ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

А.А. ВАРФОЛОМЕЕВ

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ КАРТ

Учебное пособие

Москва
2008

Аннотация

В учебном пособии дается краткое описание различных видов интеллектуальных карт и приводится области их применения. Интеллектуальные карты, или карты с интегральной схемой, включающей микропроцессор (smart-card, microcomputer card), наряду с пластиковыми картами с магнитной полосой получили широкое распространение, обладая по сравнению с последними рядом преимуществ, основное из которых связано с большей защищенностью информации. Обсуждаются особенности разработки и реализации для этих карт различных симметричных и асимметричных криптографических алгоритмов. Учебное пособие входит в серию пособий по информационной безопасности и расширяет материал пособий «Основы информационной безопасности», «Современная прикладная криптография», «Технические средства защиты информации».

Введение

Актуальность изучения вопросов защиты информации с использованием интеллектуальных карт определяется повсеместным распространением компьютерных информационных, банковских, платёжных и других видов систем, а также отдельных прикладных программ, применяющих интеллектуальные карты (ИК) в качестве средства хранения и обработки персональных данных пользователей и персонала компьютерных систем. Основные теоретические и практические результаты в этой области разработаны ведущими мировыми научными центрами и фирмами-производителями в последние 10–15 лет.

Ещё совсем недавно бывшие малоизвестным, непривычным явлением, ИК всё шире вторгаются в самые различные сферы жизни. Обладая целым рядом притягательных для пользователя свойств, они вытесняют традиционные технологии и находят всё новые и новые области применения. В современном понимании ИК – это персонализированное аппаратное или аппаратно-программное средство в виде прямоугольной пластиковой карточки с вмонтированным в неё микропроцессором, блоками памяти и интерфейсной частью, предназначенное для взаимодействия владельца карты с автоматизированными системами обработки данных. Трудно перечислить все известные на сегодняшний день области применения интеллектуальных карт: это банковские приложения, здравоохранение, коммунальное хозяйство, транспортные услуги, системы безопасности, туризм и многое другое. Несмотря на это, сфера применения ИК расширяется. В основе технологии ИК лежат самые современные разработки микроэлектроники, физики, прикладной математики, криптографии и смежных отраслей.

От студентов, изучающих предлагаемый курс, требуется предварительное изучение курса «Основы информационной безопасности», «Современная прикладная криптография». Желательно также знакомство с курсом «Открытые системы» или другим аналогичным курсом, служащим введением в системный подход к описанию функциональности и модельное представление ИТ-систем

Раздел 1. Виды пластиковых карт и особенности их применения

1.1. Классификация пластиковых карт

История пластиковых карт начинается в 50-е гг. нашего века в США. Именно тогда появляются первые «расходные» (charge), или кредитные карты, использовавшиеся для оплаты счетов в ресторанах и гостиницах. Карты имели нанесённый на них рельефный рисунок, копировавшийся на бумажный бланк счёта. Владелец карточки вручную ставил свою подпись, а для подтверждения состоятельности клиента при снятии с карточки крупной суммы продавец связывался с организацией-эмитентом карточки по телефону. Такие карты были лишь отдалённым прообразом современных интеллектуальных карт.

Во второй половине 60-х гг. началось активное практическое применение карт с магнитной полосой. Первоначально они использовались для выдачи наличных денег со счёта клиента в автоматизированных банковских терминалах, а затем и в других применениях: в качестве пропусков, на транспорте, как удостоверения личности.
В 1974 г. французский журналист Ролан Морено (Roland Moreno) запатентовал идею вмонтировать интегральную микросхему в пластиковую карту.

Первым типом таких карт стали так называемые полупроводниковые (микроэлектронные) карты - эти карты имели встроенные микросхемы памяти и простые логические схемы для доступа к памяти и выполнения некоторых простых функций. В то же время появились гибридные карты, совместившие в себе микросхемы и магнитную память.
Наконец, микропроцессорные (смарт-карты) впервые стали применяться в 1982 - 84 гг. во Франции. Микропроцессорные пластиковые карты по сути представляют собой микрокомпьютер, встроенный в пластиковую панель; в них используются самые современные достижения микроэлектроники.

В настоящее время находят применение все вышеперечисленные типы пластиковых карт, за исключением первых, морально устаревших, моделей. Выбор типа карт, используемых в конкретном приложении, осуществляется исходя из условия оптимизации стоимостных параметров, необходимого уровня надёжности и безопасности информации и возможного ущерба от утраты либо несанкционированного доступа к информации, находящейся на карте.

Наглядным примером использования различных типов карт в одной системе является автоматизированная система оплаты проезда в Московском метрополитене, внедряемая с 1997 г. В качестве малоразовых и месячных проездных билетов применяется магнитный билет, соответсвующий стандартам ISO, в то время как льготные и др. типы билетов долговременного использования выполняются в виде бесконтактных смарт-карт. Одни и те же устройства считывания (кард-ридеры) поддерживают работу как с бесконтактными смарт-картами, так и с билетами с магнитной полосой.

Кроме перечисленных выше типов пластиковых карт, разработаны и находят ограниченное применение некоторые другие типы карт [9, 15, 44]. Среди таких карт наиболее известными являются оптические, имеющие ряд особенностей:

- возможность хранения больших объёмов информации;
- стойкость к внешней, в том числе агрессивной, среде;
- информация с карты только считывается (технология подобна CD-ROM);
- карты сложны в изготовлении и дороги по сравнению с обычными картами с памятью.

Физические свойства и техника линейной записи данных на оптическую карту определяются стандартами ISO/IEC 11693, 11694.
Известны также и другие, «экзотические», типы карт: штрих-кодовые, перфорационные, голографические, карты с устройствами ввода/вывода (микроклавиатура, жидкокристаллический дисплей, сенсоры и др.). Однако данные карты не получили широкого распространения по различным причинам: лёгкость подделки, неудобство работы, дороговизна и др.

Классификация пластиковых карт приведена на рис. 1. Каждая разновидность пластиковых карт далее будет рассмотрена более подробно.

Рис. 1. Классификация пластиковых карт

Наиболее распространённым носителем, основой для карт, служит пластмасса, откуда они и получили своё название. Но в ряде случаев, например при тяжёлых условиях эксплуатации (резкие перепады температур, агрессивные среды, сильные электромагнитные поля и др.), могут применяться и другие носители. Карты, например, могут быть металлическими. Для магнитных карт с коротким сроком использования может применяться плотная бумага или картон.
В ряде специальных случаев находят применение гибридные модели карт, совмещающие, например, магнитную полосу и встроенный микропроцессор [25].

1.2. Карты с магнитной полосой

Карты с магнитной полосой (magnetic stripe cards) начали использоваться в конце 60-х гг. в США в автоматах для выдачи наличных денег (Automatic Teller Machines - ATM) [67]. Магнитные карты имеют функции хранения данных, записи на карту и чтения с карты. В соответствии со стандартами ISO [50, 51] магнитные карты (рис. 2) имеют три магнитные дорожки, на одну из которых разрешена запись данных, другие доступны только для чтения.
Основными недостатками карт с магнитной полосой являются:

- возможность их сравнительно лёгкой подделки;
- низкая надёжность. Карты не выдерживают сильных магнитных полей, при этом хранимые данные искажаются и карта становится неработоспособной, следовательно, необходимо тщательно соблюдать условия их эксплуатации;
- очень ограниченная память;
- они совершенно пассивны, и их содержание может быть легко прочитано или переписано;
- устройства чтения магнитных карт содержат дорогостоящие и не всегда надёжные механические части.

В магнитных картах используются достаточно простые средства защиты от подделки: магнитные водяные знаки (magnetic watermarks) и метод «сэндвича» — одна полоса содержит участки с различными уровнями намагниченности [9].

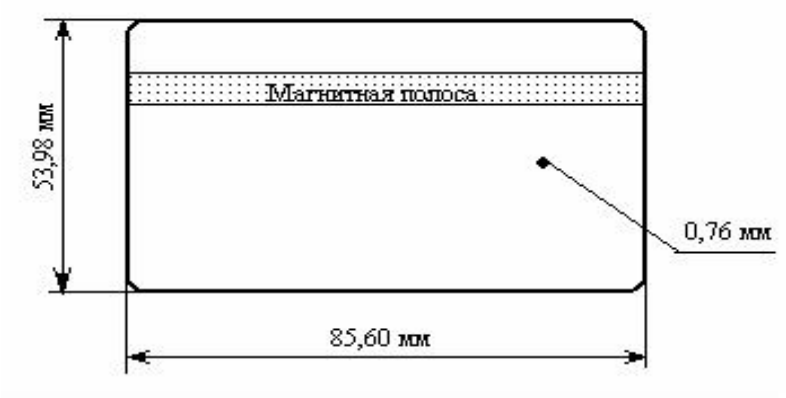


Рис. 2. Геометрия карты с магнитной полосой

В настоящее время магнитные карты используются в основном в системах с малоценной информацией, где подделка карты или её выход из строя по техническим причинам не нанесёт большого ущерба системе: например, в качестве проездных документов ограниченного срока действия на транспорте. Во многих странах, однако, сохраняется проблема перевода платёжных систем, созданных в прежние годы и использующих магнитные карты, на более совершенные микропроцессорные карты, поэтому в банковских системах до сих пор могут применяться магнитные карты. Несмотря на то, что в России мировые банковские платежные системы появились сравнительно недавно, проблема перетекла и к нам вместе с проблемами мировых платежных систем. Поэтому возможно использование карт и с микропроцессором, и с магнитной полосой. Более того, магнитная полоса, по-видимому, будет сосуществовать и с другими технологиями.

Основным преимуществом магнитных карт является их низкая стоимость и простая технология производства. Последним технологическим достижением в области магнитных карт является разработка метода удалённого (бесконтактного) чтения данных с карточки [32]. Данный метод (The Remote Read Magnetic Tag System) позволяет совмещать преимущества радиоинтерфейса, применяемого в

микропроцессорных картах, с низкой стоимостью и простотой использования магнитных носителей данных. Это позволяет предположить, что магнитные карты всё ещё будут использоваться в некоторых автоматизированных системах, главным образом там, где это выгодно по экономическим соображениям.

1.3. Полупроводниковые карты

Следующим этапом развития пластиковых карт стало появление полупроводниковых карт. Такая карта содержит в своём составе интегральную микросхему, в которой объединены как минимум два типа памяти: постоянная (ROM) и электрически перепрограммируемая (перезаписываемая) постоянная память (EEPROM) - и, как правило, логическая схема для управления ячейками памяти. На поверхность карты выведены металлические контакты для взаимодействия с устройством доступа. Взаимодействие с внешней аппаратурой осуществляется за счёт физического контакта электрических цепей карты и устройства доступа. При этом доступ к ячейкам памяти карты осуществляется через управляющую логическую схему.

Принято различать следующие разновидности полупроводниковых карт.

1. Карты с памятью (memory cards) - имеют постоянную память (ROM), электрически перепрограммируемую постоянную память (EEPROM) объёмом несколько десятков или сотен байт и логическую схему для управления блоком памяти.

В более совершенных моделях для управления памятью используется микроконтроллер с небольшим набором команд, ориентированных на формирование управляющих сигналов для доступа к памяти. Это дало возможность создать *карты с защищённой памятью*, в которых используется механизм разрешения операций чтения, записи и стирания информации при помощи секретного ключа, вырабатываемого из идентификационной информации владельца. В ряде случаев ключ вычисляется динамически как функция нескольких параметров самой карточки, терминала, системного времени и ключа пользователя.

Среди карт с простой, незащищённой, памятью выделяются так называемые *карты-счётчики*, осуществляющие дискретное снижение заранее записанной в память величины. Такого типа карты используются в системах с информацией, не представляющей большой ценности, например, в качестве телефонных карт (что, кстати говоря, приводит к систематическим недостачам в таких системах, но всё равно обходится дешевле, чем выпуск в обращение микропроцессорных карт). Для обеспечения совместимости с прежними моделями некоторые виды таких карт также снабжались рельефными обозначениями, одновременно выполнявшими функцию защиты от подделки.

2. Карты с логической схемой (hardwared logic cards) - имеют ROM, PROM (программируемую постоянную память), EEPROM для хранения данных, схему управления памятью и логическую схему, конструктивно выполненные в одной интегральной микросхеме. Карты с аппаратной логикой могут реализовывать простые, предопределённые алгоритмы обработки данных и разрешения обращения к памяти. Такие карты явились как бы «переходным звеном» от карточек с памятью к микропроцессорным картам.

С целью обеспечения совместимости с системами, использующими магнитные карты, появились также *гибридные карты* с магнитной полосой, интегральной микросхемой и металлическими контактами. Такая карта может использоваться в различных случаях либо как карта с магнитной полосой, либо как карта с микросхемой, но передача данных между магнитной и полупроводниковой памятью возможна только через внешние устройства.
Общие недостатки всех рассмотренных до сих пор типов карт:

- их неспособность самостоятельно обрабатывать находящуюся на них информацию;
- невозможность перепрограммирования предопределённых функций, выполняемых картой.

Наиболее известные фирмы-производители полупроводниковых карт - Gemplus, Schlumberger (Франция), Giesecke & Devrient, Orga Kartensysteme (ФРГ). Все карточки соответствуют требованиям стандартов ISO 7816 - 1,2,3. Средняя стоимость карт с аппаратной логикой составляет $0,15...0,40.

Типичные применения таких карт - таксофоны, медицина, удостоверения личности, торговые автоматы, системы парковки автомобилей, предоплаченные схемы. Выполняемые функции - непополняемая платёжная карточка (возможно, с функциями аутентификации), счётчик совершённых по карте транзакций, в ряде случаев - пополняемая платёжная карточка с проверкой идентификационной информации, защитой от чтения/записи, счётчиком ошибок.

1.4. Микропроцессорные карты (смарт-карты)

За пластиковыми картами со встроенным микропроцессором закрепилось английское наименование «смарт-карты». Наиболее удачным русскоязычным названием является, на наш взгляд, наименование «интеллектуальные карты», хотя единства в терминологии и классификации пластиковых карт до сих пор нет. Заметим, что в других работах понятие «интеллектуальная карта» может отличаться по смыслу от используемого здесь: иногда смарт-картами или интеллектуальными картами называют более широкий класс пластиковых карт, включая карты с магнитной полосой, а в ряде случаев отождествляя их со всеми пластиковыми картами вообще. Когда говорят о потребительских качествах карт и рассматривают их лишь как платёжный инструмент, чаще всего употребляют термин «смарт-карта»; когда рассматриваются технические вопросы, касающиеся внутреннего устройства карт, их работы в автоматизированной системе, говорят об «интеллектуальной карте». В данной работе термины «смарт-карта» и «интеллектуальная карта» используются как синонимы для обозначения микропроцессорной пластиковой карты.

Итак, *интеллектуальные карты (ИК)* - это пластиковые карты со встроенным программируемым микропроцессором. Геометрические параметры таких карт не отличаются от описанных ранее типов пластиковых карт.

Главное отличие ИК от пассивных устройств, рассмотренных ранее, заключается в способности обрабатывать хранящуюся и поступающую информацию при помощи встроенного микропроцессора. Применение микропроцессора позволило кардинально изменить роль пластиковой карты в автоматизированной системе: микропроцессор позволил, например, осуществлять контроль доступа к памяти ИК во время взаимодействия с автоматизированной системой, выполнять ряд других специфических функций, как правило, криптографического характера. ИК, кроме выполнения алгоритмов, связанных с их целевым назначением (например, осуществления финансовых транзакций), выполняют в основном криптографические преобразования информации (схемы шифрования, электронной цифровой подписи, аутентификации и др.). Кроме того, ИК могут дополнительно снабжаться средствами аутентификации (как биометрического, так и логического характера) владельца интеллектуальной карты (более подробно см. п. 3.2.3.).

Основные характеристки современных интеллектуальных карт таковы: объём ROM - 2 ... 20 Кбайт, RAM - 128б ... 1 Кб, EEPROM - 1 ... 8 Кбайт, в них используются в основном 8-разрядные микропроцессоры (существуют проекты смарт-карт с 16- и 32-разрядными RISC-процессорами; в качестве примера можно привести европейский проект разработки 32-разрядного RISC-процессора CASCADE - Chip Architecture for Smart Cards and Portable Intelligent Devices), тактовая частота МП - 5...15 МГц. Наиболее часто используемый МП для интеллектуальных карт - 8-разрядный МП 68HC05 фирмы Motorola. Средняя стоимость МП-карт - $ 0,60 ... 5,00.

По сути, достигнутые для смарт-карт показатели вплотную приближают их по своим функциональным возможностям к первым моделям персональных компьютеров. Главное отличие состоит в том, что смарт-карта не имеет собственного источника питания, а питается за счёт энергии, передаваемой от устройства считывания в момент взаимодействия с картой, а также в большинстве случаев не имеет встроенных средств ввода/вывода и отображения информации. Однако некоторые последние модели карт с радиоинтерфейсом имеют и собственный источник питания.

Существуют два типа микропроцессорных карт, различающихся принципом взаимодействия с устройством считывания: контактные и бесконтактные. Рассмотрим основные типы выпускаемых в мире интеллектуальных карт.

1. Контактные карты, как и рассмотренные ранее полупроводниковые карты с памятью, имеют набор металлических контактов на поверхности и взаимодействуют с устройством считывания посредством передачи электрических сигналов (рис. 3). Стандарт ISO 7816 предусматривает наличие на любой карте с микросхемой восемь контактных площадок, из которых реально используются лишь шесть:

- Vcc - контакт подачи рабочего напряжения питания (5 В);
- GND - "земля";
- RST - контакт инициализации карточки;
- CLK - контакт тактового генератора;
- I/O - контакт ввода/вывода;
- Vpp - контакт подачи напряжения записи данных в память (обычно 12,5...15 В).

Наиболее известные фирмы, производящие контактные смарт-карты: Bull PTS, GemPlus Card International, Schlumberger Technologies, Motorola, Siemens Nixdorf, Philips, SGS Thompson, Solaic, Orga Kartensysteme GmbH.

2. Бесконтактные карты взаимодействуют с терминалом (ридером) при помощи радиоканала обмена данными (используется фазовая модуляция сигнала). Карта и ридер снабжаются антеннами (контурами индуктивности) (рис. 4).

Важнейшей характеристикой бесконтактных карт является предельное расстояние взаимодействия. Оно варьируется от 2 мм до 1 м и более. В последнее время появляются сообщения о разработке карт с дальностью связи до нескольких метров.

Второй важной характеристикой является частота передаваемого между картой и устройством доступа электромагнитного сигнала. В соответствии со стандартом ISO/IEC 14443 используются следующие частоты сигнала:

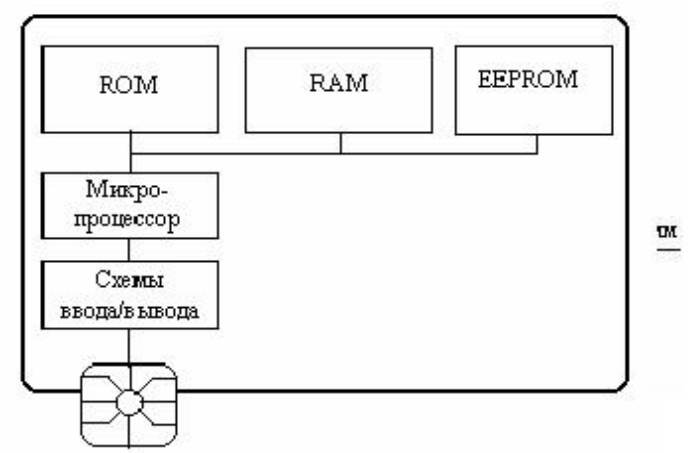
- в низкочастотной области - до 135 кГц;
- в диапазоне средних волн - 6.78 и 13.56 МГц;
- в высокочастотном диапазоне - 915 МГц, 2.45 и 5.8 ГГц.

Бесконтактные карты подразделяются на «близкодействующие» (proximity, close coupling cards) и «дальнодействующие» (remote couple cards), или карты удалённого доступа.

«Близкодействующие» карты для выполнения сеанса связи с устройством доступа требуют физического (но не электрического!) контакта с устройством доступа: владелец карты должен прикоснуться картой к поверхности устройства доступа. Предельное расстояние взаимодействия таких карт - 2 мм. Преимущества такой карты перед обычной контактной в том, что:

1) в ней нет быстроизнашивающихся и загрязняющихся металлических контактов;

2) процедура взаимодействия бесконтактной карты с устройством доступа происходит быстрее, чем контактной.



см

Карты удалённого доступа осуществляют радиочастотную передачу данных на расстоянии до устройства доступа от 1 ... 10 см до 1 м. Существуют два вида карт этого типа [36]: пассивные и активные. Рис. 3. Схема устройства контактной смарт-карты

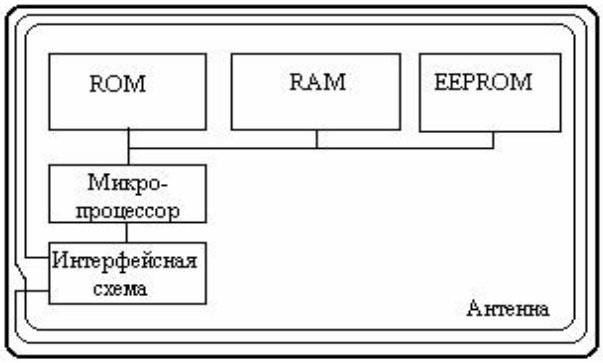


Рис. 4. Схема устройства бесконтактной смарт-карты

Пассивные карты не имеют внутреннего источника питания. Энергия доставляется через электромагнитное поле от устройства доступа. Основные элементы пассивной бесконтактной карты - антенна, защищённый модуль микросхемы и пластиковая основа. В зависимости от используемой частоты радиообмена антенна может быть выполнена различными способами: травлением, печатью по пластику, в виде напыления металлической полосы и др.

Активные карты имеют встроенную батарею, обеспечивающую их энергией для радиосвязи. При частоте обмена >300 МГц карта требует обязательного наличия встроенного источника питания. При частотах <13,56 МГц возможно, при ограничении расстояния между ридером и картой, получать энергию для питания смарт-карты от радиосигнала.

Карты удалённого доступа, в свою очередь, принято подразделять на *карты фиксированного взаимодействия* (remote fixed couple) - с максимальным растоянием связи <10 см - и *карты свободного взаимодействия* (remote loose coupling) - с максимальным расстоянием связи >10 см. Карты фиксированного взаимодействия для обеспечения устойчивой связи с ридером должны быть внесены в ограниченную область вблизи приёмной антенны. Карты свободного взаимодействия (иногда их называют «free-hand cards», что отражает способ их использования) взаимодействуют с устройством доступа с большого расстояния, что позволяет человеку, предъявляющему её, даже не держать карту в руках, а, например, прикрепить её к карману.

3. Гибридные смарт-карты (hybrid cards) - это комбинация обычных смарт-карт с контактами и бесконтактных карт. Микросхема и антенна объединены в одну пластиковую карту, но в карте нет внутренних соединений между микросхемами, имеющими контактный и бесконтактный (антенный) интерфейс. Обмен данными возможен только через внешнее устройство (подобно гибридным картам с полупроводниковой памятью и магнитной полосой). Примером использования такой технологии может быть комбинация платёжной карты и бесконтактной карты-пропуска в закрытое помещение.

4. Смарт-карты с двойным интерфейсом (dual interface, combi-cards) объединяют преимущества смарт-карт обоих типов. Одна интегральная микросхема имеет два интерфейса: контактный и бесконтактный (радиоинтерфейс), обладая при этом доступом к общей памяти и одному микропроцессору (рис. 5) [25], [29].

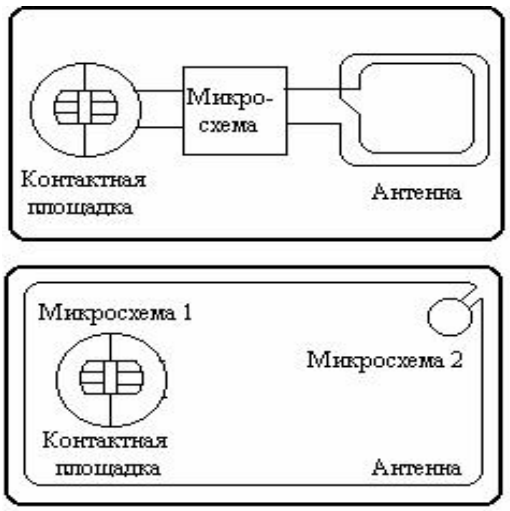
Двойной интерфейс обеспечивает доступ к одним и тем же ресурсам. Это позволяет, например, выполнить авторизацию карты и зачислить на неё некоторую сумму на стационарном контактном устройстве, а проверять карту либо списывать с неё сумму оплаты (например, в городском транспорте, при посадке в поезд и т.п.) при помощи бесконтактного ридера.

На рис. 6 показаны различия в устройстве карты с двойным интерфейсом и гибридной карты: карта с двойным интерфейсом имеет одну микросхему МЭС, к которой через интерфейсные схемы подсоединены контактные площадки и антенна в виде контура индуктивности; гибридная карта имеет две электрически не соединённые между собой микросхемы МЭС1 и МЭС2, к одной из которых подсоединены металлические контакты, к другой - антенна.

Карты с двойным интерфейсом, в свою очередь, могут различаться по типу внутренней организации и доступа к памяти (рис. 7): область памяти может быть общей для программ с обоми типами интерфейсов либо быть разделённой на области совместного и общего использования.

Некоторые модели бесконтактных карт, в том числе карт с двойным интерфейсом, имеют также встроенный криптографический сопроцессор, что позволяет, например, осуществлять при помощи таких карт удалённый доступ к вычислительной сети (для этого необходима процедура аутентификации пользователя, использующая криптографические методы, а также протоколы безопасной передачи данных между картой и узлами сети).

Данный тип карт является наиболее совершенным с технологической точки зрения и удобным с точки зрения пользователя устройством. Особое значение смарт-карты с двойным интерфейсом приобретают в связи с разработкой многофункциональных карт, способных работать в различных системах, имеющих, возможно, и разные типы интерфейса.
Одними из наиболее известных идеологов и разработчиков ИК с двойным интерфейсом являются фирмы IBM, AT&T, Siemens Nixdorf.



Иногда также говорят о *суперинтеллектуальных картах*, что чаще всего подразумевает наличие у карты собственного источника питания и средств ввода и отображения информации (микроклавиатуры, ЖК-дисплея, сенсорных контактов и т.п.). Такие модели карт приближают их к электронным записным книжкам и ПК-блокнотам, но пока остаются достаточно дорогими для широкого использования. Рис. 5. Гибридные смарт-карты и карты с двойным интерфейсом

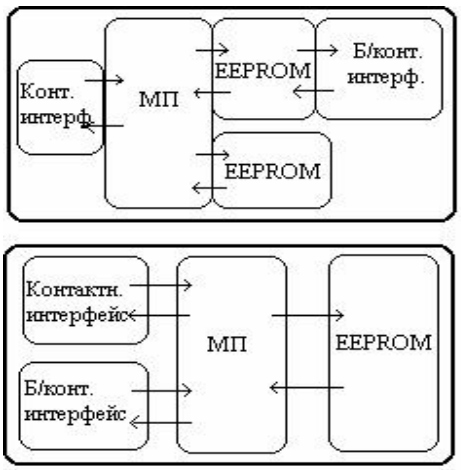


Рис. 6. Способы внутренней организации смарт-карт с двойным интерфейсом

Методы защиты смарт-карт от подделки. Как уже отмечалось выше, производство смарт-карт возможно только в промышленных условиях. Особенности технологии их производства таковы, что достичь низкой себестоимости карт возможно только при достаточно значительных объёмах их выпуска. Далеко не все средние и даже крупные фирмы, взявшиеся за выпуск смарт-карт, смогли продолжить их выпуск и достичь безубыточности производства. Подделка единичной карты или небольшой их серии, скорее всего, окажется нецелесообразной по экономическим соображениям.

Однако разработчики и производители смарт-карт предусматривают дополнительные методы защиты смарт-карт от возможного «обмана» злоумышленником устройств (терминалов), работающих с ИК. Перечислим некоторые из них:

- эмбоссирование - нанесение термическим способом рельефных надписей (например, имени, фамилии владельца, названия банка и т.п.) на поверхности пластиковой карты;
- голографические изображения;
- нанесение дифракционной решётки;
- нанесение рисунков и надписей, видимых в ультрафиолетовом свете;
- использование специальных красителей;
- нанесение микротекста и микрорисунка;
- полноцветная графика и фотография и другие.

1.5. Сферы применения различных типов пластиковых карт

На сегодняшний день известно огромное число применений интеллектуальных карт, и даже просто перечислить их все затруднительно в рамках данной работы. Однако представляется возможным кратко рассмотреть сферы применения интеллектуальных карт, классифицировав их по типам выполняемых функций:

1. Удостоверение личности. Карта как удостоверение личности владельца может использоваться в охранных системах, системах безопасности, системах контроля доступа на объекты и им подобных. В данном случае предъявление системе карты должно сопровождаться обязательной идентификацией личности самого предъявителя для карты. Конкретное назначение карт в таких системах может различаться: они используются как пропуск для доступа на закрытые объекты и территории, как средство разграничения прав и полномочий доступа в режимные помещения и хранилища, как ключ для доступа к средствам администрирования, в том числе удалённого, автоматизированных охранных систем, как ключ для доступа к файлам, хранящимся на диске, и т.д.

Преимущества использования карты как удостоверения личности очевидны: это трудность их подделки (изготовление возможно только промышленным способом, следовательно, производство можно контролировать), удобство использования и автоматизированный контроль, возможность надёжной аутентификации владельца биометрическими методами (вероятность ошибки в таком случае гораздо ниже, чем при ручном контроле).

2. Платёжное средство. Интеллектуальная карта в качестве платёжного инструмента используется в большом количестве банковских информационных систем по всему миру (см. п. 4.3), выполняя в них роль инструмента осуществления платёжных операций. Можно выделить несколько аспектов их использования в финансовых операциях:

- осуществление платежей через банковские автоматы (банкоматы), автоматизированные торговые терминалы и кассовые аппараты (point-of-sale, POS);
- оплата услуг, предоставление которых клиенту носит часто повторяющийся, систематический характер (например, телефонные карточки, покупка бензина на автозаправочных станциях и т.п.);
- оплата и контроль пользования транспортными услугами (оплата поездок на метрополитене, наземном городском транспорте, железной дороге, такси, заказ билетов на авиалинии и т.д.);
- некоторые другие виды финансовых и торговых услуг.

3. Сбор и хранение личных данных владельца карточки. Растущий объём памяти, встраиваемой в карточку, позволил использовать её как средство сбора, накопления и хранения личных данных её владельца. В качестве примеров можно привести медицинские применения (история болезни, отпуск лекарств, рецепты, страхование и т.д.), использование карточки в качестве страхового полиса, трудовой книжки и т.п.

4. Обеспечение анонимности владельца при обращении к информационной системе. Данная задача является противоположной задаче 1 (удостоверение личности) и в основном связана с реализацией систем работы с «электронными деньгами» (см. п. 4.5), на данный момент не является широко распространённой и встречает определённые технические трудности в связи с необходимостью реализации этих функций в так называемом «электронном кошельке» («электронном бумажнике») [64, 68, 70, 74].

Заметим, что в каждой из перечисленных сфер структура информации, хранимой на карте, и реализуемые алгоритмы могут несколько отличаться, в зависимости от характера и объёма обрабатываемой информации. Более того, конкретные реализации систем с интеллектуальными картами могут совмещать в себе несколько функций. Одним из наиболее перспективных направлений развития технологии интеллектуальных карт сегодня являются так называемые многофункциональные карты, которые более подробно рассматриваются в п. 2.6.

Приведённая классификация не претендует на полноту и всеобъемлемость, однако представляется, что на сегодняшний момент указанные функции интеллектуальных карт являются основными и наиболее распространёнными.

1.6. Некоторые другие классы устройств для индивидуальных банковских расчётов

Со времени появления смарт-карт предпринимаются попытки создания портативных устройств, совмещающих в себе функциональность и компактность смарт-карт с производительностью современных персональных компьютеров. Кроме того, как известно, один из основных недостатков смарт-карт связан с отсутствием на них средств ввода-вывода и отображения информации. Портативные устройства позволяют преодолеть недостатки смарт-карт, а также дополнить их возможности специфическими функциями, необходимыми для обеспечения безопасности пользователя автоматизированной системы методами криптографии: большим объёмом памяти для хранения ключей и данных, аппаратными реализациями алгоритмов шифрования для высокоскоростной обработки данных и т.п. Некоторые из этих устройств создаются с целью замены смарт-карт на более совершенные средства для индивидуальных банковских расчётов.

