БЕЗОПАСНОСТЬ ПЛАТЕЖНОЙ СИСТЕМЫ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ

Царегородцев Анатолий Валерьевич,
Заведующий кафедрой Информационной безопасности, д.т.н., профессор,
Всероссийская государственная налоговая академия Минфина РФ
academic_tsar@mail.ru

Аннотация. *В статье рассматривается один из подходов к обеспечению защиты от масштабных атак на платежную систему и от угроз конкретным участникам платежной системы: банкам, клиентам, пунктам предоставления услуг, обслуживания населения и др.*

Ключевые слова: *инфокоммуникационная система, платежная система, управление доступом, интеллектуальные карты.*

PAYMENT SYSTEM SECURITY BASED ON INTELLIGENT CARD

Tsaregorodtsev Anatoly Valerievich,
Russian State Tax Academy Ministry of Finance RF
Head of Information Security Department, Doctor of Science (Eng.), Professor

Abstract. *The approach of payment system protection from large-scale attacks and protection from the threats to the participants of the payment system: banks, clients, point of service, public services, are considered in this article.*

Keywords: *infocommunication systems, payment system, access control, smart cards.*

Введение

В настоящее время практически все информационно-коммуникационные системы (ИКС) корпораций, так или иначе, имеют в своей основе распределенные хранилища (банки) данных, предоставляющие возможность оперативного доступа к данным из любой точки сети. Но это несомненное удобство в работе становится весьма спорным, если принимать во внимание вероятность информационной атаки, под которой следует понимать любое несанкционированное воздействие на ИКС. В этих условиях информационные ресурсы представляют собой огромную материальную ценность, а несанкционированный доступ к ним, если они недостаточно защищены, может привести к глобальным катастрофам или, в условиях конкуренции корпораций, фирм и целых государств, может радикально изменить ситуацию в пользу тех, кто получил такой доступ.

Надо сказать, что в нашей стране решен вопрос о защите информации, содержащей сведения, составляющие государственную тайну. Однако, именно конфиденциальные сведения, не содержащие государственную тайну, составляют львиную долю информации, циркулирующей в ИКС в кредитно-финансовой сфере страны. При этом ущерб от утечки или искажения экономически значимой конфиденциальной информации может быть ничуть не меньше, чем в случае утраты сведений, составляющих государственную тайну [2].

1. Угрозы безопасности информации в кредитно-финансовой сфере

Прежде чем рассмотреть угрозы безопасности информации в кредитно-финансовой сфере и меры по защите информационных ресурсов от этих угроз, определим, что же представляет собой платежная система страны.

Под *платежной системой* будем понимать совокупность юридических, организационных, технологических, технических и информационных средств, обеспечивающих проведение расчетов

между субъектами банковской системы в стране. Платежная система представляет собой механизм, через который обязательства, возникающие в результате экономической деятельности, выполняются посредством перевода денежных средств [3]. Систему платежей можно представить в виде структуры, включающей различных участников, предоставляющих и использующих платежные средства:

- в основе этой структуры находятся предприятия и частные лица, обменивающиеся безналичными деньгами и имеющие счета в банках;
- посредником в этой системе являются коммерческие банки (КБ), предоставляющие в распоряжение участников средства платежа и осуществляющие перевод финансовых средств;
- в вершине этой структуры находится Центральный банк России (ЦБ РФ).

Основными объектами обеспечения безопасности в обобщенной модели платежной системы являются финансовые организации (банк-эмитент, банк-эквайер, клиринговый центр и т.д.), процессинговый центр обработки транзакций (ПЦОТ), производящий обработку транзакций в платежной системе, терминальное оборудование (торговые терминалы, банкоматы и другое оборудование), предназначенное для непосредственных операций с банковскими карточками и передачи информации в центр обработки транзакций, платежная пластиковая карта и ее владелец (клиент), транспортная подсистема, объединяющая указанные выше компоненты, прикладная подсистема, обеспечивающая согласованную работу автоматизированных средств обслуживания финансовых операций.

В целом участники платежной системы заинтересованы в обеспечении своей информационной безопасности, причем не любыми средствами, а в зависимости от величины ущерба, в общем случае потенциального, который им может быть нанесен.

