**Безопасность персональных платежей физических лиц**

Выделяют три вида персональных платежей:

- домашнее (телефонное) обслуживание,

- расчет с автоматическим кассовым аппаратом (банкоматом),

- расчет в точке продажи.

В настоящее время появился четвертый вид — финансовый сервис с использованием всемирной сети Интернет.

Домашнее банковское обслуживание позволяет клиентам получить доступ к банковским и информационным услугам не выходя из дома.

Достоинства этого вида обслуживания:

- для клиента - большая доступность данных и управление своими финансовыми делами;

- для банка - уменьшение стоимости обслуживания.

Ввод данных для платежа при голосовой связи (идентификатор, номер счета, размер платежа) производится клиентом либо с клавиатуры телефона либо голосом (что менее надежно с точки зрения безопасности, но более технически доступно).

Системы домашнего (телефонного) обслуживания начали внедряться банками с начала 80-годов, однако, до настоящего времени широкого распространения не получили.

Этот вид обслуживания в разных странах находится на различном уровне. Например, в США домашнее обслуживание не приняло больших масштабов в то время как во Франции около 3.5 млн. домов подключено к сети MiniTel.

Некоторое распространение получило телефонное обслуживание и в Великобритании. Основным банком, обеспечивающим эти услуги является там Trustee Savings Banks. Его система SpeedLink в настоящее время обслуживает более 250.000 клиентов, не имеющих специального оборудования, за исключением современного телефона. [12]

Для получения доступа к услугам SpeedLink клиенту необходимо соединиться с ним и назвать свой номер счета и свой идентификатор (PIN SpeedLine) для подтверждения личности. После установления связи клиенты SpeedLink могут получить уведомление на факс-аппарат или по почте (если факс отсутствует). Система предоставляет также такие услуги как оплата счетов, передача денег, ознакомление с последними шестью транзакциями, перевод денег. Соотношение персональных и корпоративных клиентов этой системы находится в отношении 2:1.

First Direct - полная система телефонного обслуживания клиентов на дому. Она введена в действие Midland Bank Group в 1989 году.

Основное ее отличие в том, что она не использует синтезируемый голос или персональный компьютер для проведения расчетов.

Проведенные после установки First Direct исследования показали, что 30% населения посещают банки для того, чтобы использовать банкоматы, а 30% пользуются телефоном.

В системе First Direct особое внимание уделяется начальной идентификации и проверке абонента. Для идентификации используется десятисимвольный пароль, устанавливаемый клиентом и известный только ему. Проверка абонента осуществляется при взаимодействии с оператором. В начале работы оператор запрашивает наугад одну или несколько букв из пароля пользователя. Дополнительно клиент снабжается кодовым словом, которое используется при этой процедуре. Детали процедуры идентификации и аутентификации системы First Direct держатся в секрете.

Будущее этого вида услуг сильно зависит от прогресса в области распознавания речи и создания надежных и сравнительно недорогих устройств с приемлемыми характеристиками такого распознавания. [12]

Банковский автомат-кассир (АКА, банкомат) - специализированное устройство, предназначенное для обслуживания клиента в отсутствие банковского персонала. Это наиболее существенная часть банковской системы, предназначенная, в основном, для выдачи наличных денег. Помимо этой функции АКА может выполнять ряд дополнительных, а числе которых:

\* проверка состояния счета клиента;

\* изменение параметров счета клиента;

\* осуществление различных платежей;

\* предоставление информации о:

- страховом полисе клиента;

- котировках ценных бумаг на фондовом рынке;

- покупке и продаже акций;

- обменных курсах валют и т.д.

Автоматический кассовый аппарат состоит из трех устройств ввода (считыватель с пластиковых карточек, цифровая и функциональная клавиатура), двух выходных устройств (микродисплей и принтер) и устройства обработки информации. Взаимодействие клиента с АКА осуществляется при помощи пластиковой карточки, на которой записана необходимая информация, выносной клавиатуры и микродисплея.