Укажем некоторые примеры реализации таких устройств:

- «суперинтеллектуальные» карты (Super Smart Cards) - бесконтактные интеллектуальные карты (с радиоинтерфейсом), имеющие миниатюрные средства ввода (микроклавиатура, сенсоры) и отображения (жидкокристаллический дисплей) информации;
- карманные устройства типа «запрос – ответ», похожие на калькуляторы, для удалённого доступа в информационные системы (например, устройство CRYPTOCard);
- электронные блокноты и органайзеры со встроенными, аппаратно реализованными функциями криптографической защиты информации;
- «интеллектуальные диски» - магнитные или магнитооптические носители информации со встроенной интегральной микросхемой (микроконтроллером) для обработки информации;
- мобильные сетевые компьютеры - ПК-блокноты, ориентированные на работу в сети Internet и в других распределённых информационных системах в качестве терминала, имеющего встроенные средства защиты.

Раздел 2. Архитектура интеллектуальных карт

2.1. Аппаратная организация интеллектуальных карт

Основой аппаратного обеспечения интеллектуальных карт (смарт-карт) является интегральная микросхема, вмонтированная в пластиковую основу, находящаяся под металлическими контактными площадками. Физически интегральная микросхема занимает лишь небольшую часть площади поверхности карты. Карта имеет больший размер только из соображений удобства пользования ею.

В основе аппаратной организации интеллектуальной карты лежит шинная архитектура вычислительной системы, широко распространённая в вычислительной технике. Основные компоненты интегральной микросхемы карты - это микропроцессор, схемы памяти, схемы ввода-вывода, схемы синхронизации, схемы защиты, схемы инициализации (стартовые цепи) и внутренняя шина (электрическая магистраль) (рис. 7).

Интегральная микросхема карты чаще всего выполняется в виде физически защищённого от внешних воздействий модуля, на поверхность которого в особо ответственных случаях может наноситься специальное оптически непрозрачное покрытие, не позволяющее «увидеть» внутреннюю структуру модуля.

Микропроцессорспособен исполнять набор команд, записанных производителем в постоянную память (ROM) и набор команд операционной системы. Предопределённый набор команд выполняется всегда, независимо от приложения, с которым работает карта, и обеспечивает вступление карты в контакт с внешним устройством и подготовку её электрических цепей к передаче данных. Более высокоуровневые команды операционной системы, как правило, также реализованы аппаратно в ROM карты, чтобы достичь более высокого быстродействия при ограниченных аппаратных возможностях карты. Интеллектуальные карты имеют следующие виды ***памяти***:

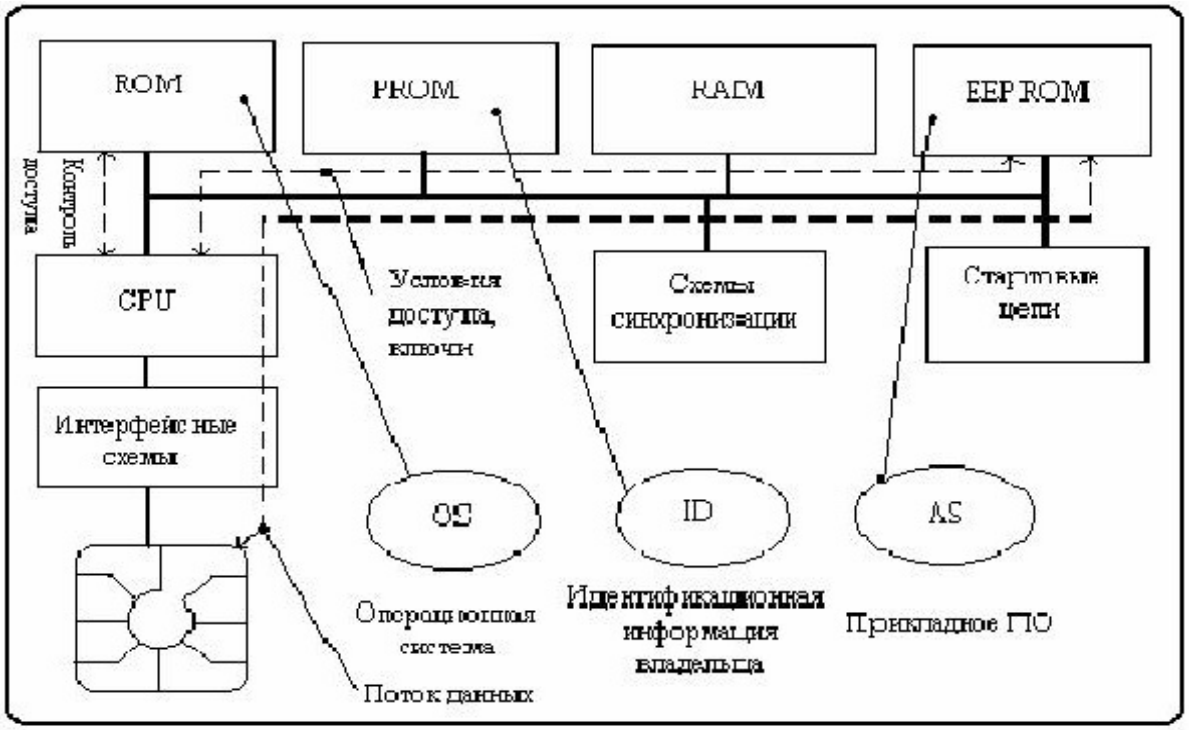


Рис. 7. Аппаратная организация, программное и информационное обеспечение интеллектуальной карты

1. ***Постояннаяпамять*** *(ROM - Read-Only Memory).* В ней хранится операционная система (ядро ОС и команды ОС), последовательность операций инициализации карты, выполняемых в начале каждого сеанса связи с внешним устройством. Запись этих данных выполняется предприятием-изготовителем смарт-карты.

2. ***Программируемаяпостояннаяпамять*** *(PROM - Programming Read-Only Memory).* Информация в эту память может быть записана в любой момент времени, но только однажды. В последующем информация может только считываться. Физически PROM представляет собой матричный набор логических вентилей (так называемое масочное ПЗУ). В PROM записываются идентификационные данные о владельце карточки, прикладных программах, эмитенте карты, ставится подпись центра авторизации и т.п. Запись производится центром авторизации (см. п. 4.1) на специальном оборудовании, как правило, встроенном в кард-ридер.

3. ***Программируемая постоянная память со стиранием*** *(EPROM - Erasable Programming Read-Only Memory)* отличается от предыдущего типа памяти тем, что позволяет стирать ранее записанную информацию. Однако стирание производится чаще всего при помощи ультрафиолетового света на специальном оборудовании. Процесс стирания является очень сложным и дорогостоящим. Поэтому данный тип памяти в настоящее время используется очень редко.

4. ***Электрически перепрограммируемая постоянная память*** *(EEPROM — Electrically Erasable Programming Read-Only Memory)* - обязательно присутствует в любой модели смарт-карт. Преимущество состоит в том, что стирание и запись информации в логические ячейки выполняются электрическими импульсами, кроме того, такие микросхемы памяти достаточно дёшевы.

Наличие микропроцессора позволяет организовать не только управление памятью, но и защиту некоторых областей памяти. EEPROM делится на системную область и область прикладных программ.

Системная область доступна для чтения/записи только операционной системе карты. В ней хранятся ключи доступа к файлам, отметки времени, вырабатываемые при совершении транзакций, счётчик транзакций, некоторая другая информация, доступ к которой прикладным программам должен быть закрыт.

Область прикладных программ содержит файловую систему карты: таблицу определения файлов и файлы, хранящие коды и данные прикладных программ. Доступ к этой области возможен не только операционной системе, но и прикладным программам. Поскольку эта область не имеет аппаратной защиты от чтения/записи, информация в ней должна обязательно храниться в зашифрованном виде, во избежание несанкционированного считывания злоумышленником в обход парольной защиты.

Все перечисленные выше виды памяти могут хранить информацию не только в период активной работы смарт-карты, но и при отключённом питании.

Сейчас EEPROM-память в смарт-картах всё чаще заменяется на FRAM-память (Ferrit Random Access Memory) - разновидность оперативной памяти на ферритовых логических элементах, которая позволяет хранить данные при отключённом источнике питания, а благодаря прогрессу технологии легко размещается в интегральной микросхеме.

5. ***Оперативная память*** *(RAM - Random Access Memory)* предназначена для временного хранения данных при выполнении микропроцессором карты операций в ходе осуществления транзакции. При отключении питания вся хранящаяся в ней информация стирается.

Схемы ввода - вывода (интерфейсные схемы, I/O System) зависят от типа интерфейса карты. Если интерфейс - электрические контакты, схемы ввода/вывода обеспечивают сопряжение шины с металлическими контактными площадками. Если карта имеет радиоинтерфейс, схемы ввода - вывода включают в себя антенну, выполняемую чаще всего в виде тонкой металлической рамки, проходящей по контуру смарт-карты, и обеспечивают преобразование электрических импульсов в радиочастотный сигнал и обратно.

Схемы синхронизации используются для синхронизации внутренних цепей карты и включают генератор тактовых импульсов, делители частоты, счётчик-таймер и др.

Схемы инициализации (стартовые цепи). Начало сеанса связи между картой и устройством доступа (кард-ридером) инициируется их стартовыми цепями. Когда карта вводится в ридер, схема инициализации ридера посылает сигнал по контакту RST аналогичной цепи смарт-карты. Ответный сигнал смарт-карты вырабатывает специальное сообщение для ридера о начале коммуникационного протокола. После этого все дальнейшие сообщения между картой и ридером передаются в режиме шифрования. Эта поцедура является обязательным начальным шагом процесса взаимной аутентификации смарт-карты и ридера.
Необязательным, но часто используемым на практике элементом аппаратной части смарт-карты является ***криптопроцессор***, обладающий следующими возможностями и функциями:

- контроль доступа к данным прикладных программ через функции ОС;
- аппаратно реализованные алгоритмы шифрования и цифровой подписи;
- аппаратно реализованные функции для работы с паролями и идентификационной информацией.

Программное и информационное обеспечение интеллектуальных карт

Программное и информационное обеспечение интеллектуальной карты включает операционную систему карты, прикладные программы (приложения) и идентификационную информацию.

1. Операционная система интеллектуальной карты *(COS - Card Operating System)* - упрощённый аналог «настоящих» операционных систем. На самом деле представляет собой набор микрокодов, записанных в ROM, которые принято разделять на ядро COS и команды COS. Термин «операционная система» взят по аналогии, чтобы сохранить строгость терминологии в отношении аналогичных функций компьютеров и смарт-карт, хотя операционные системы современных смарт-карт, и

особенно многофункциональных, по своей сложности всё больше напоминают полноценные компьютерные операционные системы.

Ядро COS - это набор микрокоманд, выполняемых при установлении сеанса связи с ридером, обеспечивающих работу с аппаратурой карты и интерфейс с внешним устройством. Ядро COS является аналогом загрузочных программ обычной ОС.

Команды COS - это специфицированный набор процедур, также, как правило, для повышения быстродействия реализованных аппаратно, предназначенный для работы с прикладными программами и данными, обеспечения механизма безопасности карты. Выделяют следующие группы команд COS:

- *команды работы с данными прикладных программ*: создание и удаление файлов, чтение данных из файлов различных форматов: структурированных и бесструктурных, выбор директории (для иерархической файловой системы), позиционирование указателя, обновление записей в файлах различных типов, добавление записи к файлу;
- *команды обеспечения безопасности* - их часто выделяют в отдельную группу, называемую "системой безопасности" смарт-карты (SF - Security Features). Это довольно большая группа команд, предназначенных для обеспечения безопасности данных, хранящихся и обрабатываемых картой, защиты файлов, операций с ключевой и идентификационной информацией. В SF входят следующие команды: выработка случайного числа, смена PIN владельца, аутентификация внешнего устройства, аутентификация смарт-карты для внешнего устройства, загрузка файла ключей, закрытие файла, объявление файла недействительным и снятие этой блокировки, аутентификация пользователя, блокировка аутентификации пользователя, изменение условий доступа к файлам и др. Если карта поддерживает работу с асимметричными криптографическими алгоритмами, то к перечисленным командам добавляется группа команд для работы с открытыми ключами: внутренняя и внешняя аутентификация с открытым ключом, загрузка ключа, чтение ключа, вычисление хэш-функции, проверка ключа, проверка цифровой подписи;
- *команды обслуживания карты* предназначены для выполнения вспомогательных операций: блокировка карты при неоднократных попытках несанкционированного доступа, транспортная блокировка, форматирование файловой системы и др.;
- *специфические команды, зависящие от назначения карты*. Например, если карта используется для электронной торговли, в ОС могут быть включены специальные команды увеличения/уменьшения величины, хранящейся в структуре данных, представляющей счёт владельца карты, простановка криптографических отметок («штампов», зависящих от времени). Это помогает значительно повысить скорость выполнения часто повторяющихся операций;
- *некоторые другие команды*: чтение файла статистики транзакций, выбор коммуникационного протокола, изменение скорости обмена с внешним устройством и т.п.

2. Прикладное ПО *(AS - Application Software)*, как правило, записывается на смарт-карту процессинговым центром (см. гл. 4). Частично прикладное ПО может быть записано в PROM-память, частично - в EEPROM. ПО смарт-карты должно разрабатываться в связи с ПО устройств, осуществляющих работу с ними, работа всех компонентов ПО должна быть согласована между собой и с форматами файлов, хранящихся на смарт-карте. Отдельное ПО необходимо для авторизации карты в центре авторизации, т.е. записи на неё информации о владельце, эмитенте, порядкового номера, ключей, идентификаторов и т.п.

Программирование памяти смарт-карт осуществляется с помощью специальных инструментальных пакетов, включающих транслятор текстов программ с языков высокого уровня и ассемблера в коды микропроцессора смарт-карты, а также программный эмулятор микропроцессорной системы смарт-карты для отладки и тестирования ПО.

В качестве примера можно привести интегрированное программное средство ASE Soft для разработки приложений для смарт-карт, разработанное фирмой ALADDIN Software Security R.D. ASE Soft включает в себя библиотеку функций API высокого уровня, API нижнего уровня, криптографического API,

примеры приложений для смарт-карт на языках C++, Visual Basic, Java. Пакет обеспечивает безопасный обмен данными между смарт-картой и приложением, работающим на терминале, использование различных типов смарт-карт и протоколов в одном приложении с использованием как высокоуровневых процедур программных библиотек, так и набора команд ISO 7816, возможность работы на одном компьютере с несколькими кард-ридерами и др. возможности. ASE Soft API содержит функции, реализующие алгоритмы шифрования, алгоритмы работы со случайными числами, антиотладочные и антитрассировочные механизмы. Пакет поддерживает многие известные языки программирования высокого уровня: C, C++, Pascal, Clipper, Visual Basic и язык Assembler. Интегрированная программная среда и эмулятор МП-системы позволяют наблюдать заполнение ячеек памяти, пароли доступа к данным, последовательность микрокоманд процессора. Полный комплект разработчика включает в себя также специальный кард-ридер ASE Drive с программируемой EEPROM-памятью и набор смарт-карт с различным объёмом памяти, протоколами обмена, встроенными специальными функциями и аппаратными алгоритмами шифрования.

3. Идентификационная информация записывается на карту в центре авторизации. В банковских системах запись осуществляется на рабочем месте оператора банка, кассира или другого лица, выдающего клиенту карту. С помощью специального кард-ридера на карту записывается PIN-код владельца, который в запечатанном конверте передаётся клиенту. Клиент впоследствии по своему желанию может сменить его.

2.3. Организация файловой системы

Так же, как и понятие «операционная система», термин «файловая система» перенесён на интеллектуальные карты из области «полноценных» компьютерных систем. Для интеллектуальных карт он обозначает способ логической организации хранения данных в перезаписываемой памяти (EEPROM) карты и также является упрощённым, адаптированным аналогом «настоящих» файловых систем.

Логическая структура памяти (здесь и далее имеется в виду EEPROM) зависит от операционной системы смарт-карты. В современных смарт-картах применяются два основных способа организации файловой системы: зонная и иерархическая.

Более простым является *зонный* способ организации файловой системы (или *зонирование*). В этом случае область прикладных программ EEPROM логически разбивается на зоны. В каждой зоне организуется структура данных в виде таблицы записей, называемой файлом. Для каждого из них определяется его формат (структура записей), зависящий от конкретного приложения. Каждый файл при зонной организации памяти представляет собой форматированную таблицу, состоящую из одинаковых записей. По младшим адресам области прикладных программ EEPROM формируется так называемая *таблица определения файлов* (FDT - File Definition Table) - аналог FAT - File Allocation Table (рис. 8). FDT - это также таблица, конкретный формат которой оговаривается стандартами ISO и спецификациями производителей, в которую записываются для каждого файла: адрес начала файла в памяти, метки защиты файла по чтению/записи, расширение метки защиты, длина записей файла, число записей, тип файла, имя файла, указатель текущей записи, указатель конца файла.

В ОС смарт-карты определяются следующие операции с файлами, реализованные в виде команд ОС:

- запись в файл;
- чтение из файла;
- запись определения файла в FDT;
- чтение записи о файле из FDT;
- установка метода защиты файла;
- позиционирование указателя записи файла

и др. команды, связанные в том числе с криптографической защитой, которые будут рассмотрены ниже.

Более сложной и совершенной является *иерархическая* файловая система, имеющая древовидную логическую структуру (рис. 8). Так же, как и зонная, иерархическая файловая система (ФС) состоит из FDT и файлов. Файлы иерархической ФС подразделяют на три типа:

- *мастер-файл (MF - Master File)* - помещается в корне ФС (аналог корневой директории жёсткого диска);
- *файлы-ветви (DF - Dedicated Files)* - содержат данные, атрибуты, и в ряде случаев, выполняемые программы (возможно, относящиеся к различным приложениям);
- *элементарные файлы (EF - Elementary Files)* - содержат текущие данные выполняемых программ и результаты транзакций (также, возможно, относящиеся к различным приложениям).

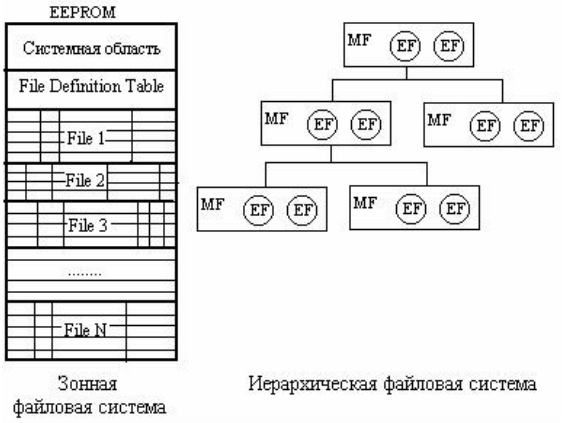


Рис. 8. Типы файловых систем интеллектуальных карт: зонная и иерархическая

Особенно удобна иерархическая ФС для многофункциональных смарт-карт.

Элементарные файлы, в общем случае, могут быть нескольких типов (рис. 9):

- линейный файл с фиксированной длиной записей;
- линейный файл с переменной длиной записей;
- линейный циклический файл с фиксированной длиной записей;
- «прозрачный» файл - бесструктурный файл, допускающий чтение/запись по указателю в произвольный адрес в пределах области, отведённой под файл;
- файлы команд приложений (ASC - Application Specific Command Files) - файлы, содержащие исполняемые коды прикладных программ, записанные в виде последовательности команд операционной системы. Смысл ASC-файлов в том, что они позволяют приложению создавать свои макрокоманды операционной системы, необходимые данному конкретному приложению, состоящие из последовательности команд COS, уже реализованных аппаратно, что позволяет достичь высокого быстродействия.

Каждый файл иерархической ФС может иметь предопределённые условия доступа, оговаривающие перечень допустимых операций с ним, которые уже нельзя будет изменить в процессе эксплуатации карты.

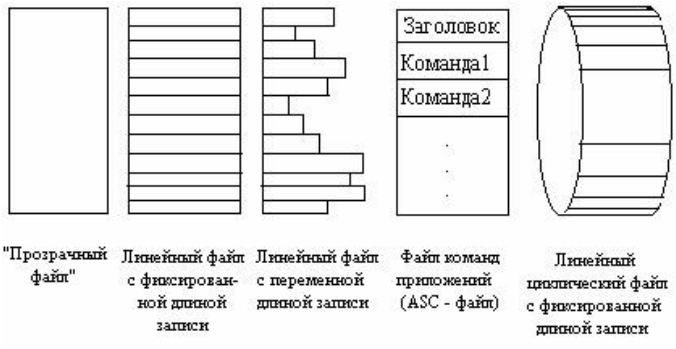


Рис. 9. Форматы файлов, используемые в смарт-картах

2.4. Методы обеспечения безопасности интеллектуальных карт

Важнейшим аспектом разработки и эксплуатации автоматизированной системы, использующей смарт-карты, является обеспечение безопасности информации, хранящейся и обрабатываемой на смарт-карте как в период её взаимодействия с терминальным оборудованием, так и в то время, когда карта находится в пассивном состоянии. В указанной проблеме можно выделить два аспекта:

- проблема защиты информации, технологический цикл обработки которой включает этап нахождения на смарт-карте;
- проблема собственной безопасности смарт-карты, которая, в свою очередь, включает защиту от взлома и подделки карты различными методами.

Решение проблемы состоит прежде всего в комплексном подходе к этому вопросу. В связи с этим представляется целесообразным всю совокупность используемых методов обеспечения безопасности разделить на следующие группы:

1. Защита от физических методов атаки и подделки:

- интегральная микросхема смарт-карты строится по принципу «защищённого модуля», т.е. любое физическое вмешательство, «вскрытие» модуля приводит к немедленному обнулению, стиранию всей хранимой в памяти информации либо карта аппаратно блокируется;
- на поверхность защищённого модуля наносится специальное защитное покрытие (металлизированное или оптически непрозрачное) с целью предотвращения возможности “прочтения” содержимого карты оптическим микроскопом высокого разрешения. Остаётся возможность чтения данных электронным микроскопом, но этот способ очень дорог и, вероятнее всего, окажется нецелесообразным по экономическим соображениям.

2. Аппаратно-программные методы защиты смарт-карт:

- функции безопасности ОС - набор команд ОС, обеспечивающих защиту файлов и работу с конфиденциальной информацией (см. п. 2.2.);

- защищённая файловая система (см. п. 2.3.).

3. Криптографические методы защиты:

- *Ведение ключевой системы карты* - файлы данных защищены трёхуровневой системой ключей: ключ эмитента, ключ пользователя смарт-карты (вырабатываемый из его PIN-кода) и ключи приложений. Ключи хранятся в системной области EEPROM. Применение того или иного ключа либо их комбинации зависит от типа выполняемой команды:
- *ключ эмитента* требуется предъявить, например, при форматировании ФС, снятии блокировки, записи других видов ключей;
- *ключ пользователя* необходим для выполнения любой транзакции, изменяющей данные на карте. В принципе, карта может иметь несколько пользовательских ключей. Тогда её могут совместно использовать несколько физических лиц, что удобно, если карта принадлежит предприятию или организации (юридическому лицу);
- наконец, *ключи приложений* необходимы для защиты отдельных файлов по чтению/записи при обращении к ним.
- *Безопасное управление паролями* - предполагает хранение паролей только в зашифрованном виде, обработку их в открытом виде только в пределах физически защищённого модуля, активизацию карты только после поступления правильно введённого PIN-кода (пароля).
- *Функция шифрования* - карта может содержать аппаратно реализованные алгоритмы симметричного шифрования (чаще всего DES) с отдельной областью памяти для хранения ключей (такой модуль часто называют «карманным шифратором», «шифровальной машинкой» и т.д.), что позволяет организовать защищённый обмен данными и протокол аутентификации по «протоколу рукопожатия» (см. п. 3.2.2.).
- *Аутентификация* - данный механизм включает в себя аутентификацию пользователя для смарт-карты, аутентификацию смарт-карты для терминала, с которым она работает и аутентификацию терминала для карты (последнее является необязательным, зависит от конкретной системы).
- *Проверка целостности сообщений*. Применяется механизм подсчёта контрольных сумм (CRC) сообщений, передаваемых между картой и ридером.

Помимо рассмотренных, необходимо отметить ***организационно-технические и нормативные методы***, но их подробное рассмотрение выходит за рамки данной работы, поскольку они скорее имеют отношение к автоматизированной системе в целом, чем к конкретному её элементу, каковым являются смарт-карты.

2.5. Устройства доступа. Организация обмена данными

Автоматизированная система, в которой используются пластиковые карты, независимо от её назначения, области применения и типа используемых пластиковых карт имеет ряд обязательных элементов. Так, доступ пользователя к ресурсам автоматизированной системы осуществляется через оконечное оборудование - терминалы, в случае банковских систем - банкоматы, автоматы выдачи наличности и т.п., снабжённые аппаратурой для приёма пластиковых карт, которая позволяет владельцу пластиковой карты взаимодействовать со средствами и ресурсами автоматизированной системы при посредстве принадлежащей ему пластиковой карты, носит название устройства доступа. Устройства доступа физически могут выполняться в виде отдельного блока, связанного с терминалом кабелем, либо встраиваться в терминал (кассовые аппараты, банкоматы). Устройства доступа называют также кард-ридерами (card-reader) или просто ридерами. Терминал, снабжённый устройством доступа, может быть автономным (при отсутствии линий связи). В этом случае накопленная в нём информация периодически снимается обслуживающим персоналом. Один или несколько терминалов могут быть подсоединены к

локальной вычислительной сети, имеющей, в свою очередь, выход в глобальную сеть. В ряде систем, использующих интеллектуальные карты, наличие связи терминала с сетью является обязательным, так как ИК делает запросы не только к терминалу, но и к хосту этой сети.

В данной работе не рассматривается подробно техническая и организационная структура банковской расчётной системы с использованием интеллектуальных карт. Необходимые сведения можно найти в главе 4. За подробной информацией можно обратиться к учебному пособию [9]. Интеллектуальная карта непосредственно взаимодействует с устройством доступа - весь обмен сообщениями между ИК и системой происходит через это устройство. Устройства доступа должны удовлетворять ряду очевидных условий:

- надёжность функционирования;
- дешевизна;
- защищённый обмен данными;
- возможность программирования выполняемых функций.

Устройства доступа выпускаются практически всеми фирмами-производителями смарт-карт. Рассмотрим, каким образом удовлетворяются обозначенные выше требования производителями этих устройств.

Надёжность функционирования обеспечивается тем, что ридеры для смарт-карт, в отличие от устройств чтения магнитных карт, не имеют механических частей, которые быстро изнашиваются, изнашивают карты, требуют профилактического обслуживания. В силу отсутствия дорогостоящих механических элементов стоимость кард-ридера ниже, чем устройства чтения магнитных карт - стоимость наиболее дешёвых моделей составляет $ 30 ... 60.

Возможность программирования выполняемых функций обеспечивается наличием в кард-ридере EEPROM объёмом до нескольких Кбайт. Специальные инструментальные пакеты для прикладных программистов позволяют разрабатывать все компоненты прикладной системы, связанной с обслуживанием смарт-карт: программное обеспечение (ПО) смарт-карты, серверные и клиентские (ПО терминала) компоненты и ПО кард-ридера. Возможность программирования может потребоваться, например, если кард-ридер работает с различными видами смарт-карт и требуется ввести в систему новый вид карт.

Например, фирма IBM разработала специальный интерфейс прикладного программирования CT-API (Chipcard Terminal API) в рамках специфицированной ею открытой архитектуры терминальных устройств Open SmartCard Terminal Architecture [45]. Как практическую реализацию данных принципов IBM выпускает серию кард-ридеров:

- IBM 4779 Hybrid Smart Card Device Models 001, 002;
- IBM 5948-B02/B03 Smart Card Accepting Device;
- IBM 4754 Smart Card Reader Device, обеспечивающий защищённый интерфейс SIU (Security Interface Unit) считывания информации с карты, который дополнительно может быть оснащён ручкой подтверждения подписи IBM 7446.

Наиболее сложной из перечисленных проблем является вопрос обеспечения безопасности взаимодействия карты и устройства доступа (кард-ридера). Рассмотрим последовательность сеанса связи карты и устройства доступа.

1. Установление сеанса связи схемами инициализации карты и устройства доступа. Когда контактная карта вводится в ридер, схема инициализации ридера посылает сигнал по линии RST схеме инициализации смарт-карты. Смарт-карта вырабатывает ответный сигнал, который посылает специальное сообщение ридеру о начале коммуникационного протокола. Оперативная память смарт-карты обнуляется.

Взаимодействие бесконтактной смарт-карты с ридером начинается, когда карта попадает в область видимости антенны ридера.
Коммуникационный протокол для контактных карт определяется стандартом ISO 7816, а для бесконтактных карт стандарты находятся в стадии разработки: ISO 10536-3,4, ISO 14443-2,3.
Следующий этап - выбор типа коммуникационного протокола, если система допускает использование нескольких протоколов. Основными типами коммуникационных протоколов являются асинхронные протоколы обмена ISO 7816-3 T=0 и ISO 7816-3 T=1. Последний является протоколом блочной передачи, обладающим возможностями обнаружения и коррекции ошибок.

2. Взаимная аутентификация ИК и устройства доступаразбивается, в свою очередь, на две подзадачи:

- аутентификация ИК для устройства доступа (выполняется в том или ином виде всегда);
- аутентификация «внешнего мира» для ИК (под «внешним миром» прежде всего подразумевается кард-ридер и терминал, к которому он подсоединён, но в ряде случаев карта может требовать аутентификацию хоста, к которому подсоединён терминал, чтобы исключить возможность общения карты с ложным, «подставным», терминалом.

В ряде случаев аутентификация может выполняться не только в начале сеанса связи, но и перед выполнением команды доступа к конфиденциальным данным, если это предусмотрено режимом доступа к файлу в COS (см., например, п. 2.6.).
Методы и протоколы аутентификации ИК и устройства доступа рассматриваются в п. 3.2.

3. Аутентификация владельца карты для самой ИКнеобходима для защиты ИК от деперсонификации.
Деперсонификация - это использование ИК незаконным владельцем, возможно, противником законного пользователя или лицом, желающим получить из этого определённую выгоду для себя.
В ряде приложений аутентификация владельца ИК является не только необязательной, но и ненужной, т.к. карта не несёт никакой информации о владельце, которая может нанести ему финансовый, материальный или какой-нибудь ещё ущерб (кроме, быть может, морального). Примерами являются медицина, транспортные услуги.
В остальных случаях такая аутентификация выполняется, особенно она важна в системах безопасности и финансовых (банковских) системах. В ряде случаев аутентификация владельца необходима не только в начале сеанса связи, но и перед выполнением некоторых ответственных операций с конфиденциальными данными, например при смене PIN-кода, разблокировании карты, изменении некоторых файлов, если это предусмотрено режимом доступа к ним.

4. Проверка карты по стоп-листу. Осуществляется проверка вхождения карты в перечень карт, по которым запрещено проведение одной или нескольких транзакций (например, карты, утерянные законным владельцем).

5. Выполнение технологических операций. Осуществляется проверка ключей, находящихся на карте, подсчёт контрольных сумм файлов (не осуществлялся ли несанкционированный доступ к содержимому памяти карты), простановка меток времени, установка блокировки (в случае отрицательного результата проверки по стоп-листу).

6. Выполнение операций, определяемых функциональным назначением карты (функциональный протокол). Далее следует выполнение тех операций, для которых собственно и предназначена ИК, например, снятие наличных денег со счёта, оплата каких-либо услуг, чтение/запись данных о владельце и т.д. (В дальнейшем данный этап будем называть *функциональным протоколом.*) В зависимости от назначения карты основным условием этого этапа может являться обеспечение безопасности считываемых, передаваемых и записываемых на ИК данных. Основным механизмом здесь также являются криптографические методы защиты информации (шифрование, хэш-функция, цифровая подпись, управление ключами).

Заметим, что этапу, когда происходит обмен информацией между картой и устройством доступа, в ряде случаев (например, при вычислении цифровой подписи) может предшествовать этап т.н. *предвычислений* (предварительных вычислений). В основном, этот этап протокола присутствует при выполнении сложных криптографических операций, когда некоторые арифметические вычисления можно выполнить предварительно, до интерактивного взаимодействия с устройством доступа, экономя тем самым время выполнения интерактивного взаимодействия.

7. ***Завершение протокола связи.*** Завершается сеанс связи посылкой сообщения об окончании коммуникационного протокола и деактивизацией контактов карты устройством доступа.

В соответствии со стандартом ISO 7816-4 обмен данными между ИК и устройством доступа осуществляется в пакетном режиме. ИК общаются с «внешним миром» при помощи специальных пакетов данных (APDU - Application Protocol Data Unit) по схеме «ведущий - ведомый» (master - slave), где ИК выполняет роль «ведомого». Пакеты APDU содержат либо команду, либо ответное сообщение. ИК всегда ждёт извне пакет APDU, выполняет указанное командой действие и отсылает ответный пакет. Между ИК и терминалом происходит непрерывный обмен пакетами, содержащими команды и ответы на них. Пакеты имеют следующий формат.

