Смарт-карты

Е.Н. Пономарёва[1], В.С.Оскерко[2]

[1]-студентка 1 курса, факультета МЭО, группы УВЭД-2, Белорусского государственного экономического университета.
[2]-научный руководитель, доцент кафедры информационных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр. 26, тел.(8017) 249-19-81, e-mail: oskerko@bseu.minsk.by

Аннотация. Смарт-карту можно считать идеальным средством платежа, поскольку она обладает функциями "электронного кошелька". Последний хранит в своей памяти сумму денежных средств, которыми клиент банка может расплатиться за покупку, и предусматривает технологию off-line. "Электронный кошелек" удобен клиенту, поскольку последний легко контролирует свои активы на карте и при необходимости может их пополнить, кредитуя карту в банке. Память "электронного кошелька" защищена секретным паролем клиента PIN-КОДОМ, который клиент должен набрать на клавиатуре платежного терминала при проведении любой операции по карте. Таким образом, клиент может не опасаться использования смарт-карты без его санкции (если, разумеется, он хранит свой PIN-КОД в тайне от других).

Ключевые слова: смарт-карта, PIN-KOD, Mondex, «электронный кошелёк».

1.Введение

Компьютерные технологии всё глубже проникают в повседневную жизнь и практическую деятельность человека. Тенденции, способствующие появлению так называемой электронной банковской системы, зародились приблизительно двадцать лет назад. Наряду с развитием электронных платёжных систем появляются всё новые и новые инструменты по проведению операций – электронные деньги (e-cash), смарт-карты и т.д. При этом усовершенствованные технологии находят применение не только в деятельности финансовых институтов, но и в повседневной деятельности обычного покупателя.

Смарт-карта - это карта, носителем информации в которой является интегральная микросхема. Когда стандарты и технология производства смарт-карт еще только разрабатывались, их надежности и высокой степени защиты данных на них уделялось самое пристальное внимание. В отношении защиты данных смарт-карты обладают целым рядом преимуществ по сравнению с традиционными магнитными картами.

Во-первых, поскольку процесс создания смарт-карт достаточно сложен и под силу только крупной промышленной компании попытки "взломать" микросхему в кустарных условиях неминуемо приведут к ее разрушению.

Во-вторых, при производстве карточек в каждую микросхему заносится уникальный код. Благодаря этому коду кодирование данных невозможно ни для кого, кроме производителя карт. Производитель, отправляя партию смарт-карт в адрес организации, выпускающей их в обращение, посылает коды отдельно, так что даже в случае потери всей партии, карты оказываются непригодными для использования.

В третьих, при выдаче карточки пользователю на нее заносится один или несколько секретных кодов (паролей), так называемых PIN-КОДОВ, известных только владельцу карты. Если карта утеряна или украдена, ее владелец сообщает о случившемся в банк и программа банка вносит эту карту в список недействительных карт, рассылаемый на все терминалы продаж. Любая попытка использовать потерянную

или украденную карточку будет немедленно пресечена.

Это дает возможность осуществлять авторизацию в режиме off-line, что позволяет экономить значительные средства и время на организацию процедуры доступа к центрам авторизации. Говоря о значительной дешевизне с магнитных карт, следует обратить внимание на стоимость всей системы, включая аренду каналов, связное оборудование и т.д.

Первый вопрос, который задают исключительно все желающие использовать пластиковую карточку в виде платежного средства: какой тип карты более всего подходит в качестве платежной? К сожалению, однозначного ответа на этот вопрос не существует (можно лишь сказать, какие типы карт не подходят). Эффективность платежной системы зависит не только от правильно выбранных технических средств, но и от тщательно отлаженной технологии, от грамотной финансовой политики эмитента, от многих других факторов, которые могут свести все преимущества того или иного типа карт к нулю.