Исходя из интересов участников платежной системы и структуры автоматизированной информационной системы, рассмотрим наиболее характерные угрозы информации в платежной системе:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступа;
- несанкционированное копирование программ и данных;
- перехват и последующее раскрытие конфиденциальной информации, передаваемой по каналам связи;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- случайное или умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи, в том числе и навязывание ранее переданного сообщения;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- ошибки в работе обслуживающего персонала;
- разрушение файловой структуры из-за некорректной работы программ или аппаратных средств;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования;
- ошибки в программном обеспечении;
- сбои оборудования, в том числе и за счет отключения электропитания и других факторов, препятствующих работе оборудования.

Опыт показывает, что гарантированную защиту от несанкционированного доступа к подлежащей защите финансовой информации, циркулирующей в платежной системе, можно обеспечить только при условии возможности проведения исчерпывающего анализа реализованных в этой системе аппаратно-программных и организационно-технических решений. Возрастающие убытки банков в результате использования платежных пластиковых карт подтверждают неоспоримый факт: пластиковая карта – инструмент повышенного риска. Определенные возможности для мошенничества предопределены здесь самой сущностью технологии, основанной

на доверии между банком и клиентом, а также на технических особенностях функционирования пластиковых карт, таких как степень защиты, характеристики карты (магнитная полоса, ЧИП), коммуникационные возможности банка-эмитента и банка-эквайера, технологическое обеспечение торгово-сервисной сети. Безопасность такой платежной системы требует комплексного подхода, включающего в себя ряд аспектов: правовой и технической поддержки, стандартизации моделей, средств и методов защиты [4].

Основными принципами защиты информации (ЗИ) в платежной системе являются:

- конфиденциальность передаваемой и хранимой информации, включая информацию на всех материальных носителях, используемых в платежной системе;
- целостность хранимой и передаваемой информации в платежной системе;
- доверенная программно-техническая платформа функционирования прикладной подсистемы (производящей расчеты) и подсистемы защиты;
- защита от несанкционированного доступа к компонентам (аппаратным и программным) расчетной системы;
- организационно-техническая и правовая поддержка функционирования платежной системы;
- аппаратная поддержка работы средств защиты;
- изготовление ключевых компонентов (исключая персональную идентифицирующую информацию) специализированной организацией;
- единая политика администрирования и управления защитой объектов платежной системы.

Основные архитектурные решения платежной системы связаны с использованием интеллектуальных карт (ИК) отечественной и импортной разработки; операционных сред общего применения, в том числе и содержащих механизмы защиты; прикладного программного обеспечения и модулей российского и иностранного производства.

Для реализации изложенных принципов необходимы [2]:

- проектирование программно-аппаратных компонентов платежной системы, исходя из принципа изолированности модулей и обеспечения механизма виртуального взаимодействия;
- обеспечение подсистем защиты от НСД информации во всех компонентах платежной системы, начиная от уровня терминала с механизмами идентификации и аутентификации пользователей, а также контроль доступа к локальным и удаленным ресурсам системы, создание журнала событий;
- аппаратная поддержка аутентификации операторов платежной системы, невозможность использования их собственного программного обеспечения, включая и операционную среду;
- зашита подлинности и целостности транзакций в платежной системе с применением криптографических алгоритмов, базирующихся на отечественных стандартах ГОСТ Р 28147-89 и ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, реализация механизма гарантированного завершения и учета транзакций в платежной системе;
- организация централизованной службы управления ЗИ, ответственной за использование ключевых элементов средств защиты платежной системы, аудирование и устранение нештатных ситуаций, возникающих при работе платежной системы, формирование единой политики безопасности системы;
- реализация надежного механизма персонализации владельца ИК и взаимной идентификации ИК и терминального оборудования с использованием упомянутых криптографических алгоритмов.

2. Новые направления, стимулируемые банковскими приложениями

Широкомасштабное проникновение в банковскую сферу России зарубежных карточных технологий приводит к оттоку средств коммерческих банков-эмитентов в зарубежные расчетные банки и процессинговые компании. Для нормального развития отечественных технологий в данной сфере организовано серийное производство российских ИК различного применения. Следует отметить, что иностранные фирмы-производители кристаллов и карт, детально публикуя перечень потребительских характеристик, тем не менее, специальные характеристики относят к конфиденциальной информации. И хотя часть из них может быть предоставлена партнеру на условиях заключения договора о неразглашении (например, некоторые параметры алгоритмической и физической защищенности), все-таки существенная часть специальных характеристик,

как правило, не разглашается, делая практически невозможным обоснование надежности защиты карт и их сертификации.

