МАГНИТНЫЕ КАРТЫ

ВЫПОЛНИЛИ:

СТУДЕНТЫ ГРУППЫ 592

ПРОНИН А.В.

БЕЙСЕНБАЕВ А.К.

ОПРЕДЕЛЕНИЕ

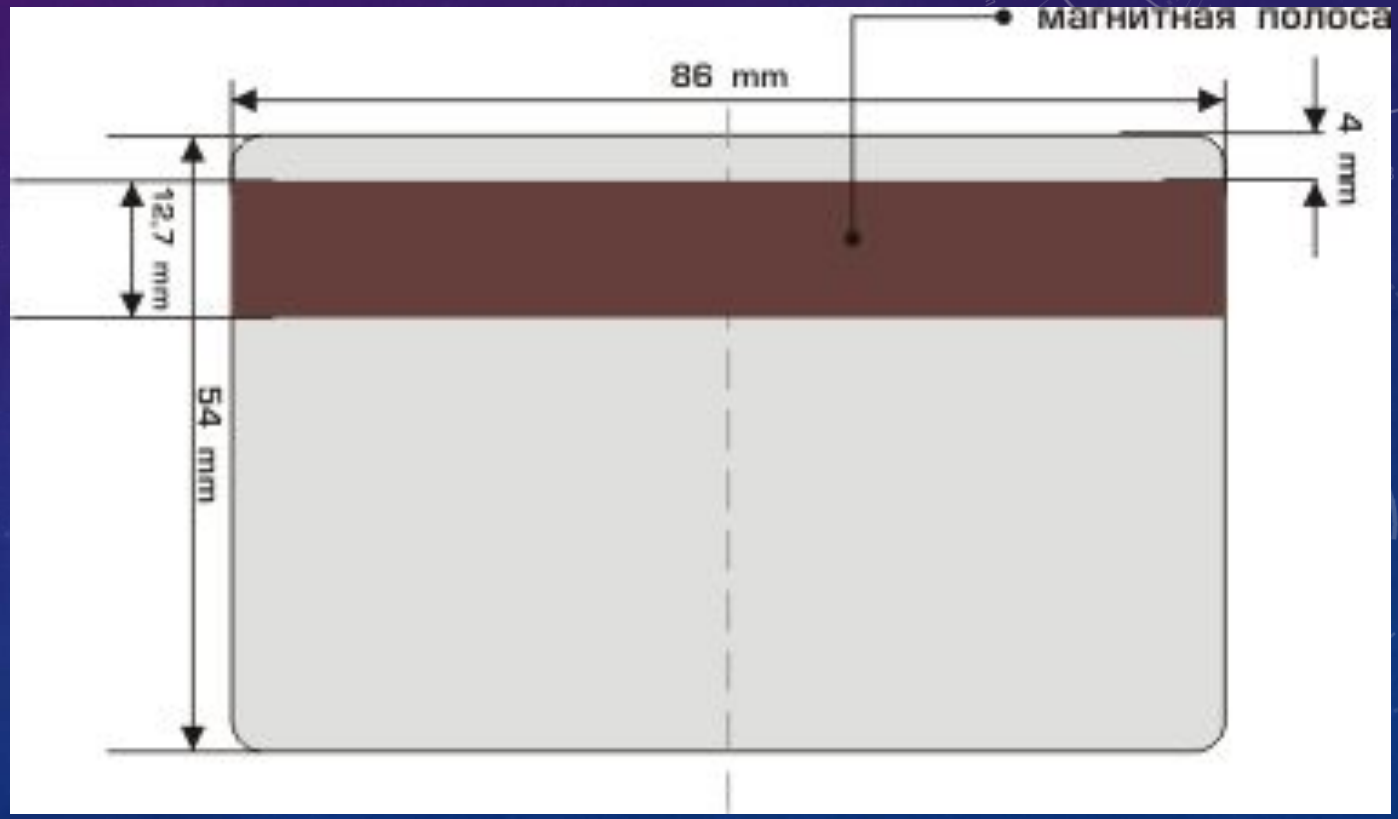
Карта с магнитной полосой — тип карт, отличающийся наличием магнитной полосы. Магнитная полоса предназначена для хранения какой-либо информации. Запись информации выполняется путём намагничивания крошечных частиц, находящихся на поверхности полоски и содержащих железо (магнитный материал). Чтение информации выполняется путём проведения полосы по магнитной головке.

ГАБАРИТЫ

Размеры карточки:

- Ширина - 85,595 ± 0,125 мм
- Высота - 53,975 ± 0,055 мм
- Толщина - 0,76 ± 0,08 мм
- Радиус окружности в углах - 3,18 мм.

