вся жизнь – игра

методика оценки рисков при использовании пластиковых карт

Основное направление развития безналичных расчетов предполагает широчайшее использование пластиковых карт международных платежных систем. Данные пластиковые карты являются удобным платежным средством для выполнения расчетов в торговых предприятиях, средством получения наличных денег в банкоматах, а также для выполнения операций по вкладам в различных финансовых учреждениях.

Бузин А.А.
аспирант кафедры информационной безопасности Российского государственного социального университета

С каждым годом во всем мире неуклонно возрастает объем использования пластиковых карт. Однако их использование в качестве инструмента безналичных расчетов за товары и услуги сопровождается определенными рисками, под которыми понимается возникновение финансовых потерь из-за совершения ряда мошеннических действий с конфиденциальной информацией, содержащейся на пластиковых картах и передающейся по каналам связи между участниками безналичных расчетов.

Поэтому всем участникам безналичных расчетов (банками-эквайерами, банкам-эмитентам, торговым предприятиям, платежным системам) постоянно необходимо повышать эффективность обмена конфиденциальной информацией пластиковых карт для совершенствования системы экономической безопасности безналичных расчетов с использованием данного вида финансовых инструментов, которые одновременно являются и финансовыми документами.

Такая эффективность обмена может быть достигнута за счет рационального применения

средств защиты (СЗ) информации, под которыми понимаются аппаратные, программные средства или материалы, используемые для защиты информации.

Одним из возможных решений данного вопроса является использование *средств криптографической защиты информации* (СКЗИ). Характерной особенностью этих средств является то, что при построении информационно-телекоммуникационных систем именно криптографические методы обеспечивают наиболее высокий уровень эффективности обмена конфиденциальной информацией пластиковых карт между участниками безналичных расчетов.

К настоящему времени разработано большое количество различных методов шифрования, и подавляющие их число может быть успешно использовано для решения поставленной задачи. Криптографические методы реализуются либо программным, либо аппаратным способом.

При *аппаратной* реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами в отдельных устройствах. Наибольшее распространение получили комбинированные модули, реализующие одновременно криптографические алгоритмы DES (Data Encryption Standard), Triple DES, RSA (Rivest, Shamir, Aldeman). Возможность же *программной* реализации обуславлена тем, что все методы криптографического преобразования формальны и могут быть представлены конечным детерминированным алгоритмом. Однако следует отметить, что между программными и аппаратными способами защиты информации имеется ряд существенных различий.

Перечислим сначала преимущества аппаратных и аппаратно-программных способов защиты, которые:

- позволяют физически и логически изолировать узлы, в которых хранятся и обрабатываются секретные объекты системы защиты (ключи, а также модули, выполняющие наиболее важные операции защиты, – шифраторы);
- резко затрудняют, а часто и полностью исключают возможность логического доступа к за-

эффективность обмена конфиденциальной информацией пластиковых карт может быть достигнута за счет рационального применения средств защиты информации

щищаемым компонентам со стороны любых субъектов (во многих случаях только аппаратные средства обеспечивают надежную защиту от несанкционированных действий квалифицированного персонала, в том числе злоумышленников, системных администраторов и программистов);
- более устойчивы к несанкционированной модификации их параметров и хранимых данных;
- относятся к специализированным средствам - каждое из них в отличие от универсальных систем общего применения выполняет одну заданную функцию (защиту и проверку специализированных устройств выполнить существенно проще, чем универсальных).

Основные преимущества аппаратных и аппаратно-программных средств защиты концентрированно выражает концепция так называемых *модулей безопасности*, т.е. физически и логически изолированных электронных устройств, выполняющих функции защиты и хранящих секретные параметры (примером являются используемые банками-эквайерами и банками-эмитентами модули HSM компаний Thales и Eracom для шифрования/дешифрования ПИН-кода). При создании таких модулей выполняются следующие процедуры:
- принимаются меры по защите от физического доступа к электронным узлам (используются корпуса повышенной прочности, секретные болты крепления и т.д.);
- затрудняется восстановление алгоритмов их функционирования (удаляется маркировка с электронных компонентов, применяются заказные и специализированные микросхемы);
- предусматривается стирание секретных данных при попытках вскрытия корпуса устройства.

