**Аннотация.**

В данном реферате был сделан обзор современных средств электронных платежей – как перспективного современного оборота нематериальных денег, рассмотрен принцип криптографической защиты информации на магнитной карточке, а также перспективы дальнейшего развития систем электронных платежей.

**Содержание**

Вступление. 3

1. Основные понятия и принципы использования карточек. 5

1.1. Виды платежных карт, основные понятия. 5

1.2. Классификация пластиковых карточек. 6

1.3. Платежная система. 7

2. Технические средства. 9

2.1. Способы идентификации пластиковых карт. 9

2.2. Особенности устройства смарт-карты. 11

3.Применение криптографии для карт с магнитной полосой 16

3.1. Простое шифрование. 17

3.2.Обмен динамическим ключом. 18

3.3. Обработка ПИН. 18

3.4. Обработка VCC. 19

3.5.Работа с ключами. 19

3.6.Физическое приложение. 20

3.7. Другие приложения шифрования в финансах. 21

4. Устройства обслуживания электронных платежей. 21

4.1. Использование POS-терминалов. 21

4.2. Использование банкоматов. 22

5. Стандарты электронных расчетов. 23

5.1. Стандарт SET. 23

5.2. Концепция Cyber Cash. 23

5.3. Платежи без кодирования - система First Virtual. 23

5.4. Система Digital Cash. 24

6. Выводы 25

# Вступление.

Существующие в настоящее время в Украине системы расчетов по операциям с платежными картами классифицируют следующим образом:

- национальная система массовых электронных платежей НСМЭП;

- международная платежная система VISA International;

- международная платежная система EURO PAY (MASTER CARD) International;

- платежные системы AMEX, Diner’s Club.JCB;

- внутренние межбанковские платежные системы (ОНИКС, ОБЕНИКС);

- локальные внутренние монобанковские платежные системы (СБОН, МЕТАКАРТ, ПИБ).

Проект НСМЭП разработан НБУ совместно с рядом отечественных поставщиков программно – технических средств, основан на чип – картах и широком использовании off-line технологий. Особенностью проекта является использование собственных операционных систем, системы безопасности и финансовых приложений чип – карточки, позволяющих внедрить два основных платежных инструмента – электронный кошелек и электронный чек, реализующих дебетовые схемы осуществления платежей.

Международные платежные системы VISA International и EURO PAY (MASTER CARD) International присутствуют на Украине с 1995 г. и реально начали работать с 1997 г., когда украинские банки стали полноправными членами этих систем. Эмитировано более 800 тысяч карт (лидерами являются ПРИВАТБАНК, ПУМБ, АВАЛЬ).

Созданию системы электронных платежей в Украине, способствовало ряд причин:

- расчеты с использованием наличных денег чрезвычайно дорого обходятся государственным и коммерческим финансовым структурам (выпуск в обращение новых купюр, обмен старых, содержание большого персонала);

- около 10..12% стоимости каждой купюры уходит на поддержание ее собственного же обращения;

- достаточно удобное средство для расчетов в магазинах;

- удобное средство для перевода или вызова денег за границу (не смотря на то, что карточки принимаются не везде, лимит на снятие наличных, комиссионный сбор т.д. как показывает практика это намного выгоднее, чем носить при себе большое количество наличных).

- международная карточка дает возможность оплачивать товары через Интернет.

Из истории карточки следует отметить, что первая кредитная карта была выпущена в 1914 году известной американской фирмой Mobil Oil(раньше фирма называлась General Petroleum Corporation of California). Выпущенные этой компанией карты использовались при оплате торговых операций по нефтепродуктам. Первые карточки были картонные, данные на них были либо написаны, либо выдавлены. В1928 году Бостонской компанией Farrington Manufacturing были выпущены первые металлические пластинки, на которых выдавливался (эмбоссировался) адрес и которые кредитоспособным клиентам. Продавец вкладывал эту пластину в импринтер и буквы, выдавленные на ней, отпечатывались на торговом чеке. Подходящий материал для карточки был найден лишь в 60-е годы, было найдено приемлемое решение – пластиковая каточка с магнитной полосой. В 1975 году Ролан Морено изобрел и запатентировал электронную карту памяти. Спустя несколько лет компания Bell (Франция) разработала и запатентировала смарт-карту со встроенным микропроцессором.

В настоящее время рас­ши­ри­лось ис­поль­зо­ва­ние ком­пь­ю­тер­ных се­тей, в частности глобальной сети Интернет, по ко­то­рым пе­ре­да­ет­ся боль­шие объ­е­мы ин­фор­ма­ции го­су­дар­ст­вен­но­го, ком­мер­че­ско­го и ча­ст­но­го ха­рак­те­ра. По этому остро стоит проблема защита информации от посторонних лиц. Проблемой защиты информации путем ее преобразования за­ни­ма­ет­ся крип­то­ло­гия (*kr*y*p*to*s* - тай­ный, lo*g*o*s* - нау­ка). Криптология раз­де­ля­ет­ся на два на­прав­ле­ния - крип­то­гра­фию и крип­тоа­на­лиз. Це­ли этих на­прав­ле­ний прямо про­ти­во­по­лож­ны.

Крип­то­гра­фия за­ни­ма­ет­ся по­ис­ком и ис­сле­до­ва­ни­ем ма­те­ма­ти­че­ских ме­то­дов пре­об­ра­зо­ва­ния ин­фор­ма­ции.

Сфе­ра ин­те­ре­сов криптоанализа - ис­сле­до­ва­ние воз­мож­но­сти рас­шиф­ро­вы­ва­ния ин­фор­ма­ции без зна­ния клю­чей.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хра­не­ние ин­фор­ма­ции (до­ку­мен­тов, баз данных) на но­си­те­лях в за­шиф­ро­ван­ном ви­де.

# 1. Основные понятия и принципы использования карточек.

## 1.1. Виды платежных карт, основные понятия.

Пластиковая карточка - это персонифицированный платежный инструмент, предоставляющий пользующемуся карточкой лицу возможность безналичной оплаты товаров и/или услуг, а также получения наличных средств в отделениях (филиалах) банков и банковских автоматах (банкоматах). Принимающие карточку предприятия торговли/сервиса и отделения банков образуют сеть точек обслуживания карточки (или приемную сеть).

