специальные компьютерные программы.

## Программные решения.

### Примеры, достоинства и недостатки.

Защита информации выделяет несколько решений – психологическое, организационное, техническое. В защите электронных документов добавляется программное решение. Три основных направления защиты: защита документов, защита каналов утечки и мониторинг действия пользователей, применяемые в комбинации друг с другом и с другими решениями, обеспечивают наиболее эффективное решение.

## Защищенный документооборот

Защита электронных документов наиболее эффективна в специализированных приложениях: системах защищенного документооборота, защищенных клиент-серверных и web-приложений. Основной принцип таких систем – защита документа с момента его создания и до момента его уничтожения. В тех организациях, в которых весь документооборот ведется в системах защищенного документооборота, конфиденциальные документы наиболее защищены от внутренних угроз. Все действия авторизованных пользователей с конфиденциальными документами, включая их сохранение в неавторизованном месте, печать и другие, представляющие угрозу утечек информации, мониторятся и документируются. Такие системы хранят все черновики и версии документов, любые изменения и попытки несанкционированных действий фиксируются.

Однако внедрения таких систем с целью защиты от внутренних угроз имеют и существенные недостатки. Рассмотрим их более пристально.

1. Существенные расходы на внедрение. Такие системы достаточно дороги и требуют одновременного внедрения во всей компании, как минимум, а оптимально – у всех контрагентов. Этот путь достаточно дорог – стоимость ПО для одной рабочей станции иногда превышает сотни долларов, не считая серверных лицензий.

2. Непривычная для работы среда. Владение системами документооборота не является обязательным при приеме на работу, в отличие от знания офисных и почтовых приложений. Поэтому всех пользователей придется обучать работе с новой системой. В последнее время появились системы, интегрирующиеся в стандартные офисные пакеты, но они еще не так распространены.

3. Собственный формат файла. Для реализации стратегии защиты документа все системы защищенного документооборота используют закрытый формат файлов, который может быть открыт только в конкретной системе документооборота. Слабость этой системы защиты заключается в том, что, поскольку не все контрагенты имеют эти системы документооборота, для передачи файлов им, необходимо конвертировать защищенный формат в общепринятый. После конвертации файлы остаются незащищенными для нецелевого использования.

4. Незащищенность на рабочих станциях. Как бы не было защищено документное хранилище, открытый на рабочей станции документ или запрос к базе данных уязвим дважды: во-первых, его содержание находится в буфере экрана, т.е. возможно копирование его или его части в буфер Windows командами `Сору` или `PrintScreen`, во-вторых, образ экранного буфера находится во временном файле, который находится на диске рабочей станции и может быть скопирован с помощью файлового менеджера. Сохранение этой информации в незащищенном формате позволяет пользователю иметь конфиденциальную информацию в незащищенном виде и поступать с ней по своему усмотрению.

## Мониторинг (аудит) действий пользователей

В организациях, в которых возможен доступ сотрудников к государственной тайне давно используются специализированные рабочие места для работы с ней. Кроме мониторинга движений мыши и клавиатуры, на этих станциях осуществляется также шифрование информации на лету, а также использование специальных экранных фильтров для избежания фотографирования информации с экрана или подглядывание за экраном через плечо работающего. Кроме того, такие рабочие станции лишены возможности подключения сменных носителей, а печать осуществляется с разрешения офицера-секретчика.

Для доступа к информации, составляющей гостайну, это решение, безусловно, оправдано, т.к. риск утечки имеет гораздо более высокий приоритет, чем удобство использования. Однако подобные регламенты работы с конфиденциальной информацией в динамичных рыночных структурах, осложняющие доступ и манипуляции с информацией, могут помешать рыночному успеху компании. Большое количество сотрудников и операций с документами будет порождать такое количество информации, которое не сможет обработать ни один человек. Поэтому тотальный контроль будет лишь давать иллюзию контроля – воспользоваться его результатами будет сложно.