В настоящее время устройства обработки информации АКА разрабатываются на основе микропроцессоров. Так, например основой АКА компании NCR являются процессоры Intel 80486 и Pentium. Фактически АКА компании NCR представляет собой персональную ЭВМ, работающую под управлением ОС OS/2 и имеющую до 64 Мбайт оперативной памяти, до 3200 Мбайт дисковой памяти, накопитель на гибких магнитных дисках, дисплей, принтер и другие периферийные устройства. Выполнение операций осуществляется с помощью прикладного программного обеспечения. Шифрование конфиденциальной информации при передаче по каналам связи или при записи на диск осуществляется на основе стандарта DES. Кроме крипто-защиты предусмотрены и другие меры безопасности.

В 90-х годах по данным Американской Ассоциации Банкиров в США услуги АКА использовались половиной национальных банков и всеми крупными банками. [2, с.377].

Системы, обеспечивающие расчеты продавца и покупателя в точке продажи, (point-of-sale, POS) получили распространение в США более 25 лет назад. В основном, все терминалы, подключенные к этим системам размещены на предприятиях торговли. Большинство таких терминалов установлены в супермаркетах, так как там совершается большое количество покупок в течении дня, а также в других магазинах и на автозаправочных станциях.

Системы POS обеспечивают следующие услуги:

- проверку и подтверждение чеков;

- проверку и обслуживание дебетовых и кредитных карточек;

- использование системы электронных расчетов.

Банки, финансирующие систему расчетов в точке продажи, таким образом расширяют список своих клиентов путем предоставления им больших удобств для покупок в магазинах с использованием удаленных устройств. Торговля, в свою очередь, увеличивает количество клиентов, расширяет управление имуществом, сохраняет время клиентов и уменьшает риск потери наличных денег.

Существует два типа систем POS. Основной из них предполагает, что продавец и покупатель имеют счета в одном и том же банке. Данные, необходимые для платежа, передаются через терминалы системы POS банковскому компьютеру, производится платеж и деньги переводятся со счета покупателя на счет продавца. В более сложной системе участвуют два или более банков. При платеже сначала вызывается банк покупателя, производится платеж и записывается на магнитную ленту для передачи в расчетную палату. Расчетная палата в свою очередь пересылает данные о платеже в банк продавца, который кредитует платеж.

***Проблемы идентификации клиента при удаленном обслуживании.***

Персональный номер (идентификатор) (Personal Identification Number, PIN) - это последовательность цифр, используемая для идентификации клиента. Для ввода PIN как в АКА, так и в терминалах систем POS предусмотрена цифровая клавиатура, аналогичная телефонной. По способу назначения можно выделить следующие типы PIN:

- назначаемые выведенные PIN;

- назначаемые случайные PIN;

- PIN, выбираемые пользователем.

Клиент различает только два типа PIN: PIN, который назначен ему банком, выдавшим карточку, и PIN, который пользователь может выбирать себе самостоятельно.

В связи с тем, что PIN предназначен для идентификации и аутентификации клиента, его значение должно быть известно только клиенту. Однако на практике PIN трудно удержать в памяти и поэтому клиент банка куда-нибудь его запишет (иногда - на саму карточку). В результате задача злоумышленника бывает сильно облегчена.

Использование PIN, назначенных банком, неудобно даже при небольшом их количестве. Много цифр не удержишь в памяти и их придется записывать. Для большего удобства клиента используются PIN, выбираемые им самим. Такой способ определения PIN, во-первых, позволяет клиенту использовать один и тот же PIN для различных целей, и, во-вторых, позволяет задавать PIN как совокупность букв и цифр.

PIN обычно состоит из 4-6 цифр. Следовательно, для его перебора в наихудшем (для защиты естественно) случае необходимо осуществить 10.000 комбинаций (4-х символьный PIN). Такой перебор возможен за короткое время. Поэтому в системах, использующих такой PIN , должны быть предусмотрены меры защиты от подбора PIN.

Всего существуют два основных способа проверки PIN: алгоритмический и неалгоритмический.