Для аппаратных решений основным способом криптографических преобразований является осуществление многошаговых процедур модифицирования исходного блока данных под управлением секретного ключа (обычно от 64 до 256 бит), размещенного не в основной памяти ЭВМ, а в аппаратном модуле.

криптографические методы реализуются либо программным, либо аппаратным способом

Однако применять аппаратные модули следует

с учетом анализа экономической эффективности системы защиты в целом, так как их приобретение и использование характеризуется большими материальными затратами – цены на них варьируются от 4000 до 45000 долларов США. В связи с этим массовое использование банками таких модулей является нецелесообразным с экономической точки зрения, так как для обеспечения эффективного обмена конфиденциальной информацией пластиковых карт потребуется установка отдельного модуля на каждом терминальном устройстве (банкомате, POS-терминале, кассовом терминале), что, естественно, является просто не осуществимым из-за сверхмасштабных материальных затрат.

Программная реализация криптографических алгоритмов позволяет получить следующие положительные эффекты:

- создать инструмент криптографической защиты для широкого использования в области обмена конфиденциальной информацией пластиковых карт;
- существенно уменьшить финансовые затраты на криптографическую защиту конфиденциальной информации пластиковых карт при использовании более дорогих аппаратных средств;
- сократить сроки разработки защищенных систем для передачи конфиденциальной информации пластиковых карт и ввода их в действие.

Таким образом, использование именно программных средств криптографической защиты информации (ПСКЗИ) для обеспечения эффективного обмена конфиденциальной информацией пластиковых карт позволяет получить значительный экономический эффект благодаря предоставлению удобных и надежных средств программного шифрования, упрощающих решение многочисленных практических задач защиты конфиденциальной информации пластиковых карт и заменяющих более дорогие аппаратные средства.

Однако практика функционирования системы безналичных расчетов показывает, что достижение почти стопроцентного уровня эффективности обмена конфиденциальной инфор-

применять аппаратные модули следует с учетом анализа экономической эффективности системы защиты в целом

мацией пластиковых карт не всегда оправдано экономически. Стоимость средств защиты информации (СКЗИ, ПСКЗИ) составляет, как правило, около 10-15 процентов от общих затрат на построение и эксплуатацию информационных систем в целом. А так как стоимость систем составляет нередко миллионы, а подчас десятки миллионов долларов США, то сумма получается весьма солидной.

Учитывая глубокую дифференцированность банковских структур по масштабам бизнеса, а также экономический аспект в соотношении стоимости организации эффективного обмена конфиденциальной информацией пластиковых карт и величины убытков, возникающих в результате мошеннического использования данной информации, необходимо оценивать *целесообразность вложения средств* в организацию эффективности ее обмена. Рассмотрим этот вопрос. Для этого введем следующие обозначения:

$D_з$ – убытки, возникающие в результате мошеннического использования конфиденциальной информации пластиковых карт для защищающейся стороны;

$D_а$ – финансовая прибыль, получаемая в результате мошеннического пользования конфиденциальной информацией пластиковых карт атакующей стороной;

$S_з$ – средства, выделяемые на организацию эффективного обмена конфиденциальной информацией пластиковых карт;

$S_а$ – средства, выделяемые на добывание конфиденциальной информации пластиковых карт;

$P_з$ – вероятность успеха защищающейся стороны;

$P_а$ – вероятность успеха атакующей стороны.

Очевидно, что нерентабельно вкладывать в организацию эффективного обмена конфиденциальной информацией пластиковых карт или ее добывание средств больше, чем составляет реальная величина убытков или, соответственно, финансовой прибыли. Кроме этого, следует также учитывать и вероятности того, что атакующей стороне удастся получить доступ к конфиденциальной информации пластиковых карт, а защищающейся стороне удастся обеспе-

чить ее защиту.