Можно провести аналогию с голосовой связью – технически возможно прослушивать и записывать все разговоры, ведущиеся по телефонам, но в реальности воспользоваться этой информацией в оперативном порядке невозможно – тогда на каждого говорящего придется один слушающий. Другое дело – наблюдение за конкретным сотрудником, находящимся в оперативной разработке, т.е. подозреваемым в чем-то. Также важно иметь возможность ретроспективного анализа накопленной информации при проведении расследований.

Поэтому чаще всего применяется программное обеспечение, контролирующее определенные действия пользователя в пассивном режиме – ведущее журнал доступа. Довольно редко бывает необходимо мониторить нажатие каждой клавиши и каждое перемещение мыши, обычно выделяются опасные операции (файловые – copy и rename, документные SaveAs, Print и Copy\Paste, системные PrintScreen и т.п.). Эти операции монитруются особо тщательно. Причем, если эти операции проводились с документом, не содержащим конфиденциальную информацию, то программное обеспечение лишь фиксирует его в базе событий, если же эти действия совершались с конфиденциальным документом – посылается сообщение о запрещенной операции.

Часто за неимением информации о специальных решениях, в целях мониторинга при меняют решения, предназначенные для других целей. Так, для мониторинга движения файлов используются программные агенты, предназначенные для аудита состояния программного обеспечения. Это дает иллюзию защиты, т.к. эти агенты контролируют лишь перемещения файлов с помощью файловых менеджеров. Если же перемещать файлы при помощи операций над ними, например, при конвертации формата или используя программы для записи на оптические диски типа Nero, эта операция пройдет незамеченной для агента.

## Защита каналов утечки

Под защитой каналов обычно понимают два взаимодополняющих процесса – управление доступом к каналу и контроль информации, передающейся через канал. Собственно каналов выхода информации из компании немного – электронная почта, интернет, сменные носители (дискеты, пишущие CD/DVD, USB-устройства и т.д.), порты вывода (COM, WiFi, Bluetooth и др.), печать, и мобильные устройства – ноутбуки и КПК.

Для контроля доступа к каждому из них есть свои программы, как входящие в средства управления соответствующего приложения, так и продающиеся отдельно. Обычно процесс открытия доступа в компаниях регламентирован и осуществляется на базе заявок, визируемых непосредственным руководителем. Конечно, факт отказа сотруднику в доступе к каналу гарантирует отсутствие утечек по этому каналу от этого сотрудника. Но не стоит забывать, что сохранение конфиденциальной информации не есть основная задача бизнеса. Не имея доступа к корпоративной электронной почте или принтеру, сотрудник не сможет выполнять свои служебные обязанности, а имея такой доступ – станет потенциальным похитителем информации.

Последнее время часто говорят о решениях по управлению доступом к сменным устройствам, как о решении проблемы похищения информации. Т.е. утверждается, что если мы ограничим доступ, например к USB-портам, мы будем защищены от утечек информации. Некоторые программы позволяют разрешить использование только определенного USB-носителя и запретить использование всех остальных. Действительно, пример, приведенный в самом начале статьи, не реализовался бы в случае, если бы USB-порт не заблокированного пользователем компьютера был бы открыт только для использования определенного диска или был бы открыт только для чтения. Однако, напомним, что чужие USB-диски – это инструмент реализации не внутренних угроз, а внешних. Злонамеренный нарушитель всегда имитирует производственную необходимость или просто купит КПК и потребует открыть порт для синхронизации его с компьютером. Сменные карты расширения памяти КПК достигают емкости 2 Гб, поэтому при наличии желания через КПК можно вынести любое количество информации.

Вот почему, кроме факта открытия доступа к каналу, необходимо мониторить информацию, проходящую через него, на предмет содержания запрещенной к выносу за пределы компании. Для этого

используются различные технологии - контентная фильтрация, метки на конфиденциальных файлах и др. Кроме того, есть программные решения, сохраняющие копии скопированных, посланных и напечатанных файлов для создания доказательной базы при расследовании инцидентов.