Таким образом, государственная политика в сфере информатизации потребовала создания и организации серийного выпуска российских ИК, обеспеченных надежной защитой и криптографической компонентой на основе отечественных стандартов [4].

Российская интеллектуальная карта (РИК) выполнена на основе микроконтроллера КБ5004ВЕ1 с операционной системой UniCos.

Микроконтроллер КБ5004ВЕ1 является оригинальной разработкой ОАО «Ангстрем». Его ядром является восьмиразрядный RISC-процессор с одноуровневым конвейером на три команды, имеющий встроенный тактовый генератор с частотой около 15 МГц. В состав контроллера также входят ОЗУ объемом 256 байт, масочное ПЗУ команд объемом 16 Кб (8Кх16 бит) и энергонезависимая память на 2 Кб, обеспечивающая 100 тыс. операций перезаписи и хранение информации в течение 10 лет.

Применение конвейера и двухмагистральной структуры позволяет микроконтроллеру выполнять любую команду за два такта. При этом в отличие от большинства процессоров, использующих конвейер, при выполнении команды перехода его содержимое не теряется, а значит, время выполнения команд не увеличивается. А за счет того, что собственная тактовая частота микроконтроллера как минимум втрое превышает частоту тактовых импульсов, поступающих от POS-терминала или банкомата, любая команда процессора выполняется менее чем за один такт этих устройств (для сравнения: контроллер SLE 44Cx0 такого известного производителя, как Siemens, выполняет одну команду не менее чем за шесть тактов). Это существенный момент при выполнении криптографических операций, которые реализуют алгоритм шифрования по ГОСТ 28147-89 в защищенном исполнении со скоростью до 5 Кб/с.

Так как ЭСППЗУ имеет большое время записи (порядка 3-5 мс), чтение и запись в него производится многоразрядными блоками. При этом запись информации в ЭСППЗУ осуществляется параллельно с работой процессора.

Микроконтроллер КБ5004ВЕ1 имеет высокую степень защиты от несанкционированного доступа к информации, хранящейся на карточке. Это достигается с помощью следующего комплекса мер:

- кристалл не имеет точек подключения, кроме предусмотренных стандартом ISO 7816-3;
- использование средств самотестирования для отбраковки при производстве и при каждом включении кристалла;
- специальные меры по предотвращению снятия информации и анализа работы кристалла;
- меры противодействия вводу микроконтроллера в нештатный режим работы путем внешних воздействий.

Особое место в развитии РИК имели работы по введению в микроконтроллер РИК программно-аппаратных средств, позволяющих эффективно реализовывать асимметричные криптографические алгоритмы, в частности стандарт электронной цифровой подписи ГОСТ Р-34.10. Разумное сочетание симметричной и открытой криптографии по разработке конкретных систем защиты на базе РИК позволило обеспечить криптографически стойкую и эффективную в администрировании систему безопасности. В первую очередь это повысило специальные и эксплуатационные свойства платежных систем – позволило существенно передвинуть центр тяжести защиты электронных платежей с физической защиты модуля безопасности к его криптографической защите.

По условиям эксплуатации микроконтроллер удовлетворяет одному из отраслевых стандартов на микросхемы военного применения (диапазон рабочих температур составляет от – 65 до 85^{0}С), что значительно превышает требования стандарта ISO и в большей степени соответствует российским климатическим условиям.

Операционная система UniCos имеет следующие характеристики:

- соответствие стандарту ISO 7816-4;
- криптографические протоколы на основе алгоритма ГОСТ 28147-89;
- гибкая система разграничения доступа;
- возможность встраивания дополнительных функций;
- внутреннее самотестирование;
- система защиты от сбоев.

Операционная система обеспечивает платформу, которая позволяет реализовать на РИК весь спектр приложений для осуществления безналичных расчетов с использованием платежных карт, в том числе: электронный кошелек, электронный чек, дебетовая карта, карта продавца, телефонная карта и другие.

Система информационной безопасности РИК основывается на системе физической безопасности кристалла микроконтроллера и дополняется программно-алгоритмическими мерами защиты, реализованными в составе криптографического модуля и операционной системы.