Особенностью продажи и выдачи наличных по карточкам является то, что эти операции осуществляются магазинами и, соответственно, банками "в долг" - товары и наличные предоставляются клиентам сразу, а средства в их возмещение поступают на счета обслуживающих предприятий чаще всего через некоторое время (не более нескольких дней). Гарантом выполнения платежных обязательств, возникающих в процессе обслуживания пластиковых карточек, является выпустивший их банк-эмитент. Поэтому карточки на протяжении всего срока действия остаются собственностью банка, а клиенты (держатели карточек) получают их лишь в пользование. Характер гарантий банка-эмитента зависит от платежных полномочий, предоставляемых клиенту и фиксируемых классом карточки.

При выдаче карточки клиенту осуществляется его персонализация - на нее заносятся данные, позволяющие идентифицировать карточку и ее держателя, а также осуществить проверку платежеспособности карточки при приеме ее к оплате или выдаче наличных денег. Процесс утверждения продажи или выдачи наличных по карточке называется авторизацией. Для ее проведения точка обслуживания делает запрос платежной системе о подтверждении полномочий предъявителя карточки и его финансовых возможностей. Технология авторизации зависит от схемы платежной системы, типа карточки и технической оснащенности точки обслуживания. Традиционно авторизация проводится "вручную", когда продавец или кассир передает запрос по телефону оператору (голосовая авторизация), или автоматически, карточка помещается в POS-терминал или торговый терминал (POS - Point Of Sale), данные считываются с карточки, кассиром вводится сумма платежа, а держателем карточки со специальной клавиатуры - секретный ПИН-код (ПИН - Персональный Идентификационный Номер). После этого терминал осуществляет авторизацию либо устанавливая связь с базой данных платежной системы (on-line режим), либо осуществляя дополнительный обмен данными с самой карточкой (off-line авторизация). В случае выдачи наличных денег процедура носит аналогичный характер с той лишь особенностью, что деньги в автоматическом режиме выдаются специальным устройством - банкоматом, который и проводит авторизацию.

При осуществлении расчетов держатель карточки ограничен рядом лимитов. Характер лимитов и условия их использования могут быть весьма разнообразными. Однако в общих чертах все сводится к двум основным сценариям.

Держатель дебетовой карточки должен заранее внести на свой счет в банке-эмитенте некоторую сумму. Ее размер и определяет лимит доступных средств. При осуществлении расчетов с использованием карточки синхронно уменьшается и лимит. Контроль лимита осуществляется при проведении авторизации, которая при использовании дебетовой карточки является обязательной всегда. Для возобновления (или увеличения) лимита держателю карточки необходимо вновь внести средства на свой счет.

Для обеспечения платежей держатель карточки может не вносить предварительно средства, а получить в банке-эмитенте кредит. Подобная схема реализуется при оплате посредством кредитной карточки. В этом случае лимит связан с величиной предоставленного кредита, в рамках которого держатель карточки может расходовать средства. Кредит может быть как однократным, так и возобновляемым. Возобновление кредита в зависимости от договора с держателем карточки происходит после погашения либо всей суммы задолженности, либо некоторой ее части.

## 1.2. Классификация пластиковых карточек.

По способу расчетов:

- кредитные карточки, дает владельцу пользоваться кредитом при покупке товаров при получении кассовых суд;

- дебетовые карточки, предназначенные для получения наличных в банковских автоматах или для расчетов за товары и услуги через электронные терминалы. При этом средства списываются со счета владельца карточки в банке. Дебетовые карточки не позволяют оплачивать покупки при отсутствии денег на счете. Преимущество дебетовой карточки перед кредитной состоит в отсутствие лимита платежа.

По способу записи информации на карточку:

- графический;

- эмбоссирование;

- штрихкодирование;

- кодирование на магнитной полосе;

- чип;

- лазерная запись (оптические карты).

Графическая запись – наиболее простая форма записи информации на карточку. Графическим методом наносится фотографическое изображение держателя карты и лазерный образец подписи.

Эмбоссирование(emboss) нанесение данных на карту в виде рельефных знаков – позволило быстрее оформлять операции оплаты картой, делая оттиск слипа. В целях борьбы с мошенничеством используются слипы без копировального слоя, но способ информации остался прежним – механическое давление.

Штрих-кодирование – способ записи на карту применялся до изобретения магнитной полосы и в платежных системах распространения не получил.

Магнитные карточки – пластиковые карточки с магнитной полосой, которая содержит объем информационной памяти около 100MB, которая считывается специальным устройством. Информация, содержащаяся на магнитной полосе, совпадает с записями на передней стороне карты: имя, номер счета владельца и дата окончания действия карточки.

В настоящее время магнитная запись является самый распространенный способ нанесения информации на пластиковые карточки. Однако магнитная полоса не обеспечивает необходимого уровня защиты от подделок.

Карты памяти (смарт-карты) – пластиковая карточка со встроенной микросхемой, содержащая запоминающее устройство. Уровень защиты карты памяти достаточно не высок, и они используются для оплаты телефонных разговоров и других операций, не требующих высокого уровня защиты информации. Смарт-карта внешне похожи на карты памяти, однако микросхема смарт-карты представляет собой микропроцессор. Название смарт-карта (smart-умный, разумный) связано с возможностью выполнять сложные операции по обработке информации. Микросхемы смарт-карты представляют собой полные микроконтроллеры, способные выполнять расчеты. Изготовление смарт-карт дороже других видов пластиковых карточек: стоимость зависит от объема памяти и уровня защиты встроенной микросхемы.

Карты оптической памяти – имеют большую емкость, запись и считывание производится специальной аппаратурой. Большого распространения в банковских технологиях не нашла в связи с высокой стоимостью карт так и считывающего оборудования.

По принадлежности к учреждению-эмитенту:

- банковские карточки (эмитент банк или консорциум банков);

- коммерческие карточки (эмитент нефинансовое учреждение).

По сфере использования:

- универсальные карточки – для оплаты любых товаров и услуг;

- частные коммерческие карты – для оплаты специальных услуг (карты гостиничных сетей, автозаправочных станций, супермаркетов).

