
Банковские
платёжные
технологии
Вводный курс

Содержание курса:

1. Банковские карты
2. Оборудование для приёма карт
3. Хосты и протоколы
4. Эквайринг
5. Комиссии МПС с банков
6. Элементы безопасности

Банковские карты – предыстория

Начало 20-го века – крупные американские отели, нефтяные компании и магазины выпускали товарные карточки, которые имели два назначения:

- следить за счетом клиента

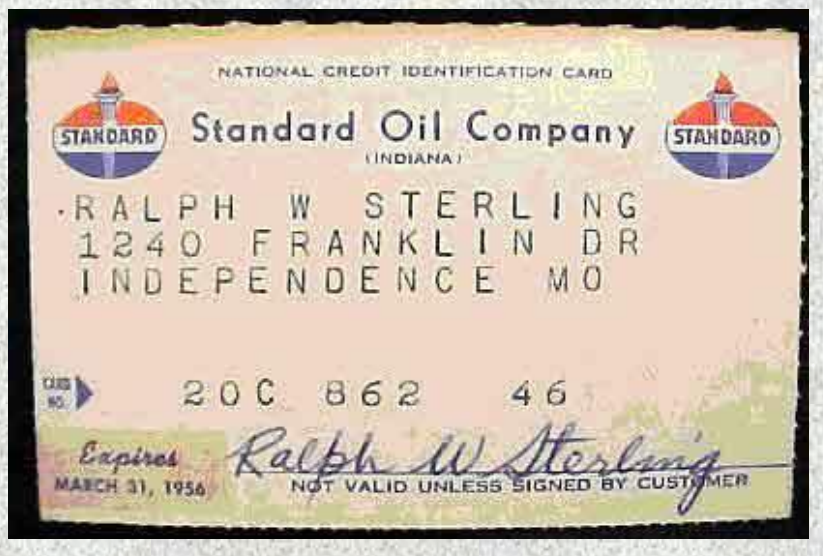
- обеспечить механизм записи его покупок

Их появление было логическим продолжением оплаты в рассрочку

1914 – торговые предприятия стали выпускать карточки для самых богатых клиентов, чтобы привязать их к своей сети магазинов и продавать им наиболее дорогие товары

Банковские карты – предыстория

Начало 1920-х – нефтяные компании стали выпускать «карты учтивости» (courtesy cards), с помощью которых водители могли делать покупки на любой бензоколонке



Банковские карты – предыстория

В следующие 30 лет крупные компании предложили такие нововведения, как:

- *минимальная месячная плата*
- *плата за финансовые услуги*
- *30-дневный период отсрочки по платежам*

Жесткая конкуренция заставила компании пойти на значительные расходы и начать эмиссию кредитных карт

Банковские карты – история

1949 – Встреча внука основателя одного из американских универмагов Альфреда Блумингдейла, главы небольшой финансовой компании Hamilton Credit Corporation Фрэнка МакНамары (Frank McNamara – на фото) и юриста этой компании Ральфа Шнайдера

Банковские карты – история

Результат встречи – появление на свет карточки Diners Club – первой массовой платёжной карточки в мире

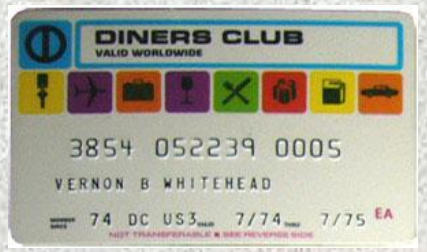
Первоначально карточка Diners Club предназначалась для расчётов за обеды, причём расчёты производились в кредит, но быстро стала универсальной, то есть предназначенной для расчёта за товары и услуги по всей стране, а также снятия наличных

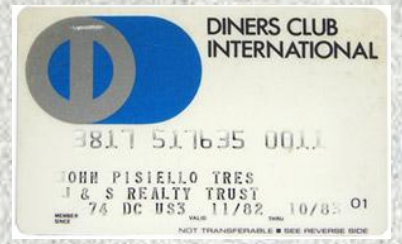
Банковские карты – история

Важная особенность – появление третьей стороны в кредитных операциях, Diners Club – посредник между покупателем и фирмой, обеспечивая кредит одному и другому и беря плату за услуги

Стартовый капитал Diners Club – 75 тысяч долларов

Прибыль – с фирмы-продавца, которая должна давать 7% скидки с суммы покупки, а также с владельца карты в виде ежемесячной платы





Банковские карты – история

1958 – American Express, крупнейшая компания дорожных чеков, и Carte Blanche одновременно вышли на рынок универсальных кредитных карт

1958 – первый и второй банки страны – Bank of America и Chase Manhattan Bank также приступили к операциям с кредитными картами

Банковские карты – история

1966 – Bank of America даёт лицензии другим банкам на проведение операций с картами BankAmericard

Ответ других крупных банков – Interbank Cards Association (ICA) – вторая национальная система карт
1969 – ICA выкупила права на карту MasterCharge, выпускаемую банками западных штатов, и перешла на её выпуск

Июль 1970 – Банки, выпускающие BankAmericard настояли на выведении её из-под контроля Bank of America – National BankAmericard Incorporated (NBI)

Банковские карты – история

1976 – NBI поменяла имя на VISA

1980 – ICA стала Master Card

1969 – 1981 – число банков, присоединившихся к MasterCard увеличилось с 4461 до 12504, присоединившихся к VISA – с 3751 до 12518.

Банковские карты – история

American Express быстро обошла своих конкурентов Diners Club и Carte Blanche. К 1970 у нее было в два раза больше клиентов, чем у первой и в четыре раза больше, чем у второй. В середине 70-х разрыв еще больше увеличился: держателей карт American Express было в 7,5 раз больше, чем у Diners Club и в 10 раз больше, чем у Carte Blanche

Diners Club и Carte Blanche были куплены CitiBank, способного более серьезно соперничать с American Express. Несмотря на это, у последней сейчас в 12 раз больше клиентов, чем Diners Club и Carte Blanche вместе взятых.

Банковские карты – история

Начало 1950-х – British Hotel&Restaurant Association выпустила карту BHR в Европе

Среди американских компаний, действовавших в Европе, доминировала Diners Club

1972 – NBI заявила о начале операций в 72 странах, но быстрое распространение происходило только в Великобритании, где компания приобрела карту Barclay's

Банковские карты – история

ICA достигло соглашений с EuroCard, крупнейшей системой универсальных карт в Европе, и с Access, крупнейшей системой Великобритании

JCB-банк, дочернее предприятие American Express, возглавлял рынок, имея в два раза больше клиентов, чем VISA и MasterCard вместе взятые

1980 – Япония, несмотря на поздний старт индустрии карт, обошла все европейские страны и вышла на второе место после США по количеству карт

Банковские карты – история

1969 – первой платёжной карточкой в СССР была карта Diners Club, которая стала в приниматься в системе магазинов “Берёзка”

1988 – спортсменам советской Олимпийской сборной, направлявшейся на соревнования в Сеул, выдали карты VISA

У магазина „Берёзка". Москва, 1962. Фото А.Павлова.

Банковские карты – история

1993 – в России были созданы российские платёжные системы STB Card и Union Card, в которых работали несколько сотен банков, затем появились Золотая Корона и Сберкард

После кризиса 1998 года российские платёжные системы начали уступать свои позиции, хотя до сих пор их картами пользуются несколько десятков миллионов человек, а в той же Union Card, например, работают такие крупные банки, как Банк Москвы, ТрансКредитБанк и Уралсиб, а в Золотой Короне – Русский Стандарт, Мастербанк, МДМ-банк

Банковские карты – история

Март 2002 – появилась China UnionPay (CUP) – национальная платежная система КНР

Сегодня CUP принимается в 135 странах, выпущено около 2,5 миллиардов карт

Банковские карты – история

Август 2008 – в России первая операция по CUP (накануне открытия Олимпийских игр в Пекине)

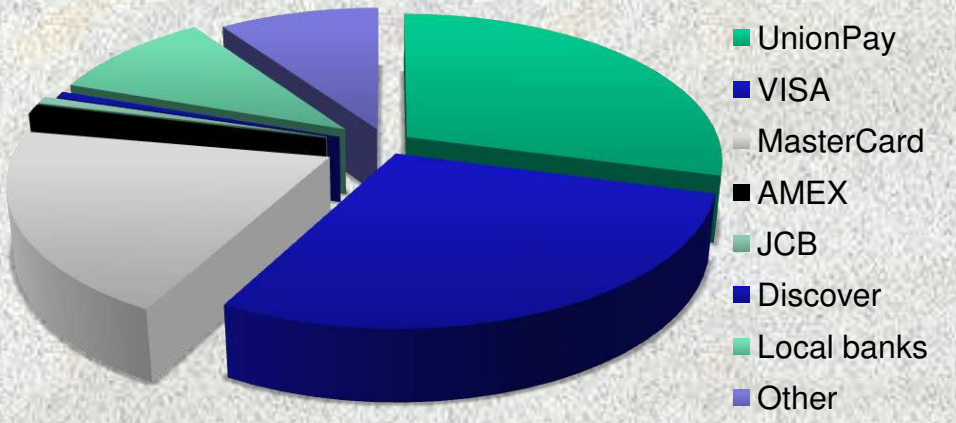
Сейчас в России количество операций по картам Union Pay превышает аналогичный показатель American Express, а эмитентами являются, например, Мастербанк и ВТБ

Банковские карты – современность

По данным исследовательской компании Retail Banking Research (RBR), China UnionPay обогнала Visa и стала крупнейшей мировой платежной системой

В 2010 году в обращении находилось 8 миллиардов платежных карт, из которых выпущено:

29,2% - UnionPay
28,6% - Visa
20,0% - MasterCard
1,1% - American Express
0,8% - JCB
0,7% - Discover



Карты торговых марок составили примерно 10% от общего числа, столько же приходилось на местные банки

Банковские карты – современность

2011 – мировые секторы предоплаченных и дебетовых карт выросли более чем на 10% каждый, в то время как кредитно-карточный сектор сократился на 6%

Сегодня:
62% - дебетовые карты
28% - кредитные
3% - предоплаченные

К 2015 году количество карт в обращении составит 10,1 миллиарда, замедление эмиссии в развитых североамериканском и западноевропейском регионах компенсируется быстрым ростом в остальных странах

Банковские карты – современность

По данным ЦБ РФ на 1 января 2013 года в России выпущено 239 миллионов 545 тысяч карт, по которым за 2012 год проведено 5,6015 миллиарда** операций на общую сумму 21,2838 триллионов*** рублей (в том числе, по оплате товаров и услуг: 2,7580 миллиарда операций на сумму 3,266 триллиона рублей)*

* 1 миллион = 1 000 000
** 1 миллиард = 1 000 000 000
*** 1 триллион = 1 000 000 000 000

Банковские карты – описания

Карты различаются по:

1. *Принадлежности платёжной системе (VISA, MC, CUP и т.д.)*
2. *Статусу (например, VISA Electron, VISA Classic, VISA Gold, VISA Platinum, VISA Infinite)*
3. *Типу носителя информации (магнитные, чиповые, бесконтактные)*
4. *Возможности использования заёмных средств (дебетовые, кредитные)*
5. *Персонификации (именные, не именные)*
6. *Способу нанесения информации (эмбоссированные, не имбоссированные, индент)*
7. *Глобальности (международная, региональная, локальная)*

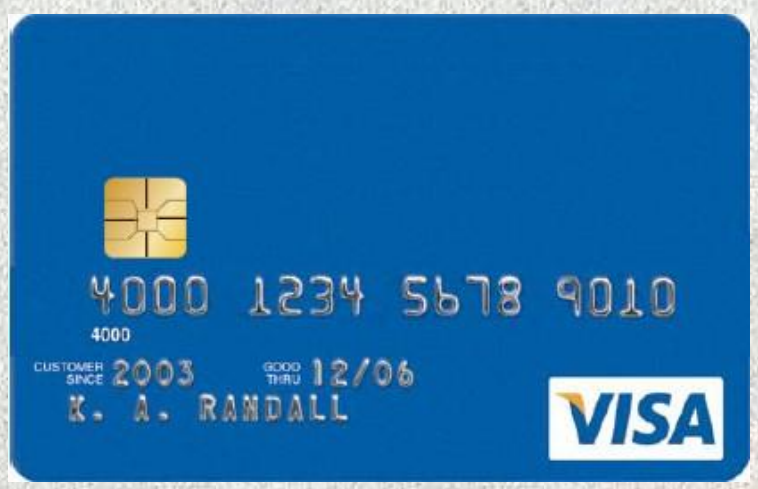
…

Банковские карты – дизайн – VISA

Лицевая сторона карт VISA:

- логотип "VISA" дизайна располагается в правом верхнем или нижнем углу карты. На чиповых картах дополнительно в левом верхнем углу

- на логотипе расположен ультрафиолетовый элемент в виде буквы V, повторяющей по форме букву V из логотипа. Ультрафиолетовый элемент обязателен для всех карт Visa и Visa Electron



Банковские карты – дизайн – VISA

Лицевая сторона карт VISA:

- номер карты, срок действия, имя держателя могут быть как эмбоссированы, так и нанесены инденторпечатью. В случае нанесения информации инденторпечатью на лицевой стороне карты должна присутствовать надпись “Electronic use only”

- BIN (первые 4 цифры номера) должен быть нанесен типографским способом

при использовании голографической магнитной полосы голограмма отсутствует. Со стандартной магнитной полосой наличие голограммы обязательно

- чиповые карты Visa и Visa Electron могут быть вертикального расположения. В этом случае информация на них должна быть нанесена инденторпечатью

Банковские карты – дизайн – VISA

Оборотная сторона карт VISA:

- панель для подписи нового дизайна – стандартная (в виде чередующихся горизонтальных желтых и синих полос) или разработанная по дизайну эмитента

- на панели для подписи, с наклоном в левую сторону, нанесен номер карты (или его последние 4-е цифры) и трехзначный код безопасности. Код безопасности может быть вынесен за пределы панели для подписи

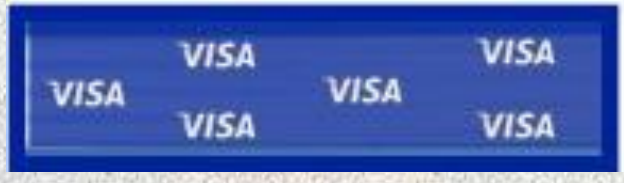
Банковские карты – дизайн – VISA

Оборотная сторона карт VISA:

- панель для подписи обязательно содержит ультра-фиолетовый элемент в виде слов “VISA”

- магнитная полоса должна быть впаяна в пластик, а не наклеена. Располагается в верхней части карты, а для неэмбоссированных карт может располагаться и в нижней части карты

- магнитная полоса может быть как стандартной (аналогичной картам старого дизайна), так и голографической. При использовании стандартной магнитной полосы на лицевой стороне карты должна присутствовать голограмма



Банковские карты – дизайн – VISA

Оборотная сторона карт VISA:

- голографическая магнитная полоса содержит:

а) параллельные вертикальные и горизонтальные линии

б) изображение летящего голубя в трех фазах полета

в) микрошрифт в виде повторяющегося слова “VISA” на горизонтальной линии, проходящей по центру магнитной полосы

г) над микрошрифтом вдоль магнитной полосы 2-3 раза повторяется голографическое изображение слова “VISA” внутри круга

Банковские карты – дизайн – VISA Electron

Лицевая сторона карт VISA Electron:

- логотип "VISA ELECTRON" нового дизайна располагается в правом верхнем или нижнем углу карты. На чиповых картах дополнительно в левом верхнем углу

- на логотипе расположен ультрафиолетовый элемент в виде буквы V, повторяющей по форме букву V логотипа. Ультрафиолетовый элемент обязателен для всех карт Visa и Visa Electron

Банковские карты – дизайн – VISA Electron

Лицевая сторона карт VISA Electron:

- номер карты, срок действия, имя держателя нанесены индент-печатью. Номер карты может быть нанесен не полностью – только 4-е последние цифры номера