## Организационные и психологические меры защиты от внутренних угроз

### Психологические меры

Не вдаваясь подробно в психологические аспекты защиты, выделим два способа внедрения систем – открытый и закрытый. Как внедрять такую систему – решает сам заказчик, причем на самом высоком уровне. Безусловно, полностью реорганизовать документооборот незаметно для пользователей невозможно, тем более, что часть процесса внедрения – ознакомление пользователей с процедурами доступа. Однако, если основная цель внедрения системы – выявления уже действующего канала утечки, определение всех его звеньев, причем не только исполнителей внутри компании, но и заказчиков информации вне ее, имеет смысл повременить с объявлением процедур и ставить в первую очередь мониторы активности пользователей и контентную фильтрацию почты. В случае оперативной разработки в отношении сотрудников компании по договоренности с производителем имеет смысл замаскировать программные агенты на рабочих станциях под программы, которые не вызовут подозрений – антивирус или мониторы аудита программного обеспечения.

Если же внедрять систему защиты от внутренних угроз открыто, то за счет психологического фактора можно даже сэкономить. Известно, что при внедрении систем видеонаблюдения для защиты периметра на некоторых направлениях можно ставить неподключенные камеры, т.к. сам факт наличия видеонаблюдения уже останавливает большую часть нарушителей. Для этого камеры должны стоять на виду. По аналогии, организация новой системы хранения, ознакомление сотрудников с новыми регламентами, появление и предание гласности инцидентов с попыткой вынести запрещенную информацию за пределы компании наверняка предотвратит хищения информации саботажниками и нелояльными сотрудниками.

### Организационные меры

#### Права локальных пользователей

Было бы неправильным считать, что любое, даже самое совершенное программное обеспечение может решить все проблемы с утечками. Даже будучи установленным, такое программное обеспечение будет время от времени проверяться сотрудниками на возможность преодоления защиты. Кроме постоянного тестирования системы безопасности, необходимо ограничить возможности потенциальных взломщиков. В первую очередь это достигается за счет лишения пользователей прав локального администратора на их рабочих местах. Эта, казалось бы, простая мера до сих пор не применена в большинстве компаний. Иногда оправданием этого служит наличие в компании унаследованного программного обеспечения, неспособного работать с операционными системами, поддерживающими удаленное управление. Выходом из этого может быть локализация рабочих мест с правами локального администратора для работы с унаследованным приложением, в отдельном сегменте сети, физическое или программное лишение рабочих мест устройств вывода и концентрация их в одном месте под контролем сотрудника, персонально ответственного за отсутствие утечек информации. Однако, нужно понимать, что это решение является временным и стратегически необходимо стремиться как можно скорее портировать унаследованные приложения в более современные операционные системы.

## Стандартизация ПО

Мало в каких компаниях автору встречался такой документ, как список программного обеспечения, допустимого к установке на рабочих станциях, а там где он есть, на его составление ответственные лица подвигло не беспокойство за утечки конфиденциальной информации, а, скорее, понимание того, что сотрудники могут использовать предоставленный им для работы компьютер для развлечений. Иначе не возможно объяснить наличие в этом списке файлового менеджера FAR. Возможно, встроенный в операционную систему Windows Explorer действительно неудобен, но зато он не позволяет копировать временные файлы Windows. Что выгоднее компании – заставить сотрудников пользоваться штатными средствами операционной системы или оставить мощный инструмент похищения данных – ответ напрашивается сам собой, но большинство компаний, видимо, не ставит даже этот вопрос.

После составления списка программного обеспечения необходимо обеспечить установку на все рабочие станции и ограничить запуск других программ без участия администратора. Принцип «все, что не разрешено – запрещено» в этом случае должен выполняться неукоснительно. Это избавит компанию от будущих проблем с утечками через злонамеренных нарушителей – они не смогут использовать программное обеспечение, которое может использоваться для обмана, например, механизмов контентной фильтрации – шифрование и стеганографию.