Алгоритмический способ проверки заключается в том, что у пользователя запрашивается PIN, который преобразуется по определенному алгоритму с использованием секретного ключа и затем сравнивается со значением PIN, хранившемся на карточке. Достоинством этого метода проверки является:

- отсутствие копии PIN на главном компьютере, что исключает его раскрытие персоналом банка;

- отсутствие передачи PIN между АКА и главным компьютером банка, что исключает его перехват злоумышленником или навязывание результатов сравнения;

- облегчение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

Неалгоритмический способ проверки PIN, как это следует из его названия, не требует применения специальных алгоритмов. Проверка PIN осуществляется путем прямого сравнения полученного PIN со значениями, хранимыми в базе данных. Часто сама база данных со значениями PIN шифруется прозрачным образом, чтобы не затруднять процесс сравнения, но повысить ее защищенность.

Как же происходит генерация PIN? Вначале номер счета клиента дополняется нулями или другой константой до 16 шестнадцатеричных цифр (8 байт). Затем получившиеся 8 байт шифруются с использованием секретного ключа. Из получившегося шифртекста (8 байт), начиная с младших байт выделяются по 4 бита. Если значение числа, образуемого этими битами менее 10, то полученная цифра включается в PIN, иначе значение отбрасывается. Таким образом обрабатываются все 8 байт (64 бита). Если в результате обработки не удалось получить требуемое количество десятичных цифр, то из неиспользуемых комбинаций вычитается 10.

В том случае, когда необходимо получить выбираемый пользователем PIN, то каждая его цифра складывается по модулю 10 с соответствующей цифрой выведенного PIN (без учета переноса). Получаемое десятичное число называется «смещением» и запоминается на карточке. Так как выводимый PIN имеет случайное значение, то невозможно получить выбранный пользователем PIN по его «смещению».

В настоящее время ведется большая дискуссия по поводу применения PIN для идентификации клиентов [12]. Сторонники применения утверждают, что вскрытие PIN в Великобритании, например, составило несколько случаев в месяц против несколько сотен миллионов проведенных транзакций в год. Противники же доказывают, что идентификация клиента с использованием PIN работает только в следующих случаях:

- отсутствует перехват карточки и/или PIN при передаче от банка клиенту;

- банковские карточки не воруют, не теряют и их невозможно подделать;

- PIN невозможно узнать при доступе к системе другим пользователем;

- PIN иным образом не может быть скомпрометирован;

- в электронной системе банка отсутствуют сбои и ошибки;

- в самом банке нет мошенников.

В качестве альтернативы PIN предлагается применять устройства идентификации, основанные на биометрическом принципе. Их широкое применение сдерживается высокой стоимостью. Например, устройство, предлагаемое компанией Sats и предназначенное для идентификации человека по геометрии его руки, стоит около $3.500. [12]

Однако в настоящее время к биометрическим системам проявляется все больше интереса.

***Безопасность при использовании пластиковых карт.***

Использование систем POS и АКА потребовало появления некоторого носителя информации, который мог бы идентифицировать пользователя и хранить некоторые учетные данные. В качестве такого носителя стали выступать пластиковые карточки.

В настоящее время выпущено более миллиарда карточек в различных странах мира [5, с.26]. Наиболее известные из них:

- кредитные карточки Visa (более 350 млн. карточек) и MasterCard (200 млн. карточек);

- международные чековые гарантии Eurocheque и Posteheque;

- карточки для оплаты путешествий и развлечений American Express (60 млн. карточек) и Diners Club.

По принципу действия можно выделить пассивные и активные пластиковые карточки. Пассивные всего лишь хранят информацию на том или ином носителе. Отличительной особенностью активных карточек является наличие встроенной в него микросхемы. Карточка с микропроцессором называется «интеллектуальной» (smart card).

По характеру расчетов, проводимых с использованием пластиковых карточек, можно выделить кредитные и дебетовые карточки.

По характеру использования карточки подразделяются на корпоративные и личные. Главное отличие корпоративных (которые могут быть выданы только юридическим лицам) от индивидуальных состоит в том, что их владельцы имеют право на получение дополнительных услуг.