Средствами операционной системы РИК реализуются алгоритмические меры защиты, такие как тестовые проверки при включении питания карты, криптографическая защита данных, контроль их целостности и др.

Криптографическая компонента операционной системы помимо ГОСТ 28147-89 включает также алгоритмы DES и TripleDES. В карте имеется встроенный программно-аппаратный датчик случайных чисел, обеспечивающий поддержку со стороны РИК надежных криптографических протоколов взаимной аутентификации и выработку разовых сеансовых ключей шифрования данных для взаимодействия с терминальным оборудованием.

Система разграничения доступа ОС UniCos РИК позволяет:

- создавать файлы с однократной записью;
- разрешать чтение файла только после предъявления пароля и/или осуществления криптографической аутентификации;
- разрешать добавление данных в файл только после предъявления пароля и/или осуществления криптографической аутентификации;
- разрешать модификацию данных в файле только после предъявления пароля и/или осуществления криптографической аутентификации;
- зашифровывать передаваемые данные и расшифровывать получаемые на ключе, записанном в карту;
- обеспечивать защищенный обмен данными между терминалом и картой с помощью шифрования (дешифрования) на сеансовом ключе, вычисляемом в результате проведения криптографической аутентификации;
- снабжать передаваемые данные криптографической имитовставкой, обеспечивающей контроль целостности, при этом имитовставка может быть выработана как на ключе, записанном в карту, так и на сеансовом ключе.

Разработанная карточка следующего поколения (РИК-2) обладает рядом дополнительных функций и работает еще быстрее как за счет внедрения нового технологического процесса с проектной технологической нормой 0.5 мкм (что позволило увеличить тактовую частоту), так и за счет того, что в состав микроконтроллера вошел дополнительный сопроцессор, обеспечивающий более высокую скорость выполнения криптоопераций.

ОС РИК-2 обеспечивает:

- возможность односторонней и взаимной аутентификации карты и внешнего устройства на основе методов симметричной криптографии;
- возможность идентификации владельца карты на основе секретного кода (пароля);
- функции шифрования/расшифрования данных на основе российского криптоалгоритма ГОСТ 28147-89;
- функцию выработки имитовставки;
- функцию диверсификации ключей;
- возможность проверки целостности масочного ПЗУ программ микроконтроллера криптографическими методами.
- структурированный доступ к информации, хранящейся в энергонезависимой памяти карты;
- возможность криптографически защищенного обмена информацией между картой и терминальным оборудованием;
- возможность использования карты в качестве шифратора данных.

Свои функции ОС РИК-2 реализует посредством выполнения команд, подаваемых карте внешним устройством (ВУ).

ОС обеспечивает обмен карты с внешним устройством с использованием протокола передачи данных T0 в соответствии с ISO 7816-3. Допускается передача блоков данных размером до 64 байт в обоих направлениях. Тип обмена (тип кодировки) - прямой. Логический интерфейс обмена данными карты с внешним устройством (ВУ), реализованный в ОС РИК-2, соответствуют международному стандарту ISO 7816-4.

Заключение

С учетом функциональных характеристик *российской интеллектуальной карты* и реализованных возможностей защиты от несанкционированного доступа к хранимой в ней информации, в целом отвечающих зарубежным аналогам, *в платежных системах* в сочетании с необходимыми системными

мерами информационной безопасности она способна обеспечить защиту как от масштабных атак на платежную систему с целью ее дезорганизации и наводнения системы фальшивыми платежными карточками, так и от угроз конкретным участникам платежной системы: банкам, клиентам, пунктам предоставления услуг, обслуживания населения и др.

Список литературы

1. Царегородцев А.В., Кислицын А.С. Основы синтеза защищенных телекоммуникационных систем. – М.: Радиотехника, 2006.
2. Матюхин В.Г., Пярин В.А. Концепция обеспечения информационной безопасности платежной системы на основе интеллектуальных карт // В кн. Обеспечение информационной безопасности в экономической и телекоммуникационной сферах / Под ред. Сухарева Е.М. – М.: Радиотехника, 2003.
3. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М.: МИФИ, 1997.
4. Пярин В.А. Основные результаты разработки российских интеллектуальных карт и перспективы их применения в системах и средствах защиты информации // В кн. Обеспечение информационной безопасности в экономической и телекоммуникационной сферах / Под ред. Сухарева Е.М. – М.: Радиотехника, 2003.