Смарт-карту можно считать идеальным средством платежа, поскольку она обладает функциями "электронного кошелька". Последний хранит в своей памяти сумму денежных средств, которыми клиент банка может расплатиться за покупку, и предусматривает технологию off-line. "Электронный кошелек" удобен клиенту, поскольку последний легко контролирует свои активы на карте и при необходимости может их пополнить, кредитуя карту в банке. Память "электронного кошелька" защищена секретным паролем клиента PIN-КОДОМ, который клиент должен набрать на клавиатуре платежного терминала при проведении любой операции по карте. Таким образом, клиент может не опасаться использования смарт-карты без его санкции (если, разумеется, он хранит свой PIN-КОД в тайне от других).

Не всякая смарт-карта может быть "электронным кошельком".

Рассмотрим типологию смарт-карт. В зависимости от внутреннего устройства и выполняемых функций смарт-карты можно разделить на три типа:

- карты-счетчики;
- карты с памятью;
- микропроцессорные карты.

Практически любую карту любого типа можно использовать в качестве платежной. Однако лишь весьма ограниченное число карт будет удовлетворять всем требованиям, которыми должна обладать массовая платежная смарт-карта: невысокой стоимостью, возможностью проводить любые (а не только специфичные) платежи, хорошей защищенностью и необходимым уровнем "интеллектуальности" для обеспечения технологии off-line.

Карты-счетчики. Данный тип карточек применяется для такого типа расчетов, когда требуется вычитание фиксированной суммы за каждую платежную операцию. Подобные карточки еще называются карточками с предварительно оплаченной суммой. Примером таких расчетов может быть плата за телефонный разговор. Обычно в телефонах-автоматах единица времени разговора имеет фиксированную цену. Абонент оплачивает время разговора монетками или специальными жетонами, которые подсчитывает соответствующее устройство телефона. При применении карточек минимальной сумме платежа ставится в соответствие один бит памяти карты. В процессе разговора устанавливается связь между телефоном и картой, и за каждую единицу времени "пережигается" некоторое количество бит. Таким образом, карта заменяет монеты или жетоны.

Аналогичным образом карты-счетчики применяются при подписке на платное телевидение, при оплате за проезд, автостоянку и т. п.

Первоначально использовались карты с однократно программируемой памятью. После полного использования карты приходилось выбрасывать. Современные карты такого типа позволяют после полного использования "восстанавливать" содержимое счетчика. Восстановление содержимого может быть выполнено только при знании определенного кода, разрешающего это действие. Помимо этого, карты содержат область, в которую записываются идентификационные данные. Эти данные не могут быть изменены впоследствии. Карты, позволяющие перезаписывать информацию, относятся к типу карт с энергонезависимой перепрограммируемой памятью. Карты с памятью-это название весьма условно, так

как все смарт-карты имеют память. Этот тип карт выделен как промежуточный при переходе от карт-счетчиков к микропроцессорным картам.

Обычно карты подобного типа используются для хранения информации. Существуют два подтипа подобных карт: с незащищенной и с защищенной памятью. Карты второго подтипа отличаются от карт первого более высоким «интеллектом», направленным на предотвращение несанкционированного доступа к данным на карте. Однако той «интеллектуальности», которая характерна для карт с микропроцессорами, карты с защищенной памятью не имеют.

В картах с незащищенной памятью нет ограничений по чтению или записи данных. Иногда их называют картами с полнодоступной памятью; работа с ними (в смысле логической структуры данных) напоминает работу с бинарным файлом. Можно произвольно структурировать карту на логическом уровне, рассматривая ее память как набор байтов, который можно скопировать в оперативную память или обновить специальными командами.

Карты с незащищенной памятью использовать в качестве платежных крайне опасно. Достаточно легально приобрести такую карту, скопировать ее память на диск, а дальше после каждой покупки восстанавливать ее память копированием начального состояния данных с диска, причем, ничуть не интересуясь тем, какая информация хранится на карте (т. е. шифрование данных в памяти карты от мошенничества подобного рода не спасает). Разумеется, такую операцию может проделать лишь квалифицированный программист.