По территориальной принадлежности:

- международные;

- национальные;

- локальные;

- карты, действующие в одном учреждении.

По времени использования:

- ограниченные временным промежутком;

- неограниченные (бессрочные).

Банковские и другие карты, используемые для расчетов:

- автономный «электронный кошелек»(работает в режиме off-line);

- ключ к счету – средство идентификации.

Большинство современных карточек, являются идентификаторами, а не электронными кошельками.

## 1.3. Платежная система.

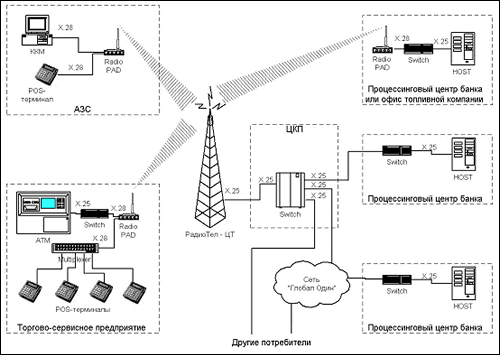
Платежной системой будем называть совокупность методов и реализующих их субъектов, обеспечивающих в рамках системы условия для использования банковских пластиковых карточек оговоренного стандарта в качестве платежного средства. Одна из основных задач, решаемых при создании платежной системы, состоит в выработке и соблюдении общих правил обслуживания карточек входящих в систему эмитентов, проведения взаиморасчетов и платежей. Эти правила охватывают как чисто технические аспекты операций с карточками - стандарты данных, процедуры авторизации, спецификации на используемое оборудование и пр., так и финансовые стороны обслуживания карточек - процедуры расчетов с предприятиями торговли и сервиса, входящими в состав приемной сети, правила взаиморасчетов между банками, тарифы и т.д.

Таким образом, с организационной точки зрения ядром платежной системы является основанная на договорных обязательствах ассоциация банков. В состав платежной системы также входят предприятия торговли и сервиса, образующие сеть точек обслуживания. Для успешного функционирования платежной системы необходимы и специализированные нефинансовые организации, осуществляющие техническую поддержку обслуживания карточек: процессинговый и коммуникационные центры, центры технического обслуживания и т.п.

Процессинговый центр - специализированная сервисная организация - обеспечивает обработку поступающих от эквайеров (или непосредственно из точек обслуживания) запросов на авторизацию и/или протоколов транзакций - фиксируемых данных о произведенных посредством карточек платежах и выдачах наличных. Этот центр ведет базу данных, которая, в частности, содержит данные о банках - членах платежной системы и держателях карточек. Центр хранит сведения о лимитах держателей карточек и выполняет запросы на авторизацию в том случае, если банк-эмитент не ведет собственной базы (off-line банк). В противном случае (on-line банк) , процессинговый центр пересылает полученный запрос в банк-эмитент авторизуемой карточки. Очевидно, что центр обеспечивает и пересылку ответа банку - эквайеру. Кроме того, на основании накопленных за день протоколов транзакций процессинговый центр готовит и рассылает итоговые данные для проведения взаиморасчетов между банками-участниками платежной системы, а также формирует и рассылает банкам - эквайерам (а, возможно, и непосредственно в точки обслуживания) стоп - листы. Процессинговый центр может также обеспечивать потребности банков-эмитентов в новых карточках, осуществляя их заказ на заводах и последующую персонализацию. Следует отметить, что разветвленная платежная система может иметь несколько процессинговых центров, роль которых на региональном уровне могут выполнять и банки - эквайеры.

Коммуникационные центры обеспечивают субъектам платежной системы доступ к сетям передачи данных. Использование специальных высокопроизводительных линий коммуникации обусловлено необходимостью передачи больших объемов данных между географически распределенными участниками платежной системы при авторизации карточек в торговых терминалах, при обслуживании карточек в банкоматах, при проведении взаиморасчетов между участниками системы и в других случаях.

Примером такой коммутационной системы является сеть "РадиоТел-ЦТ"



Сеть "РадиоТел-ЦТ" является радиопакетной сетью передачи данных общего пользования, построенной по сотовому принципу.

Сеть "РадиоТел-ЦТ" предназначена для предоставления услуг передачи данных с пропускной способностью 4800 бит/сек. С учетом этого услуги сети "РадиоТел-ЦТ" целесообразно использовать для подключения низкоскоростного терминального оборудования - банкоматов, POS-терминалов. Потенциальными потребителями услуг сети "РадиоТел-ЦТ" являются банки, топливные компании, торгово-сервисные предприятия. При этом пользователи сети "РадиоТел-ЦТ" могут подключать и использовать: настольные и персональные компьютеры, кассовые аппараты, банкоматы, лотерейные терминалы, аппаратуру оповещения и ряд других устройств.

Для подключения терминального оборудования к сети "РадиоТел-ЦТ" используется устройство Radio PAD, которое имеет два асинхронных порта V24, что позволяет обеспечить два дуплексных канала связи. Скорость работы по порту: 9600 бит/сек - при использовании одного порта, 4800 бит/сек - при одновременном использовании двух портов. Взаимодействие терминального оборудования с устройством Radio PAD осуществляется по протоколу X.28. Скорость выполнения транзакции на POS-терминалах и банкоматах в сети "РадиоТел-ЦТ" составляет порядка 8 - 12 секунд

# 2. Технические средства.

## 2.1. Способы идентификации пластиковых карт.

Пластиковая карточка представляет собой пластину стандартных размеров (85.6 мм 53.9 мм 0.76 мм), изготовленную из специальной, устойчивой к механическим и термическим воздействиям, пластмассы.



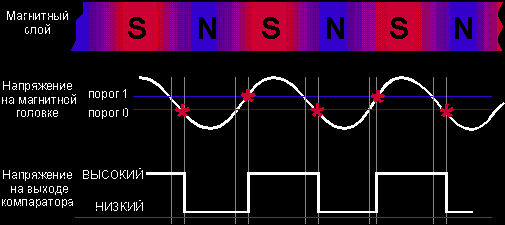
Одна из основных функций пластиковой карточки - обеспечение идентификации использующего ее лица как субъекта платежной системы. Для этого на пластиковую карточку наносятся логотипы банка-эмитента и платежной системы, обслуживающей карточку, имя держателя карточки, номер его счета, срок действия карточки и пр. Кроме этого, на карточке может присутствовать фотография держателя и его подпись. Алфавитно-цифровые данные - имя, номер счета и др. - могут быть эмбоссированы. Это дает возможность при ручной обработке принимаемых к оплате карточек быстро перенести данные на чек с помощью специального устройства, импринтера, осуществляющего "прокатывание" карточки (в точности так же, как получается второй экземпляр при использовании копировальной бумаги).