Исходя из этих соображений, сумма средств, выделяемых на организацию эффективного обмена конфиденциальной информацией пластиковых карт или ее добывание, не должна быть больше финансовой выгоды в случае успеха:

$$S_З \le P_A D_З , \quad (1)$$
$$S_A \le P_З D_A . \quad (2)$$

Вероятности сложно оценить, поскольку они зависят от действий противоборствующих сторон - финансовых средств ($C_З$ и C_A), выделяемых, соответственно, на организацию эффективного обмена и добывание конфиденциальной информации пластиковых карт, а также от технических возможностей защищающейся и атакующей сторон (данные возможности будут определяться весовыми коэффициентами $k_З$ и k_A). Исходя из этого, определим значения вероятностей $P_З$ и P_A следующим образом:

$$P_З = \frac{k_З \cdot S_З}{k_З \cdot S_З + k_A \cdot S_A} , \quad (3)$$

$$P_A = \frac{k_A \cdot S_A}{k_З \cdot S_З + k_A \cdot S_A} . \quad (4)$$

Для того чтобы оценить, сколько средств разумно вложить в организацию эффективного обмена конфиденциальной информацией пластиковых карт, подставим значение вероятности успеха атакующей стороны (4) в (1):

$$k_З \cdot S_З^{\,2} + k_A \cdot S_З \cdot S_A - k_A \cdot S_A \cdot D_З \le 0 . \quad (5)$$

Предполагая, что сумма средств, выделенная атакующей стороной на добывание конфиденциальной информации, равна величине убытков, возникающих в результате мошеннического использования данной информации ($S_A=D_З$), и технические возможности атакующей и защищающейся сторон равны ($k_З=k_A$), упростив выражение 5, получим зависимость допустимых затрат на организацию эффектив-

достижение почти стопроцентного уровня эффективности обмена конфиденциальной информацией пластиковых карт не всегда оправдано экономически

нерентабельно вкладывать в организацию эффективного обмена конфиденциальной информацией пластиковых карт больше, чем составляет реальная величина убытков

ного обмена конфиденциальной информацией пластиковых карт от величины убытков, возникающих в результате мошеннического использования данной информации:

$$S_3 \leq 0{,}6 \cdot D_3 \qquad (6)$$

Точность данной модели оценки затрат, требуемых для организации эффективного обмена конфиденциальной информацией пластиковых карт, зависит от того, насколько точно можно сформулировать вероятность успеха в формулах (1) и (2).

В случае отсутствия возможности оценки вероятности успеха и в предположении равных условий для атакующей и защищающейся сторон, сумму затрат на организацию эффективного обмена конфиденциальной информацией пластиковых карт S_3 (6) можно рассматривать как максимальный экономически обоснованный предел.

вся жизнь — игра

Литература

1. Андреев А.А. Пластиковые карты. – 2-е издание, переработанное и дополненное. – М.: Изд. Концерн «Банковский Деловой Центр», 1998. – 312 с.

2. Симонов С.В. Методология анализа рисков в информационных системах. // Информационно – методический журнал «Защита информации. Конфидент» – Спб.: Изд. Конфидент, 2001, №1, с. 72 – 75.

3. Карасев Р.Ю. Моделирование оценки затрат, требуемых для обеспечения защиты информации. // Сборник научных трудов – Ст.: Изд. СевКавГТУ, 2004, №1.

4. Логинов А.Л., Елхимов Н.С. Электронные расчеты и платежи: Общие принципы функционирования международных электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества. // Информационно – методический журнал «Защита информации. Конфидент» – Спб.: Изд. Конфидент, 1995, № 2, с. 48 – 54.

5. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. Методические материалы. – М.: Изд. МИФИ, 1997. - 274 с.