В карточках с защищенной памятью используется специальный механизм для разрешения чтения/записи или стирания информации. Чтобы провести эти операции, надо предъявить карте специальный секретный код (а иногда и не один). Предъявление кода означает установление с ней связи и передачу кода “внутрь” карты.

Сравнение кода с ключом защиты чтения/записи (стирания) данных проведет сама карта и “сообщит” об этом устройству чтения/записи смарт-карт. Чтение записанных в память карты ключей защиты или копирование памяти карты невозможно. В то же время, зная секретный код (коды), можно прочитать или записать данные, организованные наиболее приемлемым для платежной системы логическим образом. Таким образом, карты с защищенной памятью годятся для универсальных платежных применений, хорошо защищены, и при этом недороги. Как правило, карты с защищенной памятью содержат область, в которую записываются идентификационные данные. Эти данные не могут быть изменены впоследствии, что очень важно для обеспечения невозможности подлога карты. С этой целью идентификационные данные на карте “прожигаются”.

Необходимо также, чтобы на платежной карте были по меньшей мере две защищенные области. Уже отмечалось, что в технологии безналичных расчетов по картам участвуют обычно три юридически независимых лица: клиент, банк и магазин. Банк вносит деньги на карту (кредитует ее), магазин снимает деньги с карты (дебетует ее), и все эти операции должны совершаться с санкции клиента. Таким образом, доступ к данным на карте и операции над ними надо разграничивать. Это достигается разбиением памяти карты на две защищенные разными ключами области - дебетовую и кредитную.

Каждый участник операции имеет свой секретный ключ. У клиента это PIN-КОД. Его правильное предъявление открывает доступ к карте (по чтению данных), однако не должно менять информацию, которой распоряжается кредитор карты (банк) или ее дебитор (магазин).

Ключ записи информации в кредитную область карты имеется только у банка; ключ записи информации в дебетную область - у магазина. Только при предъявлении сразу двух ключей (PIN-кода клиента и ключа банка при кредитовании, PIN-кода клиента и ключа магазина при дебетовании) можно провести соответствующую финансовую операцию - внести деньги либо списать сумму покупки с карты.

Если в качестве платежной используются карты с одной защищенной областью памяти, - значит, банк и магазин будут работать с одной и той же областью, применяя одинаковые ключи защиты. Если банк, как эмитент карты, может ее дебетовать (например, в банкоматах), то магазин права кредитовать карту не имеет. Однако такая возможность ему дана -

поскольку, в силу необходимости дебетования карты при покупках, он знает ключ стирания защищенной зоны.

То обстоятельство, что и кредитор карты, и ее дебитор (обычно разные лица) пользуются одним ключом, нарушает сразу несколько основных принципов защиты информации (в частности, принципы разделения полномочий и минимальных полномочий). Это рано или поздно приведет к мошенничеству. Не спасают ситуацию и криптографические способы защиты информации.

Из известных карт с защищенной памятью лишь упоминавшаяся уже карта GPM896 обладает двумя защищенными областями памяти и удовлетворяет требованиям по разграничению доступа к информации, как со стороны банка, так и со стороны магазина.

Микропроцессорные карты. Эти карты представляют собой последние достижения в области смарт-карт. Их применение весьма обширно. Микропроцессоры, установленные на этих картах, обладают следующими основными характеристиками:

- тактовой частотой до 5 Мгц;
- емкостью ОЗУ до 256 байт;
- емкостью ПЗУ до 10 Кбайт;
- емкостью перезаписываемой энергонезависимой памяти до 8 Кбайт.

В карту встраивается специализированная операционная система, обеспечивающая большой набор сервисных операций и средств безопасности.