Формат пакета APDU:

Заголовок пакета (обязат.)				Тело команды			
CLA	INS	P1	P2	Lc	Поле данных	Le	

В заголовке кодируется выбранная команда, код которой состоит из 4-х полей:

- *CLA: байт класса* - используется для идентификации приложений в многофункциональных картах (см. п. 2.6);
- *INS: байт инструкции* - содержит код инструкции;
- *P1, P2: байты параметров* - содержат дополнительную характеристику или операнды инструкции.

Формат пакета ответа на команду APDU:

Тело ответа	Концевая часть (обязат.)	
Поле данных	SW1	SW2

- *SW1, SW2: байты состояния* - обозначают статус обработки ИК команды APDU.

2.6. Особенности устройства многофункциональных смарт-карт

Разработка и создание многофункциональных смарт-карт - одно из ведущих и наиболее перспективных направлений развития интеллектуальных карт. В этот процесс включились практически все ведущие мировые компании-разработчики и производители смарт-карт и оборудования для работы с ними: IBM, Bull, Siemens Nixdorf, Motorola и многие другие.

Стандарты для многофункциональных смарт-карт находятся пока в основном в стадии разработки или согласования в таких международных организациях и группах разработчиков, как EMV (Europay, Mastercard, Visa), OpenCard Framework, PC/SC, JavaCard. Поэтому представляется целесообразным

рассмотреть данную проблему на основе конкретного проекта фирмы IBM - семейства многофункциональных смарт-карт IBM MultiFunction Card. [44]

С точки зрения пользователя (держателя карты) её работу можно представить следующим образом [4]. Пользователь помещает карту в устройство доступа. Карта, взаимодействуя с терминалом, определяет, к какой системе относится данный терминал (платёжная система, система контроля доступа и т.д.). Если карта настроена на работу с данной системой, то в RAM подгружается программный модуль работы с конкретной системой. Далее карта, терминал и пользователь «общаются» по стандартам этого протокола.

Необходимость обеспечения в течение срока эксплуатации карты работы с несколькими автоматизированными системами накладывает определённые требования на физическое устройство и методы программной организации такой смарт-карты, и прежде всего это касается интерфейсной части, файловой системы, методов организации работы операционной системы карты и защиты памяти, в связи с чем многофункциональная ИК обладает рядом специфических особенностей аппаратно-программной организации, отличающих их от обычных ИК:

1. Иерархическая файловая система. Многофункциональная ИК предназначена для работы в среде нескольких автоматизированных систем, и её назначение и условия применения в рамках каждой из этих систем могут быть совершенно различными. Каждая из систем имеет своё прикладное ПО для взаимодействия с ИК (одно или несколько приложений). Каждое из приложений хранит на многофункциональной ИК свои файлы с данными, а иногда и с фрагментами исполняемых кодов программ приложения.Иерархическая файловая система наиболее естественным образом соответствует такому режиму работы ИК. Каждая прикладная система использует для хранения своих кодов и данных отдельный каталог ФС, в котором, в свою очередь, могут быть выделены подкаталоги для хранения данных отдельных приложений.

В семействе карт IBM MultiFunction Card нет ограничений на число уровней вложенности каталогов ФС - оно ограничено только ёмкостью EEPROM. Условия доступа к файлам определяются по двухуровневой схеме.

Во-первых, при создании каждого файла на этапе записи прикладного ПО на карту в процессинговом центре, в зависимости от назначения файла, предопределяются права доступа к нему. Они записываются в PROM и уже не могут быть изменены в процессе эксплуатации карты. Определены три варианта прав доступа:

- *чтение* - разрешено чтение данных, позиционирование указателя файла и т.д.;
- *обновление* - разрешено обновление записей файла, уменьшение величин, хранящихся в специальных структурах и т.д.;
- *администрирование* - разрешено создание/удаление файла, блокирование/разблокирование, чтение/запись и т.д.

Во-вторых, для файлов могут дополнительно определяться условия доступа, которые могут меняться в процессе эксплуатации карты и контролируются COS:

1) *ALW (Always)* - команда может осуществлять доступ к данным в любое время без ограничения;
2) *CHV1 (Card Holder Verification)* - перед выполнением команды, которая запрашивает доступ к данным прикладной программы, защищённой этим условием, владелец карты должен быть идентифицирован по стандартному протоколу;
3) *CHV2* - то же самое, но владелец карты идентифицируется по другому протоколу, что может использоваться, например, для разблокирования карты после попыток НСД;
4) *AUT (External Authentication)* - доступ к защищённым данным может быть предоставлен, только если закончилась с положительным результатом аутентификация внешнего по отношению к карте устройства (ридера, терминала, хоста);
5) *PRO (Protected)* - выполнение команды, запрашивающей доступ к защищаемым данным, должно выполняться в защищённом режиме (в частности, обязательно используются криптографические механизмы для проверки целостности - MAC (Message Authentication Code);
6) *ENC (Encrypted)* - в дополнение к условиям, устанавливаемым режимом PRO, запрос и ответ при доступе

к данным должен шифроваться. Применяется при доступе к секретной информации (такой как ключи и идентификаторы пользователя);
7) *NEV (Never)* - доступ к данным запрещён при любых обстоятельствах.

Изменение условий доступа может потребоваться, например, в следующем случае: многофункциональная карта предполагает возможность обращения клиента к нескольким поставщикам услуг (продавцам). В случае, если клиент по каким-либо причинам пожелает сменить продавца, необходимо будет перепрограммирование прикладного ПО карты и изменение прав доступа к файлам.

2. Наличие двух интерфейсов. Это позволяет использовать одну карту в приложениях, работа с которыми требует различных интерфейсов, например, сотрудник организации получает в своё распоряжение одну смарт-карту многоцелевого применения, которая используется и для разграничения доступа в помещение, и для защиты от НСД к компьютерам, и для начисления заработной платы и т.д. Но система доступа в помещение может использовать замок с радиоинтерфейсом, а система защиты от НСД к компьютерам - контактные кард-ридеры, встроенные в компьютеры;

3. Защита памяти и контроль операций ввода-вывода. Операционная система многофункциональных ИК должна обладать рядом особенностей, связанных с разделением оперативной памяти между различными приложениями:

- ОС должна обеспечивать защиту системной памяти от всех приложений и области приложений в EEPROM друг от друга;
- ОС должна обеспечивать защиту областей RAM от взаимного проникновения приложений.

Кроме того, ОС должна контролировать обмен данными с внешними устройствами [35].
4. Специальная архитектура микропроцессора. В [31] сообщается о разработке специального микропроцессора с PicoRISC-архитектурой для многофункциональных смарт-карт. Перечислим основные идеи, лежащие в основе PicoRISC архитектуры:

- выбор RISC-архитектуры нацелен на упрощение архитектуры процессора и системной шины, сокращение набора команд при увеличении скорости выполнения элементарных операций, из которых состоит набор команд RISC-процессора;
- формат команд однороден, а множество регистров общего назначения позволяют ограничить количество обменов с памятью, занимающих много времени работы процессора;
- особое внимание уделяется конструированию набора команд PicoRISC-процессора, который оптимизируется по трём критериям: простота, поддержка приложений на языке С, простота конструирования адаптированного компилятора, полнота набора операций;
- PicoRISC-процессор имеет два режима работы: «супервизор» и «пользователь». В пользовательском режиме доступ к памяти и внешний обмен происходит только через супервизор.

2.7. Методы технических атак на интеллектуальные карты

Различают следующие виды технических атак на ИК [18, 19, 20]: «атаки без вторжения», физические атаки, сложные методы атаки.

Первый тип атак подразумевает получение информации с ИК без физического проникновения внутрь карты. Данный метод использует технические слабости микроконтроллеров, в частности их неустойчивость к условиям окружающей среды и броскам напряжения на контактах. Известно, что при резких скачках напряжения питания или снижении тактовой частоты некоторые модели процессоров самопроизвольно передают на контакты ввода-вывода информацию из некоторых ячеек внутренней памяти. Броски напряжения вызывает большое количество ошибок процессора, что дезорганизует нормальную работу ОС карты. Сочетание специально подобранных нестабильных условий работы и загрузки в RAM специальной программы, заставляющей, например, последовательно считывать содержимое ячеек памяти в

определённом диапазоне и выводить их в последовательный порт, позволяет прочитать конфиденциальную информацию, содержащуюся в смарт-карте.

Физические атаки разнообразны и предполагают, в большинстве случаев, физическое вскрытие карты и воздействие на них другими физическими методами. Так, легко может быть снята защита памяти с карт с EPROM путём облучения УФ-светом битов, запрещающих доступ к определённым блокам памяти.

Для извлечения интегральной микросхемы из смарт-карты достаточно вырезать ножом из карты пластмассовую пластинку с микросхемой, растворить оставшуюся пластмассу каплей азотной кислоты и через несколько минут промыть микросхему в ацетоне, чтобы предотвратить дальнейшее разрушение её корпуса азотной кислотой. Некоторые микросхемы имеют специальное защитное покрытие, которое может быть удалено лазерным лучом или ультразвуком. Вскрытая микросхема может быть подвергнута различным методам изучения её структуры, например, с помощью оптических или электронных микроскопов. Информация с системной шины может быть считана специальными тестовыми микропробниками, которые имеются в микроэлектронных лабораториях.

Более сложные методы атак могут быть осуществлены лишь в специально оборудованных лабораториях, так как требуют специальных установок, стоимость которых очень высока. Такого типа методы получили название «reverse engineering» - «обратная инженерия». Они позволяют по уже готовому изделию изучить его структуру и разобраться в принципах функционирования.

Так, в [19] говорится о разработке метода послойного анализа структуры интегральной микросхемы. Отображения последовательных слоёв микросхемы затем вводятся в систему обработки изображений, которая идентифицирует элементы чипа и даже может классифицировать стандартные элементы, найденные в чипе. Авторы успешно опробовали свой метод на процессоре Intel 80386: анализ был выполнен за две недели работы. Фирмой IBM разработан исключительно мощный технический приём, позволяющий при известной послойной структуре и функциях чипа при помощи ультрафиолетового пучка лазера наблюдать его в процессе работы, фиксируя прохождение электрических сигналов по цепям схемы. Чувствительность метода такова, что может быть прочитан сигнал напряжением 5 В на частоте 25 МГц. Очевидно, что этот метод позволяет легко проанализировать микропроцессор смарт-карты, так как его тактовая частота обычно не превышает 15 МГц, а стандартное напряжение питания - 5 и 12 В. Для защиты от такого метода анализа предложены специальные «клеи» - покрытия, которые не просто непрозрачны и проводимы, но активно сопротивляются попыткам сдвинуть их с места, повреждая при этом саму микросхему. В ответ появились методы лазерного и ионного анализа, позволяющие наблюдать микросхему сквозь это покрытие.

В качестве мер защиты от физических атак возможны прежде всего криптографические методы. Один из первых предложенных методов - шифрование данных, передаваемых по системной шине микропроцессора смарт-карты. Такой приём используется, например, в микроконтроллерах Dallas DS5002FP и Dallas DS5002FPM, где применена модификация алгоритма DES: 15-битовый блочный шифр для шифрования адресов и 8-битовый блочный шифр для шифрования данных. Ключ последнего зависит от адреса зашифрованного байта, но маленький размер блока данных, обусловленный тем, что процессоры - байт-ориентированные, позволяет «вскрыть» алгоритм методом дифференциального криптоанализа [18]. Другой известный метод - использование асимметричной криптографии и механизма сертификации открытых ключей, но этот метод требует высокой производительности процессора. Однако методы криптографии чаще всего оказываются бессильными, если при проектировании или изготовлении процессора допущены грубый конструкторский просчёт либо нарушение технических условий, позволяющие, например, провести «атаку без вторжения».
В работе [20] выделяются также следующие виды атак на защищённые устройства:

- атаки, основанные на перепрограммировании микросхемы (chip rewriting attacks);
- перезапись ROM;
- модификация EEPROM;

- атака методом «разрушения входа» (gate destruction attacks) - основана на разрушении аппаратных устройств лазерным лучом;
- атаки, основанные на возможности «запоминания» RAM информации, хранившейся в ней в течение длительного периода времени, например PIN-коды клиентов в RAM ATM (automatic teller machine);
- атаки, основанные на слабостях реализации протоколов.

В [18] рассматриваются сценарии атак на ATM, в том числе систем VISA и Mastercard, и методов криптографического анализа шифров, используемых в этих системах, а также даётся обзор работ, связанных с этой проблемой.

Раздел 3. Реализация криптографических алгоритмов на интеллектуальных картах

3.1. Особенности применения криптографических алгоритмов на интеллектуальных картах

Особенности применения криптографических алгоритмов на интеллектуальных картах обусловлены следующими группами причин:

- ограниченностью рабочего пространства ИК, её аппаратных возможностей и быстродействия;
- функциональным назначением и применениями ИК: исторически первой функцией пластиковых карт являлась аутентификация, в которой карта выступала носителем идентификатора пользователя (поэтому широкое распространение получило наименование «идентификационные карты»), необходимость аутентификации очевидна в финансовых транзакциях;
- сменой приоритетов в защите информации в банковских системах по сравнению с системами, в которых обрабатывается информация, составляющая государственную тайну. Если в государственных системах на первое место ставится конфиденциальность информации, далее следуют целостность и готовность, то в банковских системах на первое место ставится готовность, на второе - целостность и на третье место - конфиденциальность.

Каким образом влияют эти причины на выбор криптографических алгоритмов и каковы особенности?

Алгоритмы шифрования. Интеллектуальная карта может использоваться как «шифровальная машинка», или «карманный шифратор» с аппаратно реализованным алгоритмом блочного шифрования и хранящимися на ней ключами шифрования. Здесь можно отметить следующие особенности:

- при создании шифраторов основной целью является стойкость системы, поэтому необходимо использовать стандартные алгоритмы (ГОСТ, AES, 3DES, FEAL, IDEA, ...);
- стандартный алгоритм симметричного шифрования удобен для реализации протоколов аутентификации данных, логической аутентификации пользователя, «протокола рукопожатия»;
- немаловажной является простота реализации симметричных алгоритмов;
- ограниченная производительность процессора смарт-карт.

В силу указанных причин наибольшее распространение на сегодняшний день получили протоколы, основанные на использовании симметричных алгоритмов, хотя всё более широкое распространение получают асимметричные алгоритмы (например, в спецификациях EMV и PC/SC).

Указанный случай применения интеллектуальной карты как шифратора является самым простым. Алгоритмы шифрования используются как «строительные блоки» (криптографические примитивы) для конструирования сложных криптографических протоколов.

Схемы аутентификации. Задача аутентификации появилась в связи с развитием технических систем, в особенности осуществляющих финансовые транзакции - ранее она не стояла. Исследования в области протоколов аутентификации начались в конце 80-х гг. Для аутентификации могут быть применены различные схемы, следовательно, есть возможность выбрать наиболее эффективную или предложить новую, усовершенствованную. Задача аутентификации носит многоплановый характер - как будет показано далее, для ИК задача распадается на две составляющие: взаимная аутентификация технических средств (ИК и сети) и аутентификация пользователя в системе.

Схемы цифровой подписи. ИК могут применяться в качестве персонализированного аппаратного средства для генерации владельцем своей цифровой подписи. Далее будет рассматриваться стандартный метод преобразования асимметричного протокола аутентификации в схему цифровой подписи, но здесь также есть возможность выбора наиболее эффективной или наиболее удобной схемы. Причём, учитывая ограниченные аппаратные возможности смарт-карт, в ряде случаев идут на некоторое снижение стойкости схемы ЦП за счёт повышения эффективности выполняемых операций, производительности. Действительно, не всегда необходимо использовать схемы ЦП с большим «запасом прочности» от вскрытия: можно найти «золотую середину» между стойкостью схемы и временной сложностью выполняемых при её генерации и проверке операций. Схема ЦП используется в качестве криптографического примитива в более сложных схемах, например, в протоколе динамической аутентификации сообщений.

Схемы управления ключами. ИК могут использоваться для генерации и распространения ключей криптосистемы. Для симметричных и асимметричных криптосистем эти схемы различны, и при использовании интеллектуальной карты в качестве персонализированного генератора и носителя ключей возникают свои особенности. Одно из наиболее перспективных направлений связано со схемой сертификации ключей, используемой в асимметричных криптосистемах с большим числом участников.

Специальные алгоритмы и протоколы, включающие криптографические механизмы. В последнее время получила развитие идея об использовании в сетевых вычислительных средах так называемых «электронных денег» и «электронных чеков» - аналога обычных расчётных средств. К данному классу алгоритмов относятся, в первую очередь, криптографические протоколы для расчётов «электронными деньгами», протоколы, связанные с использованием ИК в качестве «электронного кошелька» - носителя «электронных денег», так называемые «предоплаченные» схемы и др. Данные протоколы относятся, в основном, к прикладному уровню.

3.2. Схемы аутентификации

3.2.1. Задачи аутентификации

Интеллектуальная карта предназначена для взаимодействия лица, предъявляющего карту, со средствами автоматизированной системы. Взаимодействие осуществляется при помощи терминала (в случае банковских систем - чаще всего банкомата или POS-терминала) или устройства доступа. Задача взаимодействия держателя ИК с автоматизированной системой распадается на две задачи (рис. 10):

- взаимодействия ИК со средствами автоматизированной системы (в частности, с устройством доступа) - взаимная аутентификация, передача данных и выполнение операций с данными, в частности, финансовой транзакции;
- аутентификация предъявителя ИК для самой карты и для средств автоматизированной системы.

Рис.10. Аутентификация элементов автоматизированной системы с интеллектуальными картами

Эти задачи являются важнейшими составными элементами протокола взаимодействия ИК с устройством доступа при осуществлении транзакции (см. п. 2.5). Напомним, что аутентификация ИК и средств автоматизированной системы может быть как взаимной, так и односторонней, если необходимости во взаимной аутентификации не возникает (в последнем случае, как правило, осуществляется только аутентификация ИК).
Следует отличать:

- аутентификацию ИК для терминала;
- аутентификацию терминала для ИК (в ряде случаев требуется более «глубокая» аутентификация: хоста или целого сегмента сети, к которому подсоединён терминал);
- аутентификацию приложения для ИК.

Для аутентификации могут быть применены различные схемы, которые можно разделить на группы, соответствующие схемам, основанным на асимметричных криптографических алгоритмах (рассматриваются в п. 3.2.4), и схемам, основанным на симметричных алгоритмах (п. 3.2.5).

Аутентификация предъявителя ИК необходима для защиты законного владельца ИК от деперсонификации. Говоря об аутентификации предъявителя карты принято различать следующие понятия.

Владелец карты - это лицо, которое владеет ИК на законном основании. Следует отличать понятие «*держатель карты*» - это лицо, фактически владеющее ИК и предъявляющее её средствам автоматизированной системы. Он мог получить карту в своё распоряжение как законным путём, так и незаконно (например, украсть у законного владельца, найти потерянную законным владельцем карту, изготовить «фальшивую» карту и т.п.). Задача аутентификации физического лица, предъявляющего карту системе, заключается именно в том, чтобы установить, является ли держатель карты её законным владельцем.

В ряде случаев в вычислительных сетях требуется аутентификация удалённого пользователя.

Третьей важной задачей является аутентификация (проверка целостности и подтверждение достоверности источника) данных при осуществлении транзакции (передаче данных между ИК и устройством доступа). Таким образом осуществляется подтверждение подлинности транзакции.

Хотя задачи обеспечения целостности и конфиденциальности сообщений в коммуникационном протоколе могут быть решены стандартными криптографическими средствами (хэш-функция, блочные шифры, симметричные алгоритмы в режиме аутентификации сообщений) и широко используются в реальных системах, появляются дополнительные задачи, связанные с «доказательством транзакции» - должна обеспечиваться юридическая значимость транзакции.

3.2.2. Аутентификация держателя карты

Различают два метода аутентификации владельца ИК: логический и биометрический.

3.2.2.1. Логическая аутентификация

Логическая аутентификация основана на принципе «пользователь знает», т.е. лицу, предъявившему ИК, предлагается ввести некоторую информацию (число, пароль и т.п.), которую знает только законный владелец карты. Рассмотрим основные способы логической аутентификации владельца ИК.

PIN-код (Personal Identification Number). Перед началом выполнения финансовой транзакции (снятие денег со счёта, оплата покупки и т.д.) предъявителю карты предлагается ввести известный только ему персональный (личный) идентификационный номер, сокращённо называемый PIN - Personal Identification Number. Как правило, число попыток ввода PIN ограничено (не более 3-х). В случае, если PIN введён неверно, карта блокируется (временно или постоянно) либо задерживается терминалом и выдаётся владельцу ИК в отделении банка после удостоверения его личности. Смарт-карта хранит у себя в системной области EEPROM зашифрованный PIN её владельца. В случае совпадения значений PIN'ов карта активизируется для выполнения финансовой транзакции.

PIN-код является наиболее распространённым на сегодняшний день методом в автоматизированных банковских системах. Технология работы с PIN-кодами хорошо отработана и используется подавляющим большинством банков. PIN-код выдаётся клиенту при получении карты в запечатанном конверте. Никто из персонала банка не знает PIN-кода клиента. Однако в целях повышения степени защищённости клиента он может впоследствии во время совершения транзакции поменять свой PIN-код.

Парольная защита. Пользователю предлагается ввести некоторый пароль. Ввод пароля может осуществляться по-разному: просто набор пароля на клавиатуре терминала без отображения на дисплее, ввод пароля в определённых позициях более длинной строки, ввод числа, которое владелец должен сосчитать в уме по известным ему правилам из выведенного на дисплее числа и т.п.

На основании сравнения предъявленной информации с информацией (соответственно PIN или паролем), хранящейся на ИК в зашифрованном виде, определяется, является ли предъявитель карты аутентичным. В этом случае нельзя исключить вероятности того, что в случае утери, кражи ИК или подбора пароля противник получит доступ к системе.

Рассмотрим некоторые протоколы логической аутентификации держателя карты. Общие условия протоколов:

1) держатель карты в процессе выполнения протокола (или перед ним) вводит свой PIN (пароль) с использованием аппаратуры доступа к автоматизированной системе;

2) PIN (пароль) владельца карты в том или ином виде хранится в памяти ИК.

Сразу отметим, что логическая аутентификация пользователя может иметь место не только в случае обращения пользователя к локальным средствам автоматизированной системы, но также в случае обращения держателя ИК к удалённым процессам через сетевую среду. В этом случае пользователь рассматривается как удалённый (remote entity); для такого взаимодействия протоколы несколько видоизменяются. Лицо, обращающееся к системе в режиме удалённого доступа, трактуется именно как

пользователь, а не держатель карты, и должна быть установлена аутентичность пользователя как целого (физическое лицо + ИК), чаще понимаемая как аутентичность клиентского процесса.

Стандартным методом логической аутентификации является так называемый метод CHV (Cardholder verification) - ввод PIN или пароля (объединяемые понятием CHV-код) по запросу от приложения, передаваемому ОС карты и преобразуемому в команду VERIFY (см. п. 2.2). Шифрование CHV-кода не является обязательным - устройство ввода в принципе может даже не иметь функций шифрования. CHV-код также может храниться на карте как в зашифрованном, так и в открытом виде. Однако шифрование PIN применяется практически всегда, когда существует угроза перехвата злоумышленником PIN при передаче от устройства ввода на карту.

Для *проверки PIN* могут использоваться простейшие протоколы:

1. Протокол для карты со встроенной функцией шифрования (протокол внутренней логической аутентификации) (табл. 1). Смарт-карта и устройство доступа имеют встроенные алгоритмы шифрования. PIN-код хранится на карте в системной области памяти. Смарт-карта вырабатывает случайное число *c* и посылает его устройству доступа. Устройство доступа зашифровывает введённый на нём предъявителем *PIN*, зашифровывает его вместе с числом *c* (символ // обозначает конкатенацию) на ключе приложения *A-key* и пересылает карте. Карта выполняет ту же операцию с хранящимся на ней персональным идентификационным номером *PIN′*, сравнивает результаты вычислений и принимает решение о подлинности пользователя. (Символ =? здесь и далее означает проверку выполнения равенства.)

Таблица 1

ИК	Устройство доступа
c — случ. ———	———>
<——— *PIN′ —> r′=EA-key(PIN′||c)*	——— *r=EA-key(PIN||c)*
r =? r′	

2. Протокол для карты без встроенной функции шифрования (протокол внешней логической аутентификации). Смарт-карта не имеет встроенной функции шифрования, PIN владельца записывается на неё в зашифрованном виде и в дальнейшем только считывается. Устройство доступа вырабатывает случайное число *c*, посылает его карте. Смарт-карта вычисляет хэш-функцию *h* (контрольную сумму) от зашифрованного на общем для ИК и устройства доступа ключе *K* персонального идентификационного номера *PIN*, сцепленного со случайным числом *c* и ключом приложения *A-key*, которую отправляет устройству доступа. Устройство доступа выполняет те же действия с введённым пользователем *PIN′*, сравнивает результаты *h* и *h′* и принимает решение о допуске пользователя к системе. На карте заводится специальный файл, в котором хранятся данные, необходимые для проверки подлинности пользователя (т.н. «код верификации держателя карты» (CHV - Cardholder Verification)): флаг разрешения/запрещения ввода; длина CHV-кода (от 4 до 16 байт); CHV-код; количество попыток неверного ввода; указатель оставшихся попыток неверного ввода; ссылка на разблокирование. Файл защищается по чтению, записи и стиранию.

Проверка PIN владельца может включаться в состав более сложных протоколов взаимной аутентификации.

Интересным примером протокола логической аутентификации для метода *парольной защиты* является протокол Мацумото - Имаи (Matsumoto - Imai) [56, 71]. Пользователю, проходящему аутентификацию, достаточно помнить пароль, состоящий из нескольких цифр, и проделывать в уме простейшие операции с этими цифрами: сравнение и размещение по ячейкам в определённом порядке в так называемом «окне». Протокол защищает от атаки методом «подглядывания» цифр, вводимых пользователем на клавиатуре, и от атаки методом перехвата пароля, передаваемого по сети.

3.2.2.2. Биометрическая аутентификация

В связи с вышесказанным всё чаще применяются биометрические методы аутентификации владельца ИК (биометрия), особенно в системах с повышенными требованиями к безопасности [72, 73].

Биометрическая аутентификация основана на принципе «пользователь имеет», т.е. у лица, предъявившего ИК устройству доступа, производится замер некоторых физиологических параметров - такая информация не может быть «утрачена» пользователем или «передана» другому лицу - и на основании сравнения их с эталоном, сформированным заранее на основании контрольных замеров, принимается решение, является ли предъявитель аутентичным. Процедура биометрии выполняется через специальные устройства, подсоединяемые к терминалу или интегрированные с кард-ридером.

Важнейшими характеристиками биометрической системы являются:
- вероятность принятия системой ошибочного решения (статистическая ошибка II рода) — принятие системой незаконного пользователя;
- вероятность отклонения системой правильного решения (статистическая ошибка I рода) - отклонение системой законного пользователя.

Очевидно, что разработчики систем стремятся уменьшить до минимума ошибку принятия ложного решения как значительно более опасную для системы, в то время как ошибка отклонения законного пользователя не несёт в себе опасности - пользователь может обратиться к системе повторно.

Для измерения биометрических характеристик выбираются признаки, единственным образом идентифицирующие каждого человека.

Система биометрического распознавания пользователя состоит из пяти основных компонент: подсистема сбора данных, подсистема обработки сигнала, подсистема принятия решения, подсистема передачи данных и подсистема хранения данных.

Биометрические методы принято подразделять на методы *физической биометрии (physical biometrics)* и *«поведенческой» биометрии (behavioural biometrics)*.
В настоящее время используются следующие методы физической биометрии: отпечатки пальцев (fingerprinting); рисунок сетчатки глаза; узор радужной оболочки глаза; рисунок кровеносных сосудов на руке; геометрия руки; распознавание лица; запах тела.

Методы «поведенческой» биометрии: распознавание голоса; динамика подписи; динамика печатания на клавиатуре.
Каждый из этих методов имеет свои достоинства и недостатки, однако в целом биометрические методы благодаря их высокой надёжности находят всё более широкое применение, предлагаются новые и совершенствуются старые методы.

Компьютерное сканирование и распознавание лица. Этот метод удобен для смарт-карт в связи с тем, что описательная информация может быть сжата одним из алгоритмов сжатия и храниться в памяти самой ИК, что позволяет провести биометрическую аутентификацию в режиме off-line. Кроме того, систему можно построить таким образом, чтобы она была самообучающейся, т.е. корректировала данные о пользователе при очередном обращении пользователя к системе.

3.2.4. Протоколы, основанные на асимметричных алгоритмах

В этом разделе мы рассмотрим наиболее эффективные и «конкурентноспособные» из известных схем аутентификации, а также некоторые их усовершенствования и расширения.
Обзор наиболее известных асимметричных протоколов аутентификации можно найти в [63].
В [2] используется следующая классификация асимметричных протоколов:

- *протоколы с центром доверия* - к ним относятся схемы, в которых идентификаторы и открытые ключи всех абонентов хранятся в общедоступном сертифицированном справочнике в центре доверия, а выполнение любого протокола начинается с предварительного шага, когда

доказывающий посылает свой идентификатор и открытый ключ проверяющему, а проверяющий устанавливает их подлинность по справочнику;

- *протоколы, основанные на идентификационной информации* — каждый абонент имеет общеизвестный идентификатор, позволяющий установить его подлинность путём выполнения некоторых вычислений над идентификатором, а участие центра доверия в таких протоколах ограничено выдачей абонентам интеллектуальных карт.

Общая идея асимметричных протоколов аутентификации состоит в том, что законный пользователь *P*, имеющий открытый и секретный ключи, и проверяющий *V* выполняют совместный криптографический протокол интерактивного доказательства, в процессе которого *P* должен доказать свою подлинность, продемонстрировав знание секретного ключа законного пользователя, но не разгласив его для проверяющего *V* (т.е. из информации, полученной *V*, вычислительно невозможно получить секретный ключ *P*).

Все протоколы имеют два этапа: предварительный и рабочий. На предварительном, который выполняется заранее, при выдаче ИК владельцу, специфицируются некоторые параметры протокола, вырабатываются необходимые величины, участвующие в рабочем этапе протокола (в частности, открытые и секретные ключи *P*). На рабочем этапе, который осуществляется в процессе выполнения транзакции, собственно выполняется доказательство подлинности *P*. Предварительный и рабочий этапы каждого протокола будут отмечены при объяснении соответствующих схем.

1. Протоколы Файге - Фиата - Шамира. Это первый из предложенных типов протоколов (1986 г.). Схема использует теорию доказательств с нулевым разглашением. Рассмотрим вначале упрощённый (первоначально предложенный) протокол (табл. 2).

Здесь и далее для наглядного отображения операций, составляющих протокол, используются таблицы следующего формата. Таблица состоит из двух частей, соответствующих предварительному (а) и рабочему (б) этапу протокола. В каждой части таблицы на первой строке перечисляются участники данного этапа протокола. В протоколе участвуют *P, V* и арбитр (центр доверия) - условное представление лица, выдающего и обслуживающего смарт-карты клиентов, которому они доверяют. Далее в столбцах таблицы, соответствующих каждому из участников протокола, последовательно отображаются их действия (вычисления, пересылка и приём сообщений от партнёров по протоколу). Целью предварительного этапа является выработка секретной и открытой информации, необходимой для каждого из участников на рабочем этапе. В последней строке таблицы, относящейся к предварительному этапу, не разделённой на столбцы, записаны общие для всех участников открытые параметры, выработанные на предварительном этапе. Пересылки сообщений между участниками изображены стрелками. Проверка выполнения равенств (сравнений) обозначена соответственно знаками =? и ≡ ?.

Таблица 2

(а) Предварительный этап		
P	V	Центр доверия
s, v		*n=pq — случ. v∈QRn s=min.{sqrt(v-1) mod n}*
n, v		
(б) Рабочий этап		
	P	V
1	*r — случ., r<n x=r2 mod n* ———	———>

2	<———	——— $b \in \{0,1\}$ — случ.
3	*if (b=0)* *r* ——— *if (b=1)* *y=r*s (mod n)* ———	———> ———>
4		*if (b=0) x=? r2 (mod n)* (Знает ли *Psqrt(x)* ?) *if (b=1) x=? y2*v (mod n)* (Знает ли *P sqrt(v-1)* ?)

На предварительном этапе центр доверия выбирает два больших простых числа *p,q* (которые он держит в секрете) и публикует большое число $n \in \mathbb{Z}$ *: n=pq, n*$\geq$ 512 бит (рекомендуется *n* ~ 1024 бит; для упрощения вычислений, но не для повышения безопасности рекомендуется выбирать *n=(4p+3)(4q+3)* - число Блюма). * - означает операцию модульного умножения. Далее арбитр выбирает $v \in QR_n$ (квадратичный вычет по модулю *n*), т.е. число *v*, такое что $\exists x: x^2 \equiv v (\mathrm{mod}\, n)$, $\exists v^{-1} \bmod n$ - это открытый ключ *P*, *s* - минимальный из квадратичных корней числа *v-1* mod *n* - секретный ключ *P*.

