

АКТУАЛЬНЫЕ БАЗОВЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ

**Ирина
Мнацеканова**

руководитель отдела
маркетинга и PR
компании StarForce
Technologies

В век цифровой информации все компании, как частные, так и государственные, переходят на электронные документы. Такой тип информации наиболее удобен, так как сразу решает многие вопросы хранения документации. Однако сегодня информация очень мобильна, документ в цифровом виде легко скопировать на оптический или flash-носитель и вынести за пределы офиса. Или воспользоваться современными способами коммуникации, приаттачив приложение к письму в электронной почте или отправив его через messenger. Для того чтобы документ гарантированно попал в предназначенные для этого руки, необходима защита электронных версий документов.

Угроз информационной безопасности сегодня существует множество: атаки хакеров, «трояны», добывающие информацию из компьютеров пользователей и по специальным каналам отправляющие заказчику, несанкционированный доступ к корпоративным системам или архивным копиям корпоративного хранилища. Однако в этой статье речь пойдет о «ячейке» корпоративного хранилища информации – электронном документе.

В течение жизни каждой компании, государственной или частной, финансовой организации или маркетингового агентства создается множество документов. Эти документы могут иметь огромную ценность как для самой компании, так и для ее конкурентов и недоброжелателей. Под угрозой выноса находятся финансовые показатели, кредитные истории, информация о готовящихся слияниях и поглощениях, маркетинговые отчеты и многое другое.

Что и как утекает

Доступ к внутренним документам компании в той или иной степени имеется у каждого сотрудника. Практически в каждой организации есть внутренняя сеть, где хранятся документы различных отделов, существует общая система электронного документооборота, или же документы «кочуют» между отделами на различных носителях (флеш-карты, CD- и DVD-диски) или по электронной почте. У каждой организации есть набор внешних контактеров и контрагентов, куда входят потенциальные и существующие клиенты, парт-



неры, подрядчики, финансовые и государственные институты. Руководство компании имеет право ожидать, что высланный за пределы компании документ с NDA (Non-Disclosure Agreement – договор о неразглашении), эксклюзивным коммерческим предложением или финансовыми данными останется известен только двум сторонам. Однако сегодня в этом нельзя быть уверенным.

Учитывая то, что различные носители информации со временем становятся все дешевле при увеличивающейся емкости, риск выноса большего объема информации увеличивается. Если раньше на дискету можно было сохранить только несколько файлов, то теперь на флеш-карту или съемный диск помещается до нескольких гигабайт информации. В основном причинами утечек информации является халатность

сотрудников, например, сотрудники могут потерять флешку или диск с записанными на них данными. Среди случайных утечек конфиденциальной информации преобладает именно этот канал (мобильные носители информации): по утверждению экспертов¹, он составляет 30% от общего количества. Для сравнения, сетевые способы передачи информации составляют 24%, а электронная почта – 7%. При умышленной же краже документов из корпоративного хранилища чаще используются сетевые способы отправки информации (41%), как ни странно, к ним не относится электронная почта. Возможно, потому, что этот способ напрашивается сам собой: его легко использовать, но легко и выявить. Ведь когда служба безопасности компании решит пересмотреть поток информации из компании, то начнет как раз с электронной почты, так что расследование тут же и закончится. Поэтому злоумышленники используют другие способы выноса информации, в частности на электронных носителях (15%), ведь сегодня намного легче вынести из компании флешку небольшого размера, чем стопку бумажных документов.

Согласно статистике, наиболее частыми объектами утечки информации являются персональные данные (96% известных случаев). Такой вид информации ценится в нелегальном обороте: можно найти базы данных с контактами, персональными сведениями заемщиков, номерами их машин и др. Кроме того, перед ответственностью или заинтересованными лицами могут быть раскрыты такие

¹ По данным InfoWatch.

виды информации, как коммерческая тайна и ноу-хау, государственная или военная тайна. Хотя они и составляют небольшую долю от общего количества утечек, но наносят компаниям огромный ущерб.

Защита электронных документов

Когда говорят о защите электронных документов, достаточно часто вспоминают про электронную цифровую подпись. Однако необходимо помнить, что ЭЦП не является защитой электронного документа в полном смысле этого слова, а скорее является подтверждением его подлинности. Соответственно в случае, если человек или компания не хочет, чтоб информация утекла во вне, нужно защищать не только систему корпоративной информации в целом, но и каждый документ в частности.

