КРИПТОГРАФИЯ: СЛЕДОВАНИЕ СТАНДАРТАМ И ЗАКОНАМ – НЕОБХОДИМОЕ УСЛОВИЕ БЕЗОПАСНОСТИ

Ю. Хитькова, *руководитель отдела Solution Marketing компании «Энвижн Груп»*

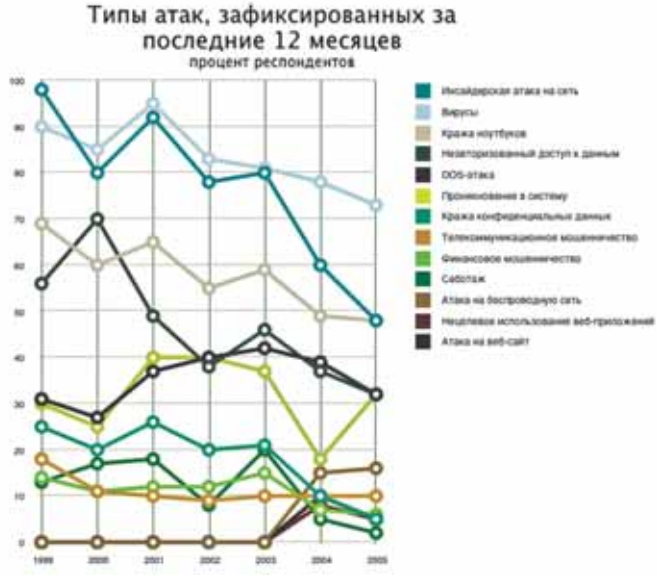
ВВЕДЕНИЕ

По мере того, как Интернет становится частью повседневной жизни большинства людей, необходимость обеспечения безопасности ощущается всё острее. Любая организация, использующая в своей деятельности общедоступные сети, должна считаться с угрозами безопасности и принимать соответствующие меры по их пресечению. Эффективное применение криптографических методов является основой большинства стратегий управления рисками.

Криптографические методы сегодня обеспечивают конфиденциальность и целостность наиболее ценного для любой организации имущества – данных. Иначе говоря, криптография осуществляет преобразование читаемых данных в бессмысленный набор символов, сохраняя при этом возможность восстановления исходной информации.

В 1995 году, с появлением в России Федерального закона «Об информации, информатизации и защите информации» был снят ряд ограничений на импорт западных средств криптографической защиты информации (далее – СКЗИ). Это решение позволило российским компаниям-разработчикам конкурировать с ведущими западными производителями. Однако, как показала практика использования СКЗИ в РФ, отечественные разработки в этой области никогда не будут вытеснены с российского рынка хотя бы потому, что соответствующие ведомства в РФ предъявляют повышенные, иногда очень жесткие требования к производителям средств криптографической защиты и алгоритмов.

Индустрия безопасности за короткое время сильно выросла, появилось много новых возможностей для внедрения методов обеспечения электронной безопасности на основе криптографии – от новых криптографических аппаратных средств до применения смарт-карт в инфраструктурах открытых ключей. Эта статья даст читателю возможность оценить, каким стандартам должны соответствовать системы информационной безопасности, в состав которых входят СКЗИ, а также на какие сертификаты стоит обращать внимание при выборе криптографических средств, чтобы впоследствии воспользоваться этими знаниями при их практическом использовании.



Источник: Отчет по компьютерной преступности ФБР, 2005 г.

ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ЭЛЕКТРОННОЙ БЕЗОПАСНОСТИ

Одним из наиболее полезных инструментов для обеспечения безопасности является криптография. Разработчики и инженеры отдела информационной безопасности (ИБ) компаний должны иметь представление о криптографии, чтобы эффективно использовать ее для повседневной защиты корпоративных данных. Лица, принимающие решения, должны знать о криптографии, чтобы делать осознанный выбор. Системные интеграторы должны разбираться в криптографии, чтобы должным образом встраивать ее в свои системы и предлагать квалифицированные услуги, связанные с поиском адекватной для клиента технологии. Даже юристы должны иметь представление о криптографии, поскольку в нашей стране существуют и действуют законы, определяющие ответственность субъектов, хранящих частную и общественную информацию и использующих для этого СКЗИ в рамках собственных информационных систем.