Например, такими карточками может одновременно пользоваться большое количество сотрудников фирмы, но счета по совершенным ими сделкам будут выставлены фирме.

На магнитной карточке расположена магнитная полоса, состоящая из трех дорожек. Каждая из них имеет соответствующее назначение. Размеры карточки, формат хранимых данных определены специальным стандартом ISO 7811 1985 года.

Процессорный тип карточек изобретен и запатентован Роланом Мореном во Франции. Микросхемы, установленные на карточке, могут быть как обычными - энергонезависимой памяти, так и достаточно сложными микропроцессорами. Емкость обычной карточки с энергонезависимой памятью составляет от 2 до 16 килобайт. В постоянное запоминающее устройство, установленное на карточке, прошивается специальный набор программ. Иначе говоря, сердцем таких карточек является не просто микропроцессор, а микроЭВМ. Эти карточки обеспечивают обширный набор функций:

- возможность работы с защищенной файловой системой (доступ к файлам требует предъявления полномочий почтению/записи информации);

- шифрование данных с применением различных алгоритмов;

- ведение ключевой системы и т.д.

Некоторые карточки обеспечивают режим «самоблокировки» (невозможность дальнейшей работы с ней) при попытке несанкционированного доступа.

Преимуществом интеллектуальных карточек является больший объем хранимой информации, устойчивость к подделке и возможность использования во многих приложениях.

Интеллектуальные карточки позволяют существенно упростить процедуру идентификации клиента. Это позволяет оказаться от работы АКА в режиме реального времени и централизованной проверки PIN. Для проверки PIN применяется алгоритм, реализуемый микропроцессором на карточке. Физическая защита интеллектуальной карты позволяет гарантировать корректность результата проверки PIN.

В то же время интеллектуальные карточки обладают и существенными недостатками которые обусловили их ограниченное распространение. Основных недостатков два:

- высокая стоимость производства карточки;

- увеличенная по сравнению со стандартом толщина, из-за чего она не может быть прочитана обыкновенным АКА. Для чтения таких карточек необходима установка специальных считывателей.

Кредитные карточки - наиболее распространенный тип пластиковых карточек. К ним относятся карточки общенациональных систем США Visa и Mastercard, American Express и AmEx's Optima, карточка Discovery Card фирмы Sears, Universal Card фирмы AT&T, местные и региональные карточки универсальных магазинов. Ими пользуются миллионы людей в США.

Карточки предъявляются на предприятиях торговли и обслуживания для оплаты товаров и услуг. При оплате с помощью кредитных карточек банк покупателя открывает ему кредит на сумму покупки и затем через некоторое время (обычно 25 дней) присылает счет по почте. Покупатель возвращает оплаченный чек обратно в банк.

Visa, MasterCard и Discover требуют от обладателей карточек производства по крайней мере фиксированного минимального платежа.

Разновидностью кредитных карточек являются affinity-карточки. Они выпускаются банком, кредитным объединением или финансовой компанией, заключившими специальное соглашение с профессиональной, общественной, религиозной или другой некоммерческой организацией. Обычно знак этой организации помещается на кредитную карточку. Производитель карточек обязуется отчислять своему контрагенту некоторый (сравнительно небольшой) процент от прибыли при использовании карточек. В ответ на это организация, с которой заключен договор, помогает производителю карточек внедрить их среди ее членов.

Дебетовые карточки используются для дебетовых расчетов. Другие ее названия: карточка наличных средств или расчетная. Она во многом аналогична кредитной. Для дебетовых транзакций чаще всего используются АКА. Дебетовые карточки предназначены для замены наличных денег и персональных чеков.

Пластиковая карточка, как основной носитель информации для АКА и оборудования POS, является притягательным объектом для злоумышленника. Поэтому перед выпуском таких карточек необходимо четко представлять степень их защиты от различных воздействий. Существует два основных требования к банковским карточкам: уникальность и необратимость.

Первое требование означает, что среди всех выпущенных банком карточек не должно быть ни одной одинаковой по характеристикам. Создание подобной карточки должно быть исключено для злоумышленника. Согласно второму требованию, не может быть восстановлена первоначальная информация на карточке.