Операционная система карты поддерживает файловую систему, предусматривающую разграничение доступа к информации. Для информации, хранимой в любой записи (файл, группа файлов, каталог), могут быть установлены следующие режимы доступа:

- всегда доступна по чтению/записи. Этот режим разрешает чтение/запись информации без знания специальных секретных кодов;
- доступна по чтению, но требует специальных полномочий для записи. Этот режим разрешает свободное чтение информации, но разрешает запись только после предъявления специального секретного кода;
- специальные полномочия по чтению/записи. Этот режим разрешает доступ по чтению или записи после предъявления специального секретного кода, причем коды для чтения и записи могут быть различными;
- недоступна. Этот режим не разрешает читать или записывать информацию. Информация доступна только внутренним программам карточки. Обычно этот режим устанавливается для записей, содержащих криптографические ключи.

Как правило, в такие карточки встроены криптографические средства, обеспечивающие шифрование информации и выработку "цифровой" подписи. Традиционно в карточках для этих целей применяется криптографический алгоритм DES. Кроме того, в карточке имеются средства ведения ключевой системы.

Карты обеспечивают различный спектр сервисных команд. Для банковских целей наиболее интересные из них - средства ведения электронных платежей.

К специальным средствам относятся возможность блокировки работы с карточкой. Различаются два вида блокировки: при предъявлении неправильного транспортного кода и при несанкционированном доступе.

Суть транспортной блокировки состоит в том, что доступ к карточке невозможен без предъявления специального транспортного кода. Этот механизм необходим для защиты от нелегального использования карточек при хищении во время пересылки карточки от производителя к потребителю. Карточка может быть активизирована только при предъявлении правильного «транспортного» кода.

Суть блокировки при несанкционированном доступе состоит в том, что если при доступе к информации несколько раз неправильно был предъявлен код доступа, то карта вообще перестает быть работоспособной. При этом, в зависимости от установленного режима карта может быть впоследствии либо активизирована при предъявлении специального кода, либо нет. В последнем случае карточка становится непригодной для дальнейшего использования.

Смарт-карты производятся многими известными фирмами. Среди них: Bull (Франция), Data Card (США), Schiumberger (Франция) - самый крупный производитель телефонных карт, Toshiba (Япония).

Общепризнанным лидером в области производства и разработки смарт-карт

является французская фирма GemPlus. Фирма производит более двух десятков разнообразных карт, как специализированных, так и универсальных. Отделения фирмы расположены во многих странах - Великобритании, США, Сингапуре, Японии, Испании, Италии, Германии.

Фирмой GemPlus Card International разработаны несколько типов смарт-карт, ориентированных на применение в качестве пластиковых денег и ведение счетов. Например, карта с защищенной памятью GPM896 предназначена для проведения платежей с небольшими суммами, а микропроцессорная карта PCOS - для ведения счетов. Карта PCOS обеспечивает высокую степень безопасности данных и поддерживает специализированный набор операций по их обработке.

Основные производители микросхем для смарт-карт: Arntel (США), Hitachi (Япония), Motorola (США), Oki (Япония), Philips (Нидерланды) и др.

Главное отличие смарт-карт от других видов пластиковых карт (с магнитной полосой или со штриховым кодом) - интеллектуальность карт с микросхемами.

При платежах по магнитным или штриховым картам применяется режим on-line. Разрешение на платеж дает, по существу, компьютер банка или процессингового центра при связи с точкой платежа.

Поэтому основная проблема, возникающая здесь, - обеспечение надежной, защищенной и недорогой связи, что в наших условиях крайне трудно.

При платежах по смарт-картам применяется принципиально новый режим off-line - разрешение на платеж дает сама карта (точнее, встроенная в нее микросхема) при общении с торговым терминалом непосредственно в торговой точке. Накладные расходы по обеспечению платежей чрезвычайно малы, проблемы связи не играют той роли, как в технологиях on-line.

Другая важная особенность смарт-карт заключается в их надежности и безопасности. Смарт-карта должна быть достаточно “интеллектуальна”, чтобы самостоятельно принять решение о проведении платежа и при этом обладать развитой системой защиты от ее несанкционированного использования.

Еще одним преимуществом смарт-карт над другими пластиковыми картами является их многофункциональность. Обладая встроенными возможностями осуществлять многие математические и логические операции и превосходя другие пластиковые карты по объему хранимой на них информации, одни и те же смарт-карты могут использоваться в различных приложениях.