Государственные организации, работающие с информацией, содержащей государственную тайну, обязаны использовать СКЗИ в рамках национальной безопасности. Коммерческие предприятия также имеют свои секреты: стратегические планы развития, прогнозы объемов продаж, техническая информация, относящаяся к производимой продукции, результаты исследований, списки персонала и др. Большинство фирм воспринимают СКЗИ как «ключ», который позволит закрыть

дверь в мир ценной информации с целью защиты от нечестных людей. Эти «злоумышленники» могут работать на конкурентов, или же являться сотрудниками фирмы, имеющими нечестные намерения, или же быть хакерами или взломщиками («крэкерами»), то есть людьми, которые проникают в компьютерные сети для похищения информации, совершения актов вандализма, создания помех для нормальной работы либо просто, чтобы показать, на что они способны.

В этих случаях криптография позволяет эффективно решить ряд важнейших проблем информационной безопасности компьютерных сетей и систем. Считается, что если злоумышленник преодолел все рубежи защиты (контроль доступа, аудит и т. п.), то криптография создаст последний барьер на его пути.

Криптография «вступает в бой» после того, как злоумышленнику удалось:

- получить локальный или физический доступ к компьютеру, на котором обрабатывается конфиденциальная информация, или сетевой доступ к ПК;
- обойти систему обнаружения вторжений, а также подсистемы идентификации, аутентификации и авторизации;
- не оставить следов в журнале аудита.

Именно на этом этапе злоумышленник чаще всего сталкивается с криптографией: он вошел в систему, нашел интересующий его файл, а содержимое файла зашифровано. Конечно, грамотно созданная система подключит криптографию к процессу защиты данных намного раньше, например, на этапе аутентификации будут использованы не регистрационное имя пользователя и пароль, а, скажем, смарт-карта и цифровой сертификат стандарта X.509 и т. д.

Однако криптография не решает всех задач, связанных с безопасностью. Это лишь одно средство из многих. Более того, криптография не обладает «защитой от дурака». Любой шифр может быть раскрыт, и, что еще более важно, при некорректной реализации криптография не обеспечит вас реальной защитой. Основная задача компаний сегодня – это использование стандартов и законов при построении систем информационной безопасности. Только в этом контексте СКЗИ принесут реальную пользу и отдачу на инвестиции.

СТАНДАРТЫ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правильно сформулировать корпоративную стратегию в области управления информационной безопасностью стремятся все компании, независимо от того, какие цели и задачи преследует построение системы защиты. Однако практика показала, что создать действительно качественное решение, удовлетворяющее текущим и будущим задачам организации, смогли только единицы. Причина неудач кроется в том, что ИБ принадлежит к ресурсоемким процессам для формулирования политики и средств ее реализации, являясь в то же время одним из самых передовых направлений с точки зрения применения информационных технологий – и в мире, и на отечественном рынке.

Информационная безопасность сегодня – это комплекс организационных, программных, технических и физических мер, обеспечивающих достижение следующих свойств информационных ресурсов: целостности, конфиденциальности, доступности и аутентичности. Из всех свойств, на наш взгляд, дополнительного пояснения может потребовать только термин «аутентичность», то есть свойство, которое обеспечивает подлинность субъектов и объектов доступа к информации.

Качество корпоративной системы управления ИБ будет определяться уровнем безопасности ее наименее защищенного компонента. Корпорациям пришлось усвоить трудный урок: можно легко получить доступ к данным, ознакомиться с ними, изменить их или уничтожить, если не обеспечена правильная защита. Соответственно, при построении системы защиты компании должны ставить во главу угла не достижение всех свойств информационных ресурсов, а специфику собственного бизнеса. Например, для операторов связи основной задачей в области ИБ является обеспечение пропускной способности каналов, то есть доступности информационных ресурсов. Для государственных клиентов это, конечно же, конфиденциальность информации, чего невозможно достигнуть без СКЗИ.

Можно по-разному реализовывать проект в области построения системы ИБ, однако качественная система всегда строится, мы повторимся, на основе стандартов, правил и законов. При реализации системы управления информационной безопасностью необходимо придерживаться требований стандарта BS 7799, признанного де-факто и определяющего спецификацию будущей системы. Система ИБ, реализованная в соответствии с BS 7799, обеспечит наличие проверенной и надежной структуры, которая инициирует, поддерживает и управляет рабочим состоянием информационной безопасности внутри предприятия.

Ключевым элементом системы ИБ является система управления рисками. Это подразумевает аудит ин-

Источник: Отчет по компьютерной преступности ФБР, 2005 г.

формационной системы и определение наименее защищенных ресурсов, потенциальных рисков и способов защиты. Практика показала, что компаниям не стоит слепо верить в жизнеспособность своей инфраструктуры и уповать на счастливый случай или приобретенные и установленные СКЗИ, а больше доверять системному подходу к решению задачи, процедурам и апробированным методологиям, где затраты всегда оправданны.