- BIN (первые 4 цифры номера) должен быть нанесен типографским способом

- на лицевой стороне карты обязательно должна присутствовать надпись “Electronic use only”

- чиповые карты Visa и Visa Electron могут быть вертикального расположения. В этом случае их реквизиты должны быть нанесены индент-печатью

Банковские карты – дизайн – VISA Electron

Оборотная сторона карт VISA Electron:
- панель для подписи нового дизайна – стандартная (в виде чередующихся горизонтальных желтых и синих полос) или разработанная по дизайну эмитента
-на панели для подписи, с наклоном в левую сторону, нанесен номер карты (или его последние 4-е цифры) и трехзначный код безопасности. Код безопасности может быть вынесен за пределы панели для подписи

При неполном номере карты на лицевой стороне - нанесение номера карты и кода безопасности не требуется

Банковские карты – дизайн – VISA Electron

Оборотная сторона карт VISA Electron:
- панель для подписи обязательно содержит ультрафиолетовый элемент в виде слов “VISA”
- магнитная полоса – стандартная, должна быть впаяна в пластик, а не наклеена. Расположена в верхней или нижней части карты, а для чиповых карт – только в нижней части

По решению эмитента может использоваться голографическая магнитная полоса

Банковские карты – дизайн

Примеры:

Победители «Лучший дизайн карт Visa»

July 2011
Issuer: Armeconombank, Armenia
Product type: Visa Infinite, Credit

June 2011
Issuer: Cosmos Bank, Taiwan
Product type: Visa Platinum, Credit

Банковские карты – дизайн

Примеры:

Победители «Лучший дизайн карт Visa»

April 2011
Issuer: Dubai Bank, U.A.E.
Product type: Visa Platinum, Credit

May 2011
Issuer: IndusInd Bank, India
Product type: Visa Signature, Credit

Банковские карты – дизайн

Примеры:

Победители «Лучший дизайн карт Visa»

March 2011
Issuer: Alta Bank, Russia
Product Type: Visa Gold, Debit

February 2011
Issuer: Bank SinoPac, Taiwan
Product Type: Visa Signature, Credit

Банковские карты – дизайн

Примеры:

Победители «Лучший дизайн карт Visa»

October 2010
Issuer: Alta Bank, Russia
Product Type: Visa Electron, Debit

September 2010
Issuer: Ural Bank, Russia
Product Type: Visa Classic, Debit

Банковские карты – дизайн – MasterCard

Лицевая сторона карт MasterCard:

- *логотип “MasterCard”, представляющий собой два пересекающихся круга красного и желтого цветов с надписью “MasterCard” на их фоне*
- *голограмма “MasterCard” - присутствует на лицевой или оборотной стороне карты только в случае использования стандартной (не голографической магнитной полосы)*

MasterCard

Банковские карты – дизайн – MasterCard

Лицевая сторона карт MasterCard:

- *эмбоссированный номер карты, начинающийся с цифры “5” и состоящий из 16 цифр: “5XXX XXXX XXXX XXXX”*
- *имя держателя и срок действия карты нанесены путем эмбоссирования*
- *под номером карты типографским способом нанесен BIN, повторяющий первые 4 цифры номера*
- *карты могут быть с вертикальным расположением логотипа и названия банка-эмитента*

Банковские карты – дизайн – MasterCard

Оборотная сторона карт MasterCard:

- магнитная полоса – должна быть впаяна в пластик, а не наклеена

- если используется стандартная магнитная полоса, голограмма “MasterCard” размещается на лицевой или оборотной стороне карты

- магнитная полоса может быть голографической, в этом случае голограммы “MasterCard” не должно быть на карте

Банковские карты – дизайн – MasterCard

Оборотная сторона карт MasterCard:
- на панели для подписи под углом 45 градусов нанесен текст из повторяющихся слов «MasterCard”, написанный красным, желтым и синим цветами
- на панели для подписи, с наклоном в левую сторону, нанесены последние 4-е цифры номера карты
- код безопасности (CVC 2), нанесенный с наклоном в левую сторону, находится за пределами магнитной полосы, справа

Банковские карты – дизайн – Maestro

Любая операция по картам Maestro, независимо от суммы, должна быть авторизована только на Электронном терминале. Обслуживание карт Maestro с использованием импринтера запрещается. При операциях по картам Maestro обязательно введение держателем PIN-кода

Лицевая сторона карт Maestro:

Банковские карты – дизайн – Maestro

Лицевая сторона карт Maestro:

- логотип Maestro – два пересекающихся круга синего и красного цветов с надписью «Maestro» белого цвета, нанесенной на их фоне. Логотип размещается в правом верхнем или нижнем углу карты

- номер карты, имя держателя и срок действия - могут быть эмбоссированы или нанесены индент-печатью

- номер карты может состоять из 16-19 цифр, начинается на «50» или в диапазонах «56-58», «60-69»

- под номером карты типографским способом нанесен BIN, повторяющий первые 4 цифры номера карты

- срок действия карты указан всегда конечный – месяц/год (00/00). На картах Maestro, эмитированных европейскими банками, может быть указан срок действия «12/49»

Банковские карты – дизайн – Maestro

Лицевая сторона карт Maestro:

- имя и фамилия держателя карты написаны латинскими буквами. Имя и фамилия могут быть написаны кириллицей – в этом случае на карте должно быть указано «VALID ONLY IN RUSSIA»

- карта Maestro может быть двух видов: персонализированная (с именем держателя карты и сроком действия) и неперсонализированная (без имени держателя карты и срока действия);

- региональные карты имеют надпись “VALID ONLY IN (страна)” («Действительно только в …») и обслуживаются только в указанной стране

Банковские карты – дизайн – Maestro

Оборотная сторона карт Maestro:
- магнитная полоса – должна быть впаяна в пластик, а не наклеена
-панель для подписи – поле белого цвета, которое, по усмотрению банка-эмитента, может содержать орнамент или текст

На панели для подписи может присутствовать номер карты (или его последние четыре цифры), нанесенный с наклоном влево

- в нижней части карты могут располагаться логотипы обслуживающих систем, например, “Cirrus”, “Edc”

Банковские карты – дизайн – Diners Club

Карта выпускаются с различным дизайном и может быть как горизонтальной, так и вертикальной

Лицевая сторона карт Diners Club:
Логотип – торговая марка компании Diners Club International. Под ультрафиолетовым освещением виден логотип «Diners Club International»
На совместной карте «Diners Club International» и какого-либо партнера имя и логотип партнера наносятся в правом верхнем углу

Банковские карты – дизайн – Diners Club

Лицевая сторона карт Diners Club:

Номер Карты – начинается с "36" и состоит из 14 цифр, которые разделены на 3 группы, состоящие из четырех, шести и четырех цифр соответственно

Имя Держателя Карты – имя человека, который может использовать Карту

Отметка членства – состоит из двух цифр, которые указывают на год вступления в систему Diners Club International

Код франчайза – состоит из двух букв, которые присваиваются каждой стране Компанией Diners Club International

Срок действия – срок действия Карты указывается двумя датами: месяц/год начала и окончания срока

Банковские карты – дизайн – Diners Club

Лицевая сторона карт Diners Club:
Код безопасности – состоит из двух букв латинского алфавита, которые назначаются Компанией Diners Club International и является необязательным реквизитом
Чувствительность на ультрафиолетовые лучи – если посмотреть на освещенную ультрафиолетовыми лучами Карту Diners Club, то станет виден схематичный рисунок, похожий на логотип компании Diners Club International (штриховой круг, разделенный пополам вертикальной штрихованной полосой, при этом штрихи имеют наклон вправо)

Банковские карты – дизайн – Diners Club

Оборотная сторона карт Diners Club:
Магнитная полоса – это магнитная дорожка, расположенная на обратной стороне, в верхней части карты и содержащая в закодированном виде информацию о карточном счете, связанном с картой и предназначена для использования в Электронных терминалах
Панель подписи – содержит подпись Держателя Карты, имя которого указанно на лицевой стороне. При нанесении повреждений или стираний появляется слово VOID

Банковские карты – дизайн – Diners Club

Оборотная сторона карт Diners Club:
Лазерная печать – на панели для подписи лазерной печатью нанесен номера Карты, эмбоссированный на ее лицевой стороне, после которого указывается трехзначный номер CVV 2, утвержденный всеми международными Платежными системами с целью защиты Карт от подделок
Голограмма – объемное изображение торговой марки Diners Club International на развернутой карте мира, совмещенное с магнитной полосой
Кроме вышеперечисленного на карте может быть фотография Держателя карты, чип, логотип другой Торговой марки, конкретный регион, где принимается карта

Банковские карты – дизайн – Discover

Лицевая сторона карт Discover:
Логотип – торговая марка компании Discover
Под ультрафиолетовым освещением в центре карты проявляются слово «Discover»
Номер Карты – начинается с "6" и состоит из 16 цифр, которые разделены на 4 группы, состоящие из четырех цифр соответственно
Имя Держателя Карты – имя человека, который может использовать Карту

Банковские карты – дизайн – Discover

Лицевая сторона карт Discover:
Наименование Компании может быть проэмбоссировано ниже имени Держателя карты
Отметка членства – состоит из четырех цифр, которые указывают на месяц и год вступления в Платежную систему Discover
Срок действия – надпись “Valid Thru” обозначает дату окончания срока действия карты в формате MM/YY
Код безопасности (спецлитера) – характеризуется эмбоссированным значком, стилизованным как прописная заглавная буква «D»
Трехмерная голограмма – должна отражать свет и создавать ощущение изображений «в движении»

Банковские карты – дизайн – Discover

Оборотная сторона карт Discover:

Магнитная полоса – это магнитная дорожка, расположенная на обратной стороне, в верхней части карты и содержащая в закодированном виде информацию о карточном счете, связанном с картой и предназначена для использования в Электронных терминалах. Магнитная полоса должна быть гладкой, без признаков постороннего вмешательства

Панель для подписи - содержит подпись Держателя Карты, имя которого указанно на лицевой стороне. При нанесении повреждений или стираний появляется слово VOID. На панели для подписи располагается текст под наклоном из повторяющихся слов “Discover Network”

Банковские карты – дизайн – Discover

Оборотная сторона карт Discover:

Лазерная печать – на панели для подписи лазерной печатью нанесены последние 4 цифры номера Карты, эмбоссированный на ее лицевой стороне, после которого указывается трехзначный номер CID, утвержденный международной Платежной системой с целью защиты карт от подделок

Голограмма – объемное изображение земного шара, совмещенное с магнитной полосой (допускается ее отсутствие)

Логотип - Торговая марка компании Discover

Банковские карты – дизайн – China UnionPay – Дебетовые карты CUP

Лицевая сторона карт China UnionPay:

В верхней части карты: название банка–эмитента, на китайском и английском языках, и логотип банка-эмитента

Ниже расположена строка, содержащая надпись на китайском языке (иероглифы) и надпись на английском языке – DEBIT CARD

В средней части карты расположен номер карты, состоящий из 19 цифр, сгруппированных в пропорции 4-4-4-4-3. Группы номеров разделены пробелами. Номер карты (19 цифр) может быть напечатан также без пробелов. Номер карты должен быть напечатан типографским способом, контрастной цвету карты краской

Банковские карты – дизайн – China UnionPay – Дебетовые карты CUP

Лицевая сторона карт China UnionPay:
Цифры номера карты должны иметь одинаковый размер, располагаться строго на одном уровне, не должны быть каким-либо образом изменены (исправлены, подклеены и т.п.) и не должны стираться
В следующей, ниже расположенной строке латинским шрифтом может быть указано имя и фамилия держателя карты (опционно), а также срок (месяц/год) по который может использоваться карта
Логотип Платежной системы изображен в виде трехцветного прямоугольника, содержащего наклонные полосы красного, синего и зеленого цветов, на фоне которых изображены две группы иероглифов, которые выполнены белым цветом

Банковские карты – дизайн – China UnionPay – Дебетовые карты CUP

Лицевая сторона карт China UnionPay:
Может присутствовать надпись – UnionPay
Логотип расположен в нижнем правом углу карты
Логотип наносится специальным типографским способом под верхний защитный слой поверхности карты, поэтому не стирается, не отслаивается и не шелушится
В нижней строке карты может присутствовать надпись, сделанная латинскими буквами – ELECTRONIC USE ONLY

Банковские карты – дизайн – China UnionPay – Дебетовые карты CUP

Оборотная сторона карт China UnionPay:
Магнитная полоса, которая впаивается в пластик и содержит закодированные данные, записанные электронным способом. Она не должна отслаиваться или иметь видимых повреждений
Под магнитной полосой расположена панель для подписи держателя карты, которая сделана из сверхчувствительного гладкого материала. На панели, с наклоном вправо, наносятся цветные полосы, содержащие надписи в виде иероглифов. Справа от панели наносится группа иероглифов и надпись в двух уровнях – AUTORIZED SIGNATURE. На панели должна присутствовать подпись держателя карты (без исправлений и признаков стирания)

Банковские карты – дизайн – China UnionPay – Дебетовые карты CUP

Оборотная сторона карт China UnionPay:
Далее (ниже) расположены строки, содержащие надписи на китайском языке, иероглифы
В нижней части карты может быть расположена овальной формы рамка, в которой имеются надписи на китайском языке (иероглифы), может быть указан контактный телефон, а также название сайта банка эмитента
В правом нижнем углу карты может располагаться (опционально) рамка прямоугольной формы, в границах которой наносится логотип эмитента кредитной карты, либо, как правило, изображается Великая китайская стена и присутствует надпись: GREATWALL CARD

Банковские карты – дизайн – China UnionPay – Кредитные карты CUP

Лицевая сторона карт China UnionPay:
В верхней части карты: название банка-эмитента, на китайском и английском языках, и логотип банка-эмитента
Ниже расположена строка, содержащая надпись на китайском языке (иероглифы)
В средней части карты расположен номер карты, состоящий из 16 цифр, сгруппированных в пропорции 4-4-4-4 и разделенных пробелами. Номер карты должен быть выполнен тиснением, проэмбоссирован. Цифры номера карты не должны быть каким-либо образом изменены (исправлены, подклеены и т.п.), иметь одинаковый размер, расположены строго на одном уровне и не должны стираться

Банковские карты – дизайн – China UnionPay – Кредитные карты CUP

Лицевая сторона карт China UnionPay:
Под выполненным тиснением номером карты, справа, расположена, изготовленная с применением лазера, голограмма CUP Card, на которой горизонтально, построчно изображены двухцветные группы иероглифов, приведен голографический символ (торговая марка) Платежной системы CUP, а также трехмерное, объемное изображение Божественного храма
В следующей, нижерасположенной строке, также тиснением, указываются месяц/год, т.е. срок, по который может использоваться карта и должны присутствовать типографским образом выполненные надписи: VALID THRU и MONTH/YEAR

Банковские карты – дизайн – China UnionPay – Кредитные карты CUP

Лицевая сторона карт China UnionPay:
Логотип Платежной системы CUP изображен в виде трехцветного прямоугольника, содержащего наклонные полосы красного, синего и зеленого цветов, на фоне которых изображены две группы иероглифов и присутствует надпись – UnionPay, которые выполнены белым цветом. Логотип расположен в нижнем правом углу карты. Логотип наносится специальным типографским способом под верхний защитный слой поверхности карты, поэтому не стирается, не отслаивается и не шелушится
В нижней строке латинским шрифтом (тиснением) должны быть указаны имя и фамилия держателя карты

Банковские карты – дизайн – China UnionPay – Кредитные карты CUP

Оборотная сторона карт China UnionPay:
Магнитная полоса, которая впаивается в пластик и содержит закодированные данные, записанные электронным способом. Она не должна отслаиваться или иметь видимых повреждений
Под магнитной полосой расположена панель для подписи держателя карты, которая сделана из сверхчувствительного гладкого материала. На панели с наклоном вправо наносятся цветные полосы, содержащие надписи в виде иероглифов. Справа от панели наносится группы иероглифов и надпись в двух уровнях – AUTORIZED SIGNATURE. На панели должна присутствовать подпись держателя карты (без исправлений и признаков стирания)

Банковские карты – дизайн – China UnionPay – Кредитные карты CUP

Оборотная сторона карт China UnionPay:
Далее (ниже) расположены строки, содержащие надписи на китайском языке, иероглифы
В правом нижнем углу карты может располагаться (опционально) рамка прямоугольной формы, в границах которой наносится логотип эмитента кредитной карты, либо, как правило, изображается Великая китайская стена и присутствует надпись: GREATWALL CARD

Банковские карты – дизайн – JCB

Лицевая сторона карт JCB:

- в центре карты – надпись JCB CARD. Может быть указано название дочерней компании JCB или название компании, совместно с которой выпускается карта

- цвет, фон или название карты могут меняться

- логотип Платежной системы – стилизованная надпись JCB на полосах синего, красного и зеленого цветов, причем каждая буква располагается на отдельной полосе. Полосы окружены прямоугольником с закругленными углами белого цвета. В нижней части прямоугольника расположена надпись JCB Card. На картах нового дизайна логотип расположен под голограммой, на картах старого дизайна логотип напечатан внутри голограммы

Банковские карты – дизайн – JCB

Лицевая сторона карт JCB:

- голограмма Платежной системы JCB располагается в правой части карты в центре в виде объемного зеркального изображения солнца, выглядывающего из-за планеты Земля. При рассмотрении карты под разными углами изображение меняется – солнце скрывается, остается только дуга планеты. Голограмма впаивается в поверхность карты специальным способом и не должна стираться или отслаиваться по краям

- номер карты в первой проэмбоссированной строке на карте, который состоит из 16, сгруппированных по четыре цифры (4-4-4-4). Последняя группа цифр номера карты должна быть эмбоссирована на голограмме. Цифры номера карты не должны быть каким-либо образом изменены (исправлены, подклеены и т.п.)