Смарт-карты по сравнению с другими пластиковыми картами обладают высокими эксплуатационными характеристиками. Например, смарт-карты фирмы GemPlus Card International - лидера в области производства карт - обладают следующими основными характеристиками: время хранения информации - 10 лет; минимальное число перезаписей - 10 000 раз; время записи одного байта информации - не более 10 мс; температура хранения - от -20 до +55 С; рабочая температура -от 0 до +50 °С.

Смарт-карты устойчивы к внешним воздействиям.

Платежные системы на основе смарт-карт обладают рядом преимуществ перед системами, использующими карты с магнитной полосой или со штриховым кодом.

Преимущества могут быть как общие, касающиеся всех пользователей системы, так и частные - для отдельных групп пользователей.

Общие преимущества сводятся к следующему:

-Все существующие операции с наличностью могут быть с легкостью заменены на операции со смарт-картами.

-Централизованный контроль за системой и финансовыми транзакциями для всех элементов системы.

-Незначительная стоимость оборудования торгового терминала, отсутствие необходимости затрат на дополнительные средства коммуникации и независимость обслуживания системы от средств коммуникации.

-Отсутствие дополнительных затрат на эксплуатацию системы.

-Надежность использования. После занесения на смарт-карту всех данных владельца связь с базой данных происходит немедленно по предъявлении карты, что очень важно для городов, в которых

отсутствуют современные телекоммуникационные средства.

-Портативность и автономность торгового терминала, обеспечивающие его широкое применение, вплоть до мобильных пунктов обслуживания и торговых киосков.

-Возможность принимать оплату с карт в различного типа автоматических устройствах: автоматы по продаже сигарет, прохладительных напитков, телефонные автоматы, автомобильные стоянки и мойки, автосервис и т. д.

-Уменьшение административных расходов на каждом уровне и расходов на поддержание работы системы, осуществление транзакций, сокращение расходов на время обслуживания, линии связи.

-Улучшение и упрощение процедур взаиморасчетов.

-Существенное увеличение скорости всех операций.

-Существенное уменьшение расходов всех пользователей системы: владельцев карт, торгующих организаций, головной фирмы эмитента смарт-карт.

-Система защищена на всех уровнях и исключает целый ряд рисков, присущих другим системам платежей (наличным, талонам, магнитным картам).

-За счет более быстрой оборачиваемости денежных средств уменьшается инфляция и сокращаются расходы на поддержание обращения наличности.

-Снижается уровень криминальности.

-Появляется возможность использования платежных карт в других сферах (государственное страхование, медицинское обслуживание) как чисто идентификационных.

-Защита карты. Смарт-карта может быть произведена только промышленным путем и содержит уникальный код производителя.

Если на вторую карту будут нанесены те же данные, что и на оригинал, различие во внутренних номерах даст возможность системе отличить одну карту от другой.

Перспективы использования смарт-карт. Хотя мировые лидеры - фирмы VISA International и Europay International уже заявили о своем неизбежном переходе в ближайшем будущем на технологию смарт-карт, платежные системы на основе карт с магнитной полосой будут продолжать использоваться еще достаточно долгое время, так как развитая международная инфраструктура для использования этих карт уже сформирована.

Смарт-карты будут внедряться, но весьма осторожно и постепенно.

Однако ряд проектов на базе смарт-карт достаточно успешно развивается. Это - Mondex, Proton, Visa-Cash.

Mondex - одна из самых известных систем в области чистых электронных денег. Решения, предлагаемые поставщиками системы, и особенно трудности, возникающие на пути ее внедрения, во многом отражают общие проблемы продвижения на рынок платежных систем на базе микропроцессорных карточек.

Идею, заложенную в основу создания системы Mondex, очень точно описывает главный рекламный лозунг ее поставщиков: Mondex - это наличные! Электронные деньги Mondex можно передавать по каналам связи. В этом случае моментальные платежи возможны между субъектами, находящимися в разных точках мира.