Магнитная полоса предполагает машинное считывание. Для стандартных считывающих устройств (ридеров) магнитная полоса делается шириной 12,7 мм (0,5 дюйма) и располагается на расстоянии 4 мм от края карточки.



МАГНИТНАЯ ЛЕНТА

На магнитной полосе (плёнка на карте, похожая на пластик) находится три дорожки, по которым можно нанести ту или иную информацию. Все три дорожки магнитной полосы используются, как правило, в крупных банковских платежных системах (например, VISA). В дисконтных системах, в локальных платежных системах, а также в системах доступа используется чаще всего одна дорожка (обычно вторая).

ЗАПИСЬ ИНФОРМАЦИИ НА МАГНИТНУЮ ПОЛОСУ

В соответствии с существующими стандартами, магнитная карта хранит информацию на трёх раздельных дорожках. Все эти дорожки обладают различной битовой плотностью (bpi - bits per inch) и закодированы наборами символов. Плотность первой дорожки – 210 bpi, на ней можно хранить данные набора символов. Символы состоят из информационных разрядов и разрядов отрицательной четности. Кодирующий формат позволяет наименее значимому разряду стоять первым , а четному разряду – последним. Таким образом, на первом треке можно хранить символьную последовательность около 79 знаков.

Плотность информации второй и третьей дорожек – 75 и 210 bpi, соответственно. На третьей дорожке могут храниться только числовые данные. Вторая и третья дорожка хранят по 40 и 107 символов, соответственно.

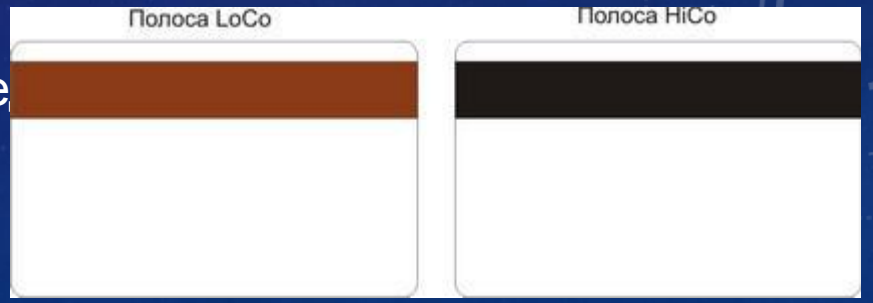
ЗАПИСЬ ИНФОРМАЦИИ НА МАГНИТНУЮ ПОЛОСУ

Формат данных, хранящихся на 1-й дорожке, создан международной ассоциацией воздушного транспорта (авиапромышленностью). Формат данных, хранящихся на 2-й дорожке, создан организацией «Объединение банкиров Америки» (American Bankers Association (англ.). Формат данных, хранящихся на 3-й дорожке, создан ссудо-сберегательной ассоциацией.

Коэрцитивная сила — это значение напряжённости магнитного поля, необходимое для полного размагничивания ферро- или ферримагнитного вещества(в системе СИ — Ампер/метр). Чем большей коэрцитивной силой обладает магнит, тем он устойчивее к размагничивающим факторам.

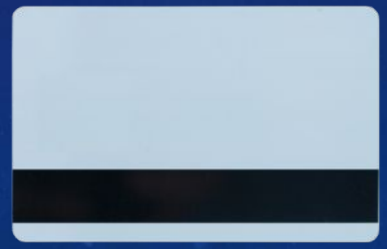
Виды магнитных полос по величине коэрцитивной силы:

- полосы с высокой степенью коэрцитивности (HiCo); 2750 эрсте
- низкокоэрцитивные (LoCo) полосы; 300 эрстед.



ЗАПИСЬ ИНФОРМАЦИИ НА МАГНИТНУЮ ПОЛОСУ

Формат на всех трёх дорожках данных можно представить следующим образом: изначально идут инициализирующие символы (не содержащие информации), они определяют способ кодирования магнитной карты, и служат для синхронизации магнитных дорожек со считывающим устройством. То есть по этим символам считыватель определяет, где начало и где конец намагниченного участка. Затем начинается считывание фактических данных. Информативная часть магнитной полосы завершается байтом LRC. Он используется для обнаружения ошибок считывания посредством суммирования считанных данных. Считанная сумма, в итоге, должна быть равна этому байту. Если же они не равны, считывание считается ошибочным. Оставшуюся часть магнитной полосы заполняют инициализирующие символы.