## Специфические решения

Небольшими организационными мерами можно решить очень большие проблемы. Когда-нибудь решение следующей задачи будут изучать в университетах. Одно федеральное ведомство серьезно страдало от регулярных утечек своей базы данных, которая имело устойчивый спрос на пиратских рынках. Мониторить все точки доступа к базе было технически очень сложно, и отдел информационной безопасности придумал следующий ход. Рассудив, что хищением информации занимается не больше десятка человек, причем вряд ли управляемых из одного центра, они попросили администраторов базы ограничить объем ежедневных запросов 20 мегабайтами. Все что больше – по дополнительной заявке с обоснованием служебной необходимости. Вряд ли нарушители захотят проявить себя регулярными просьбами об увеличении лимита. Поскольку вся база занимала несколько гигабайт, выкачать ее за месяц одному человеку не представлялось возможным. Поскольку база меняется ежедневно, сшитые куски, скопированные в разные дни, нарушали актуальность базы. Через некоторое время базу перестали покупать, а потом, ввиду отсутствия спроса – и похищать. Как видно, предотвратить утечки в данном случае удалось без дополнительных материальных затрат.

## Работа с кадрами

И, конечно, необходимо постоянно работать с пользователями. Обучение пользователей, воспитание бдительности сотрудников, инструктаж новичков и временных сотрудников во многом сможет предотвратить утечки через незлонамеренных пользователей. Любое копирование информации на сменный носитель должно вызывать вопросы коллег – ведь лояльные сотрудники пострадают вместе с компанией, а значит, они на одной стороне баррикад.

Высокая компьютерная квалификация пользователей не всегда является плюсом. В западной литературе встречается термин *overqualified* – приблизительно его можно перевести как «слишком квалифицированный» или «переквалифицированный». Причем, излишняя квалификация в компьютерных навыках является более серьезным недостатком, чем квалификация недостаточная. Ведь научить недостающим навыкам можно всегда, а как заставить человека забыть уже имеющиеся навыки? Задайте себе вопрос, правильно ли, если сотрудник бухгалтерии обладает навыками системного администратора, а оператор на атомной станции заочно учится на эксперта компьютерной безопасности? Выявление «специалистов-любителей» возможно во время традиционной аттестации. Стоит добавить в опросник вопрос «Как снять зависший процесс в Windows?» и провести разъяснительную работу с теми, кто начнет ответ со слов «Нажать одновременно кнопки Ctrl, Alt и Del». Ведь правиль-

ный ответ на этот вопрос для большинства пользователей – «Вызвать системного администратора».

### Хранение физических носителей

Еще один канал утечки информации – физический вынос носителей с резервными копиями. Понятно, что после абсолютно легального резервного копирования никакое программное обеспечение не в силах остановить физический вынос злоумышленником носителя, его копирования и занос обратно. Поэтому сейчас используется несколько способов защиты этого канала утечки. Первый – анонимизация носителей, т.е. сотрудники, имеющие доступ к носителям не знают, какая информация записана на каком носителе, они управляют только анонимными номерами носителей. Те сотрудники, которые знают, на каком носителе находится какая информация, в свою очередь не должны иметь доступ к хранилищу носителей. Второй способ – шифрование информации при резервном копировании, поскольку даже вынесенная и скопированная информация потребует некоторого времени и дорогостоящей вычислительной мощности на расшифровку. Безусловно, здесь работают все технологии хранения ценных вещей – замки, открывающиеся только двумя ключами, находящимися у разных сотрудников, несколько уровней доступа и т.д. С развитием технологий RFID, возможно, появится решение, при котором внедренные в каждый носитель радиометки будут сигнализировать о попытках вынести его за пределы хранилища.

## Направление развития процедур и технических средств защиты информации от внутренних угроз

### Модели поведения нарушителей

Развернув систему мониторинга действий с конфиденциальной информацией, кроме наращивания функционала и аналитических возможностей, можно развиваться еще в двух направлениях. Первое – интеграция систем защиты от внутренних и внешних угроз. Инциденты последних лет показывают, что существует распределение ролей между внутренними и внешними злоумышленниками и объединение информации из систем мониторинга внешних и внутренних угроз позволит детектировать факты таких комбинированных атак. Одной из точек соприкосновения внешней и внутренней безопасности является управление правами доступа, особенно в контексте симуляции производственной необходимости для увеличения прав нелояльными сотрудниками и саботажниками. Любые заявки на получения доступа к ресурсам, не предусмотренным служебными обязанностями, должны немедленно приводить в действие механизм аудита действий с этой информацией. Еще безопаснее решить вдруг возникшие задачи без открытия доступа к ресурсам.