Для практической реализации этой идеи была выбрана микропроцессорная технология. Карточка Mondex - это пятикошельковая микропроцессорная карточка.

Для зачисления на карточку средств с банковского счета и для перевода средств с карточки на карточку служат специальные устройства - Mondex-совместимые телефоны (Mondex phones). Таким образом, в качестве каналов для передачи «электронных денег» в системе используются обычные телефонные линии. По идеологии системы Mondex, телефон превращается в своеобразный персональный банкомат, круглосуточно выдающий электронные наличные.

Для хранения средств, снятых с банковского счета, помимо карточки служит еще одно устройство, условно называемое бумажником (Mondex wallet). Это - портативное устройство, позволяющее переводить средства с карточки на карточку, считывать баланс, изменять PIN-КОД и выполнять некоторые другие простые операции. Главная же функция этого устройства, определяемая его названием, состоит в хранении снятых со счета средств. Средства на карточку могут переводиться из бумажника по мере необходимости. Такой подход, по мнению создателей системы,

повышает безопасность: часть денег хранится в бумажнике, а часть - на карточке.

Кроме того, в системе предусмотрено использование банкоматов (на случай, если кому-нибудь понадобятся-таки настоящие наличные, а не "электронные") и торговых терминалов. Последние осуществляют перевод средств с карточки покупателя на карточку продавца, который затем, воспользовавшись Mondex-совместимым телефоном, может перечислить накопленные на его карточке средства на банковский счет предприятия (аналогия с наличными явно прослеживается).

Поскольку бухгалтерский контроль за операциями по карточкам Mondex не предусмотрен, в системе действует жесткий лимит суммы транзакций, проводимых с помощью «электронных денег».

Система Mondex принадлежит к системам «электронных» денег, в полной мере обладая всеми их элементами. Однако наряду с очевидными ее преимуществами в идее системы Mondex есть нерешенные задачи.

Карточка, а точнее, записанные на ней средства считаются электронными наличными, т. е. средством платежа. Однако традиционно эмитентом наличных денег может быть только центральный банк страны. В данном же случае эмиссия электронных денег как бы доверяется коммерческому банку.

Еще одна проблема, связанная с безопасностью системы, заключается в возможности мошеннического использования карточки, если удастся все же «пробить» сложную систему защиты информации, обеспечиваемую применением микропроцессорных карточек.

Безусловно, использование механизмов аутентификации и криптозащиты повышает стойкость системы на порядки. Тем не менее, многие специалисты считают, что освоение микропроцессорных технологий мошенниками - дело времени.

Таким образом, приравнивание записи на карточке к деньгам ставит общество в слишком жесткую зависимость от обеспечения безопасности платежной системы как на организационном, так и на технологическом уровне.

Электронные деньги Proton - это еще один из самых крупномасштабных на сегодняшний день проектов внедрения "электронных денег", разработанный бельгийской компанией Banksys.

Компания Banksys стала одним из пионеров освоения этого сектора. 18 февраля 1995 г. она начала пилотный проект по внедрению "электронных кошельков" Proton в двух бельгийских городах.

Идея "электронного кошелька" Proton - это карточки для мелких покупок. Развитие этой идеи Banksys ведет в направлении на разнообразие сфер ее использования. Основные сферы использования "электронных денег", по мнению авторов, проекта таковы: мелкие покупки в магазинах; покупки в торговых автоматах; парковка автомобилей; проезд в общественном транспорте; телефоны-автоматы.

Proton задумывался как национальный "электронный кошелек" для Бельгии, население которой исторически имеет сильную приверженность к дебетовым карточкам. Наличные в стране в подавляющем большинстве случаев используются для оплаты мелких покупок, именно поэтому для заменителя наличных была изначально очерчена столь четкая рыночная ниша.

Компания Banksys в основу практической реализации идеи "электронных денег" заложила два ключевых положения.

Во-первых, "электронные деньги" должны быть столь же легко доступны клиенту, как и наличные, и приниматься повсеместно там, где клиент привык расплачиваться наличными.