Возможность существования нескольких квадратичных корней по mod *n* поясним на следующем примере. Пусть *n*=15 ($p \cdot q = 5 \cdot 3$). $v = 4 (\exists x = 2 : v = 4 = 2^2 = x^2, v^{-1} = 4)$. Тогда *s*=2,7, так как $2 \cdot 2 \equiv 4 \bmod 15$ и $7 \cdot 7 \equiv 4 \bmod 15$. Минимальное *s*=2 - оно и будет секретным ключом.
Рабочий этап протокола состоит в следующем. В цикле выполняются действия (смысл цикла будет пояснён ниже; в таблице показано содержание одного цикла):
(1) *P* выбирает случайное число *r, r < n*, вычисляет *x=r2* mod *n* и отправляет его проверяющему *V*;
(2) *V* вырабатывает случайный бит $b \in \{0,1\}$ и посылает его *P*;
(3) Если *b=0, P* отправляет *V* число *r*, в противном случае (*b*=1) он отправляет *V* число *y=r*s*(mod *n)*;
(4) *V* проверяет выполнение равенств:
$x \equiv r2 \bmod n$, если *b*=0; $x \equiv y2 * v \bmod n$, если *b*=1.
В первом случае он таким образом проверяет знание участником *P* квадратного корня *sqrt(x) (*mod *n)* числа *x*, которое он ему прислал на шаге (1). Во втором случае он проверяет знание *sqrt (v-1).*

Действия (1) — (4) повторяются в цикле *t* раз. Если *P* не знает секретного ключа *s*, он может выбрать *r* так, что сможет обмануть *V*, если он прислал *P* число *b*=0, либо если он прислал *b*=1, но не сможет сделать то и другое сразу. Вероятность обмана при однократном выполнении действий (1) - (4) равна 1/2, соответственно при выполнении цикла *t* раз вероятность равна *1/2t*. Число *t* называют *параметром безопасности* протокола. Считается, что *P* прошёл аутентификацию, если проверка сравнения на шаге (4) во всех *t* циклах прошла с положительным результатом.

В качестве противника может выступать и *V* (противника будем обозначать *V'*). Заметим, что для *V* вычислительно невозможно получить *s* из числа *y*, так как для этого ему придётся решать задачу факторизации. Однако в случае, если *P* в шаге (1) вместо того, чтобы выбрать *r* случайным образом, возьмёт его из одного из предыдущих раундов, вероятность выбора участником *V'* того же бита *b*, что и в том раунде, из которого взято *r*, равна 1/2 - следовательно, вероятность того, что *V'* обманет *P*, равна 1/2. При выполнении цикла *t* раз эта вероятность равна *1/2t.* Если же *V* выберет другой бит *b*, он сможет вычислить секретный ключ *s*:

$$\left.\begin{array}{l} x \equiv r^2 \bmod n \\ x \equiv y^2 \cdot v (\mathrm{mod}\, n) \end{array}\right\} \Rightarrow r^2 \equiv y^2 * v (\mathrm{mod}\, n), r^2 \equiv (r * s)^2 * v (\mathrm{mod}\, n)$$

,

где *r, v* - известно, $s^2 * v \equiv 1 (\mathrm{mod}\, n).$

Получаем двучленное сравнение 2-й степени, решив которое, *V'* находит *s*. Отсюда следует вывод, что повторы *r* недопустимы.

Позднее те же авторы усовершенствовали протокол, показав, что параллельная конструкция протокола снижает число раундов обмена между *P* и *V*.

Число *n* выбирается как и в предыдущем случае. Далее выбираются *k* различных чисел $\{v_i\}_{i=1}^{k}, v_i \in QR_n$. Строка $\{v_i\}_{i=1}^{k}$ принимается в качестве открытого ключа *P* , а строка $\{s_i\}_{i=1}^{k}$, где $s_i = \min.\{sqrt(v_i^{-1}) \bmod n\}$ - секретный ключ абонента *P*.

Рабочий этап протокола аналогичен рабочему этапу предыдущего протокола. В цикле *t* раз выполняются следующие действия:

(1) *P* выбирает случайное число *r, r < n*, вычисляет *x=r2* mod *n* и отправляет его проверяющему *V*;

(2) *V* вырабатывает случайную двоичную строку $\{b_i\}_{i=1}^{k}, b_i \in \{0,1\}$ и посылает её *P*;

(3) *P* вычисляет $y = r^* \prod_{i=1}^{k} s_i^{b_i}$, перемножая те *si*, которые соответствуют единичным битам вектора *b,* и посылает *y* проверяющему;

(4) *V* проверяет, что $x = y^2 * \prod_{i=1}^{k} v_i^{b_i}$.

В данном протоколе вероятность обмана в *t* проходах цикла равна *1/2kt*. Авторы рекомендуют *k*=5, *t*=4.

Заметим, что в реальной системе рабочему этапу протокола всегда предшествует следующая предварительная операция. При обращении *P* к системе с его ИК считываются идентификатор *IDP* и открытый ключ. Так как число клиентов, обращающихся к системе, очень велико, терминал не может хранить открытые ключи всех клиентов. Открытые ключи хранятся в справочнике (базе данных) вместе с соответствующими идентификаторами абонентов. Проверяющий *V* проверяет подлинность предъявленных идентификатора и открытого ключа (т.е. устанавливает подлинность самого факта присутствия данного клиента в системе), обращаясь к базе данных, поддерживающейся центром доверия, где он проверяет подпись *DSP* центра доверия под этой информацией. Очевидно, что для осуществления такой проверки терминал должен работать в режиме on-line.

Авторами также предложена модификация протокола - протокол, основанный на идентификационной информации.

Замечание. Все рассмотренные выше протоколы являются протоколами односторонней аутентификации (ИК для устройства доступа). Задача взаимной аутентификации может быть решена с помощью тех же протоколов, но используемых в «зеркально симметричном» виде: *V* вырабатывает секретный и открытый ключи, *P* выступает в роли проверяющего, а все пересылки осуществляются наоборот.

Стойкость протокола Фиата - Шамира основана на сложности извлечения квадратного корня по модулю *n*, когда неизвестно разложение *n* на множители. Ohta и Okamoto в работе [60] предложили подобную схему, основанную на сложности извлечения корня степени *L* по модулю *n*. В этой схеме дополнительно к параметрам *t,k* вводится параметр *l=[log2L].* Стойкость такого протокола равна *tkl.*

В работе [53] Knobloch предложил реализацию протокола FFS для смарт-карт. На 8-битовом микропроцессоре смарт-карты, имеющей 256 байт RAM и 2 Кбайт EEPROM, время аутентификации составило около 6 с. Объём ассемблерного кода в EEPROM - около 700 байт, используемая RAM - 256 байт, длина идентификационной информации - 120 байт, вероятность принятия ошибочного решения - 2-20. При этом с целью повышения эффективности алгоритма часть вычислений (например, тесты на простоту) была

перенесена на компьютер с устройством доступа, были внесены некоторые изменения в исходный протокол FS, применены специальные алгоритмы генерации псевдослучайных чисел и модульного умножения.

2. Протокол Шнорра и основанные на нём протоколы.

Схема предложена в 1989 г. Центр доверия выбирает и открыто публикует два простых числа *p* и *q: q | p-1* и число $a \neq 1 : a^q \equiv 1 (\mathrm{mod}\, p)$. Далее выбирается случайное число *s<q*, становящееся секретным ключом *P*, и вычисляется *v=a-s* mod *p* - открытый ключ.

Протокол аутентификации состоит в следующем:
(1) *P* выбирает случайное число *r<q*, вычисляет *x=ar* mod *p* и посылает *x* проверяющему *V* (вычисления могут быть выполнены предварительно);
(2) *V* вырабатывает случайное число *e:* $0 < e \leq 2^t - 1$ и посылает его *P*;
(3) *P* вычисляет *y=(r+se)* mod *q* и посылает его *V*;
(4) *V* проверяет, выполнено ли равенство *x=ayve* mod *p*.

Как видно, проверка подписи *P* основана на том, что в вычислениях *P* на шаге (3) участвует его секретный ключ *s,* который, однако, *V* вычислить не может вследствие трудности задачи дискретного логарифмирования. *P* считается прошедшим аутентификацию, если проверка сравнения на шаге (4) прошла с положительным результатом.
Безопасность протокола основана на величине параметра *t*. Авторы указывают, что сложность вскрытия протокола — порядка *2t*, и рекомендуют: *p*~512 бит, *q*~140 бит, *t*=72. Свойство нулевого разглашения для схемы Шнорра не доказано.
Брикелл и Мак-Карли предложили в 1990-91 гг. модификацию протокола Шнорра [26].

4. Протоколы, основанные на схеме Эль-Гамаля. В качестве примера протокола, основанного на схеме Эль-Гамаля, рассмотрим протокол Beth из работы [22]. Автор указывает, что протокол построен по типу схемы Фиата - Шамира. Данный протокол относится к классу протоколов, основанных на идентификационной информации.

На предварительном этапе центр доверия выбирает секретные числа $\{x_i\}_{i=1}^m$ и публикует $\{y_i\}_{i=1}^m, y_j = \alpha^{x_i}$, где α - примитивный элемент поля *GF(q)* - общеизвестен. Также центр доверия публикует хэш-функцию *f.*

По запросу *P* центр доверия генерирует для него идентификационные номера $\{ID_i\}_{i=1}^m$, *IDj=f(name(P), j).*

Далее центр доверия выбирает секретное случайное число *k=kp* и формирует $r = \alpha^k$, а также вычисляет $\{s_i\}_{i=1}^m$ как решения сравнения $x_j r + k s_j \equiv ID_j \bmod (q-1), j = \overline{1,m}$.
Центр доверия записывает на ИК клиента *P* следующую информацию: *{r, s1, s2, ... , sm}. r* - открытый ключ *P,* $\{s_i\}_{i=1}^m$ - секретный ключ *P.*

На рабочем этапе выполняются следующие действия:
1) *V* считывает с ИК клиента *P* его имя *name(P)* и открытый ключ *r. V* вычисляет идентификационные номера *P* и числа $\{\rho_i\}_{i=1}^m$:

$ID_j = f(name(P), j), j = \overline{1,m}, \quad \rho_j = y_j^r$.

2) Следующие шаги выполняются в цикле для $i = \overline{1,n}$:

2.1. *P* вырабатывает случайное число $t_i \in Z_{q-1}$, вычисляет $z_j = r^{-t_i}$ и посылает его *V*;

2.2. *V* вырабатывает случайную строку $\vec{b}_i = (b_{i1}, b_{i2}, \ldots, b_{im}) \in R^m, R \subset Z_{q-1}$ и посылает её *P*;

$$u_i = t_i + \sum_{j=1}^{m} b_{ij} s_j \bmod (q-1)$$

2.3. *P* вычисляет и посылает его *V*;

2.4. *V* вычисляет

$$y_i = \sum_{j=1}^{m} b_{ij} \cdot ID_j,$$

$$\gamma_i = \left(\prod_{j=1}^{m} \rho_j^{b_{ij}} \right) \cdot r^{u_i} \cdot z_i - \alpha^{y_i}.$$

V принимает доказательство в случае, если $\gamma_i = 0, i = \overline{1,n}$.

Действительно,

$$\prod_{j=1}^{m} \rho_i^{b_{ij}} = \prod_{j=1}^{m} y_j^{r b_{ij}} = \alpha^{r \sum_{i=1}^{n} x_i b_{ij}},$$

$$r^{u_i} \cdot z_i = r^{\left(t_i + \sum_{i=1}^{n} b_{ij} s_i \right) \bmod (q-1)} \cdot r^{-t_i} = r^{\sum_{i=1}^{n} b_{ij} s_i},$$

$$\gamma_i = \left(\prod_{j=1}^{m} \rho^{b_{ij}} \right) \cdot r^{u_i} \cdot z_i - \alpha^{y_i},$$

но

$$\alpha^{r \sum_{i=1}^{n} x_i b_{ij}} \cdot r^{\sum_{i=1}^{n} b_{ij} s_i} = \alpha^{k \sum_{i=1}^{n} b_{ij} s_i} = \alpha^{\sum_{i=1}^{n} b_{ij} (x_i + k s_i)} = \alpha^{\sum_{i=1}^{n} b_{ij} \cdot ID_i} = \alpha^{y_i}.$$

Следовательно, $\gamma_i = 0$.

Вероятность принятия ошибочного решения проверяющим *V* равна *1/|R|m-h*.

Автор протокола показал, что для произвольных чисел *q* и *h*, фиксированного числа *m* и $|R| \in O\left((\log_2 q)^w \right)$ для данного $w \in N$ протокол является протоколом доказательства с нулевым разглашением.

В заключение отметим, что все протоколы идентификации, основанные на асимметричных алгоритмах, обладают одним интересным свойством — они стандартным образом могут быть преобразованы в схемы цифровой подписи. [63, стр. 512] Для этого участник *V* заменяется однонаправленной хэш-функцией. Сообщение не пропускается через хэш-функцию перед подписанием, вместо этого хэш-функция включается в сам алгоритм цифровой подписи. Подробнее схемы цифровой подписи рассматриваются в п. 3.3.

3.2.5. Протоколы, основанные на симметричных алгоритмах

Как было сказано выше, в системах с интеллектуальными картами может быть предусмотрена односторонняя или двусторонняя аутентификация. Рассмотрим вначале *простейший протокол, обеспечивающий одностороннюю аутентификацию*.

Обе стороны, участвующие в протоколе, знают общий секретный ключ (пароль). Проверяющий вырабатывает случайное число *c* и отправляет его стороне, проходящей аутентификацию. Последняя зашифровывает его на известном ей секретном ключе *K* и посылает полученное сообщение *r* проверяющему. Проверяющий вычисляет *r′* на основе известного ему ключа *K′*. Если *r=r′*, аутентификация прошла успешно.

В [47] такой протокол используется для удалённой аутентификации клиента: *c* - случайное 160-битное число, в качестве ключа *K* используется пароль *psw*, известный клиенту и хранящийся у проверяющей стороны. Вместо алгоритма шифрования используется функция хэширования: *r=H(name, c, psw),* где *name* - имя клиента.
Данный протокол можно усложнить и получить *протокол двусторонней аутентификации*. Идея заключается в повторе протокола два раза, при этом доказывающий и проверяющий меняются местами.

Протоколы такого типа называются «протоколами рукопожатия» (название связано с полной симметричностью протокола для обеих участвующих сторон). Заметим, что «протокол рукопожатия» состоит из двух независимо выполняемых протоколов односторонней аутентификации, которые могут выполняться параллельно, поэтому соответствующие сообщения могут передаваться параллельно в обе стороны. Для повышения стойкости протокола к передаваемым сообщениям могут добавляться отметки времени. Заметим также, что наименования сторон «*P*» и «*V*» в данном случае условны, так как каждого из участников в равной степени можно считать доказывающим и проверяющим.

Несколько видоизменённый «протокол рукопожатия» используется в [47] для смарт-карт, в нём алгоритмы шифрования заменены хэш-функциями.
На практике для работы со смарт-картами используется следующий метод [54]: терминал продавца хранит ключ *K* для общения со смарт-картами (один для всех карт) и ключ *KD* для общения с банком продавца. Смарт-карта хранит ключ *KIC* для связи с оборудованием продавца (индивидуальный для каждой карты) и ключ *KC* для общения с банком покупателя. «Протоколу рукопожатия» предшествует этап выработки общего ключа: карта клиента посылает терминалу свой идентификационный номер *CID*, терминалу известна специальная хэш-функция *fX*, которая позволяет из известного терминалу ключа *K* и идентификационного номера карты *CID* выработать ключ *KIC,* уже записанный на карту. Далее общение происходит на этом ключе.

«Протокол рукопожатия» может быть усовершенствован для обеспечения возможности выработки сеансовых ключей для общения между участниками протокола [47]. Такой протокол называется *расширенным протоколом типа «запрос – ответ» с разделением секрета* (Enhanced Shared Secret Challenge - Response Protocol). Протокол обеспечивает создание безопасного «тоннеля» для передачи сообщений между участниками.

3.2.6. Аутентификация сообщений

Стандартным способом аутентификации сообщений в коммуникационном протоколе считается использование CVC (CVV)-кодов - Card Verification Code (Card Verification Value) [54].

Рассмотрим принцип вычисления CVC-кодов (табл. 3). Блок информации *Data1* шифруется на ключе эмитента (организации, выпустившей карточку в обращение — подробнее см. п. 4.1) *I-Key*, ключе пользователя или нескольких ключах, а гарантией подлинности является совпадение шифртекста на карточке и «эталона», полученного из открытой информации и того же ключа. CVC-коды обеспечивают целостность, но не конфиденциальность данных. Блок *Data1* включает: номер транзакции покупателя, дату, время, сумму платежа, номер карты *CID* — и передаётся на терминал одновременно с CVCC-кодом.

При передаче ответа карте используется тот же механизм, только берётся ключ расчётного центра продавца *EqP-Key*. Блок *Data2* включает:

номер транзакции продавца, идентификационный номер терминала, дату, время, сумму, принятую к оплате, имя продавца - и передаётся на карту одновременно с CVCP-кодом. Карта проверяет сумму платежа и сохраняет данные, подписанные CVCP-кодом, в EEPROM.
Описанный протокол называется также «доказательством транзакции».

Таблица 3

Терминал	Смарт-карта
	Data1

(Data1, CVCc*) <——— CVCc'=EEqC-Key(Data1*) CVCc' =? CVCc**	*CVCc=EEqC-Key(Data1) ——— (Data1, CVCc)*
Data2 CVCP=EEqP-Key(Data2) (Data2, CVCP) ———	*———> (Data2*, CVCP*) CVCP'=EEqP-Key(Data2*) CVCP' =? CVCP**

Можно отметить следующие недостатки такого метода:

- проверяющий (терминал) должен хранить у себя секретную ключевую информацию и, как следствие, имеется риск компрометации ключей;
- отсутствие аутентификации ключей;
- отсутствие юридической значимости транзакций и др.

Более совершенными являются методы аутентификации данных (и доказательства транзакций), основанные на асимметричных алгоритмах, использующие цифровую подпись. Однако такой метод порождает проблемы в случае, если в платёжной системе присутствует очень большое число участников (что, как правило, и бывает в реальных системах), поэтому каждому терминалу пришлось бы хранить огромный объём открытых ключей участников системы и массу другой служебной информации, к тому же часто обновляемой (например, при вводе каждого нового клиента). Вторым сложным вопросом является проблема арбитража и процедура разрешения конфликтных ситуаций между участниками системы. Заметим, что подобные проблемы характерны для любой криптосистемы с большим числом абонентов, например, в глобальных сетях.

Теоретическое решение данной проблемы заключается в использовании криптографической схемы, называемой сертификацией ключей. Перед рассмотрением более сложных протоколов аутентификации, предусмотренных современными стандартами, представляется необходимым изложить основы метода сертификации открытых ключей [31,32,33].

Сертификация ключей - это совокупность действий, связанных с удостоверением подлинности абонента (узла, процесса, клиента и т.д.) системы посредством «связывания» его открытого ключа с идентификационной информацией, выполняемых с участием так называемого (доверенного) центра сертификации.

Сертификат (ключа) - форматированный набор данных, связывающий открытый ключ объекта системы с другой его идентификационной информацией (например, именем или почтовым адресом (e-mail)), подписанный доверенным центром сертификации.

Сертификат является общедоступным и считается достоверным, так как подменить его невозможно в силу трёх причин: массовости рассылки по системе; периодического повтора; общедоступности.

Доверенный центр сертификации (certificate authority, CA) - узел сети, являющийся третьей стороной (third-party) по отношению к абонентам сети связи, которому доверяют все абоненты и который выполняет следующие функции: сбор сведений об абонентах, необходимых для сертификации; генерация и рассылка сертификатов; уничтожение сертификатов с истекшим сроком годности; обновление сертификатов.

Основным международным стандартом (де-факто) по сертификации ключей является документ ITU X.509: Recommendation X.509 - Information Technology - Open Systems Interconnection - The directory: Authentication framework. В соответствии с этим стандартом сертификат содержит следующие данные: имя абонента; открытый ключ шифрования; открытый ключ цифровой подписи; серийный номер сертификата;

срок годности сертификата; некоторые другие данные; имя центра сертификации CA; подпись центра сертификации CA.

Преимущество сертификата в том, что два узла сети, доверяющие одному и тому же центру сертификации, могут не знать и не хранить открытые ключи никаких других абонентов, а при необходимости обратиться в центр сертификации и получить необходимые ключи. Для этого ему достаточно знать только открытый ключ центра сертификации.
Жизненный цикл сертификата включает следующие этапы: генерация ключей и создание сертификата; выпуск сертификата в обращение; использование сертификата субъектами системы; уничтожение либо обновление сертификата.

Заметим, что сертификат не обязательно должен пониматься как набор данных, рассылаемый по сети - сертификат может записываться на смарт-карту при её авторизации. Ниже будет рассматриваться применение сертификатов в схемах аутентификации сообщений для смарт-карт.

Принцип сертификации ключей получил дальнейшее развитие в так называемых системах мандатного доступа. Основная идея систем мандатного доступа заключается в распространении принципа сертификации ключей не только на абонентов, но и на ресурсы системы.

Рассмотрим методы статической и динамической аутентификации, предусмотренные в спецификации EMV [46] (о спецификации EMV см. в п. 5.2.4.1).
В обоих вариантах схем аутентификации роль доверенного центра сертификации отводится эмитенту карт. Поэтому терминалу, обслуживающему карты, необходимо знать только открытые ключи эмитентов тех систем пластиковых карт, для работы с которыми предназначен данный терминал.

Статическая аутентификация. ИК, поддерживающая статическую аутентификацию, должна содержать следующие элементы данных:
(1) Индекс открытого ключа центра сертификации - так как терминал может работать с несколькими центрами сертификации, эта величина специфицирует, какой из ключей необходимо использовать терминалу при работе с данной картой;
(2) Сертификат открытого ключа эмитента - подписывается соответствующим центром сертификации;
(3) Подписанный набор данных приложения - данные, относящиеся к одному из приложений, работающих с многофункциональной картой, подписанные эмитентом (открытый ключ эмитента можно проверить, используя сертификат), подлежащие аутентификации;
(4) Модуль и экспоненту открытого ключа эмитента.

Терминал должен хранить открытые ключи всех центров сертификации и так называемую ассоциированную информацию, относящуюся к каждому из ключей (в основном зарезервированную для будущих приложений).

Процесс статической аутентификации включает три этапа (рис. 11):
(1) Восстановление терминалом открытого ключа центра сертификации. Терминал считывает индекс (1), идентифицирует и извлекает хранящиеся в нём модуль и экспоненту открытого ключа центра сертификации и ассоциированную информацию, выбирает соответствующие алгоритмы.
(2) Восстановление терминалом открытого ключа эмитента. Терминал считывает сертификат ключа эмитента и при помощи известного ему открытого ключа центра сертификации *PCA* проверяет подпись центра сертификации под ключом эмитента *PI,* проставленную при помощи секретного ключа *SCA.*
(3) Проверка терминалом данных, подлежащих аутентификации. С карты на терминал передаются данные, подписанные эмитентом. Проверенный ключ *PI* терминал использует для проверки цифровой подписи под данными (2), сгенерированной эмитентом при помощи его секретного ключа *SI*.

Реальный протокол более сложен: спецификация [46] предусматривает выполнение 12 шагов на этапе (2) и 7 шагов на этапе (3), включающих многочисленные проверки структур данных и заголовков. Аутентификация считается выполненной успешно, только если все проверки окончились с положительным результатом.

В протоколе статической аутентификации не используется способность смарт-карты производить самостоятельную обработку информации, поэтому данный протокол подходит не только для микропроцессорных карт, но и для других типов: карт с памятью и магнитных.

К недостаткам данного протокола относится тот факт, что в нём никак не подтверждаются запросы пользователя на совершение транзакций, что может привести к обману эквайрером эмитента (например, отказ от совершённых ранее транзакций, проведение неучтённых транзакций и т.п.). Преодолеть указанные недостатки позволяет динамическая аутентификация.

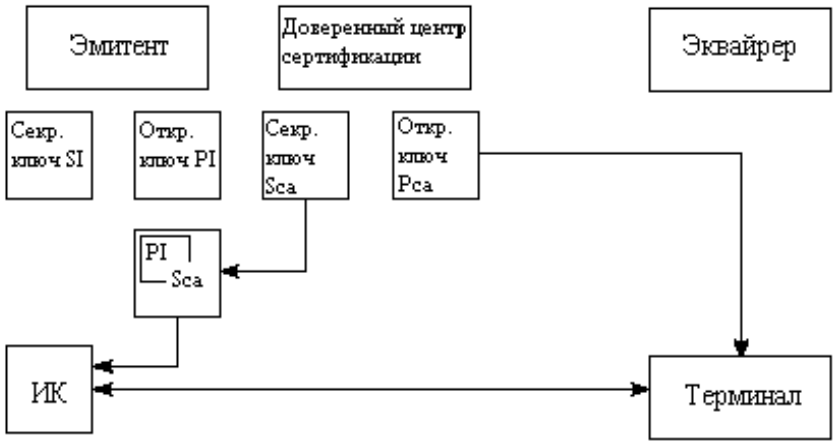


Рис.11. Статическая аутентификация данных

Динамическая аутентификация.ИК, поддерживающая динамическую аутентификацию, должна хранить следующие элементы данных:
(1) Индекс открытого ключа центра сертификации - так как терминал может работать с несколькими центрами сертификации, эта величина специфицирует, какой из ключей необходимо использовать терминалу при работе с данной картой.
(2) Сертификат открытого ключа эмитента - подписывается соответствующим центром сертификации.
(3) Сертификат открытого ключа ИК - подписывается эмитентом.
(4) Модуль и экспоненту открытого ключа эмитента.
(5) Модуль и экспоненту открытого ключа ИК.
(6) Секретный ключ ИК.

Кроме того, ИК должна иметь алгоритм вычисления цифровой подписи под данными, подлежащими аутентификации.
Терминал, поддерживающий схему динамической аутентификации, должен хранить открытые ключи всех центров сертификации и ассоциированную информацию, относящуюся к каждому из ключей. Терминал должен также уметь выбирать соответствующие ключи на основе индекса (1) и некоторой специальной идентификационной информации.

Для поддержки динамической аутентификации ИК должна иметь свою собственную ключевую пару (открытый *PICC* и секретный *SICC* ключи цифровой подписи). Открытый ключ ИК *PICC* хранится на ИК в сертификате её открытого ключа. Если говорить более точно, имеет место трёхуровневая схема сертификации открытых ключей. Каждый открытый ключ ИК *PICC* сертифицируется её эмитентом, а доверенный центр сертификации сертифицирует открытый ключ эмитента *PI.* Это означает, что для проверки подписи карты терминалу вначале необходимо проверить два сертификата для того, чтобы восстановить и аутентифицировать открытый ключ ИК *PICC,* который затем применяется при проверке подписи ИК.

Процесс динамической аутентификации состоит из пяти этапов (рис. 12):
(1) Восстановление терминалом открытого ключа центра сертификации. Терминал считывает индекс *(1)*, идентифицирует и извлекает хранящиеся в нём модуль и экспоненту открытого ключа центра сертификации и ассоциированную информацию, выбирает соответствующие алгоритмы.

(2) Восстановление терминалом открытого ключа эмитента. Терминал считывает сертификат ключа эмитента и при помощи известного ему открытого ключа центра сертификации *PCA* проверяет подпись центра сертификации под ключом эмитента *PI*, сгенерированную при помощи секретного ключа *SCA.*

(3) Восстановление терминалом открытого ключа ИК. Терминал при помощи известного ему открытого ключа *PI* эмитента проверяет подпись эмитента под открытым ключом ИК *PIC,* проставленную при помощи секретного ключа *SI.*

(4) Генерация цифровой подписи интеллектуальной картой (Dynamic Signature Generation). Терминал посылает ОС карты команду *INTERNAL AUTHENTICATE*, включающую выработанное им случайное число *sChal.* Карта хэширует набор данных *Data*, под которым нужно поставить подпись, сцепленную со случайным числом *sChal*,* полученным от терминала, генерирует на секретном ключе *SIC* цифровую подпись *resp* в соответствии с используемым в системе алгоритмом ЦП и посылает подписанную структуру данных *(Data, resp)* терминалу. Протокол этого этапа изображён в табл. 4.

Таблица 4

Терминал	Смарт-карта
sChal — случ. ———	———> *sChal**
<———	*M=H(sChal*||Data)* *val=Encode(M)* *[val=M]* $resp = Sign_{S_{IC}}(val)$ ——— *(Data, resp)*
M'=H(sChal||Data), val'=Encode(M') *val' =? val*	

(5) Проверка подписи терминалом (Dynamic Signature Verification). Терминал проверяет подпись карты под данными с помощью известного ему открытого ключа *PICC*.
Все запросы на обслуживание, исходящие от карты, подписываются её подписью. Подпись карты динамически изменяется за счёт передаваемого карте терминалом случайного числа.

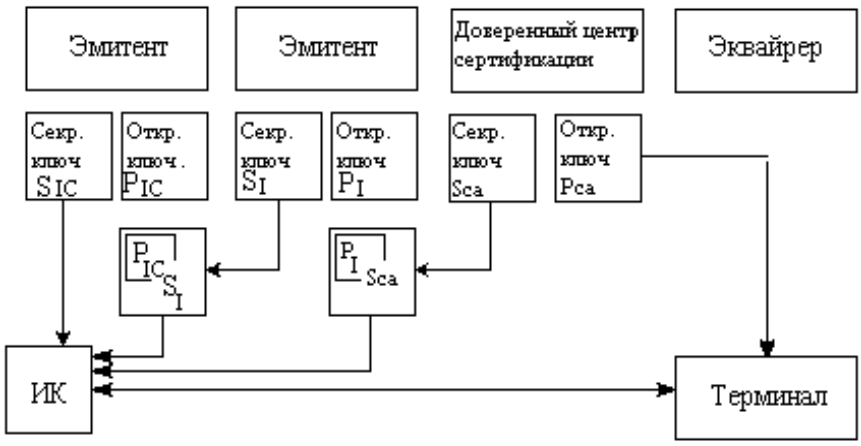


Рис.12. Динамическая аутентификация данных

Если в системе ведётся база данных транзакций, всегда можно доказать, что данная транзакция совершена по запросу данной ИК, либо опровергнуть это.
Отметим, что при нынешнем техническом уровне ИК реализация протокола динамической аутентификации сталкивается с ограничениями, вызванными низким быстродействием процессоров смарт-карт. Время выполнения протокола при длинах ключей, необходимых для обеспечения стойкости схемы, может быть столь велико, что сделает вариант динамической аутентификации непригодным.

Заметим, что в стандарте EMV предлагается использовать в качестве компромиссного варианта модификацию статического метода, предполагающую использовать стандартный механизм аутентификации с помощью симметричных алгоритмов шифрования. По аналогии с CVC-кодами вычисляется MAC-код, который передаётся вместе с данными. Но такой метод требует дополнительных организационных мер по идентификации карты и не даёт гарантии юридической значимости передаваемых сообщений.

3.3. Реализация схем цифровой подписи на интеллектуальных картах

В принципе на ИК может быть реализована любая схема цифровой подписи. Однако в силу ограниченности внутреннего пространства и производительности карты первостепенное значение имеет эффективность схемы ЦП, предлагаемой к реализации. С позиций удобства использования схемы ЦП на ИК необходимо, чтобы время выработки ЦП составляло ~1 с.

3.3.1. Схемы цифровой подписи на базе протоколов аутентификации

Как уже отмечалось в п. 3.2.4, любой асимметричный протокол аутентификации может быть стандартным образом преобразован в схему ЦП. Поскольку при разработке протоколов аутентификации большое внимание уделялось именно эффективности их выполнения на ИК, представляется целесообразным рассмотреть некоторые такие схемы ЦП.