Конечно, на большинстве компьютеров офисных работников установлена операционная система Windows, которая позволяет при работе в сетевом пространстве ограничить доступ к файлам определенными сотрудникам или группами лиц. Однако такие виды защиты знающий человек может обойти достаточно легко. В некоторых компаниях предпочитают решать вопрос с возможностью выноса электронного документа кардинально: перекрывая доступ к USB-портам, отключая DVD-приводы или запрещая пересылку файлов по электронной почте. Но в таких ситуациях это только мешает персоналу работать, так как сотрудники не могут быстро обмениваться информацией внутри компании, решать служебные вопросы, высылать документы на согласование и прочее. Чтобы безболезненно решить такую проблему, необходимо использовать для защиты данных специально созданные технологические средства. Важность защиты цифровых документов обусловлена также и тем, что конфиденциальность данных (возможно, персональных) – часть бизнеса, залог успешности любой компании.

Сегодня на рынке информационных технологий существует несколько решений, позволяющих защитить

цифровую информацию, будь то электронная книга, рукопись или корпоративный документ. Однако большинство из них не решает всех проблем. Например, ЭЦП подтверждает подлинность и легитимность документа, однако не препятствует его копированию. Некоторые электронные ключи достаточно надежны, однако их крайне не выгодно использовать при защите малых партий документов, к тому же сразу ограничивают возможность передачи документа нужному лицу.

Оптимальный способ защиты информации

Оптимальным методом решения проблемы может быть использование программного способа защиты электронного документа. Один из таких способов реализуется с помощью ПО StarForce Content от компании StarForce Technologies. При его применении для просмотра защищенного документа нужна определенная программа, которая «привязывается» к характеристикам компьютера и работает только на конкретной машине. Сами документы защищаются таким образом, что их можно просмотреть только в программе, установленной только на данном компьютере.

Такое решение позволяет ограничивать число рабочих мест, на которых можно просматривать защищенный файл, разрешать или запрещать печать документа, ограничивать число просмотров документа или срок действия серийного ключа. Кроме того, существует система отчетов, в которой можно посмотреть, на каком компьютере и когда активирован документ.

Защищенный документ может быть отправлен из организации по электронной почте, записан на диск или выложен в локальную сеть, но открыт он может быть только адресатом, имеющим определенный серийный номер и специальную программу-просмотрщик (вьювер). Вьювер и серийный номер, дающий право открыть и посмотреть документ, предоставляется тем пользователем, который защитил документ. Программу-просмотрщик можно также скачать или получить

по электронной почте, один раз установить на компьютер и далее использовать для открытия других документов, защищенных StarForce Content, имея их серийные номера. Если же пользователь захочет скопировать документ и открыть его затем на другом компьютере, то он не сможет этого сделать, используя тот же серийный номер.

На сегодняшний день защитой электронных документов пользуются в основном компании, занимающиеся продажей электронных книг, распространяющие электронные версии журналов по подписке, а также образовательные учреждения. Остальные коммерческие и государственные институты предпочитают ограничиваться системами контроля доступа к корпоративной сети, системами электронного документооборота и т.д.

Однако необходимо помнить, что лучшей защиты коммерческой тайны или любой другой конфиденциальной информации можно добиться только комплексом мер. Сюда могут входить и контроль доступа, и антивирусная защита, и защита электронных документов, и поведенческий анализ. Существуют и комплексные решения, позволяющие не только отслеживать действия вредоносных программ, но и контролировать самих пользователей корпоративной сети. Одним из таких решений является программа Safe'n'Sec Enterprise Suite (известное решение от компании S.N.Safe&Software). С помощью такого типа решений можно записывать и анализировать действия пользователей в сети, а также запрещать доступ к тем или иным файлам, не позволяя, например, прикрепить документ к электронному письму или запустить то или иное приложение без разрешения. В более общем плане, на страже интересов компании должны стоять не только технологические средства защиты информации. Необходимо решать проблему комплексными мерами IT-, HR- и маркетинговых служб, которые разъясняют и прививают политику безопасности в компании, создают и поддерживают корпоративную культуру, разрабатывают стратегию работы компании на рынке. 