Дальнейшие этапы развития системы ИБ связаны с технологическими аспектами создания системы защиты, где надлежит учитывать особенности используемых информационных технологий и требования бизнеса, так как только в этом случае можно гарантировать, что средства и методы защиты информации будут минимизировать актуальные риски и противодействовать угрозам ИБ. Кроме того, необходимо предусмотреть процедуры по технической поддержке внедренного комплекса информационной защиты в соответствии с динамическими изменениями компании.

СЕРТИФИКАЦИЯ СКЗИ В РФ

Сегодня существует целый ряд компаний, предлагающих свои разработки в области СКЗИ для создания надежных систем информационной безопасности. Однако уже в течение многих лет их усилия не дают желаемого результата и гарантий. Суть проблемы заключается в том, что только единицы отечественных компаний заслужили право продвигать на рынок свои разработки – как отдельные криптографические алгоритмы, так и СКЗИ (имея на то соответствующую лицензию).

Многие клиенты столкнулись с ситуацией, когда им предстояло выбрать из двух сертифицированных версий одного и того же решения в области СКЗИ. При этом первая версия продукта обладала сертификатом одного ведомства, а вторая – сертификатом другого. Какая же версия решения является правильной с точки зрения использования?

Начнем с ведомств, занимающихся сертификацией решений в области СКЗИ. В настоящее время в нашей стране сертификацию средств защиты информации и аттестацию объектов проводят два ведомства. Это ФСТЭК (Федеральная служба по техническому и экспортному контролю) и ФСБ России. ФСТЭК сертифицирует не криптографические, а только комбинаторно-перестановочные (то есть вероятностные) методы защиты информации (например, оценивает вероятность подбора злоумышленником пароля, исходя из реализованных в продукте требований к его качеству). Таким образом, сертификация СКЗИ, равно как и продуктов, использующих криптографию, – зона полномочий исключительно ФСБ России.

Тем не менее рынок сегодня предлагает огромный выбор тех или иных средств, способных решить даже самые нетривиальные задачи. Связано это с тем, что многие ИТ-компании, в том числе и западные, пошли по пути встраивания уже имеющегося СКЗИ от стороннего производителя в свой продукт. Для этого компаниям потребовалось получить от ФСБ лицензии на проектирование, техническое обслуживание и сопровождение, а также на распространение продукта. Чтобы понять, насколько грамотно и корректно разработчик встроил имеющийся функционал СКЗИ в свой продукт, ФСБ России регулярно проводит экспертную оценку предлагаемых систем. Например, многие разработчики систем защищенного документооборота используют в своих продуктах криптографические возможности КриптоПро CSP для формирования и проверки электронной цифровой подписи документа и/или его шифрования.

Средства криптографической защиты, принятые в западной практике, хотя и нашли массовое применение в России, но «проглядели» потенциальную угрозу: они могут остаться «в тени закона», то есть являться нелегальным программным обеспечением, так как, повторимся, в нашей стране регламентируется использование сертифицированных средств криптографической защиты информации. Однако западные продукты могут быть разрешены к импорту (на основании экспертного заключения ФСБ России, лицензий ФСБ и Минэкономразвития России) и, соответственно, к использованию. Но при проектировании корпоративной автоматизированной системы, в состав которой они входят, их криптографический функционал зачастую задействован быть не может: это трактуется как нарушение закона.

ЗАКЛЮЧЕНИЕ

Прошедшие два десятилетия были периодом интенсивного развития компьютерной индустрии, но и число случаев, связанных с незаконными вторжениями, значительно возросло. При неправильной организации защиты компаниям грозит потеря данных, раскрытие секретной информации, утрата репутации, финансовые потери. Но самое страшное – это разочарование от бессмысленно потраченных инвестиций.

В заключение следует отметить, что технология, даже самая лучшая, не обеспечит стопроцентную защиту бизнеса. Даже если ваша компания остановит свой выбор на, казалось бы, самом серьезном инструменте защиты, которым является СКЗИ, это не убережет вас от других рисков, например, риска использования незаконных с точки зрения действующего законодательства средств. Таким образом, самый плодотворный подход для организаций, занимающихся построением системы безопасности, – это изучить всё то, что известно нарушителям, чтобы остановить их, и выбрать такой инструмент, который будет способен максимально защитить компанию, а его применение не будет являться нарушением с точки зрения закона.