Банковские карты – дизайн – JCB

Лицевая сторона карт JCB:

- четыре, пять или шесть цифр, которые совпадают с первыми цифрами эмбоссированного номера карты, и должны быть напечатаны типографским способом контрастной цвету карты краской под первыми цифрами проэмбоссированного номера карты. Цифры не должны стираться

- вторая проэмбоссированная строка содержит срок действия карты в формате месяц/год с апострофом после косой черты (например, 10/’12)

- на картах должен присутствовать эмбоссированный символ J

- имя и фамилия Держателя карты, проэмбоссированные латинским шрифтом третьей строкой

Банковские карты – дизайн – JCB

Оборотная сторона карт JCB:

- магнитная полоса, которая впаивается в пластик и содержит номер карты и дополнительные закодированные данные, записанные электронным способом. Она не должна отслаиваться или иметь видимых повреждений

- панель для подписи Держателя карты, которая может быть расположена в любом месте на оборотной стороны и сделана из сверхчувствительного гладкого материала светло-голубого и зеленого фона

К обслуживанию могут быть приняты не-эмбоссированные карты JCB, у которых номер карты, срок действия, защитный символ, данные держателя карты выгравированы на карте. Данные карты обслуживаются только через Электронные терминалы

Банковские карты – карты с магнитной полосой - стандарты

ISO/IEC 7810 “Карточки идентификационные. Физические характеристики”:

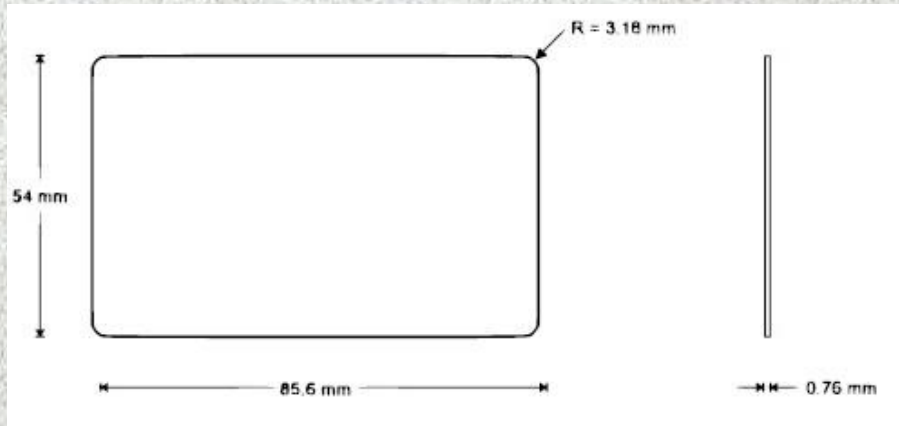
ID-1 - определяет общепринятые размеры и форму карты:

ширина - 85,595 ±0,125мм

высота - 53,975 ±0,055мм

толщина - 0,76 ±0,008мм

радиус окружности в углах прямоугольника – 3,18мм



Банковские карты – карты с магнитной полосой - стандарты

ISO/IEC 7810: карта должна состоять из поливинилхлорида, ацетата поливинилхлорида или материалов, имеющих равные или лучшие характеристики

Требования к деформации: после того, как одна сторона будет изогнута вверх на 35мм, она должна возвращаться в первоначальное плоское состояние с отклонением в пределах 1,5мм

Банковские карты – карты с магнитной полосой - стандарты

ISO/IEC 7811 "Карточки идентификационные. Метод записи" – устанавливает способы кодирования информации при помощи методов тиснения (эмбоссирования) и записи магнитной полосы

Спецификация делится на 5 частей:

- *тиснение (метод записи)*
- *магнитная полоса (метод записи)*
- *расположение символов при тиснении на карте ID-1*
- *расположение магнитных дорожек, доступных только для чтения (дорожки 1 и 2)*
- *расположение магнитных дорожек, доступных для чтения/записи (дорожка 3)*

Банковские карты – карты с магнитной полосой - стандарты

ISO/IEC 7812 “Карточки идентификационные. Система нумерации” и ISO/IEC 4909 “Карточки банковские. Карточки для финансовых операций”:
Номер карты совпадает с номером счёта (Primary Account Number - PAN)

PAN имеет длину не более 19 десятичных цифр
Состоит из:
- Issuer Identification Number (IIN)
- Идентификационного номера счёта
- Проверочного символа

Банковские карты – карты с магнитной полосой - стандарты

IIN состоит из 6 цифр, первая из которых определяет отраслевую принадлежность эмитента карты:

0 – зарезервировано на будущее
1 – авиалинии
2 – авиалинии и будущие отрасли
3 – туризм и развлечения
4 – банковские/финансовые операции
5 – банковские/финансовые операции
6 – торговые/банковские операции
7 – автозаправочные операции
8 – телекоммуникации и будущие отрасли
9 – определяется национальными органами стандартизации

Банковские карты – карты с магнитной полосой - стандарты

ISO/IEC 7811-2 – определяет методы записи, используемые для кодирования информации на магнитной полосе карты

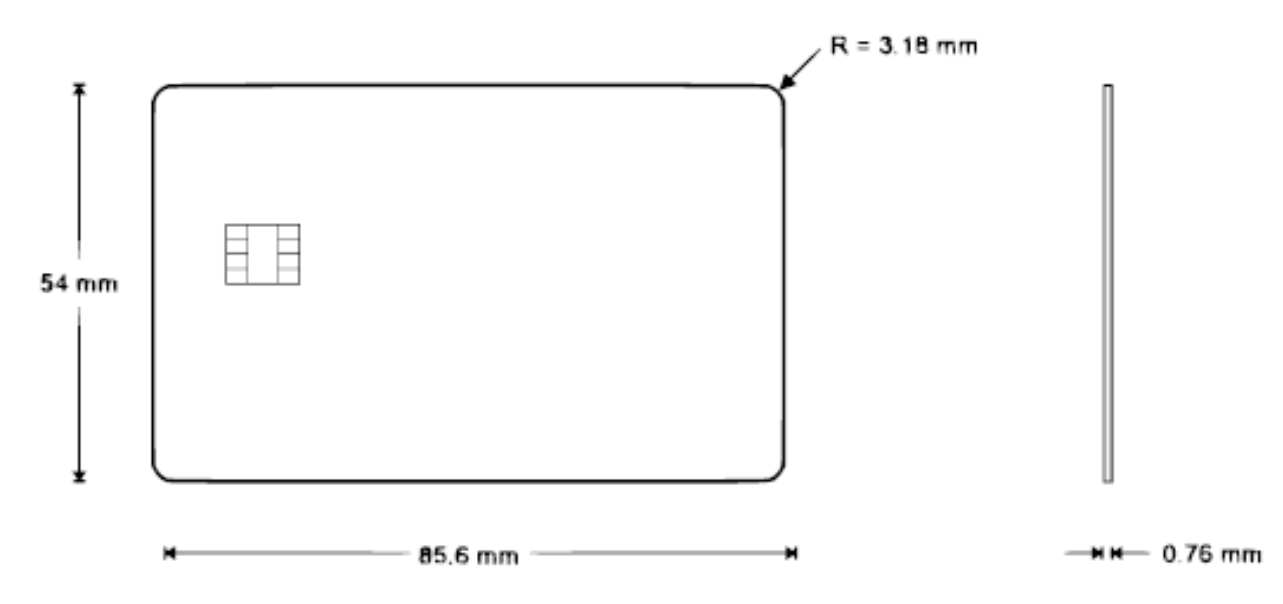
ISO/IEC 7813 – определяет форматы первой и второй дорожек магнитной полосы

ISO/IEC 4909 – определяет формат третьей дорожки магнитной полосы

Банковские карты – карты с чипом- стандарты

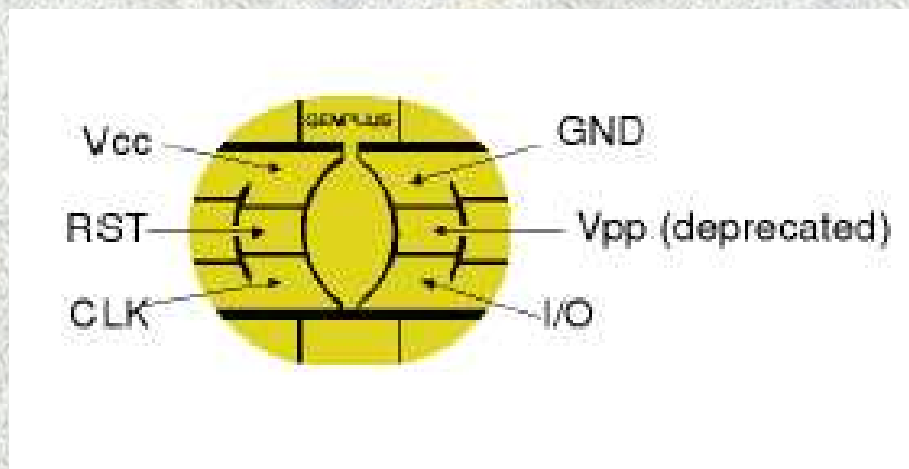
ISO/IEC 7816-1 – определяет размеры и форму карты

ISO/IEC 7816-2 – определяет положение контактов



Банковские карты – карты с чипом- стандарты

ISO/IEC 7816-3 – определяет электрические характеристики и протокол передачи



Банковские карты – карты с чипом- виды

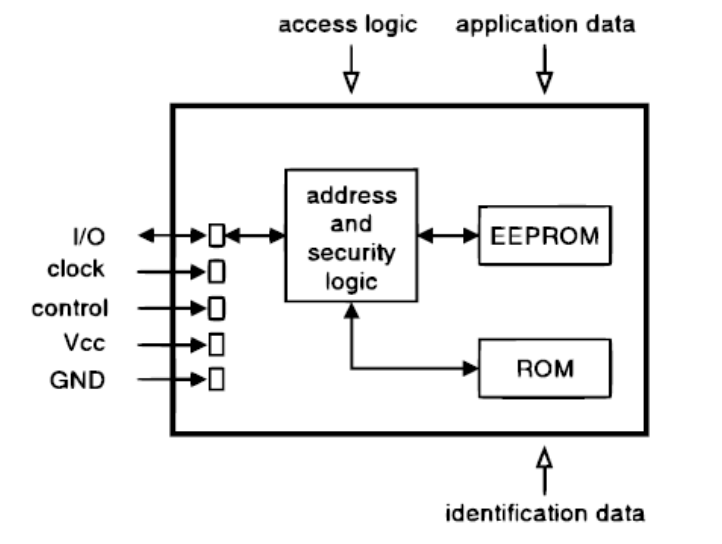
Чиповые карты бывают:

1. *Карты памяти*
2. *Микропроцессорные карты*

Банковские карты – карты с чипом- виды – карты памяти

Карты памяти – исторически первые чиповые карты - используются для множества сфер, например, телефонные карты

Архитектура карт памяти:



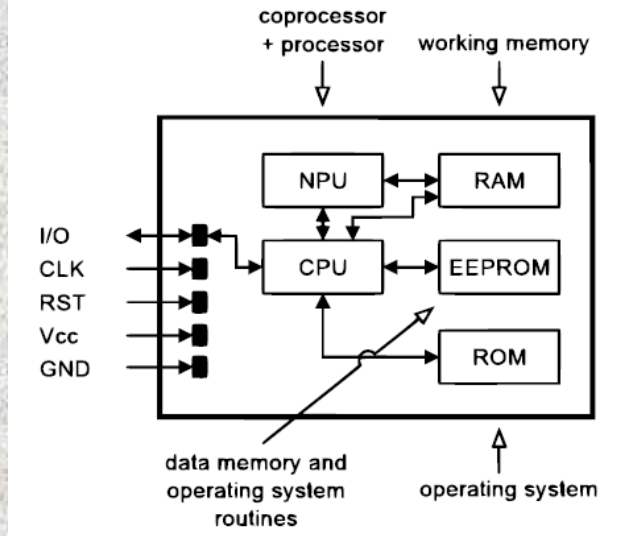
EEPROM – Erasable Electrically Programmable Read Only Memory

ROM – Read Only Memory

Банковские карты – карты с чипом- виды – микропроцессорные карты

Микропроцессорные карты – используются, например, для банковской сферы

Архитектура микропроцессорных карт:



RAM – Random Access Memory
EEPROM – Erasable Electrically Programmable Read Only Memory
ROM – Read Only Memory
NPU – Numeric Processing Unit
CPU – Central Processing Unit

Банковские карты – бесконтактные карты

Бесконтактные карты – те же чиповые, но используют другой коммуникационный интерфейс

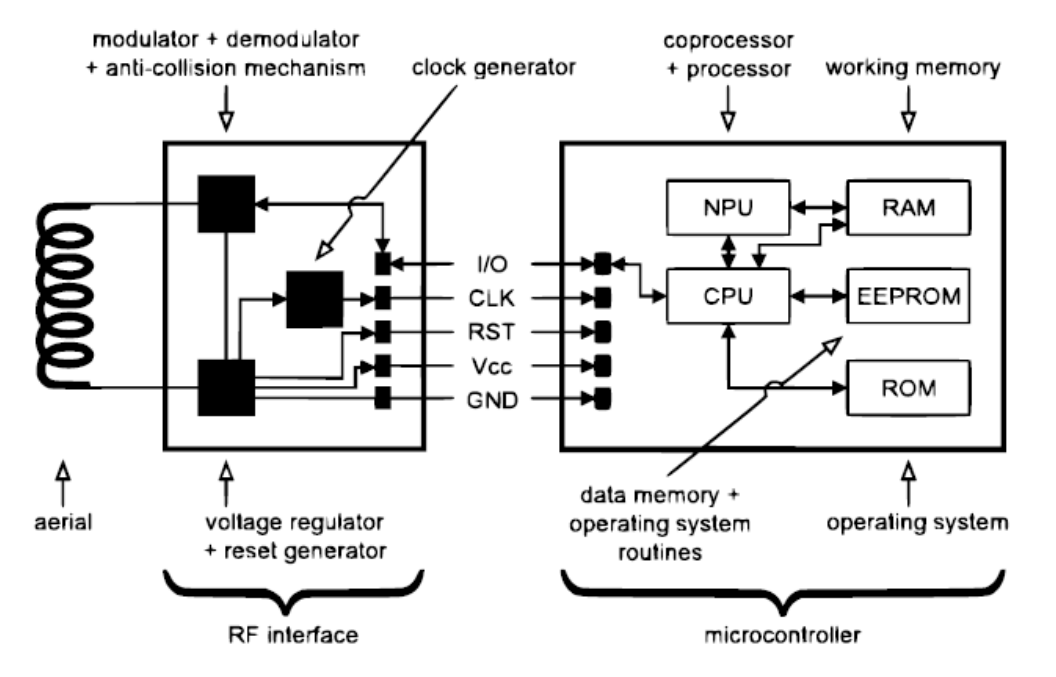
ISO/IEC 14443 – определяет бесконтактный интерфейс и протокол обмена