Во-вторых, система должна поддерживать тот же уровень безопасности, что и система обращения наличных денег.

Первое положение должно сделать систему привлекательной для клиента, второе - безопасной для экономики страны.

Удобство системы "электронных денег" определяется двумя факторами:

- удобством загрузки кошелька;
- удобством и развитостью инфраструктуры.

Здесь организационные и технологические аспекты играют равную роль. Записать некоторую сумму на карточку Proton можно с помощью как банкомата (оснащенного специальным устройством), так и специального телефонного аппарата (payphone).

В системе функционируют терминалы для приема карточек Proton; счетчики на стоянках. Значительное внимание было уделено торговым автоматам, что лишний раз иллюстрирует идею четко определенной торговой ниши, заложенной в основу проекта.

Наконец, ни одна система "электронных денег" не обходится без портативных устройств чтения остатка средств на карточке. Banksys предлагает несколько подобных приспособлений (встроенных в футляр для карточки или брелок), позволяющих с помощью одной кнопки просмотреть остаток средств в «кошельке» и суммы нескольких последних транзакций.

Второе положение - безопасность системы - обеспечивается следующим образом. Банк или иное финансовое учреждение - эмитент "электронных денег" дебетует счет клиента в момент загрузки средств в память "электронного кошелька". Одновременно соответствующая сумма переводится эмитентом в единый для всей страны резервный фонд. Процедура обязательного резервирования гарантирует, с одной стороны, невозможность бесконтрольной эмиссии ничем не обеспеченных "электронных денег" и, с другой стороны, возмещение средств организациям, принимающим их к оплате.

Средства на карточке клиента ничем не защищены: в случае утери или кражи карточки ими может воспользоваться любой, так как «электронный кошелек» анонимен и для его дебетования не требуется вводить PIN-КОД. Все операции дебетования осуществляются в режиме off-line. Данные о транзакциях передаются в процессинговый центр либо самим терминалом, либо, если терминал не подключен к центру, оператором (через компьютер и модем). В последнем случае проводится предварительная инкассация терминала. Средства на счета торговцев переводятся из резервного фонда.

Технически безопасность обращения "электронных денег" обеспечивается защищенностью как отдельных элементов системы ("электронного кошелька", терминалов и т.д.), так и самого процесса зарядки "кошелька".

Развивая систему в общенациональном масштабе, компания Banksys особое внимание уделяет работе с закрытыми группами пользователей: студентами, проживающими в институтских городках, постоянными пассажирами автобусных компаний и железных дорог и т.д. По мнению Banksys, работа с закрытыми группами может принести значительное число наиболее постоянных клиентов.

Технология Proton, также как и Mondex, активно продвигается.

Проекты внедряются в Нидерландах, в Австралии, в Швейцарии, в Швеции, в Канаде, в Бразилии.

"Электронные кошельки" VISA. В марте 1995 г. крупнейшая корпорация на рынке пластиковых денег VISA объявила, что намерена разработать специально для этого рынка новый микропроцессорный продукт - карточку с хранимой суммой, или "электронный кошелек".

"Электронные кошельки" VISA Cash предназначены для применения в открытой (термин компании VISA) системе, в состав которой входит множество эмитентов, эквайеров и предприятий торговли и услуг. Для работы открытой системы необходимы клиринговые учреждения. Карточки, выпускаемые в рамках открытой системы, могут использоваться для оплаты товаров и услуг, предлагаемых любыми участниками системы.

2.Заключение

Основное преимущество смарт-карт состоит в том, что они являются средством, которое, в первую очередь позволяет увеличить и разнообразить пакет услуг, предоставляемых клиенту. При этом платежной системе и банкам, входящим в нее, технология на основе смарт-карт обойдется дешевле за счет сокращения потерь от мошенничества и снижения расходов на авторизацию и связь.

Литература:

1.Петров А.А. Компьютерная безопасность. Изд. ДМК, М., 2000.