1. Схема цифровой подписи Файге - Фиата - Шамира (табл. 5). Начальные условия - те же, что и в протоколе аутентификации Файге - Фиата - Шамира. Открытый и секретный ключи выбираются тем же образом. В данном случае: *V* - лицо, желающее получить подпись под сообщением, *P* - подписывающий. Считается, что *V* предварительно знает открытый ключ *P.*

Таблица 5

(а) Предварительный этап

P	V	Центр доверия
s, v	*m*	*n=pq* — *случ.* $v \in QRn$ *s=min.{sqrt(v-1) modn}*
n, v, H		

(б) Рабочий этап

	P	V
1	$\{r_i\}_{i=1}^{t}$ *1<ri<n* — *случ.* $\{x_i\}_{i=1}^{t} : x_i = r_i^2 \bmod n$	
2	$H(m, x_1, x_2, \ldots, x_t) \to B = \|b_{ij}\|,$ $i = \overline{1,t}, j = \overline{1,k}$	
3	$\{y_i\}_{i=1}^{t} : y_i = r_i^{**} \prod_{j=1}^{k} s_j^{b_{ij}} \pmod n$	
4	$(m, B, \{y_i\}_{i=1}^{t})$ _____	——>

5		$\{z_i\}_{i=1}^{t} : z_i = y_i^2 * \prod_{j=1}^{k} v_j^{b_{ij}} \pmod{n}$
6		$H(m, z_1, z_2, \ldots, z_t) \rightarrow C = \|c_{ij}\| = ?$ $= ? B = \|b_{ij}\|$

Этапы протокола подписи:

(1) P выбирает *t* случайных чисел: $\{r_i\}_{i=1}^{t}, 1 < r_i < n$, вычисляет $\{x_i\}_{i=1}^{t}, x_i = r_i^2 \bmod n$;
(2) P вычисляет хэш-функцию *H (m, x1, x2, ... , xt),* где *m* — сообщение, под которым *V* желает получить подпись *P*; далее первые *k*t* битов значения хэш-функции *P* использует для получения битовой матрицы $B = \|b_{ij}\|, i = \overline{1,t}, j = \overline{1,k}$;

(3) *P* вычисляет $\{y_i\}_{i=1}^{t}$, где $y_i = r_i * \prod_{j=1}^{k} s_j^{b_{ij}} \pmod{n}$ (*sj* перемножаются в соответствии со значениями битов из матрицы *B*);

(4) *P* отправляет проверяющему *m, B,* $\{y_i\}_{i=1}^{t}$*;* совокупность этих чисел и составляет подпись под сообщением *m.*
Следующие два шага составляют проверку подписи:

(5) *V* вычисляет $\{z_i\}_{i=1}^{t}$, где $z_i = y_i^2 * \prod_{j=1}^{k} v_j^{b_{ij}} \pmod{n}$. *zi* должно быть равно *xi*, так как

$$z_i = y_i^2 * \prod_{j=1}^{k} v_j^{b_{ij}} \pmod{n} = r_i^2 * \left(\prod_{j=1}^{k} s_j^{b_{ij}} \right) * \prod_{j=1}^{k} v_j^{b_{ij}} \pmod{n} = r_i^2$$

(напомним, что $s_i = sqrt\left(v_i^{-1}\right) \pmod{n}$);
(6) *V* проверяет равенство первых *k*t* битов значения хэш-функции коэффициентам матрицы *B*, полученным от *P*.
Преимущество схемы заключается в малом числе операций модульного умножения (1 ... 4 % от схемы RSA). Авторы отмечают, что безопасность схемы пропорциональна *1/2kt* и зависит от сложности факторизации числа *n*. Схема является нестойкой, если сложность факторизации *n* значительно меньше *2kt*. Предлагается *k*=9, *t*=8.

2. Схема цифровой подписи Шнорра. Здесь, как и ранее, начальные условия - те же, что и в соответствующем протоколе аутентификации. *H(m)* - хэш-функция, *m* - сообщение.
(1) *P* генерирует случайное число *r<q*, вычисляет *x=ar* mod *p* (может быть выполнено на этапе предварительных вычислений);

(2) Получив сообщение *m, P* вычисляет $e = H(m \| x)$, y*=(r+se)* mod *q*;
(3) *P* посылает (*m,e,y*) - подпись под сообщением - проверяющему;

(4) *V* вычисляет $x' = a^y v^e \bmod p$ и $e' = H(M, x')$. Если $e = e'$, *V* признаёт подпись действительной. Достоинство данной схемы в том, что большинство вычислений могут быть выполнены на стадии предварительных вычислений, что значительно ускоряет генерацию подписи. Автор схемы отмечает, что при том же уровне безопасности длина подписи примерно вдвое меньше, чем длина подписи RSA, и меньше длины подписи Эль-Гамаля.

Другую группу схем цифровой подписи составляют схемы, специально предложенные для реализации на ИК. Рассмотрим пример такой схемы [37].

3.3.3. Реализация схем цифровой подписи с использованием эллиптических кривых

Эта тема в настоящее время особенно актуальна. С тех пор как в 1985 г. Н. Коблиц и В. Миллер независимо предложили использовать группы точек эллиптических кривых для целей криптографии, в этой области получены важные теоретические и практические результаты. Это отразилось даже в пересмотре и расширении американского стандарта цифровой подписи и появлении нового стандарта FIPS PUB 186-2. Задача дискретного логарифмирования в этих группах решается труднее, чем в группах обратимых элементов колец вычетов целых чисел по модулю простого числа. Для первоначального знакомства можно порекомендовать материалы на страницах фирмы Certicom Corp. в Интернете [*http://www.certicom.com*]. Напомним, что общая форма уравнения эллипса над любым полем имеет вид $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$

которое при характеристике поля *h*, большей 3, может быть преобразовано в виде $y^2=x^3+ax^2+bx+c.$ В важном для приложений случае, когда характеристика поля равна 2 , рассматривают кривые вида $y^2+y=x^3+ax+b$ при $4a^3+27b^2$, не сравнимом с нулем по *modp,* или $y^2+xy=x^3+x^2+b$. Множество точек (*x,y*) на кривой вместе с так называемой точкой бесконечности *O* образуют коммутативную группу относительно специфически определенной операции сложения точек. В случае, когда кривая рассматривается над конечным полем *GF(pm)*, где *p*-простое, число *n* точек (*x,y*) не превышает величины 2*pm*+1, а если более точно, то по теореме Хассе (Hasse) оно удовлетворяет соотношению $\left|n-\left(p^m+1\right)\right|\le 2p^{\frac{m}{2}}$. Это число называется порядком эллиптической кривой. Впервые полиномиальный алгоритм для нахождения числа точек в общем случае был предложен Schoof R. в 1985 г., а более практичный способ предложили R. Lercier и F. Morain на конференции Eurocrypt`95. В общем случае эта группа точек является произведением двух циклических p – примарных групп (т.е. таких, порядок которых равен p^α).

Существует много аналогий между группой точек эллиптической кривой и мультипликативной группой поля Z(p^m). Аналогом умножения двух элементов из Z_q°, q= p^m, является сложение двух точек на эллиптической кривой над полем GF(q). Отсюда аналогом возведения в k-ю степень является умножение точки на целое число k. Соответственно меняется формулировка задачи дискретного логарифмирования. Чтобы, например, достичь такого же уровня защищённости как в стандарте цифровой подписи DSA с 160-битным параметром q и 1024-битным простым числом p, порядок образующей точки должен быть 160-битным числом. Аналогией схемы ЦП из американского стандарта DSA является схема подписи на эллиптических кривых ECDSA (Elliptic Curve DSA).

Рекомендации стандарта FIPS PUB 186-2. Главными параметрами при использовании эллиптических кривых в криптографии являются сама кривая E и базовая точка G на этой кривой. Базовая точка имеет порядок r, являющийся большим простым числом. Число точек на кривой равно $n=r\cdot f$ при некотором целом числе *f*, не делящемся на *r*. По причинам эффективности реализации число *f* должно быть как можно меньшим. Для всех кривых, рекомендуемых в этом стандарте, число *f* равно 1, 2 или 4, чтобы открытый и секретные ключи были почти одинакового размера, причем размер секретного ключа в битах превосходит примерно в 2 раза размер совместно используемого симметричного шифра. Например, если используется алгоритм шифрования 3DES–EDE с 112-битным ключом, то размер простого числа *p*– параметра поля *GF(p)*, над которым рассматривается кривая, равен 224 бит. Именно при таком соотношении предполагается соблюдение баланса стойкости используемых алгоритмов.

Поля, над которыми рассматриваются эллиптические кривые, рекомендуются двух видов:

- простое поле *GF(p)*, с *p* элементами, равному большому простому числу. Часто простое число *p* ищется в виде так называемого обобщенного числа Мерсенна (Mersenne), при котором операцию умножения в конечном поле можно реализовать более эффективно, чем при произвольном простом *p*;
- поле *GF(2m),* с *2m* элементами. Элементы такого поля представляются двоичными векторами длины *m*.

Для описания операций над векторами необходимо оговорить процедуру интерпретации этих векторов в качестве элементов конечного поля. Это определяется выбором базиса конечного поля, рассматриваемого как векторное пространство.

При полиномиальном базисе двоичная строка (*Am-1, …, A0*) представляет полином $A_{m-1}t^{m-1}+\ldots+A_1t+A_0$ над полем *GF(2),* а все операции над векторами соответствуют операциям над многочленами по модулю некоторого неприводимого многочлена *p(t)*. В качестве *p(t)* желательно выбирать трехчлен вида *tm+tk+1* с наименьшим возможным значением *k*, если такие существуют при данном *m*. В противном случае берётся неприводимый пятичлен *tm+ ta+tb+tc+1*.

При нормальном базисе двоичная строка (*Am-1,…, A0*) представляет элемент поля вида $A_0t+A_1t^2+\ldots+A_{m-1}t^{2^{m-1}}$.

Сами эллиптические кривые предлагается выбирать двумя методами.

1. *Псевдослучайные кривые* – это кривые, чьи коэффициенты получены из выхода криптографической хэш-функции. По имеющемуся входу на хэш-функцию и ее выходу можно проверить, что они соответствуют друг другу. Это является своеобразным "сертификатом честности" случайного выбора коэффициентов кривой. При желании навязать какую- нибудь определенную кривую со специфичными коэффициентами пришлось бы найти соответствующие входы для хэш-функции, что по определению хэш-функции практически сделать невозможно. В качестве хэш-функции берется SHA-1. Интересно, что такой способ впервые был предложен в российском стандарте ГОСТ Р 34.10-94 и используется также с первых версий американского стандарта FIPS PUB 186-1.

Для простого числа *p* псевдослучайная кривая ищется в виде $y^2=x^3-3x+b\pmod p$, причем выбор одного из коэффициентов равным –3 определяется рекомендациями из стандарта IEEE P1363.

Коэффициент *b* найден с условием выполнения для него соотношения $b^2c=-27\pmod p$.
Для поля *GF(2m)* псевдослучайная кривая приводится в виде
y2 +xy = x3+x2+b.
Для всех приводимых в FIPS PUB 186-2 псевдослучайных кривых число точек на кривой *n=2r*.

2. *Специальные кривые* - это те кривые, выбор коэффициентов которых определяется целесообразностью оптимизации операций. Специальная кривая над *GF(2m)* называется кривой Коблица или аномальной бинарной кривой. Кривая Коблица имеет вид*y2+xy=x3+ax2+1*, где *a*=0 или *a*=1. При этом число точек на кривой равно *n*=4*r* при *a*=0 и *n*=2*r* при *a*=1.
Любая точка *G=(Gx, Gy)* на кривой *r*-го порядка может служить образующей точкой. При желании пользователи могут выбрать сами точку *G*.
Российский стандарт цифровой подписи **ГОСТ 34.10-2001** на основе эллиптических кривых излагается в курсе «Современная прикладная криптография».

Раздел 4. Интеллектуальные карты в банковском деле

4.1. Банковские платёжные системы, использующие интеллектуальные карты

Одним из основных применений интеллектуальных карт является использование их в качестве персонализированного платёжного инструмента в автоматизированных банковских системах, которые в ряде случаев называют электронными платёжными системами (системами пластиковых карт).

Любая автоматизированная банковская платёжная система со смарт-картами имеет ряд обязательных компонент: процессинговый центр, клиринговый центр, эмитент, центр авторизации карт, эквайрер, продавец и владелец карты.

Процессинговый центр **-** учреждение, организующее функционирование и обслуживание автоматизированной банковской системы, использующей смарт-карты, в определённом регионе.

Клиринговый центр - банковское учреждение, осуществляющее расчёты между участниками автоматизированной банковской системы.

Эмитент - участник автоматизированной банковской системы, осуществляющий единичный или массовый выпуск в обращение смарт-карт.

Центр авторизации **-** организация или подразделение автоматизированной банковской системы, осуществляющее запись на интеллектуальные карты персональной информации о владельце и выдачу карты владельцу.

Эквайрер - банковское учреждение, заключающее договора с продавцами о принятии смарт-карт в качестве средства платежа и обслуживании продавцов-участников коммерческой сети.

Продавец - участник автоматизированной банковской системы, осуществляющий продажу товаров или услуг и принимающий к оплате в качестве платёжного средства пластиковые карты.

Владелец карты - это лицо, которому ИК выдана центром авторизации и который владеет ею на законном основании.

Автоматизированные банковские платёжные системы принято подразделять на *централизованные*, *автономные* и *полуавтономные*. Различия между данными типами систем заключаются в основном в способе подключения в систему конечного оборудования (банкоматы, терминалы, кассовые POS-аппараты). В *централизованных* системах конечное оборудование подключено к остальной системе через каналы связи в режиме on-line, т.е. в режиме реального времени, поэтому при совершении транзакции запросы от карты и ответы на них передаются непосредственно в банк-эмитент либо процессинговый центр, где непосредственно осуществляются необходимые проверки (состояние счёта клиента, отсутствие карты в стоп-листе, аутентичность держателя карты и т.п.).

Согласно определению [3], режим функционирования системы электронных платежей в реальном времени подразумевает:
1) режим обработки данных или работы электронного терминала (банкомата), при котором устройства пересылают авторизационные запросы (т.е. запросы на аутентификацию) и получают ответные сообщения от хост-системы обслуживающего банка/процессингового центра во время осуществления транзакции;
2) режим обработки данных, при котором центральный компьютер банка (банка-эмитента или обслуживающего банка) обменивается информацией с центральным компьютером процессингового центра в процессе осуществления транзакции.

Схема совершения транзакции в централизованной системе показана на рис. 13.

Держатель карты, желая оплатить покупку, передаёт карту оператору кассового терминала (1). Карта вводится в устройство доступа (кард-ридер), которое может быть встроено в кассовый аппарат либо быть выполнено в виде отдельной приставки. Устройство доступа (УД) посылает запрос на авторизацию карты (2), который, проходя через банк-эквайрер продавца, фиксируется там, а затем поступает в банк-

эмитент (центр авторизации ИК), который осуществляет проверку состояния карты (3), т.е. не находится ли карта в стоп-листе («чёрном списке» карт, по которым запрещены транзакции), зарегистрирована ли карта с таким номером в системе и т.п. В случае положительного результата эмитент посылает ответ по авторизации (4) обратно банку-эквайреру. Эквайрер записывает транзакцию (5) в свою базу данных (отмечает состояние счётов продавца и покупателя) и пересылает ответ продавцу (6). Продавец утверждает транзакцию на ИК покупателя, после чего соответственно эквайрер передаёт запись о транзакции в клиринговый (расчётный) центр (7), вносит изменения в счёт продавца в своей базе данных (8), а эмитент вносит изменения в счёт покупателя (9).

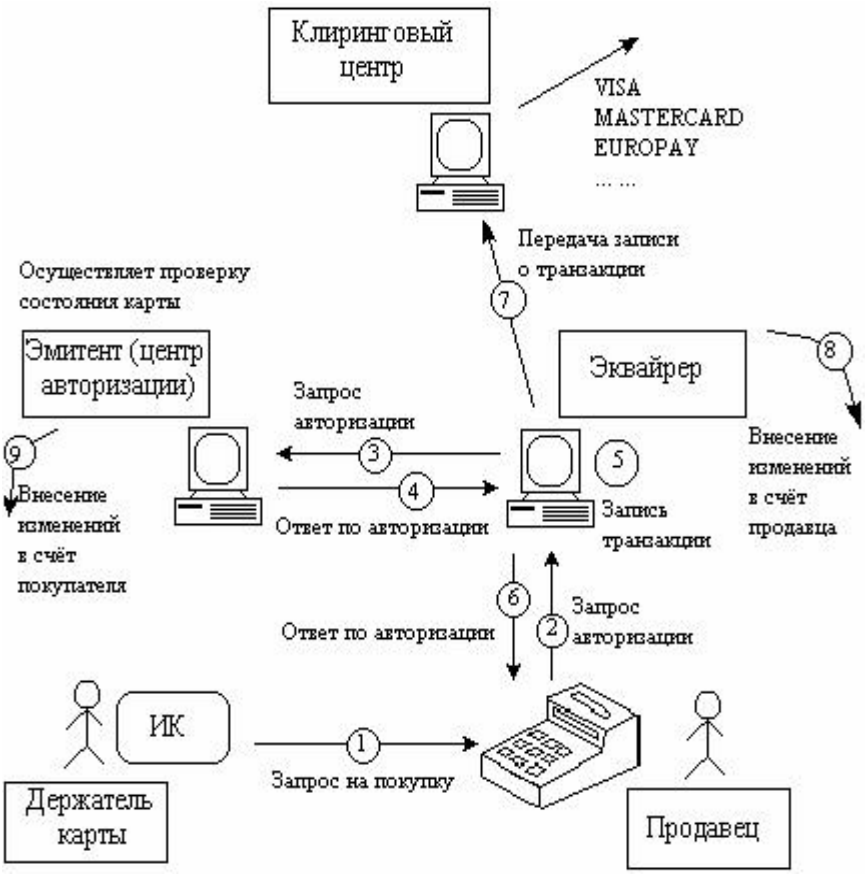


Рис.13. Схема совершения транзакции в централизованной платёжной системе с интеллектуальными картами

В *автономных* системах такой возможности нет (хотя проверки тоже выполняются, но проверке подлежат данные, хранящиеся на карте), поэтому в таких системах используется механизм так называемого «отложенного утверждения» транзакций, т.е. на карте и в терминальном оборудовании сведения о совершённых транзакциях сохраняются на протяжении некоторого времени (несколько дней) на случай, если обнаружится несоответствие суммы на счёте клиента в банке и суммы, обозначенной на карте, или возникнет спор о состоянии счёта. Аппаратура функционирует в режиме off-line (автономном, пакетном режиме) - это режим работы электронных терминалов (банкоматов), при котором устройства в течение определённого периода времени не обмениваются сообщениями с вычислительной системой обслуживающего банка; при работе в таком режиме принятие решения о проведении той или иной транзакции или частичная обработка данных о транзакциях осуществляются этими устройствами самостоятельно на основе имеющегося набора правил; контакт с сетью осуществляется только для передачи данных об уже осуществлённых транзакциях, получения стоп-листов и т.п. [3]. Аутентификация в автономном режиме выполняется при отсутствии доступа к базе данных эмитента, например, путём сверки номера смарт-карты с содержимым стоп-листа с последующей пересылкой данных о транзакциях банку-эмитенту. Данные, накопленные на терминале, периодически передаются банку-эмитенту и расчётному

центру (например, информация может сниматься 1 раз в сутки в ночное время). Примером автономной системы является UEPS (Universal Electronic Payment System).

Полуавтономные системы отличаются от автономных тем, что конечное оборудование связано с системой каналом связи, но этот канал обладает низкой пропускной способностью либо является невыделенным, поэтому в них используется смешанный механизм утверждения транзакций. Такие системы называют либо semi-off-line, либо on-line/off-line. Терминал, работающий в таком режиме, называют также «оперативно-автономный терминал» [3] - это терминал, позволяющий осуществлять аутентификацию как в режиме реального времени, так и в автономном режиме в соответствии с заранее разработанным параметром транзакции и наличием доступа к базе данных эмитента.

UEPS (Universal Electronic Payment System). Одним из важных примеров реализации криптографических протоколов и алгоритмов является система UEPS (Universal Electronic Payment System) - *Универсальная электронная платежная система* на смарт-картах. Конечно, это коммерческий продукт, и детали его не разглашаются, но существует достаточно открытых материалов, позволяющих составить представление об этой системе и её разновидностях [17, 18, 27, 63]. Характерной особенностью UEPS является осуществление платежей в режиме off-line при непосредственном взаимодействии карты покупателя и карты продавца в торговом терминале точки продажи (POS), который выполняет только транспортные функции передачи зашифрованных сообщений и не требует особых мер защиты.

Приведем сначала протокол транзакции между покупателем *A* и продавцом *B*, которая происходит при взаимодействии их смарт-карт в торговом терминале, основываясь на статье R. Anderson [17] и известной книге B. Schneier [63]. Это центральный момент всей системы.

Когда покупатель получает свою смарт-карту, то на карту записываются два ключа *K1*и *K2*. Эти ключи вычисляются с помощью одностороннего (однонаправленного) алгоритма по имени получателя (идентификатору, записанному на его карту) и некоторого секретного долговременного ключа *K*. Карты продавцов имеют этот секретный ключ *K*, чтобы по имени покупателя (идентификатору карты покупателя) вычислить тем же односторонним алгоритмом его секретные ключи *K1* и *K2*. Применение одностороннего алгоритма при выработке ключей *K1* и *K2* гарантирует, что в случае компрометации этих ключей хотя бы у одного покупателя невозможно будет найти секретный ключ *K* продавца. Естественно, сам ключ *K* продавца тоже должен быть построен таким образом, чтобы его компрометация не приводила к компрометации ключей других продавцов. Таким образом, мы видим, что для безопасности системы нужна сложная иерархическая ключевая система. Но вернемся к протоколу.

Карта покупателя посылает продавцу свое имя *A* (идентификатор), имя продавца *B* и случайное число *RA*, выработанное датчиком случайных чисел смарт-карты, зашифрованные с помощью алгоритма шифрования DES сначала на ключе *K2*, а затем на ключе *K1*, Причем свое имя карта посылает и в открытом виде, т.е.:

A : [A, EK1 (EK2 (A, B, RA))] ® B.

(Здесь не отражены детали протокола, связанные с тем, как карта узнает имя продавца *B*.)

Заметим, что шифрование открытого текста *(A, B, RA)* производится дважды на ключах *K1* и *K2*. Шифрования только на одном ключе (56 бит) недостаточно, так как на современной вычислительной технике можно найти ключ перебором с использованием простого критерия на открытый текст - то есть имен *A* и *B*, которые можно предположить известными злоумышленнику.

Карта продавца вычисляет ключи *K1*и *K2* из имени покупателя и имеющегося ключа*K* с помощью одностороннего алгоритма, расшифровывает с помощью полученных ключей*K1* и*K2* открытый текст *(A, B, RA)* и проверяет его корректность по именам *A* и *B*. Этим завершается *аутентификация карты покупателя картой продавца*, и, в случае её корректности, она выполняет дальнейшие действия, а именно: она вычисляет новый ключ *K3=EK2(A, B, RA),* шифрует на нем и на ключе*K1* открытый текст *(B, A, RB)* и посылает шифртекст карте покупателя. (Здесь*RB* обозначает случайное число, вырабатываемое датчиком случайных чисел карты продавца *B*.)

A ¬ EK1 (EK3 (B, A, RB)) : B, K3 = EK2 (A, B, RA).

Карта покупателя вычисляет (так же, как и карта продавца) промежуточный ключ *K3 = EK2(A, B, RA),* так как имеет для этого всю необходимую информацию. Она расшифровывает на ключах *K1*и *K3* полученный от *B*шифрованный текст и проверяет корректность открытого текста *(B, A, RB).* Этим завершается *аутентификация карты продавца картой покупателя*.
Далее карта покупателя вычисляет новый промежуточный ключ *K4=EK3 (B, A, RB),* шифрует на ключах *K4* и *K1* открытый текст *(A, B, C),* содержащий цифровой «чек»*C*.

«Чек» *C* содержит информацию об имени покупателя *A*, имени продавца *B*, дату, номер чека, сумму покупки и два кода аутентификации сообщений: *1MAC* и *2MAC*. Ключи шифрования и ключи, используемые для вычисления кодов аутентификации *MAC*, должны быть различными. В [63] сказано, что *1MAC* вырабатывается с помощью ключа, известного только модулю безопасности банка-эмитента, выдавшего карту покупателю, и карте покупателя, чтобы продавец не мог подделать сумму покупки и другие данные. Второй код аутентификации *2MAC* вычисляется с помощью ключа, который контролируется расчетным центром и записывается на карту перед передачей ее банку-эмитенту. Именно второй *MAC* проверяется перед тем, как деньги поступают на счет продавца, представившего чек в расчетный центр к оплате.

Карта продавца, получив от карты покупателя сообщение *EK1(EK4(A, B, C)),* сначала вычисляет ключ *K4 = EK3 (B, A, RB),* затем расшифровывает с помощью ключей *K1* и *K2* открытый текст *(A, B, C)* и проверяет его корректность, после чего принимает чек, и платёж считается состоявшимся для продавца.

Как следует из статьи [17] (сокращенный перевод которой на русский язык содержится в журнале «Конфидент», № 1, 1997), для анализа банковской платёжной системы UEPS применялся вариант так называемой BAN-логики (по именам авторов Burrows M., Abadi M., Needham R.). Оценивая этот протокол, B. Schneier отмечает, что ценным в нем является то, что ключ шифрования для каждого сообщения зависит от всех предыдущих сообщений протокола, поэтому нельзя воспользоваться перехваченным старым сообщением в новом сеансе связи (метод replay attack). Каждое сообщение содержит имена обоих участников протокола, включает уникальную информацию и зависит от всех сообщений, которые пересылались участниками протокола ранее.

Разработчиком и обладателем патента на технологию UEPS, использующую принцип взаиморасчёта двух карт, является французская компания NET1 International. Разновидности платежных систем, использующих эту технологию, были реализованы в нескольких странах с недостаточно развитыми системами телекоммуникаций. Известно, что NET1 заключило лицензионное соглашение с компанией VISA International, которая реализует в России проект VISA-COPAC (Chip Off-line Pre-Aauthorized Card), основанный на технологии UEPS. Но, отдельно от VISA, NET1 продолжает предлагать для внедрения платежные системы, основанные на своей технологии. В России эксклюзивным лицензированным агентом компании NET1 Int. является австрийская компания BGS SmartCard Systems AG (с 1997 г. она является правопреемником BGS Industrial и АО «Телеформ» по проекту UEPS), которая адаптировала и внедрила технологию UEPS, в частности, для Сбербанка РФ. Конечно, более интересным представляется проект VISA-COPAC (или Roscard) как пример международной платёжной системы на основе смарт-карт, но информация о системе безопасности этого проекта является конфиденциальной, хотя фрагменты этих сведений, изложенные в работе R. Anderson, приведены здесь. В то же время в сети Internet на странице с адресом [*http://www.bgs.ru*] можно найти достаточно подробное, хотя и не исчерпывающее описание базовой платёжной системы фирмы BGS SmartCard Systems AG с изложением концепции безопасности. Эти материалы позволяют более глубоко понять технологию UEPS и сложность всей платежной системы в целом.

Основными «действующими лицами» в платёжной системе являются: производитель (поставщик) карт, центр эмиссии, банки-эмитенты (банки покупателей), покупатели, банки-эквайреры (банки продавцов), продавцы, процессинговый центр. Некоторые участники могут выполнять несколько функций.
Эмиссия карт проходит в три этапа.

- На *первом этапе* центр эмиссии получает от производителя (поставщика) смарт-карт тираж карт трех видов: банковские карты, карты покупателей, карты продавцов, которые закрыты транспортным ключом. Получив от производителя транспортный ключ, центр эмиссии заносит на все карты свой секретный мастер-ключ *P0*, системные ключи *P7* и *P5*, устанавливает для каждой карты уникальный порядковый номер в системе (*USN*). К функциям центра эмиссии относится также сопровождение и рассылка Hot List для банков-участников. Системные ключи *P7* и *P5* (и только они) являются общими для всех банков-участников и всех карт платёжной системы.
- На *втором этапе* банк-участник, выступающий в общем случае и как банк-эмитент, и как банк-эквайрер, обрабатывает банковские и торговые карты каждого тиража:
- устанавливает значения паролей *P1* и *P6;*
- по паролю *P6* устанавливает значения ключей *KI1* и *KI2* для банковских карт (ключи банка-эмитента) и ключей *KA1* и *KA2* для торговых карт (ключи банка- эквайрера);
- заносит дополнительную информацию, например о магазине, кодах валют и т.д.
- *Третий этап* является несекретным. Это персонализация, которая выполняется в присутствии клиента оператором банка на специальном терминале в режиме диалога банковской карты и карты клиента. Клиентом может быть как покупатель, так и продавец. Банковская карта переносит на карту покупателя (продавца) банковские ключи *KI1* и *KI2* (*KA1* и *KA2*), предварительно зашифровав их на сеансовом ключе, выработка которого будет описана далее.

Клиент заносит на свою карту с отдельной клавиатуры пароли (персональные идентификационные номера): *PIN1* (на пополнение средств на карте) и *PIN2* (на расходование средств с карты). Размер каждого *PIN* - до восьми символов. Пароли *PIN1* и*PIN2* известны только карте и её владельцу, они могут меняться далее клиентом по его желанию. *PIN1* и *PIN2* могут быть одинаковыми для простоты запоминания. Для карты продавца *PIN1=PINM* - пароль кассира магазина, *PIN2=RFU* - резервный пароль.

Распределение ключей шифрования по картам участников системы показано в табл. 6.

Таблица 6

Карта банка	Карта продав-ца	Карта покупателя	Наимено-вание ключа	Описание ключа
P0	*P0*	*P0*	*Master key*	*Мастер ключ* - Неограниченный доступ к карте. Назначается и известен только центру эмиссии.
P1-PINB	*P1-PINM*	*P1-PIN1*	*PINB* *PINM* *PIN1*	*PINB* - Пароль операциониста банка *PINM* - Пароль кассира магазина *PIN1* - Пароль на зачисление средств на карту. Назначается и известен только владельцу карты. Изменяется владельцем в off-line-терминале.
P2-RFU	*P2 - RFU*	*P2-PIN2*	*PIN2* *RFU*	*PIN2* - Пароль на списание средств с карты. Назначается и известен только владельцу карты. Изменяется владельцем в off-line-терминале

				RFU - Резервный пароль
P3	*P3*	*P3*	*Password3*	Резервный пароль
P4	*P4*	*P4*	*Password4*	Резервный пароль
P5	*P5*	*P5*	*System Key*	*Системообразующий ключ* - участвует совместно с P7 в образовании сеансовых ключей SK. Общий для всех банков-участников единой расчетной системы. Назначается центром эмиссии.
P6	*P6*	*P6-RFU*	*Password6* *RFU*	*Password6* - предоставляет доступ на запись ключей *KIx,KAx*. Назначается банком-участником. *RFU* - Резервный пароль
P7	*P7*	*P7*	*System Key*	*Системообразующий ключ* - участвует совместно с P5 в образовании сеансовых ключей *SK*. Общий для всех банков участников единой расчетной системы. Назначается центром эмиссии.
KI1,KI2	——	*KI1,KI2*	*Ключи карт покупателей*	Предъявляются при зачислении средств на карту. Участвуют в шифровании записи о транзакции. Назначаются банком-эмитентом.
——	*KA1,KA2*	——	*Ключи карт продавцов*	Предъявляются при инкассации карты продавца. Участвуют в шифровании записи о транзакции. Назначаются банком-эквайрером.
SK	*SK*	*SK*	*Session Key*	*Сеансовый ключ* - формируется в памяти карт в результате диалога карты с картой и служит для шифрования всех информационных потоков между картами на протяжении сеанса связи. Уникален для каждого сеанса связи «карта —

				карта».

Далее покупатель в своем банке-эмитенте получает электронную наличность, взаимодействуя в режиме on-line (вводя пароль*PIN1*) с автоматизированной системой банка, имеющей информацию о состоянии счета покупателя. После этого покупатель имеет возможность оплатить покупку в торговой точке, где установлен торговый терминал и продавец (кассир) имеет карту платёжной системы. На карту покупателя и продавца при этом заносится полная информация о совершаемой транзакции. Эта информация имеет сложную структуру, и часть ее шифруется на ключах *KA1* и *KA2* банка продавца (банка-эквайрера), а часть - на ключах *KI1* и *KI2* банка покупателя (банка-эмитента). Продавец далее передает (инкассирует) информацию о проведенных транзакциях со своей карты банку-эквайреру. Банк-эквайрер, зная ключи *KA1* и *KA2*, расшифровывает эту информацию и определяет, клиент какого банка, когда и на какую сумму совершил покупку у его продавца, формирует платёжное уведомление для банка покупателя (банка-эмитента), у которого остается часть информации о транзакции, зашифрованная на ключах *KI1, KI2* банка-эмитента и являющаяся сертификатом. Банк-эмитент, получив платёжное уведомление и зная ключи *KI1, KI2*, проверяет корректность уведомления о транзакции и, в случае положительного результата, переводит деньги банку продавца.

Процесс образования сеансовых ключей, которые используются для шифрования сообщений, передаваемых между двумя картами в терминале, проще, чем тот, что описан в работе [17] и который используется, по словам R. Anderson, в VISA-COPAC. Приведем описание этого процесса по материалам фирмы BGS SmartCard Systems AG дословно.