Банковские карты – бесконтактные карты

Применение бесконтактных технологий:

Банковские карты – бесконтактные карты

Архитектура бесконтактных карт:



RAM – Random Access Memory
EEPROM – Erasable Electrically Programmable Read Only Memory
ROM – Read Only Memory
NPU – Numeric Processing Unit
CPU – Central Processing Unit

Банковские карты – бесконтактные карты – комбинированные, дуальные

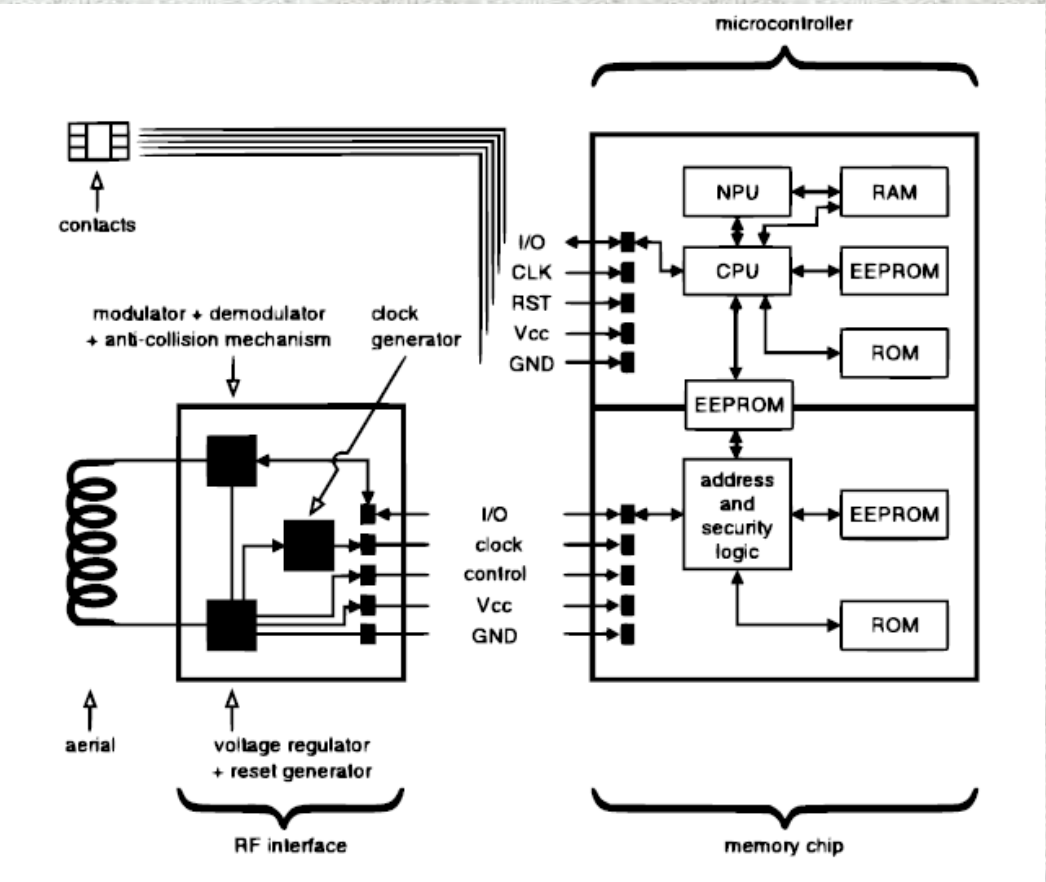
Комбинированные карты – на одном пластике фактически две карты – чиповая и бесконтактная (память и приложения на них - раздельные)

Дуальные карты – на одном пластике к памяти и приложениям имеется два интерфейса – чиповый и бесконтактный

Бывает и более сложная архитектура – например, два чипа, используемой общей областью памяти, но разными приложениями

Банковские карты – бесконтактные карты – комбинированные, дуальные

Пример архитектуры:



Банковские карты – карты с чипом- стандарты - EMV

1996 – появился стандарт EMV (Europay, Mastercard, VISA) – отраслевой стандарт, регламентирующий работу с микропроцессорной картой, используемой для безналичных расчётов

Карты стандарта EMV различных платёжных систем:

- *VSDC — VISA;*
- *MChip — MasterCard;*
- *AEIPS — American Express;*
- *J Smart — JCB*

Банковские карты – бесконтактные карты

Бесконтактные карты различных платёжных систем:

Организация	Брэнд
VISA	Visa payWave
MasterCard	paypass
	express pay
DISCOVER	zip

Банковские карты – эмитенты и эквайеры

Примеры банков, выпускающих и принимающих в эквайринговых сетях карты различных платёжных систем:

- Русский Стандарт

Сведения об эмиссии и эквайринге банковских карт

Система расчетов	Эмиссия	Эквайринг
American Express	+	+
China UnionPay		+
DINERS CLUB	+	+
JCB International		+
MasterCard Int.	+	+
VISA International	+	+
Золотая Корона		+
Русский Стандарт	+	+

Банковские карты – эмитенты и эквайеры

Примеры банков, выпускающих и принимающих в эквайринговых сетях карты различных платёжных систем:

- Газпромбанк

Сведения об эмиссии и эквайринге банковских карт

Система расчетов	Эмиссия	Эквайринг
China UnionPay		+
MasterCard Int.	+	+
VISA International	+	+
Авточип	+	
Золотая Корона		+
Объединенная расчетная система	+	+
Специальная локальная карта Газпромбанка	+	

Банковские карты – эмитенты и эквайеры

Примеры банков, выпускающих и принимающих в эквайринговых сетях карты различных платёжных систем:

- Росбанк

Сведения об эмиссии и эквайринге банковских карт

Система расчетов	Эмиссия	Эквайринг
American Express		+
China UnionPay		+
JCB International		+
MasterCard Int.	+	+
VISA International	+	+
Золотая Корона		+
Объединенная расчетная система	+	+
РОСБАНК	+	+
Таможенная карта	+	

Банковские карты – эмитенты и эквайеры

Примеры банков, выпускающих и принимающих в эквайринговых сетях карты различных платёжных систем:

- Сбербанк

Сведения об эмиссии и эквайринге банковских карт

Система расчетов	Эмиссия	Эквайринг
American Express	+	+
DINERS CLUB		+
MasterCard Int.	+	+
VISA International	+	+
ЕПСС УЭК	+	+
Программа DUET	+	+

Оборудование для приёма карт

Банковские карты могут приниматься следующими устройствами:

- *Импринтеры*
- *Пин-пады*
- *EFTPOS-терминалы*
- *Киоски самообслуживания*
- *Банкоматы*

EFTPOS – Electronic Funds Transfer at Point of Sale

Оборудование для приёма карт-электронные устройства для оплаты – классификация

Электронные устройства приёма банковских пластиковых карт для оплаты товаров и услуг:

- *Настольные EFTPOS-терминалы*
- *Переносные и мобильные EFTPOS-терминалы*
- *Банковские пин-пады*
- *Ритейловые пин-пады*
- *Ритейловые пин-пады с функцией ввода подписи*
- *Бесконтактные ридеры*
- *Встраиваемые устройства*

Оборудование для приёма карт

Настольные EFTPOS-терминалы:

Оборудование для приёма карт

Переносные и мобильные EFTPOS-терминалы:

Оборудование для приёма карт

Банковские пин-пады:

Оборудование для приёма карт

Ритейловые пин-пады:

Оборудование для приёма карт

Ритейловые пин-пады с функцией ввода подписи:

Оборудование для приёма карт

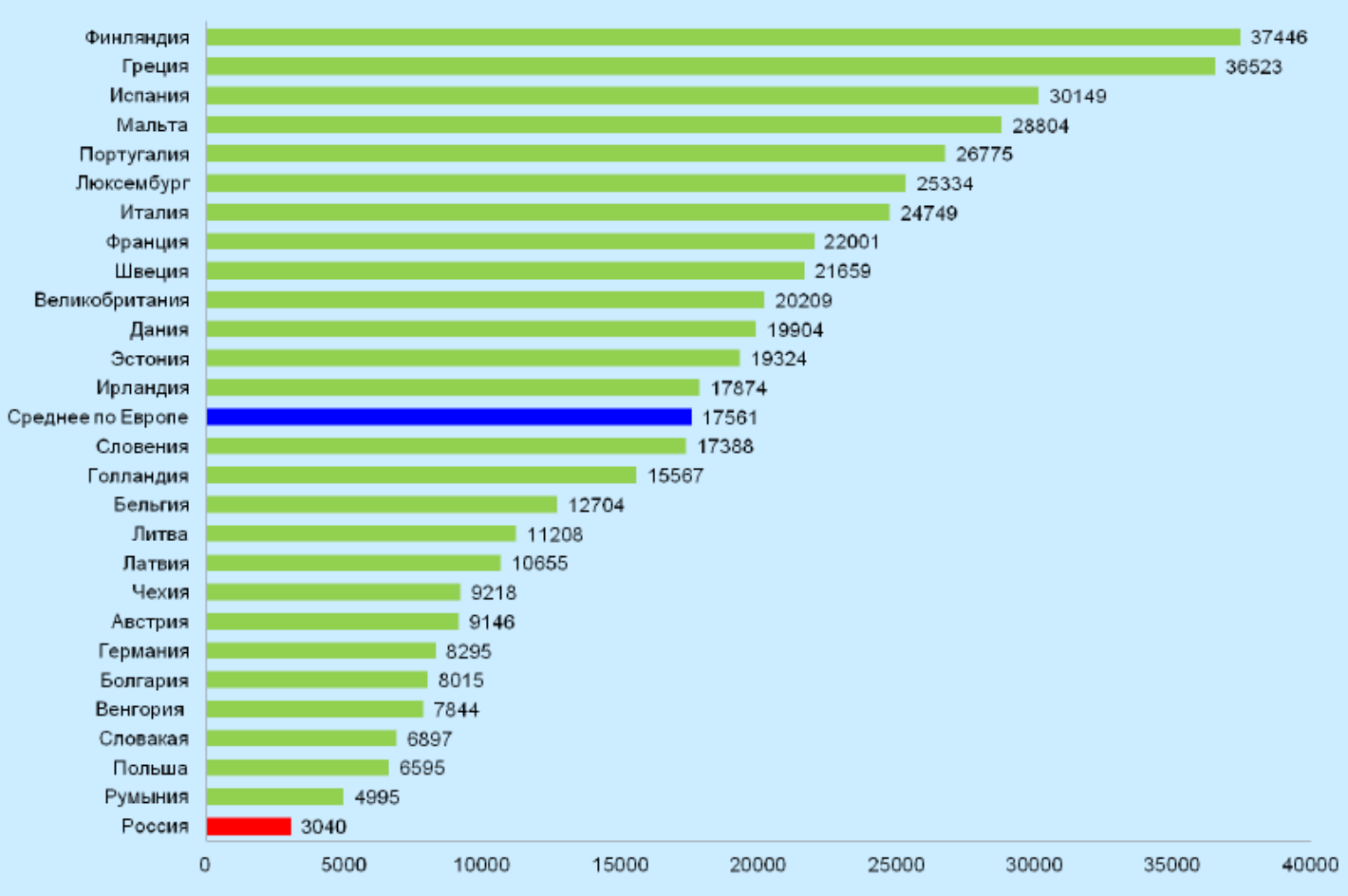
Бесконтактные ридеры:

Оборудование для приёма карт

Встраиваемые устройства:

Оборудование для приёма карт

Количество EFTPOS-терминалов и пин-падов на миллион населения в странах ЕС и в России в 2010:



Оборудование для приёма карт – современность

По данным ЦБ РФ на III квартал 2012 года в России в организациях торговли и сервиса установлено 654 952 электронных терминала

Хосты и протоколы

Вендоры процессингов и их решения:
- ACI Worldwide (США) – Base24
- Card Tech Limited (CTL, Великобритания) – CTL
- Compass Plus (Россия) – TranzWare
- OpenWay (Бельгия) – Way 4
- TietoEnator (Латвия) – TietoEnator
- Банковский Производственный Центр (БПЦ, Россия) – SmartVista
- Рукард (Россия) – Софит
- Программные Системы и Технологии (ПСИТ, Россия) – 3Card-F
- FIS (США) – Cortex
…

Хосты и протоколы

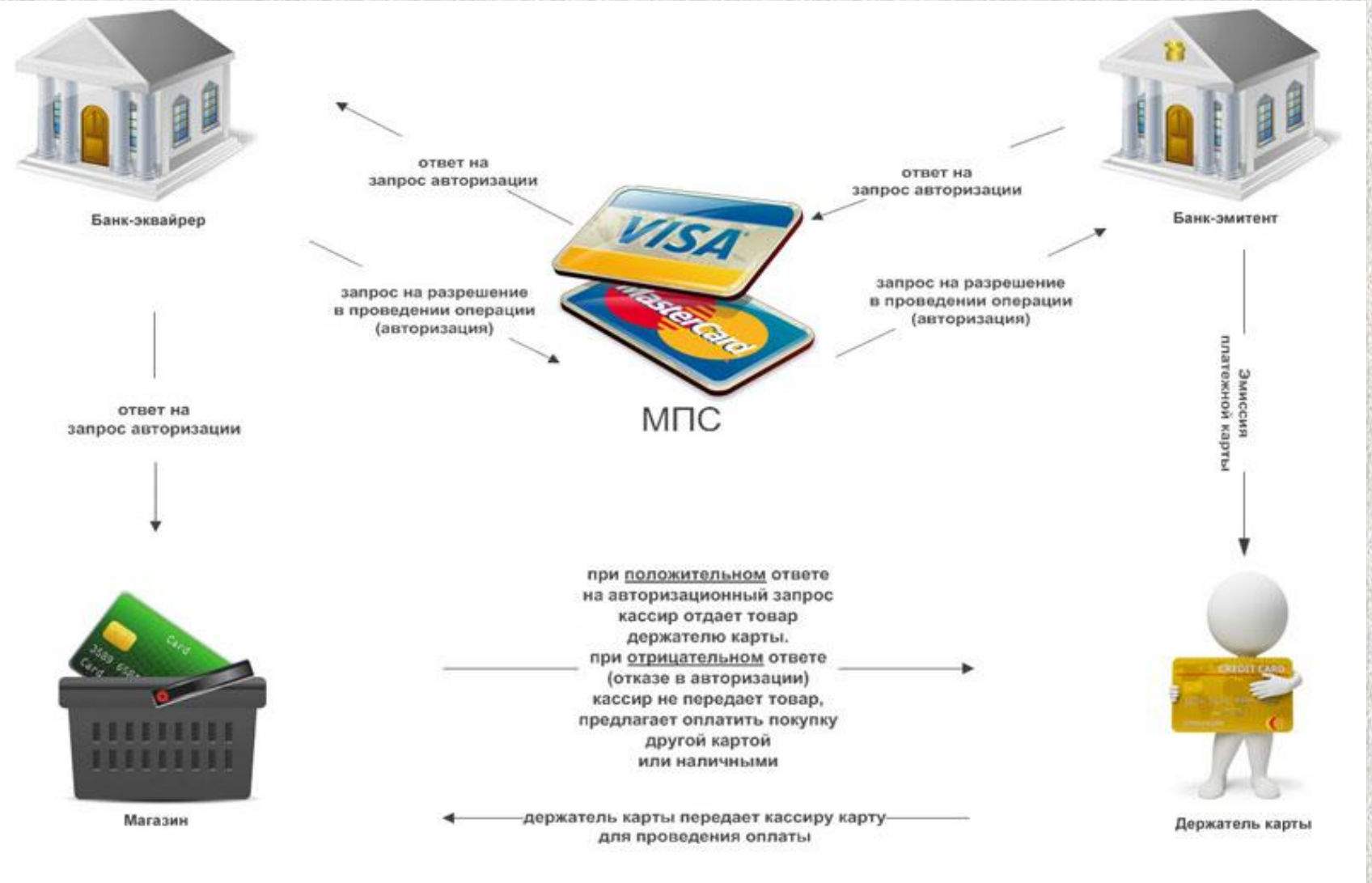
Протоколы обмена с терминалами и пин-падами:

- *ISO8583*
- *SPDH*
- *VISA II*
- *APACS 30*
- *APACS 40*
- *APACS 50*

…

В России чаще всего используются различные диалекты ISO8583, иногда – SPDH

Эквайринг- стандартная схема:



Эквайринг

Регламентирующие документы международных платёжных систем:

VISA	MasterCard
Visa International Operating Regulations (10 апреля 2011)	MasterCard Rules (15 июля 2011)
Visa International Certificate of Incorporation and By-Laws (2007)	Maestro Global Rules (25 февраля 2011)
Visa CEMEA Fee Guide (декабрь 2010)	MasterCard Consolidated Billing System (Europe Region NON-SEPA) (17 сентября 2010)

Эквайринг

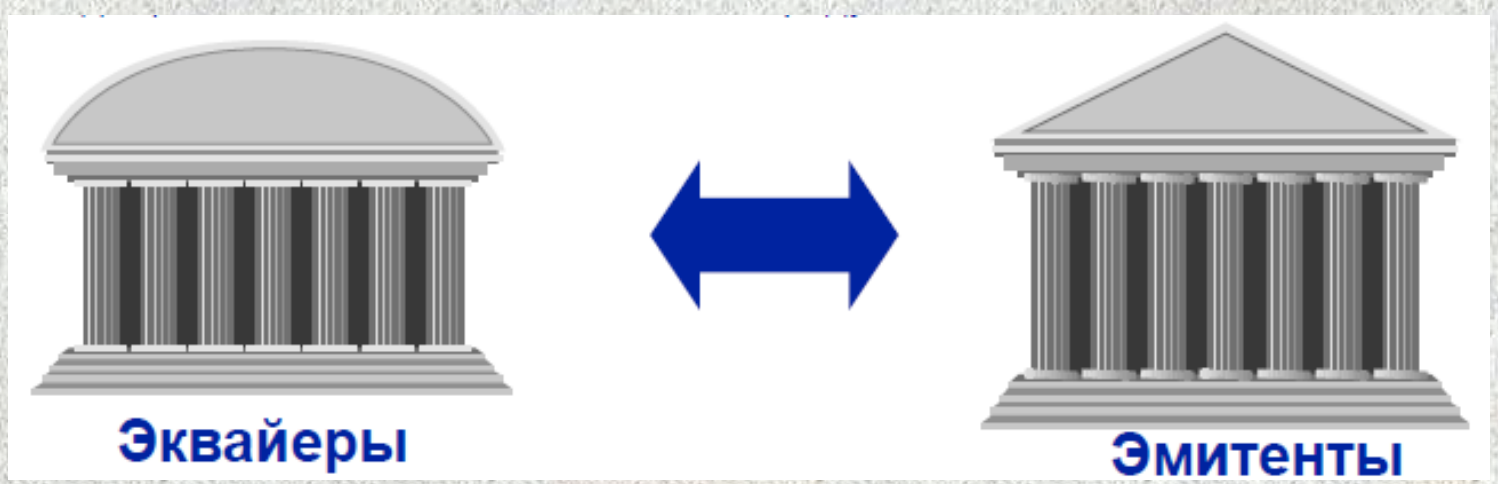
Разделение регионов международных платёжных систем:

VISA	MasterCard
08 - USA	1 - USA
07 - Canada	A - Canada
05 - Latin America/Caribbean	B - Latin America/Caribbean
04 - Asia/Pacific Region	C - Asia/Pacific Region
Europe	D – Europe: 1 **Single European Payments Area** SEPA 2 Intra-Western Europe 3 Intra-Eastern Europe - **RUSSIA**
06 - CEMEA *(Central and Eastern Europe, Middle East and Africa Region)* - **RUSSIA**	E - South Asia/Middle East/Africa

Эквайринг – межбанковская комиссия

Межбанковская комиссия — это комиссия, которой обмениваются между собой финансовые учреждения — эмитенты и эквайеры при каждой операции, проходящей с использованием платёжных продуктов Visa

Межбанковская комиссия — это комиссионные платежи, осуществляемые между двумя участниками платёжной системы и не является доходом платежной системы



Эквайринг – межбанковская комиссия

- Межбанковская комиссия устанавливается платёжной системой в целях поддержания баланса взаимной заинтересованности между банком-эмитентом банковской карты (обслуживающим держателя карты), и банком-эквайером (принимающим и обрабатывающим транзакции Visa по договору с торгово-сервисным предприятием)
- Эквайер платит эмитенту межбанковскую комиссию за каждую транзакцию по оплате приобретенного товара или услуги по карте. Эмитент платит эквайеру за каждую транзакцию с использованием банкомата
- При транзакциях по возврату межбанковская комиссия проходит в «обратном» направлении

Эквайринг – межбанковская комиссия

Межбанковская комиссия:

Доход Банка-эмитента (А)	Доход Банка-эквайера (Б)
Выдача наличных	
+ комиссия с клиента за выдачу наличных	+ комиссия с банка-эмитента
Оплата товаров и услуг	
+ комиссия с банка-эквайера	+ комиссия с торговой точки

Эквайринг – межбанковская комиссия

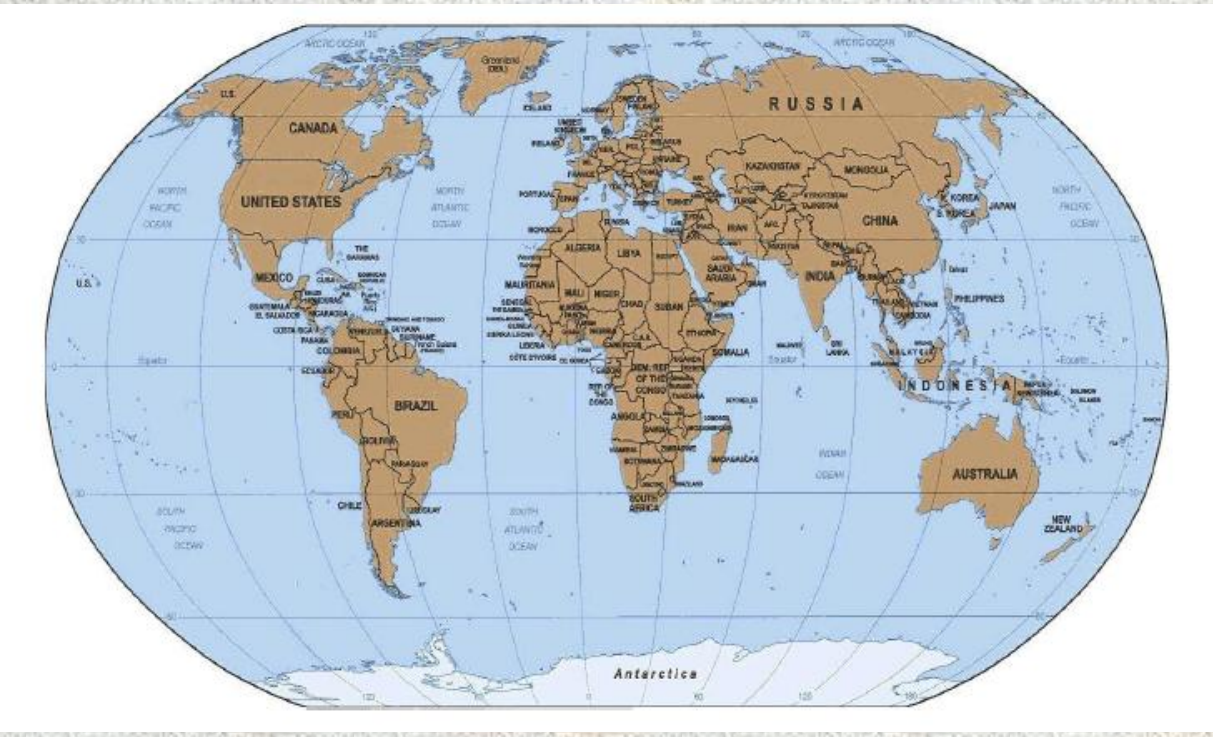
Межбанковская комиссия зависит от:

- Типа продукта (например, статусу карты)

- Категории транзакции

- Категории торговой точки

- Местонахождения эмитента и эквайера



Эквайринг – межбанковская комиссия

Категория транзакции:

VISA	MasterCard
Electronic (100% online авторизация)	**Enhanced Electronic** (100% online авторизация)
Standard (Paper-based transactions)	**Base** (Paper-based transactions)
eCommerce	**Merchant UCAF**
Chip Terminal	**Chip Terminal**
Chip full data	**Full Chip**
Chip Issuer	**Chip Card**
Small ticket transaction (≤1 000 руб.)	**Low value Payment** (≤900 руб.)

UCAF – Universal Cardholder Authentication Field

Эквайринг – межбанковская комиссия

Категория торговой точки:

Supermarket (MCC 5411)
Utilities (MCC 4900) (Electric, Gas, Water, and Sanitary)
Airline (MCC 3000 – 3299, 4511)
Recurring Payment (MCC 6012)
Petrol (MCC 5541, 5542)
Telecommunications Services (MCC 4814)

MCC – Merchant Category Code

Эквайринг – межбанковская комиссия

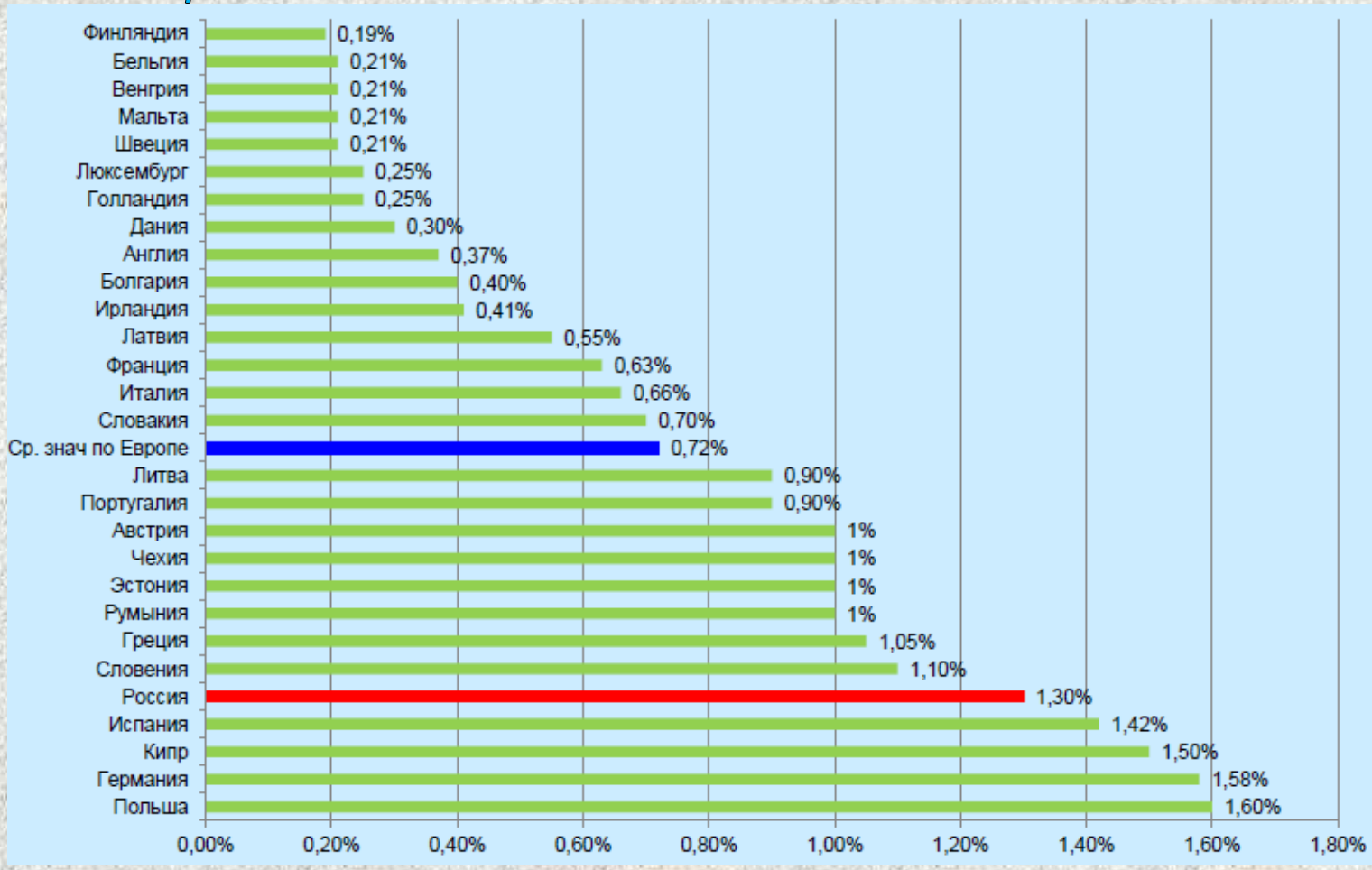
Местонахождение эмитента и эквайера:

Эмитент	Эквайер	Уровень
Россия	Россия	**National**
Россия	CEMEA	**INTRA** regional (или INTRA CEMEA)
CEMEA	Canada	**INTER** regional