Графические данные обеспечивают возможность визуальной идентификации карточки. Карточки, обслуживание которых основано на таком принципе, могут с успехом использоваться в малых локальных системах - как клубные, магазинные карточки и т.п. Однако для использования в банковской платежной системе визуальной "обработки" оказывается явно недостаточно. Представляется целесообразным хранить данные на карточке в виде, обеспечивающем проведение процедуры автоматической авторизации. Эта задача может быть решена с использованием различных физических механизмов.

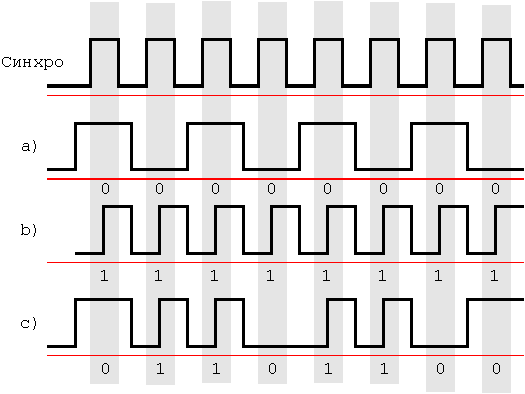
В карточках со штрих - кодом в качестве идентифицирующего элемента используется штриховой код, аналогичный коду, применяемому для маркировки товаров. Обычно кодовая полоска покрыта непрозрачным составом и считывание кода происходит в инфракрасных лучах. Карточки со штрих - кодом весьма дешевы и, по сравнению с другими типами карт, относительно просты в изготовлении. Последняя особенность обуславливает их слабую защищенность от подделки и делает поэтому малопригодными для использования в платежных системах.

Карточки с магнитной полосой являются на сегодняшний день наиболее распространенными - в обращении находится свыше двух миллиардов карт подобного типа. Магнитная полоса располагается на обратной стороне карты и, согласно стандарту ISO 7811, состоит из трех дорожек. Из них первые две предназначены для хранения идентификационных данных, а на третью можно записывать информацию (например, текущее значение лимита дебетовой карточки). Однако из-за невысокой надежности многократно повторяемого процесса записи/считывания, запись на магнитную полосу, как правило, не практикуется, и такие карты используются только в режиме считывания информации.

Как же устроена карта? Принцип магнитной записи на карту ничем не отличается от принятого в звукозаписи. Для его реализации подходит звуковая аппаратура. Стирание можно делать постоянным магнитом с пластиной - концентратором магнитного потока. Хотя при таком стирании велик уровень шумов, для цифрового считывания это не важно. Запись производят без подмагничивания постоянным или ВЧ-током, так даже достигаются более резкие переходы намагниченности носителя. Для изготовления магнитной полоски самодельных карточек подойдет старая 5" дискета на 360 Кб, имеющая слой с низкой коэрцитивностью. Кодирование данных осуществляется общепринятым методом "без возврата к нулю", который исключает длинные участки постоянной намагниченности, что облегчает синхронизацию при считывании.



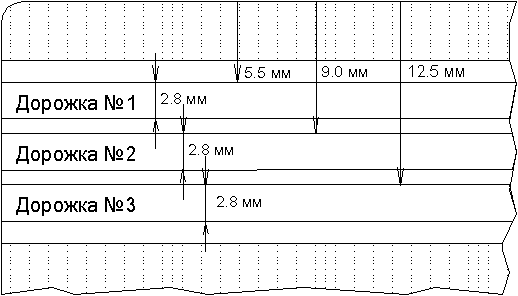
Усиленный выходной сигнал с читающей головки проходит двухпороговый компаратор, формирующий ВЫСОКИЙ и НИЗКИЙ логические уровни. Цифровые данные поступают на стандартный последовательный интерфейс (типа RS-232), передающий данные на обработку компьютеру.



На рис. видно, что если в момент синхро-отсчета уровень сигнала не меняется, то он считается равным нулю, а если сигнал имеет перепад, то единице. Типовое расположение дорожек на магнитной полосе банковской карточки показано на рисунке.

Физический стандарт записи.

Расположение дорожек на карточке показывает рисунок.



Если карточку расположить магнитной полоской к себе, так, чтобы полоска была снизу карточки, то данные записаны слева направо.

Защищенность карт с магнитной полосой существенно выше, чем у карт со штрих - кодом. Однако и такой тип карт относительно уязвим для мошенничества. Тем не менее, развитая инфраструктура существующих платежных систем и, в первую очередь, мировых лидеров "карточного" бизнеса - компаний MasterCard/Europay является причиной интенсивного использования карточек с магнитной полосой и сегодня. Отметим, что для повышения защищенности карточек системы VISA и MasterCard/Europay используются дополнительные графические средства защиты: голограммы и нестандартные шрифты для эмбоссирования.

На лицевой стороне карточки с магнитной полосой обычно указывается: логотип банка-эмитента, логотип платежной системы, номер карточки (первые 6 цифр - код банка, следующие 9 - банковский номер карточки, последняя цифра - контрольная, последние четыре цифры нанесены на голограмму), срок действия карточки, имя держателя карточки; на оборотной стороне - магнитная полоса, место для подписи.

## 2.2. Особенности устройства смарт-карты.

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 самих магнитных карт, следует обратить внимание на стоимость всей системы, включая аренду каналов, связное оборудование и т. д.

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.

Есть все основания предполагать, что работы по усовершенствованию и продвижению проектов смарт-карт в банковские технологии Украины будут интенсифицироваться. Наблюдаемое в настоящий момент дальнейшее снижение цен на карты и периферию приводит к снижению себестоимости проектов, основанных на смарт-картах, а следовательно, к еще более заметному росту популярности смарт-технологий и дальнейшему расширению сфер их применения.