- Карта клиента, используя внутренний датчик случайных чисел, вырабатывает случайное число в начале каждого нового сеанса взаимодействия с карточкой торговца, шифрует его на системных ключах *P7, P5* и сообщает карте продавца.
- Карта продавца, обладая теми же самыми системными ключами *P7, P5,* расшифровывает информацию и получает то же самое случайное число в расшифрованном виде. Далее, используя это число в комбинации с другими ключами и общими для обеих карт данными, карты одновременно вырабатывают сеансовый ключ, который идентичен на обеих картах и уникален для каждого сеанса связи карт клиента и торговца. Сеансовый ключ находится только в памяти обеих карт и никогда не покидает карты. На базе этого сессионного ключа зашифровываются все информационные потоки между картами, что делает бесполезными попытки перехвата сообщений в торговом терминале.

Заметим, что каждая карта в описанной выше системе из работы [17] обладает своими уникальными ключами *K1* и *K2* типа структурных ключей *P7* и *P5*, и их компрометация не приводит к компрометации ключей других карт. Здесь этого нет, и от этого система не защищена. Хотя эти ключи никогда не появляются в открытом виде, тем не менее в первом варианте защита от компрометации ключей одной из карт предусмотрена.

Из описания процесса генерации также не ясно, как система защищена от replay attack, т.е. от повторного использования перехваченных злоумышленником истинных сообщений. Можно предположить, что, как сказано в материалах фирмы BGS, существует схема организации сквозной уникальной нумерации и учета транзакций на основе следующей идентификационной информации: уникальный серийный номер карты клиента в системе; порядковый номер транзакции по списку транзакций на карте клиента; уникальный серийный номер карты магазина в системе; порядковый номер транзакции по списку транзакций на карте магазина; порядковый номер инкассации магазинной карты.

Здесь есть тонкое место в многократном использовании одних и тех же ключей *KA1, KA2* и *KI1, KI2* для шифрования различных сообщений. Хотя в материалах фирмы BGS и сказано о возможности изменения этих ключей в 256 вариантах, но всё равно остаётся возможность комплектования различных сообщений, зашифрованных на одних ключах, текст которых близок по структуре. Заметим, что для шифрования каждого сеанса при взаимодействии двух карт вырабатывается свой уникальный ключ.

Конечно, для анализа качества безопасности системы на основе смарт-карт необходимо проанализировать и качество датчиков случайных чисел этих смарт-карт, но информация об этом недоступна.

4.2. Жизненный цикл интеллектуальных карт

В соответствии со стандартами ISO под *жизненным циклом* промышленных изделий понимается совокупность технологических и организационных мероприятий, производимых с ним от момента производства до момента выхода из эксплуатации (уничтожения). Фазы жизненного цикла - это результат изменений, произошедших либо во внешней среде, либо в состоянии самого изделия. Событие, вызывающее переход изделия из одной фазы жизненного цикла в другую, называется транзитным.

Важно достигнуть согласования между фазами, поскольку требования к защите устройства, так же, как и средства обеспечения защиты, могут меняться при переходе из одной фазы в другую. Таблица 7

Фазы ЖЦ	Транзитные события
Производство	Завершение изготовления
Послепроизводственная фаза	Начальная загрузка ключевой информации
Предэксплуатационная фаза	Инсталляция
Эксплуатация	Снятие с эксплуатации
Послеэксплуатационная фаза	Разрушение, повторная инсталляция, ремонт

Производство включает конструирование, создание и тестирование устройств, посредством которых достигаются требуемые функциональные и физические характеристики. *Послепроизводственная фаза* включает транспортировку и хранение, вплоть до загрузки ключевой системы.

Предэксплуатационная фаза - в этот период устройство уже содержит ключи, но ещё не включено в эксплуатацию в автоматизированной системе. *Эксплуатация* - непосредственное использование устройства в работе автоматизированной системы пользователем либо обслуживающим персоналом.

Послеэксплуатационная фаза - устройство перестаёт эксплуатироваться в системе. Эта фаза может быть временной (например, когда устройство перемещается на другое местоположение в системе), либо постоянной (в связи с уничтожением, неработоспособностью или плановым выходом из эксплуатации устройства).

Применительно к интеллектуальным картам выделяют следующие этапы жизненного цикла: производство; доставка покупателю; эмиссия; персонализация; передача клиенту; эксплуатация в системе; уничтожение или повторная эмиссия.

Производство карты на предприятии-изготовителе включает изготовление пластиковой заготовки для карты, «внедрение» в карту защитных элементов, которые не могут быть поставлены на более поздних этапах жизненного цикла (например, требуют сложного промышленного оборудования), запрессовывание в карту микросхемы, антенны (для бесконтактных карт) и пр.

Безопасность ИК на этапе производства должна обеспечиваться изготовителем в основном организационными мерами: организацией технологического процесса производства, назначением ответственных лиц, учётом карт, контролем производственного процесса и доступа в производственные помещения.

Доставка покупателю - транспортировка карты к заказчику - процессинговому центру или эмитенту системы пластиковых карт.

Безопасность карты на этом этапе обеспечивается постановкой транспортной блокировки (для этого имеется специальная команда ОС карты).

Эмиссия, или выпуск карты в обращение, - выполняется банком-эмитентом. Включает запись на карту прикладного программного обеспечения, нанесение на поверхность карты защитных знаков (эмбоссирование, цветная печать, голограммы и др.). Безопасность карты обеспечивается эмитентом, который снимает с неё транспортную блокировку, и средствами операционной системы ИК (в частности, эмитент записывает в память ИК свой ключ), а нанесение на карту защитных знаков предназначено для обеспечения безопасности карты на всех последующих этапах жизненного цикла.

Персонализация - это запись в ROM (PROM) карты при помощи специальной установки или специализированного кард-ридера персональной идентификационной информации её владельца (возможно, нанесение на поверхность карты идентификаторов владельца: фотографии, фамилии, имени и др.). Выполняется организацией (например, банком-эмитентом или его филиалом), выдающей карточки в пользование клиентам. Под идентификаторами владельца понимается прежде всего PIN, секретные и открытые ключи шифрования и аутентификации, возможно, биометрическая информация о владельце. Безопасность процесса персонализации обеспечивается тем, что все операции, связанные с записью в память карты соотвестствующей информации, выполняются на ключе эмитента.

Передача клиенту карты осуществляется одновременно с выданным ему временным PIN-кодом (PIN выдаётся в запечатанном конверте и неизвестен персоналу банка), который владелец впоследствии может сменить по своему усмотрению.

Эксплуатация в системе - это период, в течение которого владелец карты пользуется ею и по ней в системе выполняются транзакции. Безопасность карты на этой фазе жизненного цикла обеспечивается всем комплексом соответствующих средств: криптографических (ключевая система, пароли, криптографические алгоритмы и протоколы), системных (команды ОС, защищённая файловая система, защита областей памяти, протоколы совершения транзакций), организационных (учёт совершённых транзакций, стоп-листы, блокировка карт, ведение баз данных в процессинговом центре и т.д.), физических (защищённость карты и устройств доступа от физического проникновения и др.).

Уничтожение выполняется по истечении срока годности карты, исчерпания кредита, предоставляемого по карте (например, «предоплаченные» системы телефонных карт, транспортные карты), негодности карты для дальнейшего использования. В ряде случаев, если стоимость карты высока (например, радиоинтерфейсные карты, карты со средствами ввода информации) и она допускает дальнейшую эксплуатацию, производится *повторная эмиссия* карты после перезаписи на неё ПО и повторной персонализации.

Помимо традиционных платёжных систем, в последнее время всё большее развитие получает концепция построения универсальных платёжных систем на платформе глобальных информационных систем, прежде всего сети Internet.

4.3. Применение интеллектуальных карт для электронных платежей через Internet

4.3.1. Назначение и возможности языка Java. Проблемы безопасности. Java-карты

В узком смысле слова Java - это объектно-ориентированный язык программирования, похожий на язык C++, но более простой. В более широком смысле Java - это целостная технология программирования, рассчитанная на интеграцию с Web-сервисом сети Internet, т.е. на использование в сетевой среде, поскольку навигаторы WWW существуют практически на всех аппаратно-программных платформах. Java-среда должна быть как можно более мобильной и в конечном итоге совершенно независимой от платформы.

Язык Java разрабатывался фирмой SUN Microsystems с 1990 г. Основой для него послужил объектно-ориентированный язык Oak, некоторые идеи были заимствованы из других языков: SmallTalk, Objective C и некоторых других, а в результате язык оказался похожим на C++, но с сокращённым набором команд и более простым синтаксисом, однако и с несколько отличающимися от него возможностями (например, многопотоковость).

Язык Java характеризуется следующими важнейшими решениями:
1. Java является полностью объектно-ориентированным языком - в нём нет данных, которые бы не являлись каким-либо объектом, и нет функций, которые бы не являлись методами каких-либо объектов).
2. Интеграция с WWW-сервисом Internet.
3. Спецификация виртуальной Java-машины (JVM), на которой должна выполняться Java-программа. Для JVM определены её архитектура, представление элементов данных и система команд. Исходные тексты программ на языке Java транслируются в коды виртуальной машины. Тем самым при появлении новой аппаратно-программной платформы в переносе на неё будет нуждаться только Java-машина; все программы, написанные на Java, будут выполняться после этого без каких-либо изменений. Таким образом, в Java реализована идея языка для создания платформенно независимых приложений.
4. Определено, что при редактировании внешних связей Java-программы и при работе Web-навигатора прозрачным для пользователя образом может осуществляться поиск необходимых объектов не только на локальной машине, но и на других компьютерах, доступных по сети (в частности, на WWW-сервере). Найденные объекты загружаются, а функции, описывающие работу этих объектов (так называемые «методы») выполняются затем на машине пользователя.

Нейтральность к архитектуре достигается прежде всего стандартизацией двоичного формата кодов виртуальной машины. Промежуточный код, генерируемый компилятором языка Java, не зависит от конкретной аппаратной платформы, ОС и типа графического интерфейса пользователя. Для того чтобы программы, написанные на Java, могли работать на данной платформе, достаточно лишь, чтобы для них была создана соответствующая виртуальная Java-машина.

В связи с этим центральным понятием технологического цикла обработки программ на языке Java становится понятие *байт-кода*. Компилятор Java производит не машинные коды, а так называемые байт-коды - высокоуровневые машинно-независимые коды для абстрактной машины, которая должна быть реализована в виде интерпретатора байт-кодов и исполняющей (runtime) системы [6].

Идея байт-кодов не нова и предложена ещё в 70-е гг., но байт-коды Java имеют следующие особенности:

- Набор кодов Java легко не только интерпретировать, но и эффективно компилировать «на лету» непосредственно в машинные коды для любой аппаратной платформы. Большинство кодов имеют длину 1 байт и не имеют дополнительных операндов. (В этом Java-машина подобна RISC-процессору, но только реализованному программными средствами.)
- Коды содержат избыточную информацию, которая позволяет проверять (верифицировать) их на безопасность выполнения.
- Java-программы могут существовать в двух видах: в качестве самостоятельных приложений (формируется загрузочный модуль для виртуальной машины, который выполняется под управлением специального интерпретатора, работающего в рамках отдельного процесса) и в виде Java-апплетов. Апплет (applet) - совокупность объектов, выполняющихся в среде WWW-навигатора под управлением виртуальной машины Java, встроенной в навигатор. Двоичный файл с интерпретируемым кодом апплета располагается на WWW-сервере. Файл апплета переписывается с сервера WWW на рабочую станцию и исполняется как Java-программа, но сильно ограничен в правах.

Сложности использования языка Java с целью разработки приложений для смарт-карт связаны, прежде всего, с определённой «громоздкостью» языка общего назначения для такой специализированной

системы как смарт-карта, избыточностью некоторых его функций и низкой производительностью процессоров смарт-карт, пока явно недостаточной для эффективной реализации на них JVM. Главным недостатком Java-технологий на сегодняшний день остаётся низкая скорость работы Java-программ, обусловленная «многослойной» структурой их компиляции и выполнения. По некоторым сведениям, производительность Java-программ в среднем более чем на порядок (до 30 раз) ниже, чем производительность аналогичных программ на C++.

Тем не менее достоинства Java, и прежде всего универсальность этого языка, переносимость на любые аппаратные платформы, позволяют предполагать, что в недалёком будущем, учитывая растущее быстродействие аппаратных устройств, эти сложности будут преодолены и язык Java будет широко использоваться в том числе и в сфере приложений для смарт-карт. Особое значение концепция языка Java приобретает в связи с растущей потребностью в создании систем многофункциональных смарт-карт, для которых необходима динамическая загрузка приложений.

Рассмотрим вкратце функциональные и структурные особенности Java-карт, вытекающие из особенностей Java-технологий [7, 14]. Во-первых, Java встраивается в верхний уровень операционной системы, команды Java-программы исполняются не аппаратурой, а интерпретатором, а потому имеется потенциальная возможность нарушения безопасности такой системы программными средствами. Поэтому особое значение в Java-картах приобретают криптографические методы защиты информации, как традиционные, так и новые: защита данных, хранящихся в памяти карты, цифровой подписью, аутентификация Java-запросов и ответов на них. Во-вторых, Java-карта может динамически загружать из терминала программное обеспечение в момент совершения транзакции - при этом ОС карты верифицирует и проверяет на безопасность это программное обеспечение. Очевидно, что динамическая загрузка приложений необходима многофункциональным Java-картам. Ещё одной проблемой при создании Java-карт является необходимость обеспечения соответствия структуры и информационного наполнения карты требованиям базового стандарта ISO/IEC 7816, в том числе сохранения всех предусмотренных этим стандартом структур данных.

В настоящее время интенсивно ведутся работы по созданию коммерческих образцов Java-карт и соответствующих автоматизированных банковских систем. Наиболее известные проекты разработки Java-карт и систем на их основе: международная рабочая группа JavaCard Forum; проект Cyberflex card фирмы Schlumberger; проект создания интерфейса прикладного программирования Java SmartCard API фирмы IBM.

В качестве примера реальной разработки рассмотрим спецификацию интерфейса прикладного программирования Java Card 2.0 API. Минимальные системные требования к смарт-карте для реализации спецификации Java Card 2.0 следующие: ROM - 16 Кбайт, EEPROM - 8 Кбайт, RAM - 256 байт.

Основные принципы построения системной архитектуры Java-карты заключаются в следующем. Для выполнения программ на языке Java карта имеет встроенную виртуальную Java-машину (JVM). Виртуальная машина - средство более высокого уровня, чем встроенная ОС карты и функции специализированных интегральных схем. Уровень JVM скрывает особенности технологических решений этих нижних уровней за общим языком программирования и программным интерфейсом. Спецификация Java Card 2.0 определяет набор классов интерфейса прикладного программирования для разработки приложений для Java-карт и набор системных сервисов. Необходимость дополнительных библиотек, например, для обеспечения безопасности, определяется спецификой решаемых задач.

В задачу прикладного программиста входит разработка апплетов, необходимых для реализации конкретных функций системы, использующей Java-карты. На одной карте может выполняться несколько различных апплетов (если карта многофункциональная), каждый из которых однозначно определяется идентификатором приложения (стандарт ISO 7816-5).

Виртуальная машина Java-карты обладает рядом особенностей по сравнению со «стандартной» спецификацией JVM для обычных компьютеров:
1. Виртуальная машина Java-карты постоянно находится в активном состоянии, и после отключения источника питания переходит в режим бесконечного цикла.

2. Виртуальная машина Java-карты имеет сокращённый набор команд (вследствие ограниченных ресурсов памяти и вычислительной мощности ИК). Однако при наличии достаточных аппаратных ресурсов ИК и в зависисмости от решаемых задач набор команд может быть расширен, например, введены диспетчер безопасности или библиотеки для операций с целыми числами большой разрядности.
3. Виртуальная машина Java-карты создаёт структуры данных (объекты) в EEPROM, запись в которую выполняется на три порядка медленнее, чем в RAM. Поэтому часто бывает выгодно не сохранять некоторые объекты в EEPROM, а восстанавливать их всякий раз перед началом протокола взаимодействия с устройством доступа.

Действие апплетов Java-карты ограничивается системой безопасности языка Java, однако модель безопасности Java-карты существенно отличается от стандартной, в частности, из-за отсутствия (по причинам низкой производительности ИК) диспетчера безопасности. Поэтому механизмы безопасности реализуются средствами самой виртуальной машины путём разграничения прав владения объектами.

Платформа Java Card 2.0 включает четыре пакета:
1) *javacard.framework* - базовый пакет Java-карты, определяющий классы для построения основных блоков прикладных программ, команд взаимодействия с устройством доступа, операционной системы и сервисных утилит;
2) *javacardx.framework* - расширенный пакет для поддержки объектно-ориентированной файловой системы, совместимой со стандартом ISO 7816-4;
3) *javacardx.crypto* и *javacardx.cryptoEnc* - эти классы реализуют криптографические механизмы, поддерживаемые Java-картами (последний - алгоритм шифрования DES).

4.3.2. Электронные платежи через Internet

В последнее время будущее Internet всё чаще связывается с понятием безопасной среды электронных услуг. Internet уже сейчас позволяет организовать доступ пользователей к таким видам электронных услуг, как: электронная торговля; банковские и финансовые сервисы; платные библиотеки, подписка на информацию и т.п.; широковещательное (broadcasting) распространение информации; электронная коммерция (электронный бизнес); голосование по компьютерным сетям и др.

Однако наиболее сложной проблемой, связанной с предоставлением электронных услуг, остаётся проблема безопасности информации. Очевидно, что ведущую роль в обеспечении безопасности таких систем будут играть алгоритмические, прежде всего криптографические методы. Уже сейчас появилось значительное количество схем осуществления банковских операций с «электронной монетой», электронной торговли и т.п. Смарт-карты являются важнейшим элементом этих схем - носителем «электронных наличных денег» и средством аутентификации законного владельца. Наиболее интересными являются схемы электронных платежей, основой которых является «электронный кошелёк» - персонализированное аппаратно-программное устройство, технически реализуемое на портативных защищённых аппаратных устройствах.

Предполагается, что широкое применение в среде Internet найдут технологии, основанные на Java-картах, а «электронные деньги» станут основой нового направления развития глобальных информационных систем – электронной коммерции. В настоящий момент предложено большое количество протоколов электронных платежей для выполнения финансовых операций с «электронными наличными деньгами», среди них такие широко известные, как SET (Secure Electronic Transactions), SEPP, STT, Mondex, e-Cash, iKP, MilliCent и другие, однако их рассмотрение выходит за рамки данной работы.

Раздел 5. Стандартизация интеллектуальных карт

5.1. Классификация стандартов и организаций по стандартизации

Стандартизация является одним из важнейших аспектов инженерного проектирования любого сложного изделия. Стандартизация интеллектуальных карт осуществляется большим числом организаций, рабочих групп, комитетов, комиссий и т.п. Для удобства дальнейшего рассмотрения организации по стандартизации и выпускаемые ими стандарты удобно разделить на несколько групп.

1. Международные организации выпускают официальные документы, имеющие юридическую силу. Среди них важнейшим органом, регулирующим вопросы стандартизации практически по всем отраслям науки и производства, является *ISO (International Organization for Standardization) — Международная организация по стандартизации.*

Она имеет сложную многоуровневую иерархическую структуру и включает в себя:
TC (Technical Committee) — технические комитеты;
SC (SubCommittee) — подкомитеты;
WG (Working Groups) — рабочие группы;
TF (Task Force) — группы, работающие над решением конкретной задачи.

Каждое отделение более высокого уровня включает несколько отделений более низкого. Правила именования стандартов ISO требуют указания в индексе стандарта разработавшего его отделения.

В рамках ISO стандартизацией в области смарт-карт занимаются следующие структуры:

1. *ISO Inter-Sector Smart Card Structure* (межсекционная группа по стандартизации смарт-карт). Главным органом этой структуры является объединённый технический комитет ISO и Международного электротехнического комитета (IEC) ISO/IEC JTC 1 (Joint Technical Committee) — Information Technology. В рамках этого технического комитета существует подкомитет SC17 — Cards and Related Devices (Идентификационные карты и устройства окружения), включающий рабочие группы, занимающиеся подготовкой, выпуском и сопровождением стандартов:
WG 1: Методы тестирования — подготовила стандарт ISO 10373;
WG 4: Контактные карты с интегральной микросхемой — подготовила стандарт ISO 7816;
WG 8: Бесконтактные карты с интегральной микросхемой — разрабатывает стандарты ISO 10536, ISO 14443, ISO 15693.

2. ISO Banking Smart Card Structure (группа ISO по банковским смарт-картам). Технический комитет ISO TC 68 занимается стандартизацией банковского и смежных финансовых сервисов. В рамках данного комитета существует подкомитет SC 6 — Financial Transaction Cards (карты для финансовых транзакций), включающий рабочие группы (перечислим, как и в предыдущем случае, только наиболее важные для нас группы):
WG 5: Данные и сигналы карт с интегральной микросхемой (стандарт ISO 9992);
WG 7: Архитектура безопасности (стандарт ISO 10202).
Любой стандарт, разрабатываемый рабочими структурами ISO, в процессе рассмотрения проходит несколько этапов от эскизных проектов до официального документа.

2. Региональные организации адаптируют и уточняют международные стандарты к условиям конкретных регионов или межгосударственных объединений, а в случае отсутствия международных стандартов разрабатывают свои собственные. В рамках Европейского Сообщества вопросами стандартизации интеллектуальных карт занимаются, в основном, следующие две организации.

- *CEN — Европейский комитет стандартизации.* CEN имеет технический комитет TC 224, занимающийся стандартизацией смарт-карт и использующих их приложений. Перечислим некоторые рабочие группы этого комитета: WG 1 — Физические характеристики;
  WG 2 — Общие концепции систем на смарт-картах с интегральной микросхемой;
  WG 3 — Характеристики интерфейсов устройств;

WG 4 — Коммуникации с картами с интегральной микросхемой;
WG 5 — Коммуникационные протоколы между устройствами доступа и хостом;
WG 7 — Представление PIN;
WG 10 — Платёжные спецификации для финансовых приложений смарт-карт.
Важным стандартом, выпущенным CEN, является стандарт **CEN/CENELEC 726 — Требования к терминальному оборудованию для смарт-карт с интегральной микросхемой и терминалов для использования в телекоммуникациях.**

- *ETSI (European Telecommunications Standards Institute)* — Европейский институт стандартов по телекоммуникациям. Является разработчиком множества широко используемых стандартов в области телекоммуникаций, в частности, стандарта мобильной телефонной связи GSM и в том числе стандартов, регламентирующих использование смарт-карт для GSM. Другим важным стандартом является ETSI D/EN/TE9 001-1 — Security Framework for Intelligent Cards and Terminals for Telecommunications (Безопасное окружение для интеллектуальных карт и терминалов для телекоммуникаций).

3. Специализированные отраслевые организации занимаются стандартизацией специальных технических условий, требований и выработкой рекомендаций для определённой отрасли промышленности. Так, *IEEE — Международный институт инженеров по электронике и электротехнике* — не разрабатывает стандартов, непосредственно касающихся интеллектуальных карт, но выпускаемые им стандарты, специфицирующие электрические параметры аппаратных устройств и требования по безопасности в сетях, лежат в основе практически всех разработок аппаратуры, в том числе и смарт-карт.

4. Национальные организации. В России пока не разработаны государственные стандарты по разработке и применению интеллектуальных карт. В системах, использующих смарт-карты, необходимо следовать лишь требованиям общих стандартов, касающихся защиты информации в автоматизированных системах:

- ГОСТ 28147 - 89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
- ГОСТ Р 3410 - 94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.
- ГОСТ Р 3410 - 2001. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.
- ГОСТ Р 3411 - 94. Информационная технология. Криптографическая защита информации. Функция хэширования.
- ГОСТ Р 50739 - 95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

Для справки приведём сведения о стандартизации смарт-карт в США. В США стандартизирующими организациями являются:

- ANSI (Американский национальный институт стандартов);
- NCITS (Национальный консультативный Совет по стандартизации информационных технологий);
- NIST (Национальный институт стандартов и технологий);
- NSSN (Сеть национальной системы стандартов).

В рамках ANSI к стандартизации смарт-карт имеют отношение три рабочие группы:

- X3: Системы обработки информации (X 3.92 — Алгоритмы шифрования данных);
- X9: Стандарты по безопасности для финансовых учреждений (X 9.8 — Управление PIN-кодами и безопасность, X 9.17 — Управление ключами в финансовых учреждениях, X9.19 — Аутентификация компьютерных данных и целый ряд стандартов, касающихся криптографических алгоритмов: управления ключами, аутентификации, асимметричной криптографии);
- X12: Обмен электронными данными (X12.42 — Криптографические сообщения для совершения транзакций, X12.43 — Управление ключами, X12.58 — Шифрование и аутентификация).

5. Промышленные стандарты. В эту категорию входят документы, не являющиеся официальными государственными или международными стандартами, разработанные в результате достигнутых соглашений между фирмами-разработчиками и производителями смарт-карт, добровольно принятые всеми договаривающимися сторонами, а также группа "внутренних" стандартов, разработанных некоторыми ведущими фирмами, такими как IBM, RSA, Intel и др., соответствие которым является обязательным для всей выпускаемой ими номенклатуры изделий.

Удачным примером здесь, на наш взгляд, является концепция фирмы IBM в области криптографических средств: основой является так называемая Системная криптографическая архитектура (System Cryptographic Architecture — SCA). Цель SCA — стандартизация основных криптографических услуг (таких как конфиденциальность, целостность, аутентификация, идентификация личности и оперирование действующими шифрключами). В основе SCA лежит анализ угроз со стороны злоумышленника: внешних нападений и нападений изнутри, со стороны легального пользователя. На основе SCA специфицирована так называемая Общая криптографическая архитектура (Common Cryptographic Architecture — CCA) для аппаратно-программных средств и систем защиты информации. В строгом соответствии с CCA разрабатываются интерфейсы прикладного программирования (API) для выпускаемых аппаратно-программных средств. Таким образом достигается универсальность интерфейса всего выпускаемого ряда устройств, полная совместимость их друг с другом снизу вверх. Данный принцип распространяется в т.ч. и на все выпускаемые IBM модели смарт-карт и устройств доступа:

- IBM Personal Security Card — семейство персональных смарт-карт общего назначения;
- IBM Multi-Function Card — семейство многофункциональных смарт-карт;
- IBM 4754 Security Interface Unit — прибор ввода/вывода, включающий криптопроцессор, числовую клавиатуру и часы-календарь, контролирующие доступ;
- IBM 5948-B01 Smart Card Terminal — терминал общего назначения для чтения/записи смарт-карт;
- IBM 4778-HS2 Hybrid Smart Card / Magnetic Stripe Reader/Writer/Encoder — многоцелевое комбинированное устройство для приёма смарт-карт и карт с магнитной полосой со средствами отображения.

Некоторые из промышленных стандартов, наиболее удачные, добровольно принимаются другими фирмами и становятся своего рода "отраслевыми" соглашениями о стандартизации, как произошло, например, с серией стандартов PKCS (Public-Key Cryptographic Standard) фирмы RSA Data Security. Наиболее известные стандарты из этой группы:

- EMV (Europay, Mastercard, VISA) — стандартизованные технические условия для платёжных систем, использующих пластиковые карты на интегральных микросхемах;
- PC/SC Interoperability Specification for ICCs & Personal Computer Systems — стандартизованные спецификации для систем с картами на интегральных микросхемах и персональными компьютерами;
- SET (Secure Electronic Transactions) - протокол электронных платежей и технические условия его использования в системах электронных платежей, разработанные фирмами VISA и Mastercard.

К этой же группе можно отнести стандартизирующие и рабочие документы, появляющиеся в результате деятельности совместных групп, образуемых фирмами, ведущими научно-практические

разработки с участием национальных и международных организаций, так называемых "открытых групп", форумов, совместных проектов и т.п. Примерами являются:

- The Open Group (ранее известная как группа X/Open и OSF);
- SmartCard Forum;
- CardEurope;
- OpenCard и др.

Некоторые из этих документов будут рассмотрены ниже.
В целом следует отметить, что развитие стандартизации в области ИК происходит очень динамично: появляются новые документы и рабочие группы, изменяется статус прежних.

Стандарт PCI DSS безопасности платежных систем

PCI DSS (Payment Card Industry Data Security Standard) - стандарт защиты информации в индустрии платежных карт, разработанный международными платежными системами Visa и MasterCard, объединяет в себе требования ряда программ по защите информации, в частности:

- Visa Europe & other regions: Account Information Security (AIS);
- Visa USA: Cardholder Information Security (CISP);
- MasterCard: Site Data Protection (SDP).

С **сентября 2006 года** PCI DSS введен международной платежной системой VISA на территории региона EMEA как обязательный, соответственно его действие распространяется и на Россию. Поэтому поставщики услуг (процессинговые центры, платежные шлюзы, Интернет-провайдеры), работающие напрямую с VisaNet должны пройти процедуру аудита на соответствие требованиям Стандарта.

Требования Стандарта PCI DSS распространяются на все компании, работающие с международными платежными системами Visa и MasterCard. В зависимости от количества обрабатываемых транзакций, каждой компании присваивается определенный уровень с соответствующим набором требований, которые они должны выполнять. В рамках требований Стандарта предусматриваются ежегодные аудиторские проверки компаний, а также ежеквартальные сканирования сетей.

Основные области контроля и требования безопасности

PCI DSS, определяет следующие 6 областей контроля и 12 основных требований по безопасности:

1. Создание и поддержка безопасной сетевой инфраструктуры.
Требование 1: разработать и обеспечить поддержку конфигураций межсетевых экранов для защиты данных о держателях карт.
Требование 2: не использовать установленные производителем системные пароли и иные параметры безопасности.

2. Защита данных о держателях карт.
Требование 3: обеспечить безопасность хранимых данных о держателях карт.
Требование 4: шифровать данные о держателях карт при передаче их через открытые общедоступные сети.

3. Поддержка программы управления уязвимостями.
Требование 5: использовать и регулярно обновлять антивирусное программное обеспечение.
Требование 6: разработать и поддерживать безопасные системы и приложения.

4. Внедрение усиленных средств управления доступом.
Требование 7: ограничить доступ к данным о держателях карт только служебной необходимостью.

Требование 8: назначить уникальный идентификатор каждому лицу, имеющему доступ к компьютерной сети.
Требование 9: ограничить физический доступ к данным о держателях карт.

5. Регулярный мониторинг и тестирование сетевой инфраструктуры.
Требование 10: отслеживать и контролировать любой доступ к сетевым ресурсам и данным о держателях карт.
Требование 11: регулярно проверять системы и процессы обеспечения безопасности.

6. Поддержка Политики информационной безопасности.
Требование 12: поддерживать политику, определяющую правила информационной безопасности для сотрудников и партнеров.

Разработанные документы и методология проверки требований стандарта предполагает проведение самооценки организацией, так и проведение внешнего аудита. В обоих случаях для документирования этой деятельности и большей объективности, необходимо выполнить целые серии действий для оценки каждого требования. Причем для каждого требования число этих шагов различно. (Именно, 1 – 25, 2 – 13, 3 – 28, 4-6, 5-3, 6-31, 7-2, 8-25, 9-23, 10-28, 11- 11, 12-41). Для 7-го требования надо проверить только 2 пункта, а для 12-го намного больше - 41.

5.2. Стандартизация устройства, функционирования и обеспечения безопасности интеллектуальных карт

Среди множества стандартизирующих документов, классификация которых приведена в предыдущем разделе, представляется целесообразным выделить наиболее существенные и значимые, необходимые для понимания принципов устройства и функционирования смарт-карт. Особо будут отмечены стандарты, относящиеся к обеспечению безопасности смарт-карт и автоматизированных систем, использующих смарт-карты.

5.2.1. Стандарты ISO для идентификационных карт (карт с интегральной микросхемой)

Стандарт **ISO/IEC 7816 — Идентификационные карты — Карты на интегральных микросхемах с контактами** является базовым, основополагающим документом среди семейства стандартов ISO по интеллектуальным картам. Стандарт включает 11 частей, каждая из которых является самостоятельным документом, регламентирующим те или иные аспекты устройства и функционирования ИК. Часть 1 этого стандарта принята в 1987 г., последние ещё находятся в процессе разработки. Но поскольку рабочая группа, отвечающая за стандарт, является постоянно действующим органом, некоторые части стандарта периодически обновляются и дополняются.

Часть 1 стандарта **ISO 7816-1: Физические характеристики** определяет геометрические размеры карты (85,60 x 53,98 x 0,76 мм) и зоны размещения на ней контактов и интегральной микросхемы. Часть 2 стандарта **ISO 7816-2: Размеры и расположение контактов** описывает геометрию и назначение электрических контактных площадок. Часть 3 этого стандарта-- **ISO 7816-3: Электрические сигналы и протоколы передачи** определяет два стандартных коммуникационных протокола: 1) символьно-ориентированный асинхронный электронный полудуплексный протокол передачи T=0; 2) блочно-ориентированный асинхронный электронный полудуплексный протокол передачи T=1. Стандартная исходная частота тактового генератора принимается равной 3,57 МГц, скорость обмена информацией — 9600 бод.