MCC – Merchant Category Code

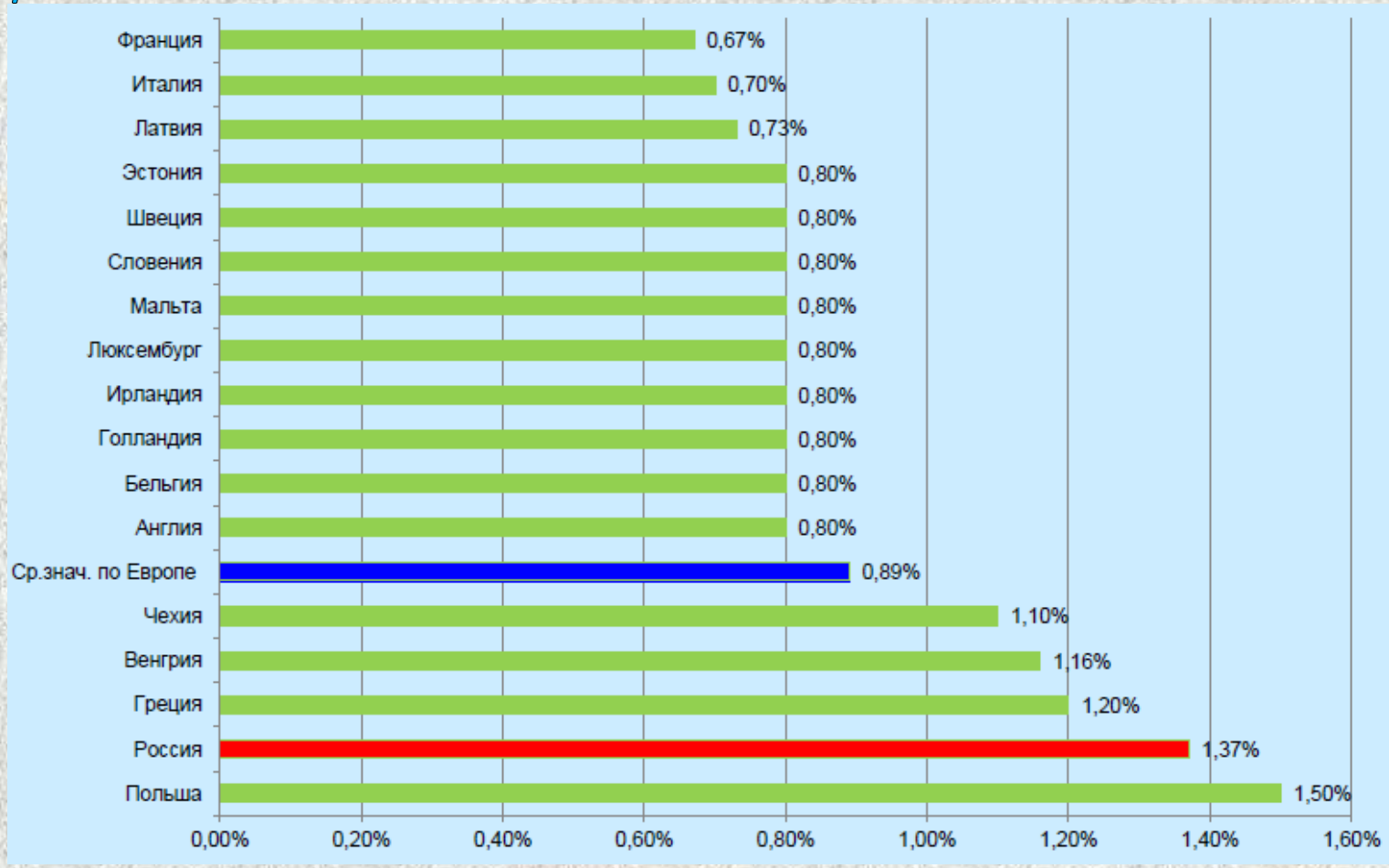
Эквайринг – межбанковская комиссия

Размер межбанковской комиссии по чиповым картам VISA в странах ЕС и в России:



Эквайринг – межбанковская комиссия

Размер межбанковской комиссии по картам MasterCard в странах ЕС и в России:



Эквайринг – торговая уступка

Торговая уступка – это комиссия за обслуживание торговых точек

Позиции, включаемые в торговую уступку в некоторых странах Европы:

	Бельгия	Дания	Франция	Германия	Италия	Нидерланды	Португалия	Испания	Велико-британия
Установка терминала / заявка на установку терминала	да	да	да	нет	нет/да	да	да	да	нет
Ежегодная / ежемесячная комиссия	нет	нет	да	нет	нет	нет	нет	да	нет
Минимальная ежемесячная комиссия	нет	да	да	нет	нет/да	да	да	да	нет
Терминал	нет	нет	нет	нет	нет/да	нет	Нет данных	да	нет
Поддержка терминала	нет	нет	нет	нет	нет/да	нет	Нет данных	да	нет
Телекоммуникации	нет	нет	нет	нет	нет	нет	нет	да	нет
Выписки	да	да	да	да	да	да	да	да	да
Расходные материалы	нет	нет	да	нет	нет	нет	нет/да	да	нет
Голосовая авторизация	да	да	да	нет	да	Нет данных	да	да	нет
Обслуживание за опротестование транзакций	да	да	нет	нет	да	да	да	да	нет
Плата за превышение уровня опротестований транзакций совершенных в ТСП	да	да	нет	нет	да	Нет данных	да	да	нет
Выписка счетов	нет	да	Нет данных	нет	да	нет	нет	Нет данных	да

Эквайринг – торговая уступка

- Торговая уступка отражает общую стоимость обслуживания ТСП для эквайера
- Размер торговый уступки может определяться с учётом стратегических приоритетов банка-эквайера и характера его отношений с торгово-сервисным предприятием
- Размер торговой уступки в значительной мере определяется конкуренцией на рынке предоставления эквайринговых услуг
- Ставка торговой уступки зависит от технических и иных требований к эквайрингу со стороны торгово-сервисного предприятия

Эквайринг – схема работы

Пример взаимодействия:

Эквайринг – факты – Россия

1. По безналичному расчёту совершается:
   - в Ашан – более 10% покупок
   - в “Ленте” – 18% покупок
2. Средний чек тех клиентов, которые начали платить картами, вырос примерно:
   - в Metro Cash & Carry – на 20%
   - в “Пятёрочках” – на 30%
   - в супермаркетах и гипермаркетах X5 – на 10%

Комиссии международных платёжных систем с банков – VISA

Комиссии VISA:

Наименование комиссии	Значение
GENERAL FEES	
VisaNet indirect access fee	1 500 USD ежемесячно
Annual active BIN license fee	1 000 USD ежегодно
Annual inactive BIN license fee	5 000 USD ежегодно
Global Customer Assistance Service (GCAS) Fees - Emergency card replacement (Electron, Classic/Gold и выше) - Emergency cash disbursement - Cardholder Inquiry Service/Visa Assistance Centre	 225/250 USD за запрос 175 USD за запрос 7,5 USD за запрос
Card Design Review Fees	200 USD единовременно

Комиссии международных платёжных систем с банков – MasterCard

Комиссии MasterCard с Аффилиата:

Наименование комиссии	Значение
Единовременные	
ADDITIONAL BIN ASSIGNMENT	250 EUR
SI RANGE BLOCKING SETUP	100 EUR (range)
Ежегодные	
Merchant Acquiring Risk Management Fee	10 000 EUR (с разбивкой на поквартальные платежи)
Ежеквартальные	
MATCH Quarterly Subscription	875 USD
Ежемесячно	
BIN Management – Active	8 EUR за БИН

Комиссии международных платёжных систем с банков – MasterCard

Комиссии MasterCard с Аффилиата:

Наименование комиссии	Значение
Еженедельные	
SI RANGE BLOCKING RESIDENCY	7 EUR за диапазон
FILE TRANSMISSION FEE	0,0000034 за Байт
GCMS REPORT IP727010-AA	0,01 EUR за 1 строку отчета
KEY MANAGEMENT SERVICES RESIDENCY	7,5 EUR за ключ
Authorization, clearing, settlement	% от объема транзакций
Ежедневные	
MARKET DEVELOPMENT FEE - DOMESTIC	0,1% от объема транзакций
CROSS BORDER INTER-R	% от объема транзакций

Комиссии международных платёжных систем с банков – MasterCard

Комиссии MasterCard с Принципала:

Наименование комиссии	Значение
Weekly connectivity fee	770 EUR еженедельно
ATM LOCATOR PROGRAM FEE ENHANCED	500 USD ежемесячно
ANNUAL ADMIN FEE AML COMPLIANCE	144 USD ежегодно
QUARTERLY VOLUME MASTERCARD/MAESTRO/CIRRUS	Ежеквартально, % от объема транзакций
MINIMUM VOLUME FEE-T1 ISS PL DOM	Ежеквартально, % от объема транзакций
MONTHLY ISSUER SAFE FEE	1000 EUR ежемесячно
MONTHLY ACQUIRER SAFE FEE	1000 EUR ежемесячно
MCOnline MEMBER PUBLICATIONS	425 EUR ежемесячно

Элементы безопасности – терминалы

Требуемые сертификаты для терминалов и пин-падов:

1. EMV Level 1 Contact
2. EMV Level 1 Contactless
3. EMV Level 2
4. TQM Contact
5. TQM Contactless
6. PCI PTS
7. VISA PayWave
8. MasterCard PayPass
9. AMEX ExpressPay
10. Discover DiscoverZip

TQM – Terminal Quality Management
PCI – Payment Card Industry
PTS – PIN Transaction Security

Элементы безопасности – PIN

Стандарты, отражающие требования к ПИН по безопасности:

1. ANSI

ANSI X3.92: Data Encryption Algorithm

ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

ANSI X9.44: Key Establishment Using Integer Factorization Cryptography

ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA

Элементы безопасности – PIN

ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography

ANSI X9.65: Triple Data Encryption Algorithm (TDEA) Implementation

ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

2. EMV

EMV: Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management

3. FIPS

FIPS PUB 140–2: Security Requirements for Cryptographic Modules

Элементы безопасности – PIN

4. ISO

ISO 9564: Personal Identification Number Management and Security

ISO 11568: Banking – Key Management (Retail)

ISO 11770–2: Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques

ISO 11770–3: Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)

ISO 13491: Banking – Secure Cryptographic Devices (Retail)

ISO 16609: Banking – Requirements for message authentication using symmetric techniques

ISO/IEC 18033-3: Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers

ISO TR19038: Guidelines on Triple DES Modes of Operation

Элементы безопасности – PIN

5. NIST

NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

6. PCI SSC

Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements

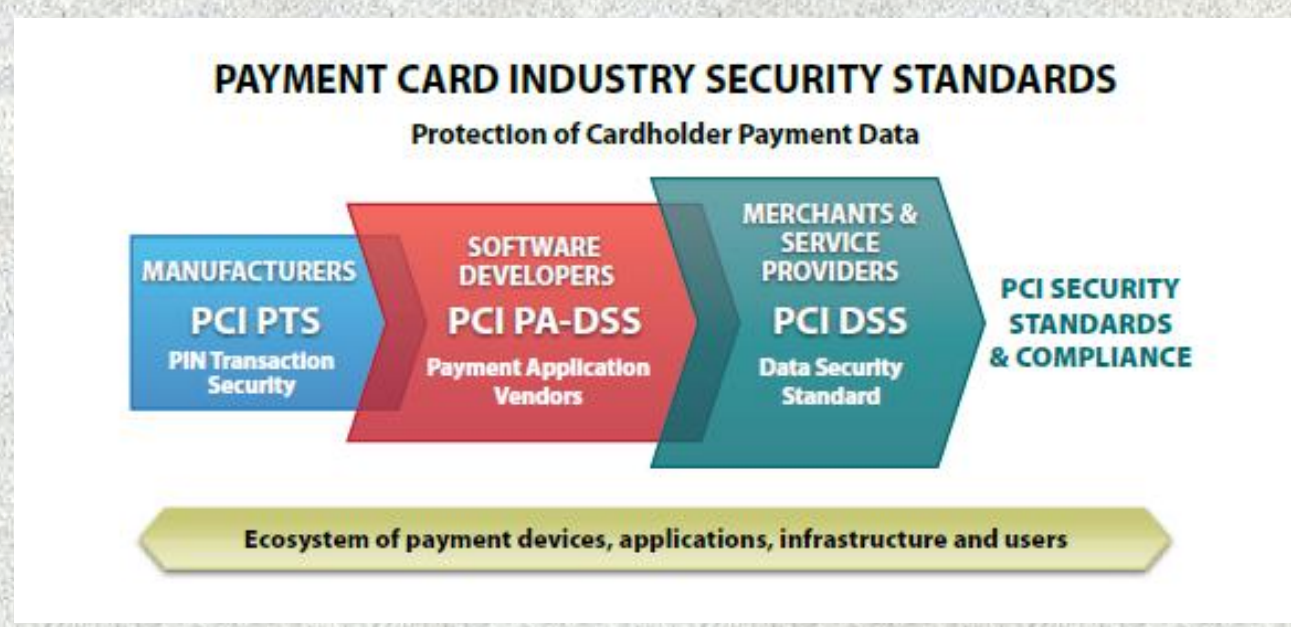
Payment Card Industry (PCI) PIN Transaction Security Point of Interaction Modular Derived Test Requirements

Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements

Payment Card Industry (PCI) Hardware Security Module (HSM) Derived Test Requirements

Элементы безопасности – вся сеть

Технические и операционные требования к защите данных владельцев банковских карт:
- PCI DSS



ОСНОВАТЕЛИ PCI SSC

AMERICAN EXPRESS
DISCOVER NETWORK
JCB
MasterCard Worldwide
VISA

PCI DSS – PCI Data Security Standard
PA DSS – Payment Application Data Security Standard
PCI PTS – PCI PIN Transaction Security
PCI SSC – PCI Security Standards Council

Элементы безопасности – вся сеть

Требования PCI DSS:

Построение и обслуживание защищенной сети

Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт

Требование 2: Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

Защита данных о держателях карт

Требование 3: Обеспечить безопасное хранение данных о держателях карт

Требование 4: Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования

Элементы безопасности – вся сеть

Требования PCI DSS:

Управление уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение

Требование 6: Разрабатывать и поддерживать безопасные системы и приложения

Внедрение строгих мер контроля доступа

Требование 7: Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью

Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре

Требование 9: Ограничить физический доступ к данным о держателях карт

Элементы безопасности – вся сеть

Требования PCI DSS:

Регулярный мониторинг и тестирование сети

Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности

Поддержка политики информационной безопасности

Требование 12: Разработать и поддерживать политику информационной безопасности

Элементы безопасности – вся сеть

Требования PCI DSS:

1. *Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт*

1.1. Должны быть разработаны стандарты конфигурации межсетевых экранов, которые должны включать в себя:

1.1.1. Формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурации межсетевого экрана

1.1.2. Актуальную схему сети с указанием всех каналов доступа к данным о держателях карт, включая все беспроводные сети

Элементы безопасности – вся сеть

1.1.3. Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании

1.1.4. Описание групп, ролей и ответственности за управление сетевыми устройствами

1.1.5. Обоснованный документированный перечень всех разрешенных для использования сервисов, протоколов и портов, необходимых для работы бизнес-приложений, включающий документальное описание внедренных механизмов защиты небезопасных протоколов

1.1.6. Требование пересмотра настроек межсетевых экранов и маршрутизаторов не реже одного раза в полгода

Элементы безопасности – вся сеть

1.2. Должна быть создана конфигурация межсетевых экранов, которая контролирует все соединения между недоверенными сетями и всеми системными компонентами в среде данных о держателях карт.
Примечание: недоверенной является любая сеть, которая не контролируется проверяемой организацией
1.2.1. Входящий и исходящий трафик должен быть ограничен только необходимыми соединениями для среды данных о держателях карт
1.2.2. Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов межсетевых экранов

Элементы безопасности – вся сеть

1.2.3. Необходима установка межсетевых экранов между любой беспроводной сетью и средой данных о держателях карт, такие межсетевые экраны должны быть настроены на блокирование любого трафика из беспроводной сети, либо его контроля в том случае, если такой трафик необходим для бизнес-приложений

1.3. Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды данных о держателях карт

1.3.1. Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только протоколами, необходимыми для среды данных о держателях карт

1.3.2. Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ

Элементы безопасности – вся сеть

1.3.3. Должны быть запрещены любые прямые маршруты входящего или исходящего трафика между сетью Интернет и средой данных о держателях карт

1.3.4. Необходимо запретить соединения с внутренними адресами от источника из Интернета к адресам, расположенным в DMZ

1.3.5. Необходимо ограничить исходящий трафик из среды данных о держателях карт в сеть Интернет таким образом, чтобы исходящий трафик имел доступ только к IP адресам, расположенным в DMZ

1.3.6. Необходимо включить динамическую пакетную фильтрацию с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений)

Элементы безопасности – вся сеть

1.3.7. Необходимо размещать базы данных во внутреннем сегменте сети, отделенном от DMZ

1.3.8. Должен быть реализован механизм трансляции IP-адресов для предотвращения раскрытия внутренних адресов. Для этого следует использовать такие технологии, как PAT и NAT

1.4. Должны быть установлены персональные межсетевые экраны на все мобильные и принадлежащие сотрудникам компьютеры, имеющие прямой доступ в Интернет и используемые также для доступа к локальной сети организации

Элементы безопасности – вся сеть

2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

2.1. Всегда следует менять установленные производителем настройки по умолчанию перед установкой системы в сетевую инфраструктуру (например, сменить установленные по умолчанию пароли, строки доступа SNMP, удалить ненужные для работы учетные записи)

2.1.1. Для беспроводных устройств необходимо изменить установленные по умолчанию производителем параметры, такие как: ключи шифрования, пароли, строки доступа SNMP. Следует включить стойкие криптографические механизмы для шифрования данных и аутентификации