Для реализации этих требований каждая фирма-изготовитель предусматривает свои схемы защиты, все тонкости которых она хранит в секрете. Рассмотрим два основных способа защиты магнитных карточек от подделки: метод магнитных водяных знаков и метод «сэндвича».

Метод магнитных водяных знаков предусматривает нанесение на магнитную ленту, расположенную на карточке, специального рисунка. Этот рисунок наносится при помощи магнитного поля и выполняет ту же самую функцию, что и обычные водяные знаки на ценных бумагах. При изготовлении карточка подвергается воздействию сильного электромагнитного поля под углом 45 градусов к продольной оси. Затем на нее воздействует специальное записывающее устройство, которое преобразует направленность магнитных полей на карточке к особому виду.

Проверка карточки с нанесенными магнитными водяными знаками осуществляется специальными устройствами. Этот метод защиты не влияет на информацию, которая записана на информационных дорожках, а добавляет на неиспользуемую нулевую дорожку от 50 до 100 разрядов дополнительной информации. Эти знаки используется для дополнительной проверки.

Метод «сэндвича» является альтернативой методу водяных знаков и заключается в том, что одна полоска содержит участки с различными уровнями намагниченности, причем участок с меньшей намагниченностью расположен ближе к головке чтения/записи. Для записи информации на карточку используется сильное магнитное поле. В считывателе информации карточка вначале проходит через стирающее поле. При этом на участке со слабой намагниченностью информация стирается, а с сильной намагниченностью - не изменяется. Затем информация с полосы считывается обычным образом. Надежность этого метода защиты основана на двух предположениях: во-первых, если злоумышленник использует одинарную полосу для подделки карточки, то вся информация на ней будет затерта стирающим полем; во-вторых, для записи на двухслойную полосу требуется специальное оборудование для создания необходимого по величине магнитного поля.

Современные пластиковые карточки имеют несколько степеней (уровней) защиты. Например, карточки системы VISA имеют семь уровней защиты:

1. Торговое имя продукта, которое идентифицирует тип Visa карточки, вместе с символом защиты;

2. Вокруг панели расположена кайма впечатанных кодов идентификации банка;

3. Поле fine-line в области идентификации продукции:

- символ защиты;

- идентификатор банка над символом защиты;

- голубь (эмблема Visa), который видим только в ультрафиолетовых лучах;

- трехмерная голограмма голубя.

В настоящее время не существует достоверной статистики по потерям, которые связаны с использованием пластиковых карточек. По некоторым оценкам, они составляют до $2 млрд. в год. Основной причиной потерь является неправильное использование карточек их законными владельцами. [12]

Пропорции злоупотреблений с пластиковыми карточками зависят от структуры банковской индустрии и поэтому сильно меняются от страны к стране. Например, по сравнению с Западной Европой, в США большие потери происходят именно за счет неправильного использования карточек. Но при этом, по оценкам экспертов, ущерб от мошенничества с применением технических средств составляет не менее $500 млн. в год. [3, с.52]

Ниже приведена статистика потерь для Visa и MasterCard (данные 1993 года). [2, с.24]

|  |  |
| --- | --- |
|  | |
| Причина | Доля в общих потерях, % |
| Мошенничество продавца | 22.6 |
| Украденные карты | 17.2 |
| Подделка карт | 14.3 |
| Изменение рельефа карты | 8.1 |
| Потерянные карты | 7.5 |
| Неправильное применение | 7.4 |
| Мошенничество по телефону | 6.3 |
| Мошенничество при пересылке почтой | 4.5 |
| Почтовое мошенничество | 3.6 |
| Кражи при производстве пересылке | 2.9 |
| Сговор с владельцем карточки | 2.1 |
| Прочие | 3.5 |

Одно из важнейших требований безопасности при работе с пластиковыми карточками — обеспечение безопасности банкоматов.

В настоящее время на автоматические кассовые аппараты (АКА) возлагаются следующие задачи:

- идентификация и аутентификация клиента;

- выдача наличных денег;

- оповещение о состоянии счета клиента;

- перевод денег клиента с одного счета на другой;

- регистрация всех произведенных операций и выдача квитанций.