КАК ПРОИСХОДИТ ПРОЦЕСС ЗАПИСИ

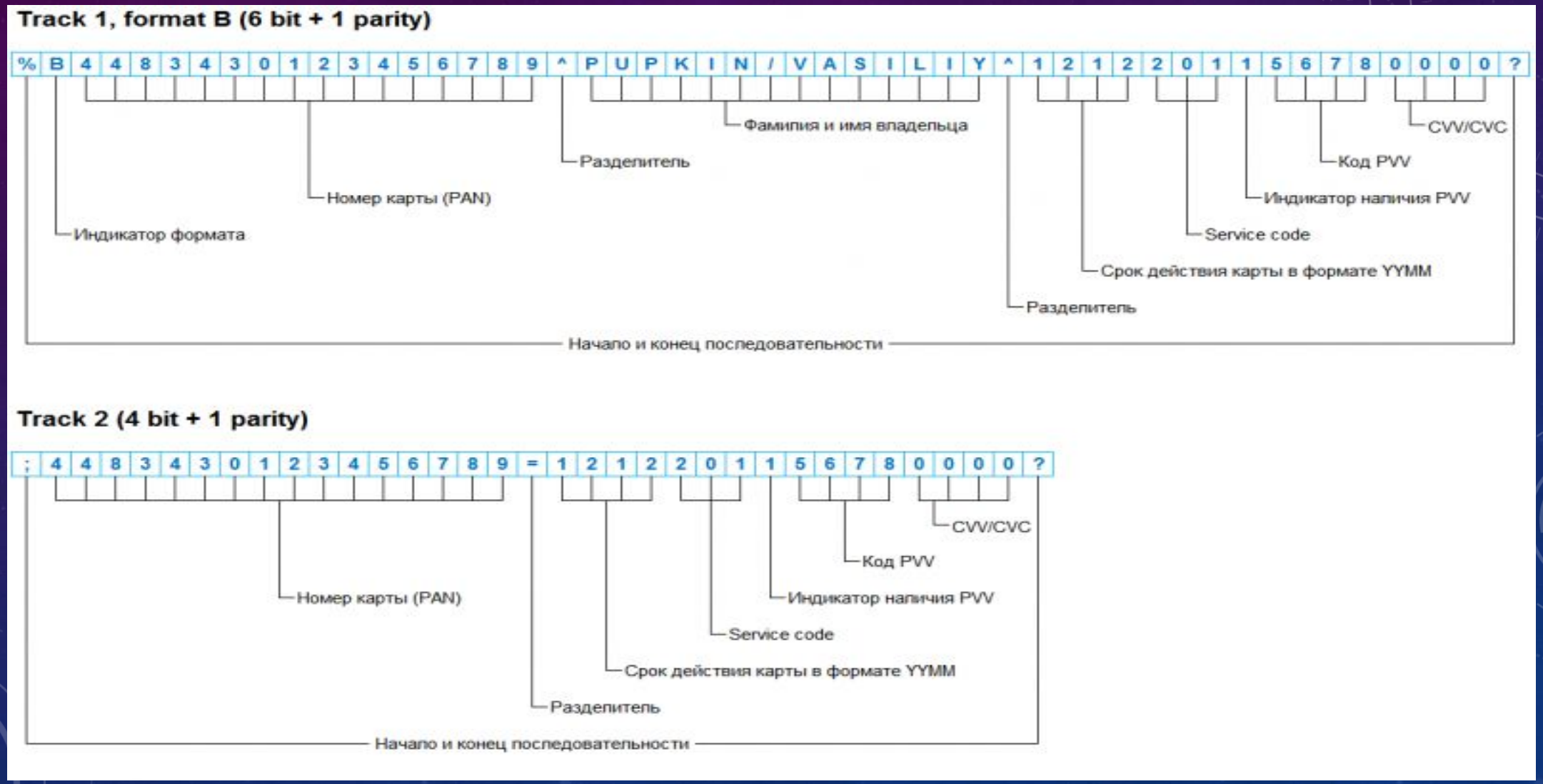
В процессе нанесения на поверхность ферромагнетик сразу проходит ориентацию — то есть поворачивается согласно линиям магнитного поля. Этим достигается некоторое улучшение магнитных свойств дорожки. Дальше наносится фиксатор и защитный слой. Затем полоску вносят в зону действия магнитного поля, в которой с течением времени происходит намагничивание частиц полоски, пока векторы магнитной индукции этих частичек не станут совпадать по величине с векторами внешнего магнитного поля. При записи головка, которая создает поле возле магнитной полосы, происходят изменения в амплитуде электрического тока. При изменении интенсивности и направления магнитных полей участков осуществляется запись цифровой информации.