В приложении приведено описание процедуры выбора типа протокола (PTS — Protocol Type Selection) в процессе взаимодействия ИК с терминальным устройством.
Следующая часть стандарта **ISO 7816-4: Команды обмена для промышленного взаимодействия** оговаривает набор и структуру команд операционной системы карты, требования, которым должна удовлетворять файловая система: типы файлов, обязательный набор команд для работы с файлами, приведён обязательный перечень команд ОС.
ISO 7816-5: Система нумерации и процедура регистрации для идентификаторов приложений является, в основном , организационным документом и определяет порядок международной регистрации приложений для смарт-карт.

Следующая часть стандарта **ISO 7816-6: Элементы данных обмена для промышленного взаимодействия** определяет перечень и структуру данных о владельце ИК, передаваемых при осуществлении транзакции: имя, адрес, идентификационный номер, срок действия карты и т.д. Эта часть является последним разделом данного стандарта, принятым на сегодняшний день.

Все последующие разделы либо находятся в стадии разработки, либо только приняты к рассмотрению, поэтому кратко перечислим их:
ISO 7817-7: Команды структурированного языка запросов для карт (SCQL);
ISO 7816-8: Команды безопасности и связанные с ними команды для промышленного взаимодействия;
ISO 7816-9: Дополнительные и расширенные команды для промышленного взаимодействия;
ISO 7816-10: Операционные процедуры и установление взаимодействия для синхронных карт;
ISO 7816-11: Архитектура безопасности.

В контексте рассматриваемой проблемы наибольший интерес, пожалуй, представляет последняя часть данного стандарта, но она была принята к рассмотрению только в январе 1997 г., поэтому конкретных сведений о содержании стандарта пока нет.

Одна из основных возможностей смарт-карты заключается в том, что она рассматривается как процессор безопасности и может быть использована как средство надёжной идентификации владельца. Карта обеспечивает средства хранения требуемой идентификационной информации, такой как PIN или какой-либо тип биометрических данных. На сегодняшний день стандарт ISO 7816 обеспечивает использование в картах симметричного алгоритма DES и (или) асимметричной схемы RSA. Выбор алгоритма предоставляется разработчику. Аспекты построения криптосистемы на основе смарт-карт и её функционирования, включая управление ключами (распределение симметричных и асимметричных ключей, сертификация), алгоритмы работы с PIN-кодами, реализация систем аутентификации, биометрические методы на сегодняшний день не отражены в стандартах, имеющих отношение к смарт-картам. Эти вопросы определяются различными спецификациями и "внутренними" стандартами разработчиков.

Одним из наиболее вероятных направлений для расширения стандарта ISO 7816 являются Java-карты. Однако проблема заключается в отсутствии основополагающих стандартов ISO по Java-технологиям.

Кроме основного стандарта по смарт-картам, имеется ещё ряд стандартов, касающихся пластиковых карт предыдущих моделей — полупроводниковых и с аппаратной логикой, широко распространённых до появления смарт-карт: стандарты ISO 7810, ISO 7811, ISO 7812, ISO 7813 (см. приложение).

Тот факт, что данные стандарты были приняты позже, чем первые части стандарта по смарт-картам, объясняется тем, что они были разработаны "в догонку", как бы утверждая факт наличия и использования данных типов карт, и оговаривают некоторые общие положения и условия их применения. Больший интерес представляют стандарты, относящиеся к новым направлениям развития смарт-карт.

Стандарт **ISO 10373 — Методы тестирования** находится сейчас в стадии принятия (выход ожидается в октябре 1998 г.). Стандарт должен определить методы и процедуры тестирования различных типов пластиковых карт: карт с магнитной полосой, карт с интегральной микросхемой, бесконтактных карт, оптических карт памяти.

Стандарт **ISO 10536 — Бесконтактные карты с интегральной микросхемой** определяет основные принципы устройства бесконтактных смарт-карт всех типов. Состоит стандарт из 4-х частей:
ISO 10536-1: 1992 — Физические характеристики;
ISO 10536-2: 1995 — Размеры и расположение областей взаимодействия;
ISO 10536-3: 1996 — Электронные сигналы и процедуры установления связи;
ISO 10536-4: 1997 — Ответ на сигнал установления связи и коммуникационные протоколы.
Данный стандарт является базовым, основополагающим в области стандартизации бесконтактных смарт-карт и выполняет роль, аналогичную стандарту ISO 7816 для контактных смарт-карт. Все другие стандарты по бесконтактным картам ссылаются на данный документ.

Стандарт **ISO 14443 — Бесконтактные карты с интегральной микросхемой — "Близкодействующие"** (proximity) **карты с интегральной микросхемой** находится в стадии разработки — выход различных его частей намечен до 1999 г. Он определяет основные характеристики и технические условия для "близкодействующих" бесконтакных смарт-карт:
ISO 14443-1 — Физические характеристики;
ISO 14443-2 — Радиочастотный интерфейс;
ISO 14443-3 — Электронные сигналы и процедуры установления связи.

Проекты стандартов **ISO 15693 — Бесконтактные карты с интегральной микросхемой — "Дальнодействующие" карты свободного взаимодействия** (hands-free) **с интегральной микросхемой** и **ISO 15639 — Бесконтакные карты с интегральной микросхемой — "Дальнодействующие" карты фиксировнного взаимодействия** (vicinity cards) аналогичны стандарту 14443, но касаются "дальнодействующих" бесконтакных смарт-карт.

5.2.2. Стандарты ISO по картам для финансовых транзакций

Упомянутая в п. 5.2.1 группа стандартов не конкретизирует областей применения смарт-карт: любые смарт-карты должны удовлетворять условиям этих стандартов. Следующая группа стандартов определяет специфические требования к картам, используемым для финансовых транзакций в банковских приложениях.

Одним из важнейших является стандарт **ISO 10202 — Карты для финансовых транзакций — Архитектура безопасности систем финансовых транзакций, использующих карты с интегральной микросхемой**. Стандарт включает восемь частей:
ISO 10202-1 — Жизненный цикл карт;
ISO 10202-2 — Процесс транзакции;
ISO 10202-3 — Взаимосвязи криптографических ключей;
ISO 10202-4 — Модули безопасности приложений;
ISO 10202-5 — Использование алгоритмов;
ISO 10202-6 — Аутентификация владельца карты;
ISO 10202-7 — Управление ключами;
ISO 10202-8 — Общие принципы и обзор.
Некоторые элементы данного стандарта были изложены в соотвествующих главах пособия.

Наибольший интерес для нас представляет часть 3 данного стандарта, поэтому остановимся на ней более подробно. Стандарт ISO 10202-3 регламентирует взаимосвязь криптографических ключей всех элементов автоматизированной банковской системы на различных фазах жизненного цикла карты от производства до вывода из эксплуатации, специфицирует процедуры выработки общих ключей. Понятие "взаимосвязь ключей" в стандарте включает все типы процедур выработки согласованных ключей: симметричные схемы с разделением секрета, асимметричные схемы с сертификацией открытых ключей, асимметричные схемы со взаимным обменом открытыми ключами. Стандарт рассматривает также

иерархические схемы ключей, генерируемых смарт-картой и устройством доступа. Выделяются следующие типы ключей: ключ аутентификации объектов, ключ сертификации, контрольный ключ, ключ шифрования, ключ для обмена ключами, ключ аутентификации сообщений, ключ производителя.

Стандарт **ISO 9992 — Карты для финансовых транзакций — Сигналы, передаваемые между картой и устройством доступа к карте** определяет набор функций, сигналов, команд и ответов на них, необходимый для выполнения функциональной части протокола взаимодействия карты с устройством доступа, а также элементы и структуры данных, передаваемые по коммуникационному протоколу.

Рассмотрим подробнее часть 2 этого стандарта — Функции, ссобщения (команды и ответы), элементы и структуры данных. Стандарт определяет девять функций для осуществления обмена финансовой информацией между смарт-картой и теминалом:
1) инициализация сеанса обмена;
2) аутентификация прикладных и системных данных;
3) аутентификация устройства доступа;
4) верификация держателя карты;
5) выбор прикладных данных;
6) решение устройства доступа об авторизации транзакции;
7) запись транзакции;
8) генерация кода сертификации транзакции;
9) завершение транзакции.

Стандарт содержит спецификации протоколов обмена для каждой из вышеназванных функций. Практически все из них предполагают выполнение тех или иных криптографических алгоритмов, выполняемых либо смарт-картой, либо устройством доступа — при этом предполагается, что соответствующее устройство является физически защищённым в соответствии со стандартами ISO 10202-4 и ISO 10202-7. Заметим, что наиболее трудоёмкими операциями согласно данному стандарту являются аутентификация устройства доступа и биометрическая аутентификация держателя карты.

Кроме того, стандарт содержит спецификации всех структур данных, которые должны записываться, храниться и пересылаться картой в процессе финансовой транзакции. Стандарт выделяет несколько групп таких данных:
1) специфические данные карты;
2) специфические данные держателя карты и эмитента;
3) специфические данные разработчика приложений;
4) авторизационные данные;
5) элементы данных для учёта транзакций;
6) аутентификационные данные.

Стандарт **ISO 9564 — Банковское дело — Управление персональными идентификационными номерами (PIN) и безопасность** определяет технику использования и защиты PIN — наиболее распространённого метода логической аутентификации пользователей в банковских системах. Стандарт включает две части:

- ISO 9564-1 — Принципы и технологии защиты PIN;
- ISO 9564-2 — Рекомендованные алгоритмы для зашифрования PIN.

Следующая группа стандартов посвящена требованиям к аутентификации сообщений и управлению ключами:
ISO 8731 — Банковское дело — Рекомендованные алгоритмы аутентификации сообщений;
ISO 8730 — Банковское дело — Требования к аутентификации сообщений (общие положения);
ISO 8732 — Банковское дело — Управление ключами (общие положения);
ISO 9807 — Банковские и смежные финансовые сервисы — Требования к аутентификации сообщений

(розничные операции);
ISO 13491 — Банковское дело — Безопасные криптографические устройства (розничные финансовые операции).

Принципы и методику управления криптографическими ключами в банковских приложениях конкретизирует стандарт **ISO 11568 — Карты для финансовых транзакций — Управление ключами в банковском деле (розничные финансовые операции).** Стандарт состоит из 8 частей:
ISO 11568-1 — Введение в управление ключами;
ISO 11568-2 — Безопасные криптографические устройства;
ISO 11568-3 — Техника управления ключами для симметричных шифров;
ISO 11568-4 — Жизненный цикл ключа для симметричных шифров;
ISO 11568-5 — Техника управления ключами для асимметричных шифров;
ISO 11568-6 — Жизненный цикл ключа для асимметричных шифров;
ISO 11568-7 — Схемы управления ключами;
ISO 11568-8 — Элементы данных для информации, связанной с управлением информацией.

Стандарт **ISO 13491 — Банковское дело — Безопасные криптографические устройства (розничные операции)** рассматривает требования к характеристикам криптографических устройств (физические и логические характеристики), требования к обслуживанию устройств, методологию оценки защищённости устройств.

Среди важнейших требований к физическим характеристикам устройств выделяются: сопротивляемость к взлому, возможность доказательства стойкости, требования по активному противодействию взлому для некоторых устройств. Логические характеристики включают несколько групп требований: гарантия подлинности устройств, конструирование функций, использование криптографических ключей, требования к защите "чувствительных" данных (паролей, PIN), система взаимосвязи криптографических ключей, требования к загружаемому ПО, минимальные требования к физически защищённым устройствам по доказательству характеристик сопротивляемости взлому.

Требования к обслуживанию устройств включают следующие разделы: требования к защите фаз жизненного цикла, методы защиты, в том числе организационные, учётность и контроль за устройствами на фазах производства, транспортировки и ввода в эксплуатацию. Методология оценки защищённости включает оценку рисков и методики формальной и неформальной оценки, даются ссылки на соответствующие нормативные документы.

5.2.3. Стандарты ISO по криптографическим методам и алгоритмам, используемым в интеллектуальных картах

Перечислим некоторые важнейшие стандарты по криптографическим алгоритмам и методам защиты информации, принятые ISO. Хотя они и не классифицируются как имеющие отношение к интеллектуальным картам, но специфицируют сами криптографические методы, реализуемые в системах, использующих смарт-карты:

ISO 9796 — Информационная технология — Технология безопасности — Схемы цифровой подписи, позволяющие восстанавливать сообщения;
ISO 9797 — Информационная технология — Технология безопасности — Механизмы обеспечения целостности данных, использующие криптографическую контрольную функцию, основанную на блочном алгоритме шифрования;
ISO 9798 — Информационная технология — Технология безопасности — Механизмы аутентификации субъектов;
ISO 9799 — Информационная технология — Технология безопасности — Механизмы взаимной аутентификации равнозначных субъектов (peer entity authentication), использующие алгоритмы открытых ключей с двунаправленным рукопожатием;

ISO 10118 — Информационная технология — Технология безопасности — Хэш-функции;
ISO 11166 — Банковское дело — Управление ключами посредством асимметричных алгоритмов;
ISO 11769 — Информационная технология — Технология безопасности — Механизмы безопасности, использующие технику доказательства с нулевым разглашением;
ISO 9798 — Информационная технология — Технология безопасности — Управление ключами.

5.2.4. Стандарты других организаций

В этом разделе будут рассмотрены несколько документов, получивших высокую оценку во всём мире и фактически претендующих на роль международных стандартов в соответствующих областях.

5.2.4.1. Спецификация EMV

Группой EMV (Europay, Mastercard, VISA) созданы две спецификации:

- Пластиковые карты на интегральных микросхемах — Стандартизованные технические условия для платёжных систем систем (EMV Integrated Circuit Card Specifications for Payment Systems);
- Терминалы для пластиковых карт на интегральных микросхемах — Стандартизованные технические условия для платёжных (Integrated Circuit Card Terminal Specifications for Payment Systems).

Эти документы предлагают стандартизованные технические условия для банковских информационных систем с многофункциональными картами. Проект системы защиты информации в стандарте EMV по общему признанию является одним из наиболее удачных на сегодняшний день. Вопросы защиты информации в стандарте EMV достаточно глубоко проработаны и логически завершены, однако, определённые сомнения вызывает выбор конкретных алгоритмов для реализации функций безопасности.

В качестве алгоритма шифрования выбран алгоритм DES(3DES), в качестве алгоритма ЦП — схема RSA, не являющаяся на сегодняшний день лучшей и порождающая известную проблему ускорения модульных операций, выполняемых на процессоре смарт-карты. Наиболее интересным представляется решение проблемы аутентификации сообщений в транзакции — предложены два метода: статической и динамической аутентификации, подробно рассмотренные в п. 3.2.4.

При конструировании системы защиты информации на первое место ставились интересы эмитента карты, поэтому во всех вариантах схем аутентификации роль центра сертификации отводится эмитенту. Предполагается, что терминал, обслуживающий многофункциональные карты, может работать с картами, выпущенными различными эмитентами и соответственно, имеет сертификаты ключей эмитентов обслуживаемых платёжных систем.

Технические условия специфицируют сообщения и команды, необходимые для обеспечения целостности, конфиденциальности данных и аутентификации источника. Целостность данных и аутентификация источника достигаются использованием стандартного приёма вычисления кодов аутентификации сообщений (MAC), конфиденциальность достигается зашифрованием полей данных в сообщениях и командах.

5.2.4.2. Спецификация PC/SC

Рабочая группа PC/SC создана ведущими компаниями -- разработчиками и производителями персональных компьютеров и смарт-карт для разработки открытых стандартов, которые обеспечили бы системную совместимость смарт-карт с персональными компьютерами. В группу PC/SC входят компании Bull CP8, Hewlett-Packard, Microsoft, Schlumberger SA, Siemens Nixdorf Informationssysteme AG, Gemplus, IBM, Sun

Microsystems, Toshiba и Verifone. Целью является выработка исчерпывающих и гибких решений по интеграции ИК с персональными компьютерами и документирование их в спецификациях. Рабочей группой выработана спецификация взаимодействия для карт с интегральной микросхемой и персональных вычислительных систем (PC/SC Workgroup Interoperability Specification for ICCs and Personal Computer Systems).
Технические решения включают:

- требования по совместимости ИК и интерфейсных устройств;
- стандартные интерфейсы для интерфейсных устройств;
- высокоуровневые интерфейсы, обеспечивающие построение, поддержку ИК-приложений и контрольных механизмов;
- спецификации по криптографическим операциям и безопасному хранению данных;
- рекомендации для устройств общего назначения, основанных на ИК, и устройств хранения данных по поддержке существующих стандартов по PC и Internet.

Спецификации базируются на сложившейся системе стандартизации, в основе которой лежит стандарт ISO 7816. Отмечается возможность интеграции приложений, поддерживающих стандарты EMV и GSM. Архитектура системы, предложенная в спецификации, — многоуровневая. Взаимодействие интерфейсных устройств с приложениями осуществляется через специальные программные компоненты — так называемые "менеджеры ресурсов" и сервисные механизмы (service providers).

Спецификации рабочей группы состоят из восьми частей:
1) обзор архитектуры системы, определённой рабочей группой, и её компонентов;
2) детализирует взаимосвязанные характеристики ИК и интерфейсных устройств и требования по их совместимости;
3) описывает интерфейс и уточняет функциональные требования к универсальным интерфейсным устройствам доступа;
4) обсуждает соглашения по конструированию интерфейсных устройств;
5) описывает интерфейсы и функции, поддерживаемые "менеджером ресурсов", соответствующие этому уровню компоненты системы;
6) описывает модель сервисных механизмов (service providers), требуемые интерфейсы и расширения модели для специфических требований приложений;
7) описывает соглашения по конструированию для разработчиков приложений и использованию компонент приложений;
8) описывает рекомендации по безопасности ИК и других устройств безопасности, набор функций ИК для поддержки общих требований по криптографии и хранению данных.

Последняя часть включает описание стандартных криптографических алгоритмов, процедур генерации ключей, выработки псевдослучайных чисел, тестов на простоту. Определяются протоколы аутентификации ИК и сетевых устройств, аутентификации держателя карты, аутентификации транзакций. Раздел, касающийся хранения данных, описывает организацию иерархической файловой системы, механизм контроля доступа к файлам, хранение аутентификационной информации пользователя и приложений, форматы специальных файлов: мандатных, криптографических — для выбора типа алгоритмов, хранения открытого и секретного ключей подписи и обмена сообщениями, пароля пользователя, — идентификационных — для хранения открытого и секретного ключей идентификации ИК. Определяется перечень и специфицируются форматы команд, связанных с обеспечением безопасности ИК, в том числе криптографических команд, команд аутентификации пользователя, блокировки карты и др.

5.2.4.3. Спецификации Open Card Framework

Open Card Framework— набор руководств, выпущенных фирмами IBM, Netscape, NCI и Sun Microsystems, по интеграции смарт-карт с сетевыми компьютерами. Данные документы специфицируют архитектуру и набор интерфейсов прикладного программирования, позволяющие разработчикам приложений встраивать системы поддержки смарт-карт в сетевые компьютеры, совместимые со спецификацией OpenCard. Архитектура является объектно-ориентированной и основывается на концепции так называемых агентов (CardAgent) — программных компонент, обеспечивающих необходимую инфраструктуру для взаимодействия со множеством операционных систем смарт-карт, но недоступных непосредственно для приложений. Агенты имеют программно доступную надстройку в виде компонент ввода/вывода, посредством которых обеспечивается работа приложений с файловой системой карт, и так называемых расширений агентов (CardAgent extensions) — интерфейсов для специализированных функций смарт-карт, например, криптографических.

Контрольные и тестовые материалы

- 1. Описание балльно-рейтинговой системы

Форма итогового контроля знаний по дисциплине – экзамен.

Система текущего контроля знаний учащихся по данному курсу строится по рейтинговому принципу: учащиеся в течение учебного семестра имеют возможность получать зачётные баллы за активную работу в течение семестра. Максимальное количество баллов, которые могут быть набраны таким образом, равно 100 ед. Если в течение семестра учащийся набирает достаточное количество баллов (80 – 100 ед.), он имеет возможность получить отличную оценку без ответа на экзаменационные билеты.

В течение семестра предполагается проведение промежуточного контроля (8-я уч. нед.) в форме ответов на вопросы теста в письменном виде (максимальное количество баллов – 30). Дополнительные баллы могут быть получены за активную работу на практических занятиях, за выполнение домашнего задания (максимально 30 баллов) и за подготовку инициативной творческой работы (максимальное количество баллов – 50 ед.)

На экзамене учащимся предлагается письменно составить конспект ответа на теоретический вопрос, с последующей устной защитой.

- 2. Вопросы для самопроверки и обсуждений по темам

Вопросы готовятся самими студентами и обсуждаются с преподавателем на занятиях или с помощью электронной почты.

- 3. Задания для самостоятельной работы по темам

Задания для самостоятельной работы формируются преподавателем на основе перечня вопросов итоговой аттестации и отсутствием возможности подробного рассмотрения указанных тем на занятиях.

- 4. Перечень рефератов и/или курсовых работ по темам

Темы для самостоятельной работы студентов при подготовке рефератов и курсовых работ определяются на основе тематики известных признанных научных конференций и семинаров, рассматривающих вопросы безопасности ИТ систем. Среди таких мероприятий выделим следующие.

USENIX Security Symposium.
IEEE Symposium on Security and Privacy.
ACM Conference on Computer and Communications Security (CCS).
ISOC Network and Distributed System Security Symposium (NDSS).
International Symposium on Recent Advances in Intrusion Detection (RAID).
GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA).
Annual EICAR Conference.
Annual Computer Security Applications Conference (ACSAC).
International Conference on Applied Cryptography and Network Security (ACNS).
ACM Symposium on Information, Computer and Communications Security (ASIACCS).
European Symposium on Research in Computer Security (ESORICS).
Financial Cryptography and Data Security (FC).
ACM Workshop on Recurring Malcode (WORM). DEFCON.
BlackHat.
The Virus Bulletin International Conference.
AVAR International Conference.
CanSecWest and EuSecWest Conferences.
RSA Conference.
Chaos Communication Congress (CCC).
CARDIS

Труды большинства этих конференций и семинаров доступны для образовательных учреждений в сети Интернет на сайте http://www.springerlink.com/ .

- 5. Тестовые задания по темам (для текущего и промежуточного самоконтроля) и итоговый тест по курсу

Тестовые задания по данному курсу являются одним из основных способов контроля знаний. В качестве примера подхода к построению тестовых заданий можно привести курсы, подготовленные Интернет – Университетом Информационных технологий (www.intuit.ru):

- Галатенко В.А. Стандарты информационной безопасности. – М.: ИНТУИТ.РУ, 2004;
- Лапонина О.Р. Основы сетевой безопасности. – М.: ИНТУИТ.РУ, 2005;
и другие.
Именно они были выбраны в качестве образца.

1. Согласно Федеральному закону «О техническом регулировании», принципом стандартизации является
- приоритет национальных законодательных и технических актов;
- обеспечение конкурентоспособности российских товаров и услуг на мировом рынке;
- применение международного стандарта как основы разработки национального стандарта.

2. В «гармонизированных критериях Европейских стран» фигурируют понятия:
- цель оценки;
- система оценки;
- объект оценки.

3. В рекомендациях X.800 фигурируют понятия:
- регулятор безопасности;
- сервис безопасности;
- механизм безопасности.

4. Элемент доверия может принадлежать следующим типам:
- элементы действий системного администратора;

- элементы действий разработчика;
Элементы физической защиты.

5. Согласно «Общим критериям», общие требования к сервисам безопасности могут быть выделены
- в профиль защиты;
- в задание по безопасности;
- в функциональный пакет.

6. Рекомендуемые общие требования доверия безопасности предусматривают
- поиск разработчиком явных уязвимостей;
- независимый анализ уязвимостей;
- устранение уязвимостей.

7. В профилях защиты для межсетевых экранов политика безопасности базируется на принципе
- все разрешено;
- все запрещено;
- все, что не разрешено, запрещено.

8. В профиле защиты ОС предусмотрены максимальные квоты
- времени одного сеанса работы пользователя;
- времени одного сетевого соединения;
Процессорного времени.

9. Для защиты от атак на доступность в проекте профиля защиты СУБД предусмотрены
- блокирование сеанса;
- базовые ограничения на параллельные сеансы;
- предупреждения перед предоставлением доступа.

10. Согласно проекту профиля защиты, концами туннелей, реализующих виртуальные частные сети (VPN), целесообразно сделать
- межсетевые экраны, обслуживающие подключение организаций к внешним сетям
- маршрутизаторы поставщика сетевых услуг
- персональные межсетевые экраны сотрудников/

11. Системы, реализующие спецификации IPsec, должны поддерживать следующие базы данных:
- базу данных политики безопасности;
- базу данных протокольных контекстов безопасности;
- базу данных управляющих контекстов безопасности.

Принцип построения тестов достаточно понятен из приведенных примеров. После проведения нескольких тестов со студентами, можно предложить им самим составить тесты и устроить соревнование между группами по их выполнению. Оценивать можно как сами тесты, так и результаты тестирования, что может войти в итоговый рейтинг студента.

- 6. Перечень вопросов итоговой аттестации по курсу

Виды пластиковых карт и особенности их применения. Классификация пластиковых карт. Основные понятия и определения. Элементы технологии интеллектуальных карт(ИК).
Физическая конфигурация пластиковых карт. Принципы хранения данных на пластиковых картах. Понятия модуля, интерфейса и протокола. Тракт передачи данных. Устройства доступа к картам.
Экономические характеристики карт.
Микропроцессорные карты (смарт-карты, интеллектуальные карты). Контактные и бесконтактные карты. Карты с двойным интерфейсом. «Близкодействующие» бесконтактные карты. Бесконтактные карты удалённого взаимодействия. Активные и пассивные карты.
Сферы применения различных типов пластиковых карт.

Аппаратное обеспечение ИК. Основные технические характеристики ИК. Аппаратное, программное и информационное обеспечение ИК.
Состав и конфигурация устройств на микросхеме, вмонтированной в ИК. Центральный процессор. Виды памяти: ROM, RAM, EPROM, EEPROM. Общая шина. Интерфейсные схемы. Схемы синхронизации стартовые цепи. Подача питания на карту. Конфигурация контактной площадки.
Российская интеллектуальная карта «РИК».
Понятие архитектуры интеллектуальных карт. Архитектура и функциональная структура ИК. Системный подход к описанию функциональности ИК. Аппаратная организация ИК. Микропроцессорная система с общей шиной. Организация доступа к памяти.
Технические особенности реализации микропроцессорной системы ИК. Типичные технические характеристики ИК.
Операционная система ИК. Прикладное ПО на ИК.
Операционная система COS. Функции операционной системы ИК. Сравнение с компьютерными операционными системами. Структура файлов и каталогов. Организация доступа прикладных программ к данным.
Организация файловой системы ИК. Зонный и иерархический методы организации файловой системы. Форматы файлов, используемые в ИК. Методы обеспечения физической безопасности ИК и защиты от подделки. Организация обмена данными с устройствами доступа. Особенности устройства многофункциональных (мультиаппликационных) ИК. Физические и технические методы атак на ИК. Требования к алгоритмическому обеспечению средств защиты информации ИК. Оценка уровня защищённости ИК.
Международный стандарт ISO/IEC 15408: функциональные требования и требования доверия к безопасности, «Профиль Защиты» и «Задание по Безопасности» для ИТ-продукта.
Спецификация функций обеспечения безопасности ИК. Спецификация требований к ЖЦ ИК.
Оценка защищённости аппаратных криптографических модулей. Американский стандарт FIPS 140-2.
Особенности применения криптографических алгоритмов на ИК. Классификация криптографических схем.
Задачи аутентификации. Двухступенчатая аутентификация: аутентификация держателя карты, аутентификация ИК для устройства доступа. Методы аутентификации физических лиц. Логическая аутентификация. Аутентификация по паролю. PIN-коды.
Биометрическая аутентификация. Аутентификация методом «запрос – ответ».
Стандарт ISO/IEC 9798.
Инструментальные средства разработки прикладных программ для ИК. Состав функций интерфейса прикладного программирования (ИПП). Особенности разработки и отладки прикладных программ для ИК.
Вероятностные доказательства (краткие сведения). Интерактивные системы доказательства. Доказательства с нулевым разглашением знания. Доказательства знания, их применение для аутентификации ИК.
Протоколы Фиата – Шамира, Файге – Фиата – Шамира, Шнорра, Guillou – Quisquater.
Сравнение различных видов протоколов аутентификации держателя карты и карты для устройства доступа.
Шифрование данных, хранящихся на ИК и (или) обрабатываемых прикладными программами ИК.
Взаимосвязь скорости шифрования и стойкости алгоритма. Управление ключами шифрования.
Иерархическая ключевая система. Протоколы удалённого шифрования с ключом, хранящимся на ИК.
Сравнительная оценка сложности аппаратной и программной реализаций алгоритма ГОСТ 28147-89.
Требования к ключам шифрования.
Аутентификация данных на ИК. Методы статической и динамической аутентификации.
Реализация схем электронной цифровой подписи (ЭЦП) на ИК. Схемы ЭЦП, основанные на протоколах аутентификации.
Специальные схемы цифровой подписи (на примере ESIGN).
Схемы ЭЦП на базе эллиптических кривых. Особенности реализации отечественной схемы цифровой подписи ГОСТ Р 34.10-2001.
Понятие управления криптографическими ключами. Стандарт ISO/IEC 11770. Особенности жизненного цикла ключей, хранящихся на ИК.
Схемы выработки и распространения криптографических ключей с использованием ИК.
Методы ускорения выполнения криптографических операций на ИК. Удалённое выполнение криптографических операций с ключом, хранящимся на ИК.
Стандартизация устройства, функционирования и обеспечения безопасности интеллектуальных карт.
Стандарты ISO для идентификационных карт (карт с интегральной микросхемой): ISO/IEC 7816.
Стандарты для бесконтактных карт: ISO 10536, ISO 14443, ISO 15693. Стандарты ISO по картам для финансовых транзакций: ISO 10202, ISO 9992, ISO 9564, ISO 11568, ISO 13491.
Спецификация EMV.
Спецификация PC/SC.
Спецификация Open Card Framework.

Распространение открытых ключей в системах с использованием ИК.
Основные понятия, связанные с банковскими платёжными системами на базе ИК. Общая схема функционирования платёжной системы. Централизованные, автономные и полуавтономные системы.
Схема совершения транзакции в централизованной платёжной системе. Протокол ISO/IEC 8583. Управление криптографическими ключами в платёжной системе. Распределение криптографических ключей по картам участников системы._
Жизненный цикл ИК в платёжной системе. Связь ЖЦ криптографических ключей с ЖЦ интеллектуальной карты._
Методы аутентификации данных на ИК в соответствии со спецификацией: SDA, DDA, CDA.
Правовые основы деятельности платёжных систем с использованием ИК. Положение ЦБ РФ 266-П "Об эмиссии банковских карт и об операциях, совершаемых с их использованием".
Квалификация противоправных деяний с использованием ИК.
Квалификация видов мошенничества по критериям международных платежных систем VISA и MasterCard.
Правовая характеристика противоправных действий с использованием банковских карт. Системы мониторинга транзакций
Программы безопасности международной платёжной системы VISA: Fraud Reporting System (FRS), Risk Identification Service (RIS), National Merchant Alert Service (NMAS).
Программы безопасности международной платёжной системы MasterCard: System to Avoid Fraud Effectively (SAFE), Member Alert to Control High-Risk (MATCH), Risk Assessment Management Program (RAMP).
Международные платёжные системы VISA, MasterCard, EuroPay, Maestro и др. Правовые основы их деятельности в России.
Развитие платежей в сети Интернет. Классификация систем электронных платежей. Основные требования по обеспечению безопасности электронных платежей в Интернет.

Методические и дидактические материалы

☐ 1. Методические указания для преподавателя

1. Достаточно легко заинтересовать слушателей излагаемым материалом ввиду его актуальности. Применение интеллектуальных карт постоянно растет, с ними можно будет столкнуться и как потребителю и как производителю или разработчику. Но важно при изложении уметь сочетать проверенные сведения и практику с новыми постоянно меняющимися технологиями в этой области.

2. С самого начала проведения занятий следует обратить внимание на согласование содержания данного курса и других связанных курсов УМК, таких как «Основы информационной безопасности», «Управление информационными рисками», «Технические средства защиты информации», «Современная прикладная криптография», где должны быть уже заложены основы для данного курса. Особенно это относится к двум последним курсам. Фактически интеллектуальные карты являются областью применения многих криптографических алгоритмов и протоколов, а особенности самих карт диктуют новые задачи для указанных дисциплин. При проведении занятий придется напоминать студентам многие из пройденных ранее понятий и результатов.