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.

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 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, ничуть не интересуясь тем, какая информация хранится на карте (т. е. шифрование данных в памяти карты от мошенничества подобного рода не спасает).

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. Так, цена карты GPM896 составляет не более 4 $ для тиражей выше 5 тыс. экземпляров.

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. 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.

Преимущества использования смарт-карт Главное отличие смарт-карт от других видов пластиковых карт - интеллектуальность карт с микросхемами.

При платежах по магнитным 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.

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.

Во время производства и инициализации карт электронные предохранители в микросхеме могут быть разрушены, тем самым предотвращая нежелательное вмешательство в хранимую информацию.

Копирование данных, кроме как их производителями, невозможно благодаря уникальному внутреннему коду, записанному на каждой карте. Даже если данные, записанные на карту, кто-либо сможет продублировать, уникальный внутренний код предотвратит использование карты. При отправке карт производителем в адрес организации, выпускающей карты в обращение, коды посылаются отдельно, так что даже в случае потери всей партии карты останутся непригодными для использования. Пока этот код не будет представлен карте, последнюю использовать невозможно. Как только карта проинициализирована и в ней записаны данные (или сумма денег), доступ к ним защищается кодированным паролем (или PIN-КОДОМ), известным только хозяину карты. Данные, записанные на карте, могут быть также зашифрованы. Все это делает смарт-карту одной из наиболее надежных форм хранения данных.

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.

# 3.Применение криптографии для карт с магнитной полосой

В то время как вводятся другие, более защищенные методы шифрования, магнитная карта намного дешевле чем другие альтернативы и карты с магнитной полосой – самый распространенный тип карт. Методы защиты магнитных карт медленно, но верно улучшаются, и при правильном применении могут предоставить отличную защиту для финансовых транзакций при низкой стоимости.

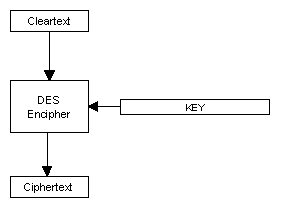
Самое распространенное использование криптографии это обеспечение ПИНа, для использования магнитной карты в местах, где нельзя осуществить контроль за правомерностью доступа , например в ATM (банкоматах), либо в каких-то других ситуациях, где осуществить предоставление обычной бумажной подписи невозможно. Все это распространяется на кредитные, дебитные и ATM-карты. На сегодняшний день не так много денежных карт, у которых не было бы наличия ПИН.

Второе по распространенности использование криптографии это предоставление механизмов контроля за оригинальностью магнитной ленты . Назначение заключается в предупреждении создания карт мошенническим путем , когда на ленту записывается значение, которое не может быть получено из видимой информации, содержащейся на карте. Когда карта проверяется в режиме on-line, это значение может быть проверено для того чтобы подтвердить подлинность карты. Для этого существует несколько различных стандартов, самые используемые это Visa Card Verification Value (CVV) или, аналог для Мастеркарда, CVC.

Другие варианты использования криптографии напрямую не относятся к картам, обычно они относятся к шифрованию ПИН и сообщениям, передаваемым в финансовом окружении, чтобы предотвратить их перехват или подделку.

## 3.1. Простое шифрование.

Большинство шифрований магнитных карт базируется на Алгоритме Шифрования Данных (DEA), называемым DES или Стандарт Шифрования Данных. Идея лежащая в этом алгоритме заключается в том что оригинальное (нешифрованное) значение, передается алгоритму DES, который может быть выпонен как в программном, так и в аппаратном виде. Затем DES шифрует чистое значение, используя ключ (секретный, 64-битный), и на выходе выдает зашифрованное значение.



Примем во внимание следующее:

- Алгоритм DES не является секретным. Он доступен для широкого использования. Однако КЛЮЧ является секретным.

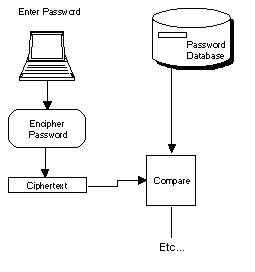
- Этот процесс является реверсивным. Функцию DES «decipher» , используя тот же самый ключ, переработает шифрованную информацию в открытую (оригинальную).

Безопасность и целостность всего процесса шифрации зависит от секретности используемого ключа. Ключ это случайное значение, которое очень жестко защищено. Большинство сложностей, связанных с шифровальными системами DES связаны с защитой, хранением и передачей ключей, и эти действия называются “key management” – операции с ключами.

Также нужно заметить что операция шифрования “encipher” , как описано выше не совсем надежна. Теоретически, большое количество параллельных процессов могут подобрать ключ в несколько дней. Эта особенность активно обсуждается в дискуссиях на тему улучшения безопасности, однако дополнительные методы могут ограничить применение данного алгоритма.

Простой пример для демонстрации: пароли на входе компьютерных систем.

Пароли, использующиеся в компьютерных системах часто шифруются, после того как они были установлены, и хранятся в файле в зашифрованном виде. Когда пользователь входит в систему, пароль вводится в скрытом поле, чистым текстом. Важно понимать, что это значение не сравнивается со значением, которое расшифровывается из файла пароля. Чистый текст зашифровывается тем же ключом и сравнивается с шифрованным значением, которое находится в файле паролей. Чистый текст, зашифрованный аналогичным ключом, всегда даст тот же самый результат и практически все криптографические системы сравнивают зашифрованный текст с зашифрованным, чтобы избежать доступа к чистым значениям в компьютерных системах, поскольку те могут быть скомпрометированы дампом памяти, взломом и т.д.



Однако в этой ситуации пользователь пароля всегда может предъявить претензию, что его пароль может быть раскрыт расшифровыванием зашифрованного значения, и это неподвластно пользователю – это правда.

## 3.2.Обмен динамическим ключом.

Много финансовых систем внедряют обмен динамическим ключом. В то время как это напрямую не относится к магнитным картам, это достаточно актуально, для того чтобы обратить на это внимание.