Основная задача АКА - выдача наличных денег клиенту. Так как внутри АКА кроме различных устройств находятся и наличные деньги, то должна быть предусмотрена его серьезная физическая защита.

По имеющимся данным [6, с.82] в Великобритании АКА установлены:

\* 67 % - в виде, вмонтированном в стену;

\* 21 % - внутри банков;

\* 5 % - в вестибюлях банков;

\* 7 % - отдельно стоящие банкоматы вне банков.

При рассмотрении дальнейшей защиты хранимой в АКА информации предполагается, что нарушение его внешней физической защиты маловероятно.

Автоматический кассовый аппарат может работать в одном из двух режимов:

1. Off-line (автономный режим). В автономном режиме АКА функционирует независимо от компьютеров банка. При этом запись информации о транзакциях производится на внутренний магнитный диск и выводится на встроенный принтер.

2. On-line (режим реального времени). Для работы в этом режиме АКА должен быть подсоединен (непосредственно, либо через телефонную сеть) к главному компьютеру банка. При этом регистрация транзакций осуществляется непосредственно на главном компьютере, хотя подтверждение о транзакции выдается на принтер АКА.

Как автономный режим работы АКА, так и режим реального времени обладают своими достоинствами и недостатками (см. табл. 17).

Преимуществами автономного режима АКА является его относительная дешевизна и независимость от качества линий связи. Это особенно следует отметить в отечественных условиях, когда качество телефонных линий, мягко говоря, не идеально. В то же время низкая стоимость установки напрямую обуславливает высокую стоимость эксплуатации этих аппаратов. Ведь для того, чтобы обновлять списки потерянных карточек, «черные списки» необходимо хотя бы раз в день специально выделенному человеку обновлять в месте расположения АКА. При значительном количестве таких устройств подобное обслуживание затруднительно. Отказ от ежедневного обновления списков может привести к большим потерям для банка в случае подделки карточки или при пользовании украденной карточкой.

Сложности возникают также и при идентификации (аутентификации) клиента. Для защиты информации, хранящейся на магнитной карточке применяется ее шифрование. Для того, чтобы АКА одного и того же банка воспринимали пластиковые карточки в них для шифрования/расшифрования должен быть использован один ключ. Компрометация его хотя бы на одном из АКА приведет к нарушению защиты на всех АКА.

Режим реального времени имеет большие преимущества по сравнению с автономным. Он позволяет клиенту не только получить наличные деньги, но и осуществлять манипуляции со своим счетом. Централизованная идентификация/аутентификация позволяет существенно повысить устойчивость системы к компрометации ключей шифрования. Централизованная проверка идентификатора пользователя делает возможным быстрое обновление списков запрещенных к использованию карточек, а также введение ограничений на количество наличных денег, которые может получить клиент в течение одного дня (для защиты от использования украденных карточек).

Однако этот режим работы возможен лишь при наличии надежных каналов связи между АКА и банком (банками), что делает его довольно дорогим.

Наличие канала связи порождает и другие угрозы безопасности по сравнению с автономным режимом работы. Это перехват информационного потока, анализ графика и имитация работы главного компьютера. При этом анализируются данные, передаваемые АКА главному компьютеру и получение на их основе информации о счетах, суммах, условиях платежей и т.д. Главный компьютер может быть имитирован компьютером злоумышленника и на запрос АКА о результатах идентификации/аутентификации выдавать положительный ответ.

В том случае, когда АКА работает в режиме реального времени для осуществления идентификации он обменивается с главным компьютером банка тремя сообщениями, каждое из которых должно соответствовать специальному алгоритму с использованием шифра, части которого находятся как в банкомате, так и в главном компьютере. Без серьезной математической подготовки и хорошего компьютерного оборудования злоумышленник не сможет осуществить перехват информации.