Элементы безопасности – вся сеть

2.2. Должны быть разработаны стандарты конфигурации для всех системных компонентов. Стандарты должны учитывать все известные проблемы безопасности, а также положения общепринятых отраслевых стандартов в области безопасности

2.2.1. Каждый сервер должен выполнять одну основную функцию

2.2.2. Должны быть отключены все небезопасные и ненужные для работы сервисы и протоколы (те сервисы и протоколы, использование которых не требуется для выполнения устройством своей основной функции)

Элементы безопасности – вся сеть

2.2.3. Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы

2.2.4. Из системы должна быть удалена вся ненужная функциональность: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы

2.3. Следует всегда шифровать канал удаленного административного доступа к системе. Для этого необходимо использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов удаленного административного доступа

Элементы безопасности – вся сеть

2.4 Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным в Приложении А: «Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)»

Элементы безопасности – вся сеть

3. Обеспечить безопасное хранение данных о держателях карт

3.1. Хранение данных о держателях карт должно быть ограничено только необходимым минимумом. Должна быть разработана политика хранения и обращения с данными. Количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований параметрами; эти параметры должны быть отражены в политике хранения данных

3.2. Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). К критичным аутентификационным данным относятся данные 3.2.1 – 3.2.3

Элементы безопасности – вся сеть

3.2.1. Запрещается хранить полную дорожку магнитной полосы, находящейся на обратной стороне карты, на чипе, либо ином месте, («полная дорожка», «дорожка», «дорожка 1», «дорожка 2»). Для ведения бизнеса, может быть необходимо хранение следующих элементов данных магнитной полосы: - имя держателя карты, - номер платежной карты (PAN), - дата истечения срока действия карты, - сервисный код. Для минимизации рисков разрешается хранить только указанные элементы данных. Дополнительная информация приведена в «Глоссарии PCI DSS: Основные определения, аббревиатуры и сокращения»

Элементы безопасности – вся сеть

3.2.2. Запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с кредитной карты (трех- или четырехзначного числа, изображенного на лицевой или обратной стороне карты). Дополнительная информация приведена в «Глоссарии PCI DSS»

3.2.3. Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока

Элементы безопасности – вся сеть

3.3. Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4). Это требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть весь PAN; также это требование не заменяет собой иные более строгие требования к отображению данных о держателях карт (например, на чеках POS-терминалов)

Элементы безопасности – вся сеть

3.4. Из всех данных о держателе карты как минимум PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий, а также данные, получаемые по беспроводным сетям). Для этого следует использовать любой из следующих методов:

- стойкая однонаправленная хэш-функция;
- укорачивание (truncation);
- использование механизмов One-Time-Pad и хранение ссылок на данные вместо самих данных (index tokens);
- стойкие криптографические алгоритмы, совместно с процессами и процедурами управления ключами. Из всей информации о держателе карты как минимум PAN должен быть преобразован в нечитаемый вид

Элементы безопасности – вся сеть

3.4.1. Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или полей базы данных), то управление логическим доступом должно осуществляться независимо от механизмов разграничения доступа операционной системы (например, локальных учетных записей). Ключи шифрования не должны быть привязаны к учетным записям пользователей

3.5. Следует обеспечить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования:

3.5.1. Доступ к ключам шифрования должен быть разрешен только нескольким ответственным за их хранение и использование сотрудникам

Элементы безопасности – вся сеть

3.5.2. Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде

3.6. Должны быть документированы все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе:

3.6.1. Генерация стойких ключей

3.6.2. Безопасное распространение ключей

3.6.3. Безопасное хранение ключей

3.6.4. Периодическая смена ключей:

- насколько часто этого требуют применяемые приложения, предпочтительно автоматически;

- не реже одного раза в год

Элементы безопасности – вся сеть

3.6.5. Уничтожение старых (просроченных) ключей, а также ключей, относительно которых существуют подозрения в их компрометации

3.6.6. Раздельное владение частями ключей с принципом контроля двумя лицами

3.6.7. Защита от неавторизованной смены ключа

3.6.8. Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с письменным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности

Элементы безопасности – вся сеть

4. *Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования*

4.1. Для защиты критичных данных о держателях карт во время передачи их через общедоступные сети, следует использовать стойкие криптографические алгоритмы и протоколы, такие как SSL/TLS и IPSEC. Примерами общедоступных сетей, на которые распространяются требования PCI DSS, являются:

- Интернет;

- Беспроводные технологии;

- GSM;

- GPRS

Элементы безопасности – вся сеть

4.1.1. При использовании беспроводных сетей, передающих данные о держателях карт, либо подключенных к среде данных о держателях карт, следует использовать передовые практические методы (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных

- Для вновь устанавливаемых беспроводных сетей запрещается использование протокола WEP с 31.03.2009;

- Для существующих беспроводных сетей запрещается использование протокола WEP с 30.06.2010

4.2. Никогда не следует пересылать незашифрованный PAN при помощи пользовательских технологий передачи сообщений (email, системы мгновенной отправки сообщений, чаты)

Элементы безопасности – вся сеть

5. Использовать и регулярно обновлять антивирусное программное обеспечение

5.1. Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах)

5.1.1. Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного ПО

5.2. Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий

Элементы безопасности – вся сеть

6. Разрабатывать и поддерживать безопасные системы и приложения

6.1. На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем. Обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем.

Примечание: Организация может применять подход к распределению приоритетов при установке обновлений, основанный на оценке рисков. Для более критичных приложений срок установки обновлений не должен превышать одного месяца, для менее критичных - три месяца

Элементы безопасности – вся сеть

6.2. Должен быть внедрен процесс выявления новых уязвимостей (например, подписка на бесплатную рассылку сообщений о новых уязвимостях). Стандарты конфигурации системных компонентов (требование 2.2 PCI DSS) должны обновляться для учета вновь обнаруженных уязвимостей

6.3. Приложения должны разрабатываться в соответствии с требованиями PCI DSS (например, безопасная аутентификация и регистрация событий). Разработка приложений должна быть основана на передовых практических методиках и принимать во внимание информационную безопасность в течение всего цикла разработки, в том числе:

Элементы безопасности – вся сеть

6.3.1. Все обновления безопасности и изменения в конфигурации должны быть протестированы перед внедрением, тестирование должно включать в себя:

6.3.1.1. Проверку всех входных данных (чтобы исключить XSS, инъекции, исполнение вредоносного файла, и т. д.)

6.3.1.2. Проверку корректной обработки ошибок

6.3.1.3. Проверку использования защищенного криптографического хранилища для критичной информации

6.3.1.4. Проверку безопасности передачи данных

6.3.1.5. Проверку корректности разграничения доступа, основанного на ролях

XSS – Cross Site Scripting

Элементы безопасности – вся сеть

6.3.2. Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга

6.3.3. Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть разделены

6.3.4. Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки

6.3.5. Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим

6.3.6. Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчикам или переводом его в производственный режим

Элементы безопасности – вся сеть

6.3.7. Программный код приложений должен быть исследован на наличие потенциальных уязвимостей перед передачей готовых приложений заказчикам или переводом их в производственный режим. Примечание: это требование применимо ко всем разрабатываемым приложениям (как внутренним, так и общедоступным) как элемент обеспечения безопасности цикла разработки, регламентируемого требованием 6.3. PCI DSS. Оценка программного кода может проводиться как компетентным персоналом, так и третьими сторонами. Веб-приложения также являются объектом применения дополнительных мер по защите; если они находятся в публичном доступе, следует учесть угрозы и уязвимости, в соответствии с требованием 6.6. PCI DSS

Элементы безопасности – вся сеть

6.4. Должны быть разработаны и внедрены процедуры управления изменениями, включающие в себя:

6.4.1. Документирование влияния изменения на систему

6.4.2. Согласование изменения с руководством

6.4.3. Тестирование производственной функциональности

6.4.4. Процедуру отмены изменения

6.5. Разработка веб-приложений должна проходить в соответствии с руководствами по безопасному программированию, такими как руководства от проекта OWASP. Программный код приложений должен быть исследован на наличие потенциальных уязвимостей, в частности, таких как:

OWASP – Open Web Application Security Project

Элементы безопасности – вся сеть

6.5.1. Атаки типа XSS
6.5.2. Инъекции, в особенности, SQL-инъекции. Также следует учесть LDAP и Xpath инъекции
6.5.3. Исполнение вредоносных файлов
6.5.4. Небезопасные прямые ссылки
6.5.5. Подделка межсайтовых запросов (CSRF)
6.5.6. Утечка данных и некорректная обработка ошибок
6.5.7. Обход системы аутентификации и управления сессиями
6.5.8. Небезопасное криптографическое хранилище
6.5.9. Небезопасная передача данных

LDAP – Lightweight Directory Access Protocol
Xpath – XML Path Language
CSRF – Cross-Site Request Forgery

Элементы безопасности – вся сеть

6.5.10. Ошибки в контроле доступа по URL

6.6. Следует обеспечить защиту веб-ориентированных приложений от известных атак одним из следующих методов:

- Проверить приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности.

- Установить межсетевой экран прикладного уровня перед веб-ориентированными приложениями

Элементы безопасности – вся сеть

7. Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью

7.1. Доступом к вычислительным ресурсам и информации о держателях карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями. Ограничения доступа должны включать в себя:

7.1.1. Доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей

7.1.2. Назначение привилегий пользователям должно быть основано на их должностных обязанностях

7.1.3. Подписание руководством заявки о предоставлении прав доступа

Элементы безопасности – вся сеть

7.1.4. Внедрение автоматизированной системы контроля доступа

7.2. Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания и применяющий принцип «запрещено всё, что явно не разрешено». Механизм контроля доступа должен включать следующее:

7.2.1. Покрытие всех системных компонентов

7.2.2. Назначение привилегий пользователям должно быть основано на их должностных обязанностях

7.2.3. По-умолчанию должен быть запрещен любой доступ

Элементы безопасности – вся сеть

8. Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре

8.1. Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт

8.2. Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей:

- пароль
- двухфакторная аутентификация (ключи, смарт-карты, биометрические параметры, открытые ключи)

Элементы безопасности – вся сеть

8.3. Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети должен быть реализован механизм двухфакторной аутентификации. Для этого следует использовать такие технологии, как RADIUS и TACACS с ключами или VPN (SSL/TLS или IPSEC) с индивидуальными сертификатами

8.4. Все пароли должны храниться и передаваться только в зашифрованном виде

RADIUS – Remote Authentication Dial In User Service
TACACS – Terminal Access Controller Access Control System
VPN – Virtual Private Network
SSL – Secure Socket Layer
TLS – Transport Layer Security
IPSEC - IP Security

Элементы безопасности – вся сеть

8.5. Должен быть установлен контроль над выполнением процедур аутентификации и управления паролями учетных записей сотрудников и администраторов, включающий в себя:

8.5.1. Контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации

8.5.2. Проверку подлинности пользователя перед сменой пароля

8.5.3. Установку уникального первоначального пароля для каждого пользователя и его немедленное изменение при первом входе пользователя

8.5.4. Немедленный отзыв доступа при увольнении пользователя

Элементы безопасности – вся сеть

8.5.5. Удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней

8.5.6. Включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ

8.5.7. Доведение правил и процедур использования и хранения пароля до всех пользователей, имеющих доступ к данным о держателях карт

8.5.8. Запрет использования групповых, разделяемых и стандартных учетных записей и паролей

8.5.9. Изменение пароля пользователя не реже одного раза в 90 дней

8.5.10. Требование использования в пароле не менее семи символов

8.5.11. Требование использования в пароле как цифр, так и букв

Элементы безопасности – вся сеть

8.5.12. Запрет при смене пароля выбора в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей

8.5.13. Блокировку учетной записи после шести неудачных попыток ввода пароля

8.5.14. Установку периода блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором

8.5.15. Блокировку рабочей сессии пользователя через 15 минут простоя с требованием ввода пароля для разблокировки терминала

8.5.16 Аутентификацию всех вариантов доступа к любой базе данных, содержащей данные о держателях карт, в том числе доступ со стороны приложений, администраторов и любых других пользователей

Элементы безопасности – вся сеть

9. Ограничить физический доступ к данным платежных карт

9.1. Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные о держателях карт

9.1.1. Следует использовать камеры видеонаблюдения, чтобы следить за критичными местами. Данные, собранные камерами видеонаблюдения, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством

Элементы безопасности – вся сеть

Примечание: критичными являются места, относящиеся к любому дата-центру, серверной комнате или иному помещению, в котором расположены системы, хранящие, обрабатывающие или передающие данные о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов

9.1.2. Доступ к сетевым разъемам, расположенным в общедоступных местах, должен быть ограничен

9.1.3. Доступ к беспроводным точкам доступа, шлюзам и портативным устройствам должен быть ограничен

Элементы безопасности – вся сеть

9.2. Должны быть внедрены процедуры, позволяющие легко различать сотрудников и посетителей, особенно в помещениях, где циркулируют данные о держателях карт.

Примечание: Под термином «сотрудники» в данном случае понимаются постоянные и временные сотрудники, а также консультанты, работающие на объекте. Под термином «посетители» понимаются поставщики, гости сотрудников, сервисный персонал и иные люди, кратковременно находящиеся на объекте, обычно не более одного дня

9.3. Следует ввести процедуру прохода посетителей на объект, обеспечивающую:

Элементы безопасности – вся сеть

9.3.1. Авторизацию посетителя, перед входом в помещения, где циркулируют данные о держателях карт

9.3.2. Выдачу посетителю материального идентификатора (например, бейджа или электронного ключа), имеющего ограничение срока действия, при входе на объект

9.3.3. Возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении срока его действия

9.4. Следует вести журнал учета посетителей и использовать его для анализа посещений. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством

Элементы безопасности – вся сеть

9.5. Носители с резервными копиями данных следует хранить в безопасных местах, желательно вне объекта, таких как запасной центр обработки данных, или же воспользовавшись услугами компаний, обеспечивающих безопасное хранение

9.6. Должна быть обеспечена физическая безопасность всех бумажных и электронных средств, содержащих данные о держателях карт

9.7. Должен быть обеспечен строгий контроль над перемещением носителей информации, содержащих данные о держателях карт, включающий:

9.7.1. Классификацию носителей информации, их маркировку, как содержащих конфиденциальную информацию

Элементы безопасности – вся сеть

9.7.2. Пересылку носителей только с доверенным курьером, или иным способом, который может быть тщательно проконтролирован

9.8. Должна быть внедрена процедура разрешения руководством выноса за пределы охраняемой территории носителей, содержащих данные о держателях карт

9.9. Должен быть обеспечен строгий контроль хранения носителей, содержащих данные о держателях карт, и доступом к ним

9.9.1. Должны поддерживаться в актуальном состоянии журналы инвентаризации всех носителей данных о держателях карт; инвентаризация носителей должна проводиться не реже одного раза в год

Элементы безопасности – вся сеть

9.10. Носители, содержащие данные о держателях карт, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, должны быть уничтожены следующими способами:

9.10.1. Измельчение, сжигание или растворение бумажного носителя

9.10.2. Уничтожение данных о держателях карт на электронном носителе, исключающее возможность их восстановления

Элементы безопасности – вся сеть

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт

10.1. Должен быть разработан процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам

10.2. Для каждого системного компонента должен быть включен механизм протоколирования следующих событий:

10.2.1. Любой доступ пользователя к данным о держателях карт

10.2.2. Любые действия, совершенные с использованием административных полномочий

10.2.3. Любой доступ к записям о событиях в системе

Элементы безопасности – вся сеть

10.2.4. Неуспешные попытки логического доступа
10.2.5. Использование механизмов идентификации и аутентификации
10.2.6. Инициализация журналов протоколирования событий
10.2.7. Создание и удаление объектов системного уровня
10.3. Для каждого события каждого системного компонента должны быть записаны следующие параметры:
10.3.1. Идентификатор пользователя
10.3.2. Тип события
10.3.3. Дата и время
10.3.4. Успешным или неуспешным было событие
10.3.5. Источник события