В обмене динамическим ключом 2 стороны обмениваются ключами «на лету» для того чтобы один ключ не использовался продолжительное время ввиду риска его расшифровки. Обычно это используется в финансовом окружении, когда две стороны обмениваются финансовыми авторизационными (подтверждающими) сообщениями – например банк получателя и банк отправителя. Когда банк получателя передает ПИН банку отправителя для подтверждения, это сообщение должно быть зашифрованным. Банку отправителя будет нужен доступ к ключу, которым шифровался ПИН, чтобы расшифровать сообщение при получении. Стороны предварительно договорились об этих ключах и ключи могут быть изменены путем динамического обмена ключей, когда ключи предоставляются (зашифрованные старыми шифровальными ключами) и меняются в реальном времени для дополнительной безопасности.

## 3.3. Обработка ПИН.

Принцип ПИН основан на том факте, что никто кроме легального владельца карты его не знает. Поэтому, когда ПИН предоставляется клиенту:

- ПИН не должен хранится нигде в открытом виде

- ПИН не должен быть реверсирован на основании информации на магнитной ленте

или базы данных.

Обычно, ПИН это 4-значное число.

Когда выпускается ПИН, очередность событий такова:

- Генерируется 4-значное число - это ПИН;

- ПИН комбинируется с другой информацией, например с номером счета, чтобы создать блок данных для процесса шифрования;

- Входной блок трижды шифруется, использую рабочие ключи ПИН;

- Выбираются цифры из зашифрованного результата. Они становится Pin Verification Value (Число Проверки ПИН) или Pin Offset (Смещение ПИН);

- Смещение ПИН сохраняется;

- Печатается конверт с ПИН;

- Память очищается нулями, чтобы скрыть все следы присутствия чистого ПИН.

На этом этапе единственное место где находится значение ПИН это конверт. ПИН не может быть получен на основании смещения ПИН.

Когда карта используется и вводится ПИН, смещение ПИН вычисляется на основании введенного ПИН, используя рабочие ключи ПИН, и сравнивается с сохраненным смещением ПИН, чтобы определить правильность ввода ПИН. Это означает, что когда ПИН проверяется, проверяющей системе нужен доступ к рабочим ключам ПИН, используемого при формировке ПИН или его изменения.

Еще раз нужно подчеркнуть, что смещение включает в себя цифры, выбранные из шифрованных данных. Обычно это 4-6 цифр. Невозможно воссоздать ключи или ПИН используя это значение.

## 3.4. Обработка VCC.

Быстро стало понятно что распространение денежных карт привело к риску финансовых институтов со стороны мошенников. В мире кредитных карт это к производству карт с или без магнитной полосы, подделывая имена и логотипы. На арене ATM карт, злоумышленники наблюдали за вводом ПИН «через плечо», сопоставляли ПИНы с информацией на квитанциях и создавали свои магнитные ленты на болванках для карт.

Эти и другие угрозы подвели к введению Card Verification Value, невозможной для получения последовательности цифр, создаваемой процессом шифровки и записанной на магнитную ленту карты. Это означает что электронный сбор информации о транзакциях (ATM или POS) эффективно защищен от мошенников.

Комбинация статичных данных как, например, номер счета трижды шифруется, используя специальную пару ключей Card Verification. Выбранные из результата цифры используются для создания CVV и пишутся на магнитную ленту.

К CVV относится все то же самое, что и к Pin Offset. Т.к. CVV состоит из нескольких цифр, и используется тройная шифрация, ключи CVV и значения хорошо защищены и наличие CVV дает дополнительный уровень подтверждения что карта не является поддельной.

Нужно заметить что CVV просто дополнительный метод защиты, он так же не 100%-но надежен. Он, например не защищает от мошеннического сбора информации с магнитных карт, например на фальшивых ATM (банкоматах).

Дальнейшее развитие CVV, CVV2, используется для авторизации по телефону. Приблизительно такая же схема расчетов как и для CVV, выбранные из результата цифры печатаются на обороте карты. Эти цифры могут быть запрошены, чтобы подтвердить правомерность сделки. Опять же, это всего лишь дополнительная проверка.

## 3.5.Работа с ключами.

Работа с ключами подразумевает собой хранение, защиту и передачу ключей. В одной финансовой организации может быть множество DES ключей, и они требуют должного обращения. Одно из самых худших случаев отладка компьютерных ошибок – это отладка программ связанных с шифрованием данных, так как дампы памяти не несут никакого смысла, и может быть очень сложно обнаружить, что используется неверный шифровальный ключ.

В хороших системах рабочие ключи никогда не хранятся в незашифрованном формате. Даже когда они создаются, часто это происходит автоматически, так что ключи никогда не известны людям.

Когда создаются инициализационные ключи, 64 бита делятся между двумя или более людьми, которые «бросают монетку» для каждого бита. Так как каждый работает с одним из сегментов ключа, целый ключ неизвестен никому, так обычно делается изначальное создание мастер-ключа.

Несмотря на простую концепцию, управление ключами может стать довольно сложным на практике.

В простой ATM сети например, мастер-ключ терминала используется для шифровки рабочих ключей при передаче. Мастер-ключ терминала (МКТ) генерируется для каждого терминала, делится на 2 части и печатается (или иногда шифруется на специальной магнитной карте). Каждый ТМК затем инсталлируется в банкомат.

Система затем закачает рабочие ключи терминала, зашифрованные мастер ключом терминалов на каждый банкомат. Затем рабочие ключи терминала используется для шифрации данных ПИН при передаче хосту во время процессинга. Если потребуется, рабочий ключ терминала может быть изменен через некоторые интервалы, либо динамически, однако этот процесс требует особой внимательности и подхода

Нужно заметить, что обмен ключами – это самое слабое место DES систем, поэтому нужно особенно тщательно продумывать систему управления ключами.

## 3.6.Физическое приложение.

Зашифрованный процессинг и управление ключами обычно проводится на специализированном защищенном оборудовании. DES может быть встроен и в программное обеспечение (используя такие продукты как например IBM’s PCF), но это менее безопасно, к тому же алгоритм DES может усиленно использовать ресурсы процессора.

Есть компании, специализирующиеся на выделенных шифровальных объектах, как например Racal и Atalla. Обычно они называются HSM (Защищенный Модуль Хоста), однако Racal решает как назвать объект.

Используя эти устройства, вся шифровка/дешифровка происходит в закрытом устройстве, и ключи в чистом виде никогда его не покидают.