Для борьбы с подбором PIN применяется ограничение на его ввод — обычно трехкратное. Если три попытки ввода PIN оказались неудачными, то в платеже клиенту отказывается. Ранние системы после трех неудачных попыток не возвращали карточку, однако, такое решение проблемы, особенно с кредитными карточками, не вызвало восторга клиентов.

Для АКА, работающих в автономном режиме, возврат карточки в случае трехкратного неудачного ввода PIN является весьма опасным, так как позволяет дальше подбирать PIN.

Кроме одиночных АКА в настоящее время эксплуатируются и сети АКА, в которых участвуют несколько банков. Участники такой сети преследуют следующие цели:

- разделение затрат и риска при разработке новых видов услуг между участниками сети;

- уменьшение стоимости операций для участников;

- придание оказываемым услугам общенационального характера и, соответственно, повышение их субъективной ценности для потребителя;

- возможность для региональных банков, так же как и для банков, расположенных в финансовых центрах, немедленно получить выгоду от либерализации законодательства, регулирующего выход на рынки других стран;

- преодоление имеющихся географических ограничений, которых не существует для небанковских учреждений. В настоящее время в США насчитывается три общенациональных сети:

1. MasterCard/Cirrus;

2. Plus System;

3. Visa U.S.A.

При совместном использовании банками сети АКА появляется новая проблема - защита конфиденциальной информации банков друг от друга (ключи шифрования, списки номеров запрещенных к использованию карточек и т.д.). Для ее успешного решения была предложена схема централизованной проверки PIN каждым банком в своем центре связи с АКА. При этом также усложняется система распределения ключей между всеми участниками сети.

К эмитенту карточки предъявляются следующие требования:

- выпускаемые им карточки должны восприниматься всеми АКА сети;

- он должен обладать технологией проверки собственных обменных PIN (если в АКА используется встроенная проверка принадлежности транзакции, то главный компьютер должен эмулировать результаты проверки в таком же формате).

К банку, выдающему «чужие» карточки, в свою очередь, предъявляются другие требования:

- в АКА или главном компьютере банка должна быть реализована проверка принадлежности транзакции;

- если нет возможности проверить правильность чужого PIN, банк должен передать данные о транзакции на сетевой маршрутизатор.

Для защиты взаимодействия компьютеров банков между собой и с АКА применяется оконечное шифрование информации, передаваемой по линиям связи.

Наиболее часто используется следующий метод: вся сеть АКА разбита на зоны и в каждой из них используется свой Главный зональный управляющий ключ. Он предназначен для шифрования ключей при обмене между сетевым маршрутизатором и главным компьютером банка. Ключ индивидуален для всех участников сети. Обычно он случайно генерируется маршрутизатором и неэлектронным способом передается в банк. Раскрытие ключа приведет к раскрытию всех PIN, которые передаются между маршрутизатором и главным компьютером банка.

В неразделяемой сети АКА достаточно на всех АКА использовать один открытый ключ, а на главном компьютере банка закрытый ключ. Это позволит шифровать запрос и подтверждающее сообщение и проверять подлинность ответного сообщения из банка, так как обеспечение конфиденциальности ответного сообщения не обязательно. Особого внимания стоит проблема защиты запроса от активных атак (изменения или введения ложного запроса). Но и она в случае неразделяемой сети может быть решена с использованием пароля для идентификации АКА.

В случае сети совместно используемых АКА применение системы шифрования с открытым ключом позволяет отказаться от зональных ключей и дорогостоящей процедуры их смены. Однако в этом случае схема идентификации АКА по паролю не будет работать. Эта проблема может быть решена в том случае, когда каждый АКА вместе с запросом будет пересылать и свой открытый ключ, заверенный банком. [7, с.49]

Системы POS предназначены для сокращения расходов по обработке бумажных денег и для уменьшения риска покупателя и продавца, связанного с этой обработкой.

Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карточку и для подтверждения личности вводит PIN. Продавец со своей стороны вводит сумму, которую необходимо уплатить за покупку или за услуги.

Запрос на перевод денег направляется в банк продавца. Тот для проверки подлинности карточки, предъявленной покупателем, переадресует запрос в банк покупателя. Если карточка подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг банк покупателя переводит деньги в банк продавца на его счет. После перевода денег банк продавца посылает извещение на терминал POS, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю извещение.