Элементы безопасности – вся сеть

10.3.6. Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие

10.4. Все системные часы на критичных системах должны быть синхронизированы

10.5. Журналы протоколирования событий должны быть защищены от изменений

10.5.1. Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями

10.5.2. Журналы протоколирования событий должны быть защищены от неавторизованного изменения

Элементы безопасности – вся сеть

10.5.3. Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования, или отдельный носитель, где их изменение было бы затруднено

10.5.4. Копии журналов протоколирования активности событий доступных извне технологий (беспроводных сетей, межсетевых экранов, DNS, почтовых систем) должны сохраняться на сервер протоколирования, находящийся внутри локальной сети

10.5.5. Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала)

DNS – Domain Name System

Элементы безопасности – вся сеть

10.6. Следует просматривать журналы протоколирования событий не реже одного раза в день. Следует анализировать журналы систем обнаружения вторжений (IDS) и серверов, осуществляющих аутентификацию, авторизацию и учет (например, RADIUS). Примечание: Для обеспечения соответствия Требованию 10.6 могут быть использованы средства сбора и анализа журналов регистрации событий, а также средства оповещения

10.7. Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев

IDS – Intrusion Detection System

Элементы безопасности – вся сеть

11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности

11.1. Следует ежеквартально проверять наличие беспроводных точек доступа, используя анализатор беспроводных сетей либо беспроводные IDS/IPS для обнаружения всех включенных беспроводных устройств

IDS – Intrusion Detection System
IPS – Intrusion Prevention System

Элементы безопасности – вся сеть

11.2. Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значимых изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления системных компонентов). Примечание: ежеквартальное сканирование должно производиться сторонней сертифицированной компанией. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании

Элементы безопасности – вся сеть

11.3. Следует проводить внешний и внутренний тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера). Эти тесты на проникновение должны включать:

11.3.1. Тесты на проникновение сетевого уровня

11.3.2. Тесты на проникновение уровня приложений

11.4. Следует использовать системы обнаружения вторжений, а также системы предотвращения вторжений для контроля всего сетевого трафика и оповещения персонала о подозрительных действиях. Системы обнаружения и предотвращения вторжений должны быть актуальными

Элементы безопасности – вся сеть

11.5. Следует использовать приложения контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов и файлов данных; проверка целостности критичных файлов должна проводиться не реже одного раза в неделю. Примечание: Обычно контролируется целостность файлов, которые изменяются нечасто, но изменение которых может служить признаком компрометации или попытки компрометации системы. Средства контроля целостности обычно содержат предустановленный перечень файлов, подлежащих контролю, в зависимости от используемой операционной системы. Другие критичные файлы, такие как файлы специализированных приложений, должны быть определены самой компанией

Элементы безопасности – вся сеть

12. Разработать и поддерживать политику информационной безопасности

12.1. Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика информационной безопасности

12.1.1. Политика информационной безопасности должна учитывать все требования настоящего стандарта

12.1.2. Политика информационной безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков

12.1.3. Политика информационной безопасности должна пересматриваться не реже одного раза в год и обновляться в случае изменения инфраструктуры

Элементы безопасности – вся сеть

12.2. Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов протоколирования событий)

12.3. Должны быть разработаны правила эксплуатации для критичных технологий, с которыми непосредственно работают сотрудники (таких как системы удаленного доступа, беспроводные технологии, съемные носители информации, мобильные компьютеры, карманные компьютеры, электронная почта и Интернет), чтобы определить корректный порядок использования этих устройств сотрудниками. Эти правила должны включать следующее:

Элементы безопасности – вся сеть

12.3.1. Процедуру явного одобрения руководством
12.3.2. Аутентификацию перед использованием устройства
12.3.3. Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам
12.3.4. Маркировку устройств с указанием владельца, контактной информации и назначения
12.3.5. Допустимые варианты использования устройств
12.3.6. Допустимые точки размещения устройств в сети
12.3.7. Перечень одобренных компанией устройств
12.3.8. Автоматическое отключение сессий удаленного доступа после определенного периода простоя

Элементы безопасности – вся сеть

12.3.9. Включение механизмов удаленного доступа для службы поддержки (производителям) только в случае необходимости такого доступа, с немедленным выключением механизмов после использования

12.3.10. Запрет хранения данных о держателях карт на локальных дисках, дискетах и иных съемных носителях при удаленном доступе к данным, а также запрет использования функций копирования-вставки данных и вывода данных на принтер во время сеанса удаленного доступа

12.4. Политика и процедуры безопасности должны однозначно определять обязанности всех сотрудников и партнеров, относящиеся к информационной безопасности

Элементы безопасности – вся сеть

12.5. Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:

12.5.1. Разработка, документирование и распространение политики и процедур безопасности

12.5.2. Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных

12.5.3. Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций

Элементы безопасности – вся сеть

12.5.4. Администрирование учетных записей пользователей, включая их добавление, удаление и изменение

12.5.5. Мониторинг и контроль любого доступа к данным

12.6. Должна быть внедрена официальная программа повышения осведомленности сотрудников о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт

12.6.1. Обучение сотрудников должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год

12.6.2. Сотрудники должны не реже одного раза в год подтверждать своё знание и понимание политики и процедур информационной безопасности компании

Элементы безопасности – вся сеть

12.7. Следует тщательно проверять кандидатов при приеме на работу (будущих сотрудников), для минимизации риска внутренних атак. (Определение термина "сотрудник" приведено в пункте 9.2) Для таких сотрудников, как кассиры в магазине, которые имеют доступ к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер

12.8. В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними, включающие:

12.8.1. Поддержку перечня поставщиков услуг

Элементы безопасности – вся сеть

12.8.2. Поддержку письменного соглашения о том, что поставщики услуг ответственны за безопасность переданных им данных о держателях карт

12.8.3. Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним

12.8.4. Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS

12.9. Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы

Элементы безопасности – вся сеть

12.9.1. Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум:

- роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем;

- процедуры реагирования на определенные инциденты;

- процедуры восстановления и обеспечения непрерывности бизнеса;

- процессы резервного копирования данных;

- анализ требований законодательства об оповещении о фактах компрометации;

- ссылки или включение процедур реагирования на инциденты международных платежных систем

Элементы безопасности – вся сеть

12.9.2. План должен тестироваться не реже одного раза в год

12.9.3. Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7

12.9.4. Персонал, ответственный за реагирование на нарушения безопасности, должен быть обучен соответствующим образом

12.9.5. План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов

12.9.6. Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли

Элементы безопасности – вся сеть

Приложение А: Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)

А.1. Обеспечить защиту данных каждого клиента, согласно требованиям с А.1.1 по А.1.4: Хостинг-провайдер должен удовлетворять всем этим требованиям, помимо требований PCI DSS Примечание: не смотря на то, что хостинг-провайдер будет соответствовать требованиям PCI DSS, каждый его клиент должен, тем не менее, проходить собственный аудит

А.1.1. Ограничить доступ приложений каждого клиента только к своей среде данных о держателях карт

Элементы безопасности – вся сеть

A.1.2. Ограничить доступ клиента только к своей среде данных о держателях карт

A.1.3. Убедиться, что протоколирование действий и событий включено для каждого клиента, и соответствует требованию 10 стандарта

A.1.4. Убедиться в наличии процессов, позволяющих провести расследование инцидентов каждого клиента

Для достижения соответствия PCI DSS компания должна выполнить все требования стандарта, независимо от того, в каком порядке они выполняются

Элементы безопасности – вся сеть

Дополнительная информация:

- *American Express:*
  www.americanexpress.com/datasecurity
- *Discover Financial Services:*
  www.discovernetwork.com/fraudsecurity/disc.html
- *JCB International:*
  www.jcb-global.com/english/pci/index.html
- *MasterCard Worldwide:*
  www.mastercard.com/sdp
- *Visa Inc:*
  www.visa.com/cisp
- *Visa Europe:*
  www.visaeurope.com/ais

Элементы безопасности – вся сеть

Практики Visa по шифрованию полей данных:
Цели безопасности

1. *Ограничить циркуляцию данных о держателях карт и критичных аутентификационных данных в открытом виде только точками шифрования и расшифрования*
2. *Использовать надежные решения по управлению ключами, соответствующие международным и/или региональным стандартам*
3. *Использовать длины ключей и криптографические алгоритмы, соответствующие международным и/или региональным стандартам*

Элементы безопасности – вся сеть

4. Защитить устройства, выполняющие криптографические операции, от физической и логической компрометации
5. Для бизнес-процессов использовать дополнительную учетную запись или идентификатор транзакции, которые не используют PAN после авторизации. Например, при выполнении повторяющихся платежных операций, поддержки программ лояльности клиента или управления инцидентами мошенничества

Элементы безопасности – вся сеть

Среда применимости

1. *Практики Visa по шифрованию полей данных имеют отношение к системам, выполняющим эквайринговые операции в таких местах, как:*

- *Платежные терминалы*
- *Точки продаж торгово-сервисных предприятий*
- *Корпоративные серверы*
- *Корпоративные системы агрегирования транзакций*
- *Платежные шлюзы*
- *Процессинговые системы*
- *Эквайеры*

Элементы безопасности – вся сеть

2. Данные о держателях карт включают в себя: PAN, имя держателя карты и срок окончания действия карты.
3. Критичные аутентификационные данные включают в себя, но не ограничиваются следующими: полное содержимое магнитной дорожки, дорожка 1 (track 1), дорожка 2 (track 2), проверочное значение карты (CVV), CVV2, проверочное значение PIN (PVV) и PIN/PIN block . Критичные аутентификационные данные не могут быть использованы ни для каких целей, кроме как для авторизации транзакции

Элементы безопасности – вся сеть

Ограничить циркуляцию данных о держателях карт и критичных аутентификационных данных в открытом виде только точками шифрования и расшифрования

1. Данные о держателях карт и критичные аутентификационные данные должны быть доступны в открытом виде только в точках шифрования и расшифрования
2. Все данные о держателях карт и критичные аутентификационные данные должны шифроваться только алгоритмами, одобренными комитетом ANSI X9 или ISO (например, AES, TDES)
3. Все данные о держателях карт и критичные аутентификационные данные должны быть зашифрованы, кроме:

Элементы безопасности – вся сеть

- Первые шесть цифр PAN могут оставаться в открытом виде для маршрутизации в процессе авторизации
- Первые шесть и последние четыре цифры PAN могут выводиться на экран платежного терминала и/или распечатываться на чеке, в отчетах об оплате, использоваться для выбора счета, и т.д. (эта рекомендация не заменяет более строгих правил и регламентов, которые имеются в организациях, касательно отображения данных о держателях карт)

4. Критичные аутентификационные данные не должны сохраняться после авторизации, даже в зашифрованном виде (согласно PCI DSS)

Элементы безопасности – вся сеть

Использовать надежные решения по управлению ключами, соответствующие международным и/или региональным стандартам

5. Управление ключами должно осуществляться в соответствии со стандартами ANS X9.24 (все части) / ISO 11568 (все части) или их аналогами, с использованием защищенных криптографических устройств (Secure Cryptographic Devices, SCD), таких как PED, HSM, и т.п., как определено в стандартах ANS X9.97 (все части) / ISO 13491 (все части) или их аналогах

6. Все ключи и их компоненты должны генерироваться с использованием одобренных процедур случайного или псевдослучайного подбора, например, NIST SP 800-22

Элементы безопасности – вся сеть

7. Документация, описывающая процесс установки и функционирования системы управления ключами, должна быть доступной по запросу для ее оценки

8. Перевозка или передача ключей по каналам связи должна быть защищена. Например, используя метод распространения ключей, описанный в X9/TR-34 Interoperable Method for Distribution of Symmetric Keys Using Asymmetric Techniques, Part 1–Using Factoring-Based Public Key Cryptography Unilateral Key Transport или эквивалентный метод

- Если используется дистанционное распространение ключей, должна осуществляться обоюдная аутентификация устройств отправки и получения

Элементы безопасности – вся сеть

9. Ключи, использующиеся в процессе шифрования поля данных, должны:

- Быть уникальными для каждого устройства

- Использоваться только для шифрования данных о держателях карт и критичных аутентификационных данных, и не должны использоваться для других целей

- Ключи, использующиеся для шифрования PIN, не могут быть использованы для шифрования поля данных (в соответствии с PCI PIN Security Requirements)

Элементы безопасности – вся сеть

Использовать длины ключей и криптографические алгоритмы, соответствующие международным и/или региональным стандартам

10. Ключи шифрования должны обладать стойкостью, эквивалентной стойкости, как минимум, 112-битного ключа. В таблице представлены эквивалентные стойкости часто используемых алгоритмов

Алгоритм	Длина в битах
TDES	112[1]
AES	128[2]
RSA	2048
ECC	224
SHA	224

Для более подробной информации касательно эквивалентной стойкости, обратитесь к ISO TR-147442 Recommendations on Cryptographic Algorithms and their Use – Technical Report

Элементы безопасности – вся сеть

11. Любые методы, использующиеся для производства шифртекста такой же длины и типа данных, как и у открытого текста, должны пройти оценку как минимум одной независимой организации по оценке безопасности. Эти методы должны внедряться в соответствии с рекомендациями, выданными при выполнении вышеупомянутой оценки, включая все рекомендации по сопутствующему управлению ключами

Элементы безопасности – вся сеть

Защитить устройства, выполняющие крипто-графические операции, от физической и логической компрометации

12. Устройства, выполняющие криптографические операции, должны подвергаться независимой оценке, для гарантии того, что их комплектующие и программное обеспечение устойчивы к атакам

13. Симметричные и закрытые ключи должны быть защищены от физической и логической компрометации. Открытые ключи должны быть защищены от подмены, а их целостность и достоверность должны быть гарантированы

Элементы безопасности – вся сеть

Для бизнес-процессов использовать дополнительную учетную запись или идентификатор транзакции, которые не используют PAN после авторизации. Например, при выполнении повторяющихся платежных операций, поддержки программ лояльности клиента или управления инцидентами мошенничества

14. Если какие-либо данные о держателях карт (например, PAN) необходимы после авторизации, то вместо них следует использовать одноразовый или многоразовый идентификатор транзакции

- Предпочтителен одноразовый идентификатор транзакции. Допустимые методы получения одноразового идентификатора транзакции включают хэширование PAN с уникальным для транзакции значением привязки, шифрование PAN одобренным

Элементы безопасности – вся сеть

алгоритмом с использованием уникального для транзакции ключа, или эквивалентным. Одноразовый идентификатор транзакции может быть получен другими методами, которые обеспечивают уникальность идентификатора для каждой транзакции, при этом данные о держателях карт не должны быть читаемы

- Многоразовый идентификатор транзакции может использоваться, если существует необходимость обеспечения взаимосвязи номера счета с несколькими транзакциями. Допустимые методы получения многоразового идентификатора транзакции включают хеширование данных о держателях карт, используя фиксированное (но разное для каждого торгово-сервисного предприятия) значение привязки или эквивалентное

Элементы безопасности – вся сеть

Примечание: Независимо от того, какой тип идентификатора транзакции используется (одноразовый или многоразовый), если применяются значения привязки, то их длина должна быть минимум 32 бита, они должны находиться в тайне и быть должным образом защищены

[1] В целях данных практик, два ключа TDES (112 бит) не должны обрабатывать более 1 миллиона транзакций. В случаях, когда количество транзакций, потенциально обрабатываемых ключом 112 бит TDES, намного превышает 1 миллион, следует использовать ключи TDES (168 бит) или AES. Схемы управления ключами, которые ограничивают количество транзакций для одного ключа, например «производный уникальный транзакционный ключ» (Derived Unique Key Per Transaction, DUKPT), могут использоваться для обеспечения того, что каждый отдельный ключ используется строго ограниченное количество раз

[2] Минимальное количество бит в ключе, которые можно использовать с AES, составляет 128 бит. Данный ключ более стоек, чем это необходимо, но если используется AES, это наименьший из доступных ключей (более длинные ключи могут быть использованы по желанию)

Спасибо за внимание!