Физически HSM защищены от вскрытия и обычно устанавливаются в защищенных компьютерных отделах. Попытки открыть их приведут к уничтожению ключей находящихся в устройстве.

Некоторые приложение используют физическую телекоммуникационную линию для дополнительной безопасности, и есть много поставщиков устройств такого типа. Они представляют собой «черный ящик» и не требуют специальных знаний.

**Пример.**

**Шифрование при выдаче денег в банкомате.**

Обычная АТМ - транзакция

- Клиент вводит карту в банкомат;

- Клиент вводит свой ПИН;

- Клиент запрашивает наличные;

- Транзакция подтверждена, наличные выданы.

В этот процесс вовлечено очень много шифровок.

1. Клиент вводит карту в банкомат

*Магнитная лента читается и сохраняется в буфере банкомата.*

2. Клиент вводит свой ПИН

*ПИН вводится в защищенный от изменения пад. Сохраненный ПИН заносится в защитный аппаратный модуль.*

3. Клиент запрашивает наличные

*Сообщение создается в ATM. ПИН шифруется ключом Терминала.*

*Сообщение посылается хосту, зашифрованное аппаратно.*

*По получении хостом, аппаратное сообщение дешифруется. Вычисляется CVV и сравнивается со значением на магнитной ленте. ПИН, зашифрованный ключом Терминала дешифрируется. Вычисляется смещение ПИН или PVV. PVV сравнивается с записью в базе данных PVV.*

4. Транзакция подтверждена, наличные выданы

Замечание: все функции шифрования хоста обычно происходят в Защищенном модуле. Никакие значения в чистом виде не передаются прикладным программам или вне защищенного окружения.

## 3.7. Другие приложения шифрования в финансах.

Так же как и обычные использования шифрования, межбанковские сети (например SWIFT) исторически были активными пользователями шифровальных техник.

Множество новых способов доставки и еще более широкое распространение прогрессивных технологий увеличило интерес и использование шифрования.

В случаях когда криптография требуется для широкого распространения среди общества (например домашний банкинг с помощью PC), обычный DES слишком сложен для безопасного управления. В такие системы внедрены более подходящие и безопасные алгоритмы , такие как RSA (система шифрования с открытым ключом).

Некоторые корпоративные приложения используют хорошо защищенный DES, комбинируя с другими алгоритмами – MAC(Код Аутентификации Сообщения, Размер MAC определен в ISO8583 как 16 байт.), физическое шифрование, обмен динамическим ключом и т.д.

# 4. Устройства обслуживания электронных платежей.

## 4.1. Использование POS-терминалов.

POS-терминалы, или торговые терминалы, предназначены для обработки транзакций при финансовых расчетах с использованием пластиковых карточек с магнитной полосой и смарт-карт. Использование POS-терминалов позволяет автоматизировать операции по обслуживанию карточки и существенно уменьшить время обслуживания. Возможности и комплектация POS-терминалов варьируются в широких пределах, однако типичный современный терминал снабжен устройствами чтения как смарт-карт, так и карт с магнитной полосой, энергонезависимой памятью, портами для подключения ПИН - клавиатуры (клавиатуры для набора ПИН - кода), принтера, соединения с ПК или с электронным кассовым аппаратом.

Кроме того, обычно POS-терминал бывает оснащен модемом с возможностью автодозвона. POS-терминал обладает "интеллектуальными" возможностями - его можно программировать. В качестве языков программирования используются ассемблер, а также диалекты C и Basic'а. Все это позволяет проводить не только on-line авторизацию карт с магнитной полосой и смарт-карт, но и использовать при работе со смарт-картами режим off-line с накоплением протоколов транзакций. Последние во время сеансов связи передаются в процессинговый центр. Во время сеанса связи POS-терминал может также принимать и запоминать информацию, передаваемую ЭВМ процессингового центра. В основном это бывают стоп - листы, но подобным же образом может осуществляться и перепрограммирование POS-терминалов.

Стоимость POS-терминалов в зависимости от комплектации, возможностей, фирмы-производителя может меняться от нескольких сотен до нескольких тысяч долларов, однако обычно не превышает полутора - двух тысяч. Размеры и вес POS-терминала сопоставимы с аналогичными параметрами телефонного аппарата, а зачастую бывают и меньше.

Основные характеристики POS-терминалов:

- занимает мало места на прилавке благодаря компактному и интеграционному дизайну;

- принимает все основные типы кредитных, дебетных и локально-корпоративных карт;

- благодаря наличию удобного встроенного рулонного принтера быстро печатает чеки и отчеты;

- расширяет ваши возможности по работе с большими аппликациями, сохраняет большие файлы данных и транзакций.



##### Платежный терминал TRANZ 460

Производитель: VeriFone

64 КB‚ EPROM-памяти и 256KB‚ 512 КB‚ или 1 МB‚ оперативной RAM-памяти, поддерживаемой резервными батареями

скорость передачи данных 300, 1200 или 2400 бод с протоколами: CCITT V.21/V.22/V.22 bis

16-ти символьный флуоресцирующий дисплей, включая десятичную точку и запятую

двухдорожечный считыватель магнитных карт

матричный рулонный принтер, 24 колонки серийный коммуникационный порт RS-232 для прямого соединения с персональным компьютером, электронным кассовым аппаратом или внешним принтером скорость обмена данными для работы с PIN PAD-ом, считыватель смарт-карт или считывателем штрих-кодов до 9600 бод

**Платежный терминал TMS**

Производитель Bull (Франция)



16-разрядный микропроцессор NEC V25

считыватель смарт-карт (ISO-7816) + считыватель магнитной полосы (ISO 1/2)

128 Кб RAM, 512 Кб Flash память

RS232 + RS232 I/O

Dallas Security module

клавиатура (24 клавиши)

графический дисплей (2\*16 символов)

встроенный принтер (48 символов на строке, скорость 1 линия/сек)

источник питания 220v/50Hz

## 4.2. Использование банкоматов.

Банкоматы - банковские автоматы для выдачи и инкассирования наличных денег при операциях с пластиковыми карточками. Кроме этого, банкомат позволяет держателю карточки получать информацию о текущем состоянии счета, проводить операции по перечислению средств с одного счета на другой. Банкомат снабжен устройством для чтения карты, а для интерактивного взаимодействия с держателем карточки - также дисплеем и клавиатурой. Банкомат оснащен персональной ЭВМ, которая обеспечивает управление банкоматом и контроль его состояния. Последнее весьма важно, поскольку банкомат является хранилищем наличных денег. На сегодняшний день большинство моделей рассчитано на работу в on-line режиме с карточками с магнитной полосой, однако появились и устройства, способные работать со смарт-картами и в off-line режиме. Для обеспечения коммуникационных функций банкоматы оснащаются платами X.25.