Необходимо обратить внимание на тот путь, который должна проделать информация прежде чем будет осуществлена транзакция. Во время его прохождения возможна потеря сообщений. Во избежание этого банк продавца должен повторять выдачу сообщений при обнаружении их потери.

Для защиты системы POS должны соблюдаться следующие требования:

1. Проверка PIN, введенного покупателем, должна производиться системой банка покупателя. При пересылке по каналам связи PIN должны быть зашифрованы.

2. Сообщения, содержащие запрос на перевод денег (или подтверждение о переводе), должны проверяться на подлинность для защиты от внесения изменений и замены при прохождении по линиям связи к обрабатывающим процессорам.

Самым уязвимым местом системы POS являются ее терминалы. Все построение системы охраны исходит из предположения абсолютно надежной физической защиты банкомата. Для терминалов POS это не так. Изначально предполагается, что терминал системы POS незащищен от внешнего воздействия.

В связи с этим предположением возникают новые типы угроз для терминала. Они связаны с раскрытием секретного ключа, который находится в терминале POS и служит для шифрования информации, передаваемой терминалом в банк продавца. Угроза вскрытия ключа терминала весьма реальна, так как они устанавливаются в таких неохраняемых местах как магазины, автозаправочные станции и пр. Эти угрозы получили следующие названия: [2, с.391]

1. «Обратное трассирование». Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, использованные в предыдущих транзакциях.

2. «Прямое трассирование». Сущность этой угрозы заключается в том, что если злоумышленник получит ключ шифрования, то он будет пытаться восстановить значения PIN, используемые в транзакциях, которые произойдут после того, как он получит ключ.

Для защиты от этих угроз были предложены три метода: метод ключа транзакции, метод выведенного (полученного) ключа и метод открытых ключей. Сущность первых двух заключается в том, что они предусматривают изменение ключа шифрования передаваемых данных для каждой транзакции.

Метод ключа транзакции был впервые предложен в 1983 году. Информация, передаваемая между каждым терминалом и каждым эмитентом карточек, должна быть зашифрована на уникальном ключе, который, в свою очередь, должен изменяться от транзакции к транзакции. Однако применение этого метода для большого количества терминалов и эмитентов карточек делает затруднительным управление ключами. Поэтому, в подавляющем большинстве практических приложений, он применяется не к связи «терминал-эмитент карточек», а к связи «терминал-получатель», так как каждый получатель имеет ограниченный набор обслуживаемых терминалов. При генерации нового ключа используются следующие составляющие: однонаправленная функция от значения предыдущего ключа, содержание транзакции и информация, полученная с карточки. При этом подразумевается, что предыдущая транзакция завершилась успешно. Такая схема обеспечивает защиту как от «обратного трассирования», так и от «прямого трассирования». Раскрытие одного ключа не дает возможности злоумышленнику вскрыть все предыдущие или все последующие транзакции.

Метод предусматривает также раздельную генерацию двух ключей - одного для шифрования PIN, другого для получения MAC. Это необходимо для разделения функций банков продавца и получателя. Недостатком схемы является ее сложность.

Метод выведенного ключа более прост в использовании, однако, и менее надежен. Он обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа здесь используется однонаправленная функция от текущего значения ключа и некоторое случайное значение. Метод обеспечивает защиту только от «обратного трассирования».

Применение открытых ключей позволяет надежно защититься от любых видов трассирования и обеспечить надежное шифрование передаваемой информации. В этом методе терминал РОЗ снабжается секретным ключом, на котором шифруется запрос к банку продавца.

Этот ключ генерируется при инициализации терминала. После генерации секретного ключа терминал посылает связанный с ним открытый ключ на компьютер продавца. Обмен между участниками взаимодействия осуществляется с использованием открытого ключа каждого из них. Подтверждение подлинности участников осуществляется специальным центром регистрации ключей с использованием своей пары открытого и закрытого ключей. Недостатком метода является его сравнительно малое быстродействие.