ЗАПИСЬ ИНФОРМАЦИИ НА МАГНИТНУЮ ПОЛОСУ

На магнитные дорожки возможна запись только латинских букв, буквы кириллицы вызывают ошибку в работе записывающего устройства.

- 1-дорожка – цифробуквенная информация: до 76 знакомест QWERTYUIOPASDFGHJKLZXCVBNM1234567890 : ; = + ( ) – ‘ - (клавиша “ ‘ Э) ! @ # ^ & * < > / \ Все латинские буквы заглавные. Служебный знак „?” добавляется в конце каждой строки базы данных и означает конец записи на магнитную полосу и при считывании не отображается.
- 2-дорожка – только цифры: 1234567890 и знак „=”, до 37 знакомест пробел отображается на магнитной полосе знаком „=”, знак „?” означает конец записи на магнитную полосу и при считывании не отображается. Знак „?” добавляется в конце каждой строки таблиц базы данных.
- 3-дорожка – только цифры: 1234567890 и знак „=”, до 104 знакомест пробел отображается на магнитной ленте знаком „=”, знак „?” означает конец записи на магнитную ленту и при считывании не отображается. Знак „?” добавляется в конце каждой строки таблиц базы данных.

ПРИМЕР ИНФОРМАЦИИ НА ДОРОЖКАХ.



ПРИМЕНЕНИЕ КРИПТОГРАФИИ ДЛЯ КАРТ С МАГНИТНОЙ ПОЛОСОЙ

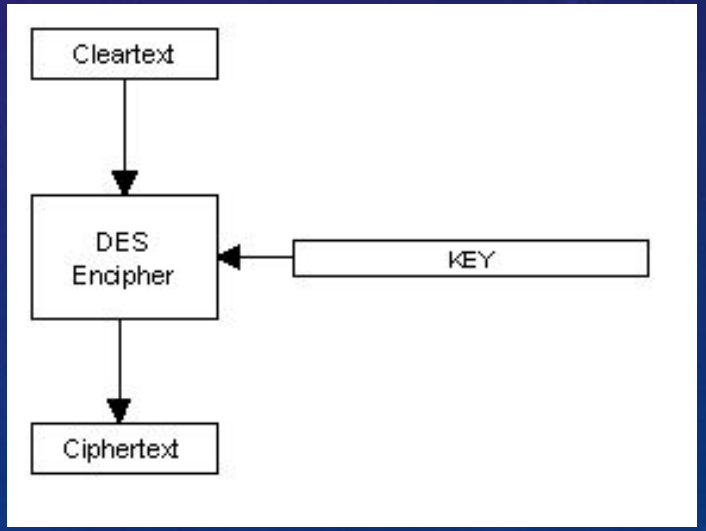
Использование криптографии в денежных магнитных картах

- Самое распространенное использование криптографии это обеспечение Персонального Идентификационного Номера, или ПИН, для использования магнитной карты в местах, где нельзя осуществить контроль за правомерностью доступа , например в АТМ (банкоматах), либо в каких-то других ситуациях, где осуществить предоставление обычной бумажной подписи невозможно. Все это распространяется на кредитные, дебитные и АТМ-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 онлайн, 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.

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 выполнен как в программном, так и в аппаратном виде. Затем DES шифрует чистое значение, используя ключ (секретный, 64-битный), и на выходе выдает зашифрованное значение.

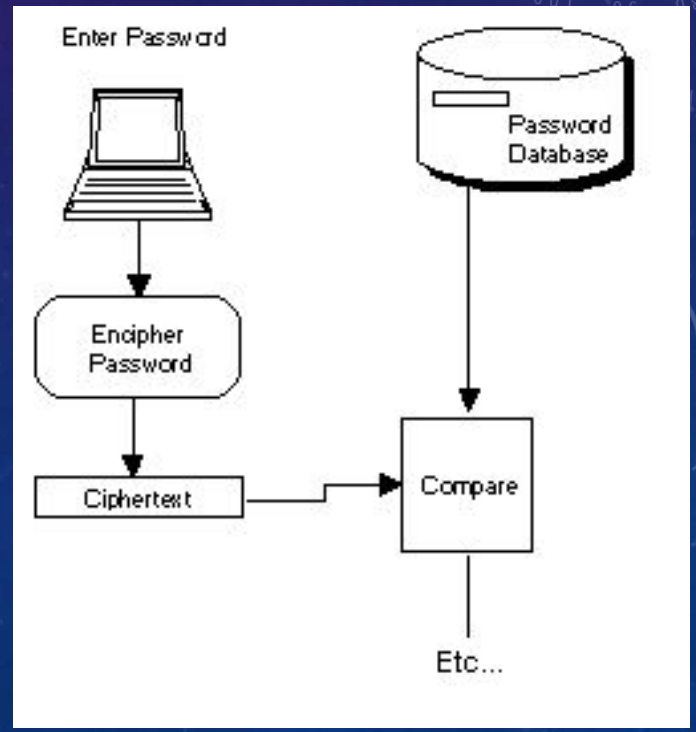
- Входная незашифрованная информация обычно называется Чистым текстом (Cleartext), в то время как зашифрованный результат – Шифрованный текст (Ciphertext). Механизм переработки Cleartext в Ciphertext, согласно терминам DES называется `encipher' операцией.