3. В данном курсе изучение интеллектуальных карт идет с привлечением международных стандартов и международной практики(ISO, EC, …). Вместе с тем большую роль играют документы и материалы ведущих фирм производителей и мировых платежных систем VISA, MasterCard и др. Большинство из них открыто и доступно в сети Интернет.

4. Исключительно полезной формой проведения занятий является совместное посещение различных выставок и семинаров по тематике интеллектуальных карт, которые проводятся в Москве различными организациями и фирмами-производителями достаточно регулярно.

- 2. Методические указания для студента, слушателя

1. Не следует ограничиваться только обязательным материалом, предоставляемым на занятиях. Необходимо как можно больше привлекать дополнительную литературу и источники из сети Интернет, которые рекомендованы преподавателем.
2. Следует иметь ввиду, что невозможно стать специалистом без знания современных информационных

технологий, изучение которых невозможно без знания английского языка в рамках технического перевода текстов. Большую помощь в этом могут оказать различные существующие программные средства. 3. Активнее использовать электронную почту для общения с преподавателем в случае возникновения проблем в изучении учебного материала, если нельзя их решить другими способами на занятиях.

- 3. Сборник задач и упражнений

Задачи и упражнения в данном курсе во многом пересекаются с задачами из курса «Современная прикладная криптография», которых достаточно много и о них говорится в соответствующем курсе. Большее внимание будет уделено задачам по криптографическим протоколам.

- 4. Состав лабораторного практикума

Проведение лабораторного практикума по тематике интеллектуальных карт может быть сопряжено с большими материальными и временными затратами ввиду уникальности и высокой стоимости оборудования, которое могут себе позволить только крупные коммерческие организации. Но и это не гарантирует от того, что будут получены навыки, которыми никогда не удастся воспользоваться. Поэтому более подходящий путь проведения практикума связан с изучением программного обеспечения используемого при разработке приложений для смарт карт.

Приведем пример задания для изучения криптографических приложений.

Каждый студент выбирает из предложенного преподавателем списка 1 статью на английском языке из числа опубликованных в электронном архиве IACR (Международной ассоциации криптологических исследований).

An Improved Remote User Authentication Scheme with Smart Cards using Bilinear Pairings, Debasis Giri and P. D. Srivastava (2206/274).

Pairing based Mutual Authentication Scheme Using Smart Cards, G. Shailaja and K. Phani Kumar and Ashutosh Saxena (2006/152).

Implementing Cryptographic Pairings on Smartcards, Michael Scott and Neil Costigan and Wesam Abdulwahab (2006/144).

Zero-Knowledge Blind Identification For Smart Cards Using Bilinear Pairings, Amitabh Saxena and Serguey Priymak and Ben Soh (2005/343).

Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, Ziv Kfir and Avishai Wool (2005/052).

Secure and Efficient AES Software Implementation for Smart Caards, E. Trichina and L. Korkishko (2004/149).

Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints, M. Scott (2004/017).

Статья содержит описание (в том числе математическую модель) какой-либо криптографической конструкции, предназначенной для реализации с использованием ИК: протокола, схемы, режима работы алгоритма шифрования и т.п. Дополнительно можно пользоваться любой литературой.

Задание заключается в следующем:

1) изучить предложенную криптографическую конструкцию по материалам статьи, при необходимости делая перевод (по желанию студента – с привлечением дополнительной литературы);

2) представить результаты изучения криптографической конструкции в виде технической документации по формам, выданным преподавателем (документы представляются в бумажном и электронном виде).

Состав оформляемой документации,

1. Титульный лист.

2. Общая характеристика объекта исследования:
2.1. Постановка задачи.
2.2. Участники криптосистемы (криптосхемы).
2.3. Схема взаимодействия участников.
3. Структура криптосистемы (криптосхемы) – схема, 1 лист.
4. Элементарные криптографические конструкции, используемые в схеме:
4.1. Требования и свойства конструкции.
4.2. Определение конструкции.
4.3. Описание реализации.
4.4. Вычислительно сложные задачи, на которых основана стойкость криптографических конструкций.
5. Спецификация структурных элементов криптосистемы (криптосхемы):
5.1. Описание конструкции.
5.2. Доказанные свойства безопасности.
5.3. Сложность схемы.
6. Области применения криптосистемы (криптосхемы).
7. Список источников.

EMV — "Europay, Mastercard, VISA" — сообщество ведущих фирм-разработчиков систем со смарт-картами, вырабатывающее общую техническую спецификацию по использованию смарт-карт в платёжных системах.

ETSI — Европейский институт стандартов по телекоммуникациям — является разработчиком множества широко используемых стандартов в области телекоммуникаций.

ISO — Международная Организация по Стандартизации — важнейший международный орган, осуществляющий стандартизацию различных сфер научно-технической деятельности, в том числе касающихся стандартизации смарт-карт.

Java-карта — интеллектуальная карта, имеющая аппаратные средства поддержки исполнения программ на языке Java.

PIN — персональный идентификационный номер — число, известное только законному владельцу ИК, используемое для логической аутентификации, при предъявлении которого он получает доступ к автоматизированной банковской системе.

POS (point-of-sale) — "точка продаж", автоматизированное рабочее место персонала торгового предприятия, позволяющее принимать интеллектуальные карты в качестве средства платежа.

RISC-процессор — процессор с сокращённым набором команд, обладающий рядом архитектурных особенностей, позволяющих увеличить его быстродействие. RISC-процессоры находят всё более широкое применение в смарт-картах.

Автоматизированная банковская система (банковская платёжная система) — совокупность технических, аппаратных и программных средств автоматизации банковской и финансовой деятельности.

Асинхронный протокол обмена —протокол обмена сообщениями или сигналами, при котором пересылка данных между устройствами не синхронизирована, аппаратура всё время находится в состоянии готовности, а сигналы принимаются и обрабатываются по мере их поступления.

Синхронный протокол обмена — протокол обмена сообщениями или сигналами, при котором пересылка данных между устройствами синхронизируется тактовыми сигналами или промежутками времени.

Аутентификация — проверка подлинности субъекта, осуществляющего доступ к автоматизированной системе по предъявленному им идентификатору.

Протокол аутентификации — криптографический протокол, имеющий целью установить подлинность одной или более сторон, принимающих участие в протоколе.

Банкомат — автономное аппаратно-программное устройство автоматизированной банковской системы, позволяющее клиенту- владельцу смарт-карты осуществлять определённые финансовые операции без участия персонала банка, общаясь только со средствами автоматизированной системы.

Бесконтактная смарт-карта (contactless smart card) — смарт-карта, не имеющая металлических контактов и осуществляющая передачу данных внешним устройствам посредством радиоинтерфейса.

Биометрия (биометрическая аутентификация) (biometrics) — аутентификация пользователя автоматизированной системы посредством проверки некоторых его физиологических параметров.

"Близкодействующая" смарт-карта (proximity cards) — бесконтактная смарт-карта, взаимодействующая с устройством доступа посредством радиоинтерфейса, но требующая физического контакта карты с поверхностью ридера.

Владелец карты — физическое лицо, которому пластиковая карта выдана эмитентом на законных основания для использования в автоматизированной системе.

Гибридная карта (hybrid card) — пластиковая карта, совмещающая в себе различные способы хранения данных или типы интерфейсов.

"Дальнодействующая" смарт-карта (remote couple cards) — бесконтактная смарт-карта, взаимодействующая с устройством доступа на больших расстояниях посредством радиоинтерфейса, не требующая физического контакта карты с ридером.

Держатель карты— лицо, фактически обладающее картой и пытающееся получить доступ к средствам автоматизированной системы с использованием смарт-карты.

Доказательство с нулевым разглашением (zero-knowledge proof) — протокол интерактивного доказательства, обладающий свойством нулевого разглашения.

Идентификация — установление и закрепление за субъектом автоматизированной системы уникального идентификатора.

Инициализация смарт-карты — запись на неё системной и прикладной информации и ПО, делающего её работоспособной в автоматизированной банковской системе.

Интеллектуальная карта (смарт-карта) — персонализированное аппаратно-программное средство в виде пластиковой карты со встроенным микропроцессором, предназначенное для взаимодействия владельца карты со средствами автоматизированной системы.

Интерактивное доказательство — криптографический протокол, в ходе которого одним из участников (доказывающим) осуществляется доказательство истинности некоторого утверждения другому участнику (проверяющему).

Полнота интерактивного доказательства — свойство протокола интерактивного доказательства, доставляющее гарантированное доказательство утверждения доказывающим участником протокола.

Карта с интегральной микросхемой (ICC(s) card) — пластиковая карта со встроенной микросхемой, содержащей блоки памяти, логические схемы или микропроцессор.

Карта с магнитной полосой (магнитная карта) (magnetic stripe card) — пластиковая карта с нанесённой на её поверхность магнитной полосой, где на магнитных дорожках хранится информация о совершаемых с участием этой карты транзакциях.

Клиринговый центр — банковское учреждение, осуществляющее расчёты между участниками автоматизированной банковской системы.

Коммуникационный протокол — последовательность сигналов и сообщений, передаваемых между интеллектуальной картой и устройством доступа во время сеанса связи.

Контактная смарт-карта — карта с интегральной микросхемой, осуществляющая контакт с внешними устройствами посредством металлических контактных площадок на поверхности карты.

Корректность интерактивного доказательства — свойство протокола интерактивного доказательства, обеспечивающее стойкость системы в том случае, когда противник выступает в роли доказывающего.

Кредитная карта — смарт-карта, принимаемая в качестве средства платежа в автоматизированной системе, по которой товары или услуги могут предоставляться в кредит на определённую сумму.

Криптографический анализ — процедура или алгоритм раскрытия криптографической системы, т.е. получения противником секретных ключей или другой конфиденциальной информации, циркулирующей в криптосистеме.

Криптографический протокол — протокол, в котором используются криптографические алгоритмы и который обеспечивает безопасность (секретность, целостность, неотслеживаемость и др.) информации.

Логическая аутентификация — метод аутентификации владельца пластиковой карты, основанный на запросе у предъявителя карты некоторой информации (PIN, пароля), которую знает только законный владелец карты.

Микропроцессорная карта — пластиковая карта со встроенным однокристалльным микропроцессором (микроконтроллером).

Многофункциональная смарт-карта — смарт-карта, способная параллельно использоваться в нескольких прикладных системах или группах приложений. Имеет иерархическую структуру файловой системы, другие аппаратные и программные особенности.

Нулевое разглашение (zero-knowledge)— свойство протокола интерактивного доказательства, обеспечивающее защиту доказывающего от противника, который, выступая в роли проверяющего, пытается в результате выполнения протокола получить какую-либо информацию о том, почему истинно доказываемое утверждение.

“Обратная инженерия” (reverse engineering) — метод анализа электронных устройств, в том числе смарт-карт, предполагающий физическое вскрытие изделия, изучение его структуры и восстановление по готовому изделию принципов его функционирования.

Операционная система смарт-карты — набор микрокоманд процессора карты, хранящийся в постоянной памяти, предназначенный для организации функционирования аппаратуры карты в процессе её взаимодействия с внешними устройствами.

Пароль (password) — набор логических символов, вводимый лицом, предъявившим карту, для аутентификации.

Персонализация — процесс, во время которого в память смарт-карты записываются персональные данные её владельца. Обычно выполняется одновременно с печатью данных о владельце на поверхности карты и серийного номера карты.

Пластиковая карта — персонализированное аппаратное либо аппаратно-программное средство, предназаначенное для взаимодействия владельца карты со средствами автоматизированных систем.

Полупроводниковая карта — пластиковая карта со встроенной микросхемой памяти и, в ряде случаев, логическими схемами.

Программируемая постоянная память (PROM — Programming Read-Only Memory) — вид постоянной памяти, допускающей запись информации в неё в любой момент времени, но

только один раз. Представляет собой матричный набор логических вентилей — масочное ПЗУ. Запись информации выполняется посредством пережигания проводников в матрице.

Программируемая постоянная память со стиранием (EPROM — Erasable Programming Read-Only Memory) — вид постоянной памяти, допускающий неоднократную запись в неё информации со стиранием ранее записанной каким-либо физическим воздействием (чаще всего облучением ультрафиолетовым светом).

Продавец — участник автоматизированной банковской системы, осуществляющий продажу товаров или услуг и принимающий к оплате в качестве платёжного средства пластиковые карты.

Протокол — это точно определённая последовательность действий, посредством которой две или более стороны совместно выполняют некоторую задачу.

Протокол "рукопожатия" — криптографический протокол, основанный на симметричном взаимном обмене информацией между участниками по схеме "запрос — ответ".

Процессинговый центр — учреждение, организующее функционирование и обслуживание автоматизированной банковской системы, использующей смарт-карты, в определённом регионе.

Раунд обмена — однократный двунаправленный обмен данными между сторонами, участвующими в протоколе.

Сертификация ключей — совокупность действий, связанных, в общем случае, с удостоверением подлинности абонента (узла, процесса, клиента и т.д.) посредством генерации некоторого набора данных с участием так называемого доверенного центра сертификации и доступного для проверки всеми участниками криптосистемы.

Сертификат ключа — набор данных заранее определённого формата, связывающий открытый ключ абонента с другой его идентификационной информацией (например, именем или почтовым адресом), подписанный доверенным центром сертификации.

Системная шина смарт-карты — часть аппаратной структуры смарт-карты, электрическая магистраль, предназначенная для передачи данных и соединяющая все остальные аппаратные компоненты смарт-карты: процессор, память, интерфейсные схемы, стартовые цепи и др.

Стартовые цепи — электрические цепи смарт-карты и устройства доступа, инициирующие коммуникационный протокол между устройствами и вырабатывающие сигнал очистки оперативной памяти смарт-карты перед началом обмена данными.

Стоп-лист — перечень смарт-карт, зарегистрированных в автоматизированной системе, по которым запрещено выполнение одной или нескольких транзакций.

Терминал — техническое устройство автоматизированной банковской системы, предназначенное для приёма интеллектуальных карт, отображения информации, ввода и обработки данных и связи с остальной системой через коммуникационный канал.

Транзакция — совокупность действий субъекта автоматизированной системы, которые отрабатываются как единое неделимое действие по отношению к содержащимся в ней данным и должны быть либо выполнены целиком до конца, либо не выполнены вообще, и только в этом случае не нарушают целостности данных, хранящихся в автоматизированной системе.

Управление ключами (key management) — комплекс мер криптографической защиты, включающий в себя генерацию ключей, распространение, хранение, уничтожение, архивацию, восстановление, порядок замены ключей и т.д.

Устройство доступа (access device, card-reader) — техническое устройство автоматизированной системы, использующей смарт-карты, предназначенное для приёма

смарт-карт, выполнения коммуникационного протокола и, в ряде случаев, записи данных в постоянную память карты.

Файловая система смарт-карты — форматированная структура системных и прикладных данных, хранящихся в памяти смарт-карты.

Функциональный протокол — часть коммуникационного протокола смарт-карты, в ходе которой выполняются действия, определяемые функциональным назначением смарт-карты в автоматизированной системе.

Целостность данных— понятие, включающее полноту и неизменность некоторого набора данных, обеспечиваемые криптографическими средствами.

Центр авторизации — организация или подразделение автоматизированной банковской системы, осуществляющее запись на интеллектуальные карты персональной информации о владельце и выдачу карты владельцу.

Эквайрер (acquirer) — банковское учреждение, заключающее договора с продавцами о принятии смарт-карт в качестве средства платежа и обслуживании продавцов-участников коммерческой сети.

Электрически перезаписываемая постоянная память (EEPROM — Electrically Erasable Programming Read-Only Memory) — вид электрической постоянной памяти, позволяющий осуществлять стирание и запись информации электрическими импульсами. Часто используется в смарт-картах для хранения текущей информации о транзакциях.

"Электронный кошелёк" ("электронный бумажник") (electronic wallet) — персонализированное аппаратно-программное средство, являющееся носителем "электронной монеты" и выступающее в качестве платёжного инструмента в системе электронных платежей.

Эмитент (issuer)— участник автоматизированной банковской системы, осуществляющий единичный или массовый выпуск в обращение смарт-карт.

Эффективность криптографической операции — понятие, отражающее меру затрат (времени, памяти, ресурсов вычислительной системы) и удобства реализации криптографической операции аппаратно-программными средствами.

Язык Java — объектно-ориентированный язык программирования, предназначенный на использование совместно с WWW-сервисом сети Internet, имеющий специфический технологический цикл обработки программ.

Литература

1. Андреев А.А., Морозов А.Г., Логинов А.И. и др. Пластиковые карты, 2-издание, М.: Концерн «Банковский Деловой Центр», 1998. – 312 с.
2. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле: Методические материалы. - М.: МИФИ, 1997.
3. Бабинова Н.В., Гризов А.И., Сидоренко М.С. Пластиковые карточки: Англо-русский толковый словарь терминов международной практики безналичных расчетов на основе пластиковых карточек. - М.: АОЗТ «Рекон», 1997. - 256 с.
4. Волчков А. К вопросам безопасности в стандарте EMV // Инф.-аналит. Бюллетень «Мир карточек» (Прилож. к журналу «Банковские технологии»), 1997, № 12,. - с. 10 - 13.
5. Воробьёв Н.Н. Основы теории игр. Бескоалиционные игры. - М., 1984.
6. Дунаев С.Б. INTRANET-технологии. - М.: Диалог-МИФИ, 1997.
7. Карри С. Знакомство с Java Ring // Java - Россия. Апрель 1998, № 8. - с. 1, 6 — 7.
8. Карташова С. Visa и Europay запускают чиповые карты в России // Деньги. Ноябрь 1996, № 41 (101). - с. 36 - 39.
9. Лубенская Т.В., Мартынова В.В., Скородумов Б.И. Безопасность информации в системах электронных платежей с пластиковыми карточками: Уч. пособие. - М.: МИФИ, 1997.
10. Матюхин В.Г., Пярин В.А. Концепция обеспечения информационной безопасности платежной системы на основе интеллектуальных карт // Банковские системы и технологии. Март-апрель, 1998. - с. 8-12.
11. Пластиковые карты на интегральных микросхемах - стандартизованные технические условия для платёжных систем. EMV, 1994. - Перевод с англ. фирмы «Анкад», 1995.
12. Рынок карточек с микросхемой // Инф.-аналит. бюллетень «Мир карточек» (Прил. к журналу «Банковские технологии»). 1997. № 17.-с.32-47.
13. Ступин Ю.В. Архитектура мини- и микроЭВМ. - М.: МИФИ, 1991.
14. Чен Ж. Основы Java Card 2.0. // Java - Россия. Март 1998, № 7.
15. Alsbrooks B., A Solution for Multiple Applications, CardTech/SecurTech'97 Conf. Proc. Vol. II: Applications. P. 335 - 344.
16. Anderson R.J., Papers on Smartcard Engineering, http://www.cl.cam.ac.uk/users/rja14/#Lib
17. Anderson R.J., The Formal Verification of a Payment System.
18. Anderson R.J., Why Cryptosystems Fail.
19. Anderson R.J., Kuhn M., Tamper Resistance - a Cautionary Note // The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18 - 21. 1996. P. 1 - 11.
20. Anderson R., Kuhn M., Low Cost Attacks on Tamper Resistant Devices.
21. Beller M.J., Yacobi Y., Fully-Fledged Two-Way Public Key Authentication and Key Agreement for Low-Cost Terminals, Electronic Letters, 1993. Vol. 29. No. 11. P. 999 - 1001.
22. Beth Thomas, Efficienf Zero-Knowledge Identification Scheme for Smart Cards, Adv. in Cryptology - Proc. of EUROCRYPT'88. P. 87 - 94, 1988.
23. Blake-Wilson Simon, Menezes Alfred, Security Proofs for Entity Authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques, 1997.
24. Blaze M., High-Bandwidth Encryption with Low-Bandwidth Smartcards, LNCS. Vol.1039, Fast Software Encryption. P. 33 - 40, 1996.
25. Bon X., How Contactless Technology Will Help Stimulate New Applications, CardTech/SecurTech'97 Proc. Vol. I. P. 585 - 606, 1997.
26. Brickell E. F., McCurley K.S., An interactive identification scheme based on discrete logarithms and factoring, Proc. on EUROCRYPT'90, LNCS. Vol. 473. P. 63 - 71, 1991.
27. Burrows M., Abadi M., Needham R. A logic of authentication. ACM Trans. on Computer Systems. 1990. No. 8(1). P. 18 - 36.
28. Chen L., Damgard I., Security Bounds for Parallel Versions of Identification Protocols, Proc. on EUROCRYPT'92. P. 461 - 466, 1992.
29. Christian F., The Contactless Smart Card Circuit You Never Thought Possible, CardTech/SecurTech'97 Proc. Vol. I. P. 575 - 584, 1997.
30. Computer security Reference Book, Ed.by Jackson K.M, Hruska J., Parker D.B.Butterworth-Heinemann Ltd, Oxford OX2 8DP, 1992.
31. Cormier Ch., Grimonprez G., van Hoecke M.-P., A secured RISC 8-bit Microprocessor for Contactless Applications, Proc. on CardTech/SecurTech'97. Vol. I. Pp. 79 - 88, 1997.
32. Dames A., Remote Read Magnetics, Proc. on CardTech/SecurTech'97. Vol. I. p. 63 - 78, 1997.
33. Dhem J.-F., Quisquater J.-J., Lecat R., Lossless Compression Algorithms for Smart Cards: A Progres Report.

Technical Report CG-1996/7 - Universite catholique de Louvain, 1996.
34. Dhem J.-F., Veithen D., Quisquater J.-J., SCALPS: Smart Card Applied to Limited Payment Systems, Technical Report CG-1996/1.2 - Universite catholique de Louvain, 1996.
35. Feiner P., Issues and Options in Multi-application Card Programs, Proc. of CardTech/SecurTech'97. Vol. I. P. 347 - 360, 1997.
36. Finn D., Antenna and Interconnection Technology for Contactless Cards, Proc. of CardTech/SecurTech'97. Vol. I. Pp. 103 - 112, 1997.
37. Fujioka A., Okamoto T., Miyaguchi S., ESIGN: An efficient digital signature implementation for smart cards, Proc. of EUROCRYPT'91, Lect. Notes in Comp. Sci. Vol.547. 1991. Pp. 446 - 457.
38. Gerck E., Certification: Extrinsic, Intrinsic and Combined, 1997.
39. Gerck E., The Intrinsic and Meta-certification Primer, 1997.
40. Gerck E., Overview of Certification Systems: X.509, CA, PGP and SKIP, 1997.
41. Goldwasser S., Micali S., Rackoff C., The knowledge complexity of interactive proof systems. SIAM J. Comput. No. 18, 1989. p. 186 - 208
42. Guillou L.C., Ugon M., Quisquater J.-J., The Smart Card: A Standardized Security Device Dedicated to Public Cryptography. p. 561 613, 1990.
43. Hendry M. Smart Card Security and Application, Artech House, ISBN 0 13476342 4, 282 p.
44. IBM Smart Card Solution Elements - Tech. Overview. IBM Corp., 1996.
45. IBM Transactions Security System Manual, IBM Corp., 1997.
46. Integrated Circuit Card. Specifications for Payment Systems,EMV`96, June 30, 1996.
47. Interoperability Specification for ICCs and Personal Computer Systems: Part 8. Recommendations for ICC Security and Privacy Devices. March 1997.
48. ISO 9992-2: Financial Transaction Cards - Messages between the Integrated Circuit Card and the Card Accepting Device, ISO, 1994.
49. ISO/DIS 10202-3: Financial Transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 3: Cryptographic Key Relationships, ISO, 1995.
50. ISO/CD 13491: Banking - Secure Cryptographic Devices (Retail), ISO,1995.
51. ISO/IEC DIS 14980: Banking and related financial services - Financial transaction cards, related media and operations, ISO, 1995.
52. de Jong E., How to Make a Java Card, Proc. of CardTech/SecurTech'97. Vol. I. p. 89 - 100, 1997.
53. Knobloch Hans-Joachim. A Smart Card Implementation of the Fiat - Shamir Identification Scheme, Proc. of EUROCRYPT'88. p. 87 - 94.
54. Kersten A.G., Smart Cards for POS-Banking, Cryptography and Coding, 1989. p. 247 — 253.
55. Mizusawa Jun-ichi, IC-cards and Telecommunication Services, Proc. on ASIACRYPT'91. p. 253 - 264, 1991.
56. Matsumoto T., Imai H., Human Identification Through Insecure Channel, Proc. of EUROCRYPT'91. 1991.
57. Montgomery P., Modular multiplication without trial division, Math. of Comput., 1985. Vol. 44. No. 170. p. 519 - 521.
58. Naccache David, A Montgomery-Suitable Fiat-Shamir-like Authentication Scheme, Proc. of EUROCRYPT'92. p. 488 - 491, 1992.
59. Naccache D., M'raihi D., Wolfowicz W., Adina di Porto, Are Crypto-Accelerators Really Inevitable? 20-bit zero-knowledge in less than a second on simple 8-bit microcontrollers, Proc. of EUROCRYPT'95. p. 404 - 409, 1995.
60. Ohta K., Okamoto T., Practical Extension of Fiat - Shamir Scheme // Electronics Letters, 1988. Vol. 24. No. 15. p. 955 - 956.
61. Patarin J., Cryptanalysis of the Matsumoto and Imai Public Key Scheme of EUROCRYPT'88. Proc. of CRYPTO'95. p. 248 - 261, 1995.
62. Russell J.F., The Maturing ICC Standards Environment - Inpact on Technology and Applications, CardTech/SecurTech'97 Proc. Vol. I, Pp. 423 - 434, 1997.
63. Schneier B., Applied Cryptography, John Wiley and Sons, 2nd ed., 1996.
64. Security protocols: international workshop, Cambridge,UK, Apr. 1996 Proc. LNCS 1189, Springer,1997.
65. Shoup V., On the Security of a Practical Identification Scheme, Proc. of EUROCRYPT'96. p. 344 - 353, 1996.
66. Shoup V., Rubin A., Session Key Distribution Using Smart Cards, Proc. of EUROCRYPT'96. p. 321 - 331, 1996.
67. Simon Stopd, Jorge Menendez, Nick Purzer, Clive Vacher, Smart Cards: Description, Evolution and Future Potential, http://web.mit.edu/purzer/ www/team
68. Trio Nic. R., Internet Security, IBM T.J. Watson Res. Center, 1995.
69. de Weleffe D., Quisquater J.-J., CORSAIR: A Smart Card for Public Key Cryptosystems, Adv. in Cryptology - CRYPTO'90 Proc. p. 502 - 513, 1990.
70. Walton Ch., Infrasructures for Electronic Commerce: Digital Certification and Smart Cards, Proc. of CardTech/SecurTech'97. Vol. II: Applications. p. 589 - 604, 1997.
71. Wang C.-H., Hwang T., Tsai J.-J., On the Matsumoto and Imai's Human Identification Scheme, Proc. of EUROCRYPT'95. p. 382 - 392, 1995.

72. Wayman J., A Scientific Approach to Evaluating Biometric Systems Using a Mathematical Methodology, Proc. of CardTech/SecurTech'97. Vol. I. p. 477 - 492, 1997.
73. Wayman J., The Science of Biometric Technologies: Classifying, Testing, Evaluating and Selecting, Proc. of CardTech/SecurTech'97. Vol. I. p. 385 - 396, 1997.
74. Wise A., Smart Card Security Architectures for Corporate Networks and the World Wide Web, Proc. of CardTech/SecurTech'97. Vol. II: Applications. p. 589 - 604, 1997.
75. Мытник К. Отечественная операционная система для микропроцессорных карточек, Мир карточек.-1999.-№2.
76. Боков А.Ю., Рахманов О.В. Обзор технологии пластиковых карт. М. БИТ, 1999, №2.
77. Варфоломеев А.А., Запечников С.В., Маркелов В.В., Пеленицын М.Б. Интеллектуальные карты и криптографические особенности их применения в банковском деле: Учебное пособие. - М.: МИФИ, 2000.
78. Anderson R. Security Engineering: A Guide to Building dependable Distributed Systems. Wiley, 2001.
79. Пярин В.А., Кузьмин А.С., Смирнов С.Н. Безопасность электронного бизнеса. - М.: Гелиос АРВ, 2002.
80. Бабенко Л.К., Ищуков С.С., Макаревич О.Б. Защита информации с использованием смарт-карт и электронных брелоков. - М.:Гелиос АРВ, 2003.
81. EMVCo/ EMV integrated circuit card specifications for payment systems. 2004. http://www.emvco.com
82. Skorobogatov S. Semi-invasive attacks – new approach to hardware security analysis. 2005.
83. PCI DSS Security Audit Procedures. V 1.1, 2006.
84. Mangard S., Oswald E., Popp T. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, 2007.337p.

Интернет-ссылки

http://csrc.ncsl.nist.gov/fips — стандарты США серии FIPS
http://web.mit.edu/purzer/www/team — краткое введение в смарт-карты
http://www.aladdin.ru — информация по инструментальным системам разработки приложений для смарт-карт
http://www.bankamerica.com — информация об автоматизации банковской деятельности
http://www.bgs.ru — информация об UEPS (Universal Electronic Payment System)
http://www.cardeurope.demon.co.uk — сервер ассоциации CardEurope
http://www.certicom.com– учебные материалы по криптосистемам, основанным на эллиптических кривых и их реализации на интеллектуальных картах
http://www.chipcard.ibm.com/JavaSmartCardAPI/index.html — проект разработки интерфейса прикладного программирования для Java-карт фирмы IBM
http://www.chipcard.ibm.com/overview — технический обзор решений по смарт-картам фирмы IBM
http://www.citmgu.ru/seminars/t9068.shtml
http://www.cl.cam.ac.uk/users/rja14 — ссылки на статьи по методам технических и криптографических атак на электронные системы
http://www.cryptocard.com, *http://ptn.wbinet.nl*, *http://www.gis.co.uk* — информация о портативных защищённых устройствах обеспечения безопасности
http://www.cryptsoft.com/scard/links.html *http://www.cyberflex.austin.et.slb.com/* — документация проекта разработки Java-карт Cyberflex
http://www.dice.ucl.ac.be/crypto/card.html — собрание ссылок на сервера фирм-производителей смарт-карт и некоторую другую информацию, связанную с платёжными системами
http://www.dice.ucl.ac.be/crypto/cascade — проект CASCADE
http://www.digicash.com/publish/digsig/digbig.ru — учебные материалы по применению ЦП на смарт-картах для схем "электронных денег"
http://www.europay.com — информация о международной системе пластиковых карт Europay
http://www.fisc.com — информация о персональных интеллектуальных криптографических устройствах
http://www.gemplus.com— фирма GEMPLUS
http://www.geocities.com/ResearchTriangle/Lab/1578/smart.htm
http://www.iat.unc.edu/guides/irg-35.html — указатель статей и учебных материалов по смарт-картам
http://www.ibm.com/Security/cryptocards/html/library.html — библиотека технической литературы по системам обработки финансовой информации фирмы IBM
http://www.iso.ch — Международная Организация по стандартизации
http://www.javacardforum.org — документация ассоциации Java Card Forum
http://www.mastercard.com/emv — материалы спецификации EMV
http://www.mastercard.com/set — материалы спецификации SET
http://www.mondex.com — информация о технологиях "электронных денег" и протоколах электронных

платежей Mondex
http://www.nsa.gov:8080/programs/missi/cat_pcc.html — информация о криптокарте FORTEZZA
http://www.opencard.org — сервер рабочей группы OpenCard
http://www.smart-card.com — собрание ссылок на большое количество материалов, связанных с технологиями, использующими смарт-карты
http://www.smartcard.co.uk — сервер новостей о смарт-картах
http://www.smartcardsys.com — сервер рабочей группы PC/SC
http://www.smartcrd.com — сервер ассоциации SmartCard Forum
http://www.ubiquinc.com/tourpage.dbm — собрание ссылок на Web-сервера, посвящённые смарт-картам
http://www.visa.com — сервер фирмы VISA
http://www.scdk.com - Scott B. Guthery & Timothy M. Jurgensen, SmartCard Developer's Kit, Macmillan Technical Publishing, 1998.
http://patents.ic.gc.ca/cipo/cpd/en/patent/670868/page/670868_19950126_drawings.pdf

Ролан Морено (Roland Moreno) (род. 11.06.1945) - французский журналист Ролан Морено (Roland Moreno) запатентовал в 1974 г. идею вмонтировать интегральную микросхему в пластиковую карту.

Хельмут Гротруп (Helmut Grottrup) (1916 - 1981) – немецкий инженер и изобретатель. С 1945 по 1946 работал над советской космической программой. В 1955 г. вернулся в Германию. В 1968 г. получил патент на изобретение в области интеллектуальных карт вместе с Jurgen Dethloff. С 1970 г. работает на фирме Giesecke & Devrient , занимающейся картами и процессинговыми системами.

Юрген Девлоф (Jurgen Dethloff) - (12.05.1924 – 31.12.2002) – немецкий инженер и один из первых изобретателей в области микропроцессоров и интеллектуальных карт.