Приведем пример из жизни. Системному администратору поступила заявка от начальника отдела маркетинга на открытие доступа к финансовой системе. В качестве обоснования заявки было приложено задание генерального директора на маркетинговые исследования о процессах покупки товаров, производимых компанией. Поскольку финансовая система – один из самых охраняемых ресурсов, и разрешение на доступ к нему дает генеральный директор, начальник отдела информационной безопасности на заявке написал альтернативное решение – доступа не давать, а выгрузить в специальную базу для анализа обезличенные (без указания клиентов) данные. В ответ на возражения главного маркетолога о том, что ему так работать неудобно, ему директором был задан вопрос «в лоб» - «Зачем тебе названия клиентов – слить базу хочешь?», после чего все пошли работать. Была ли это попытка организовать утечку информации, мы никогда не узнаем, но чтобы это ни было, корпоративная финансовая система была защищена.

## Предотвращение утечек на этапе подготовки

Другое направление развития системы мониторинга внутренних инцидентов с конфиденциальной информацией – построение системы предотвращения утечек. Алгоритм работы такой системы тот же, что и в решениях по предотвращению вторжений. Сначала строится модель нарушителя, по ней формируется «сигнатура нарушения», т.е. последовательность действий нарушителя. Если несколько действий пользователя совпали с сигнатурой нарушения, прогнозируется следующий шаг пользователя, если и он совпадает с сигнатурой – подается сигнал тревоги. Например, был открыт конфиденциальный документ, часть его была выделена и скопирована в буфер, затем был создан новый документ и в него было скопировано содержимое буфера. Система предполагает – если дальше новый документ будет сохранен без метки конфиденциально – это попытка похищения. Еще не вставлен USB-диск, не сформировано письмо, а система информирует офицера информационной безопасности, который принимает решение – остановить сотрудника или проследить, куда уйдет информация.

К слову, модели (в других источниках – «профили») поведения нарушителя можно использовать не только, собирая информацию с программных агентов. Если анализировать характер запросов к базе данных, всегда можно выявить сотрудника, который рядом последовательных запросов к базе пытается получить конкретный срез информации. Необходимо тут же проследить, что он делает с этими запросами, сохраняет ли их, подключает ли сменные носители информации и т.д.

## Аутсорсинг хранения информации

Сейчас развивается рынок услуг по аутсорсингу информационных систем, которые обеспечивают хранение информации в защищенном режиме, загрузку ее в арендуемые приложения и выдачу ее удаленно по запросам. Датацентр – ядро компании, оказывающей такие услуги, изначально проектируется таким образом, чтобы свести к минимуму вероятность утечек. Принципы анонимизации и шифрования данных для них обязательное условие организации хранения и обработки, а удаленный доступ можно организовать по терминальному протоколу, не оставляя на компьютере, с которого организуется запрос, никакой информации. Причем упомянутые программные и организационные решения для таких центров – средства производства и конкурентные преимущества, поэтому их цена является для них меньшим препятствием, чем для компаний, приобретающих эти решения для себя. Возможно, с развитием рынка этих услуг внутренняя безопасность информации трансформируется в обеспечение безопасности дата-центров.

## Заключение

Как уже говорилось в начале статьи, глубина проработки темы борьбы с внутренними угрозами зависит от уровня паранойи в компании. Предела совершенству нет – Большой Брат, придуманный Оруэллом, стремится знать все обо всех. Важно понимать, что владелец информации имеет право на ее защиту, и знать, что для этого доступны все средства – технические, психологические и организационные. И важно противопоставить комплексную систему защиты информации тем сотрудникам, которые, прикрываясь разговорами о нарушении конституционного права на невмешательство в личную жизнь, пытаются использовать данные им во исполнение служебных обязанностей ресурсы в собственных неблагоприятных целях. Перефразируя классика новейшей истории, в заключение резюмируем: «Только тот бизнес чего-либо стоит, который умеет защищаться».