ШИФРОВАНИЕ

Стоит принять 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.

ПРАКТИЧЕСКОЕ ПРИЛОЖЕНИЕ КРИПТОГРАФИИ В МАГНИТНЫХ КАРТАХ, НА ПРИМЕРЕ ШИФРОВАНИЯ ПРИ ВЫДАЧЕ ДЕНЕГ В БАНКОМАТЕ

Обычная ATM транзакция:

- Клиент вводит карту в банкомат
- Клиент вводит свой ПИН
- Клиент запрашивает наличные
- Транзакция подтверждена, наличные выданы

В этот процесс вовлечено очень много шифровок. Для простоты, предположим что банк получателя и отправителя один и тот же.

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, возможно 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.

СЧИТЫВАТЕЛИ МАГНИТНОЙ ПОЛОСЫ

Считыватели магнитных карт, а точнее, считыватели магнитной полосы (Magnetic Stripe Reader), предназначены для считывания информации с магнитной полосы, нанесенной на пластиковую или картонную основу. Принцип действия этого устройства напоминает магнитофон: магнитная головка считывает информацию с движущейся в контакте с нею магнитной полоски, декодирует ее, то есть переводит в последовательность ASCII-символов, и передает данные в компьютер.

СЧИТЫВАТЕЛИ МАГНИТНОЙ ПОЛОСЫ

Перемещение полосы в контакте с магнитной головкой чаще всего обеспечивается вручную, просто проводя картой через щель, в которой установлена считывающая головка. Такие считыватели магнитных карт называются РУЧНЫМИ. Существуют также МОТОРИЗОВАННЫЕ считыватели пластиковых карт. Они, например, применяются в банкоматах и в других устройствах, захватывающих карту на время транзакции. Достаточно слегка вставить карту в такой считыватель, и он автоматически втянет ее внутрь для прочтения. По окончании операции механизм вернет карту владельцу или изымет ее (в случае подозрения на незаконность использования).

СЧИТЫВАТЕЛИ МАГНИТНОЙ ПОЛОСЫ

Считыватель (ридер) магнитных карт – необходим для считывания информации с магнитных карт различных типов, например, с дисконтных карт, карт информации о клиенте, идентификационных карточек сотрудников компании, карт доступа и др.

Считыватели магнитных карт могут считывать одну, две или три записываемых дорожки. В зависимости от объема информации, которую требуется переносить на карте, могут быть использованы все или только некоторые дорожки. Считыватель не всех дорожек стоит несколько дешевле, но не является универсальным.

Так же считыватели магнитных карт отличаются способом подключения к интерфейсу (через USB, разрыв клавиатуры и др.). Можно разграничить по тому способу, как они интегрируются в систему (считыватели производятся в готовом корпусе и без корпуса – для встраивания в изделие). Считыватели различаются по типу читаемого носителя данных: кроме магнитной полосы, это может быть чип или сочетание обоих носителей.

ЗАКЛЮЧЕНИЕ

Магнитные карты имеют компактный размер, но при миниатюрных габаритах карты она является носителем довольно обширной информации, что очень удобно для пользователя. Производство магнитных карт имеет низкую себестоимость. Именно поэтому магнитные карты остаются самым распространенным типом карт. Они активно используются в банковской сфере и розничной торговле, а также во многих других областях экономической деятельности.

Однако при всех положительных качествах, которыми обладают магнитные карты, есть у них и свои недостатки. Это недостаточная прочность носителя (магнитная лента подвержена механическим и другим воздействиям), невозможность обновления данных, обязательное требование обслуживать карту в режиме он-лайн. Но самым главным недостатком магнитных карт была и остается недостаточная защита информации от злоумышленников.

Закономерно, что на смену магнитным картам постепенно приходят изделия нового поколения – смарт-карты. Они обладают большим потенциалом как в плане хранения данных, так и в плане безопасности.