Денежные купюры в банкомате размещаются в кассетах, которые, в свою очередь, находятся в специальном сейфе. Число кассет определяет количество номиналов купюр, выдаваемых банкоматом. Размеры кассет регулируются, что дает возможность заряжать банкомат практически любыми купюрами. Банкоматы могут размещаться как в помещениях, так и непосредственно на улице и работать круглосуточно.

Пример банкомата, а также его технические характеристики:



**Банкомат Diebold 1064ix (внутренний)**

**Основные характеристики:**

Предназначен для выдачи наличных денег, обработки запросов о состоянии счетов, перевод денег с одного счета на другой и распечатки мини-выписок.

Среднее время эксплуатации - 15 лет

Высокая надёжность

Возможность выдачи в одной пачке до 50 купюр

Большая ёмкость кассет (до 3000 купюр)

Монитор 15" (разрешение 640х480х256 цветов)

Процессор Pentium 166, память 16 Мб.

Бесшумный чековый термопринтер 2 или 4 кассеты для загрузки купюр.  
Высота 1360мм

Ширина 470мм

Длина 835мм

Вес 488кг

ПАРАМЕТРЫ ОКРУЖАЮЩЕЙ СРЕДЫ

Рабочая температура от 10° до 38° C

Рабочая влажность 20-80%, без конденсации

# 5. Стандарты электронных расчетов.

## 5.1. Стандарт SET.

Аббревиатура SET расшифровывается как Secure Electronic Transactions - безопасные (или защищенные) электронные транзакции. Стандарт SET, совместно разработанный компаниями Visa и MasterCard, обещает увеличить объем продаж по кредитным карточкам через Internet. Совокупное количество потенциальных покупателей - держателей карточек Visa и MasterCard по всему миру - превышает 700 миллионов человек. Обеспечение безопасности электронных транзакций для такого числа покупателей могло бы привести к заметным изменениям, выражающимся в уменьшении себестоимости транзакции для банков и процессинговых компаний. К этому следует добавить, что и American Express объявила о намерении приступить к внедрению стандарта SET.

Для того чтобы совершить транзакцию в соответствии со стандартом SET, обе участвующие в сделке стороны - покупатель и торгующая организация (поставщик) - должны иметь счета в банке (или другой финансовой организации), использующем стандарт SET, а также располагать совместимым с SET программным обеспечением. В таком качестве могут, например, выступать Web-броузер для покупателя и Web-сервер для продавца - оба, очевидно, с поддержкой SET.

## 5.2. Концепция Cyber Cash.

Компания CyberCash, расположенная в г. Рестон (штат Вирджиния, США) была пионером в разработке многих концепций, использованных в стандарте SET, и приняла на себя обязательство одной из первых внедрить SET. Множество покупателей и торговых организаций по всему миру используют систему SIPS (simple Internet payment system) производства CyberCash. Есть стимул для использования программного обеспечения CyberCash: в дополнение к повышенной безопасности программное обеспечение поставляется свободно (т.е. бесплатно) как покупателям, так и продавцам. Плата за использование системы CyberCash включается в оплату за обслуживание кредитных карточек.

## 5.3. Платежи без кодирования - система First Virtual.

Учитывая проблемы, возникающие в связи с необходимостью пересылки номеров кредитных карточек через Internet: необходимость кодирования и обеспечения гарантий от расшифровки третьими лицами, можно сформулировать альтернативный подход. Он состоит в полном отказе от пересылки информации, относящейся к кредитным карточкам, через Internet. Компания First Virtual (США) разработала систему, используя которую, покупатель никогда не вводит номер своей кредитной карточки. В дополнение к платежной системе First Virtual поддерживает собственную систему электронной почты, называемой InfoHaus. Это связано с тем, что основными видами товаров в First Virtual являются программное обеспечение и информация, на поддержку которых и ориентирована система электронной почты.

## 5.4. Система Digital Cash.

Digital Cash, использующая цифровые или электронные наличные (деньги) - наиболее радикальная форма электронной коммерции. Видимо, поэтому ее распространение осуществляется достаточно медленно. Рассмотренные выше системы традиционны в принципиальном плане - обычные денежные транзакции реализованы в них в электронном Internet-варианте. В то же время электронные наличные - новый тип денег. Они потенциально могут привести к радикальным изменениям в денежном обращении и его регулировании.

# 6. Выводы

Можно сказать, что сейчас в мире идет процесс поиска новых типов платежных систем, которые максимально удовлетворяли бы все стороны участвующие в денежном обращении. Очень сильно этот процесс связан с развитием всемирной компьютерной сети Internet, так как развитие Internet приводит как к появлению огромного количества дополнительных возможностей, так и к появлению огромного количества новых проблем. Можно с уверенностью сказать, что в ближайшие годы какая-нибудь из появляющихся сейчас систем платежа займет прочное место в нашей жизни. Сейчас практически невозможно определить, что это будет конкретно, но по всей видимости тенденция это совершенствование цифровых денег, действие которых, на данный момент распространяется только в пределах глобальной коммерческой сети Интернет, оформление их правовой базы и вынос их за ее пределы. По всей видимости, основой для выноса цифровых денег за пределы Интернет станут электронные кошельки, которые сейчас выпускает Mondex. Однако возможно, что в ближайшие годы будет изобретено нечто принципиально новое, что сразу вытеснит с рынка все остальные средства денежного обращения. Одно является очевидным, общая тенденция в любом случая заключена в сокращении оборота наличных денег во всем мире, и ставка делается на на многофункциональность карточки.

Наряду с очевидными преимуществами карточки 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.