1.Становление стандартов ИБ Банка России.

В России до середины 2000-х годов слово *«безопасность»* преимущественно ассоциировали с управлением [*«банковскими рисками»*](http://www.provsebanki.ru/text/196)*.* Только лишь федеральный закон [«О банковской деятельности» от 02.12.1990 N 395-1](http://www.consultant.ru/popular/bank/46_3.html) ФЗ в [ст.26 Банковская тайна](http://www.consultant.ru/popular/bank/46_3.html#p803) давал ограниченное право и возможность на защиту конфиденциальных сведений в банковской сфере. Федеральный закон [«О коммерческой тайне» 29.07.2004 N 98-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_160225/), позволяющий, наконец то, полноценно заявить о новом виде деятельности и отдельной категории вопросов таких как «информационная безопасность банков».

наметились тенденции для принятия международных банковских стандартов, в частности стандарта [Базель II](http://compress.ru/article.aspx?id=18749). В своей трактовке этот стандарт рассматривал информационную безопасность как операционный риск и, в целом, требовал мер по аудиту и контролю за информационной сферой, что являлось абсолютным новшеством для российских банков в то время.

2004 год с выпуском Центральным Банком России первой редакции пакета [отечественных отраслевых стандартов по информационной безопасности СТО БР ИБСС](http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd). Стандарт ЦБ по ИТ-безопасности считался лучшим отраслевым стандартом на то время, ведь он вобрал в себя лучший мировой опыт и практику, объединяет в себе основные положения стандартов по управлению ИТ-безопасностью (ISO 17799, 13335), регламентирует описание жизненного цикла программных средств и критерии оценки ИТ-безопасности (ГОСТ Р ИСО/МЭК 15408-1-2-3).

Среди основных положений стандарта ЦБ можно было отметить ориентацию на решение проблемы инсайдеров. Значительное внимание уделено внешним угрозам. Несмотря на все эти очевидные преимущества стандарт носил рекомендательный характер.

Учитывая все эти нововведения (149-фз, 152-фз) и меняющиеся реалии общества, в свет выходили и новые редакции СТО БР ИББС. Так, [в третьей редакции стандарта от 2008 года](http://www.orioncom.ru/demo_base_bkb/bnd/tema55_1.htm), пакет документов был значительно переработан, повелись новые, были уточнены некоторые требования по обеспечению безопасности; обновлены требования к системе менеджмента информационной безопасности. Также стандарт обзавелся собственной моделью угроз и нарушителей ИБ организаций БС РФ. Введены новые блоки по требования ИБ в автоматизированных банковских системах, регламентирован процесс банковских платежных и информационных технологических процессов, применение средств криптографической защиты информации.

Изменения в [четвертой редакции](http://abiss.ru/standards/document_library/) (2010г) главным образом касались обновленной методики защиты Персональных данных (ПДн). (Документ отменили так как он повторял текущее законодательство по защите ПДн).

В 2011 году председатель правительства Владимир Путин подписывает федеральный закон [«О национальной платежной системе «от 27.06.2011 N 161-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_158430/). Для выполнения поручения президента спустя год Приказом Банка России выходит документ «[Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…»  от 09.06.2012 N 382-П)](http://www.consultant.ru/document/cons_doc_LAW_149221/).

[национальную систему платежных карт](http://ria.ru/economy/20140505/1006613510.html). И в июне 2014 года вступила в силу обновленная пятая, и пока последняя на сегодняшний день, редакция [СТО БР ИББС - 2014](http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd). СТО привели в соответствие с 382-П.

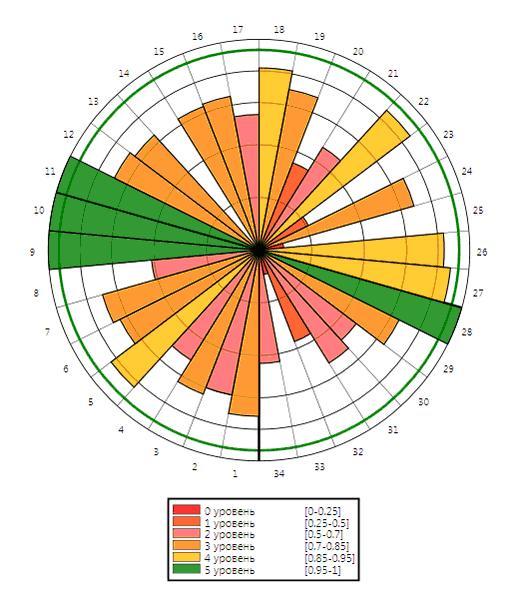
2. Информационная безопасность в Банках с учетом СТО БР ИББС-2014.

В настоящий момент распоряжением Банка России пакет документов СТО БР ИББС состоит из следующих частей: являются обязательными для всех банков

1. [СТО БР ИББС-1.0-2014. «Общие положения (5 редакция)»](http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf); ‑ основа для формирования всех мероприятий по защите информации. Вся структура разбита на отдельные блоки. В них подробно описываются требования к обеспечению безопасности, даются конкретные перечни мер защиты по тому или иному блоку.
2. [СТО БР ИББС-1.1-2007. «Аудит информационной безопасности»;](http://www.cbr.ru/credit/gubzi_docs/st11.pdf) указывает на необходимость проведение аудита системы ИБ, а также дает отсылку к проведению ежегодной самооценки по требованиям стандарта. Данные итоговой самооценки служат базой как для формы отчетности в случае проверки Центральным Банком, так и заключением соответствия уровня защищенности системы информационной безопасности банка выявленным рискам и угрозам ИБ.
3. [СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)»;](http://www.cbr.ru/credit/Gubzi_docs/st-12-14.pdf) ‑это свод методик оценки и таблиц с соответствующими полями для заполнения. Каждое мероприятие и мера защиты дают определенное весовое значение в оценке называемый групповой показатель. По результатам групповых показателей выстраивается круговая диаграмма соответствия требованием СТО БР ИББС.

Кроме того, Банком России разработаны и введены следующие рекомендации в области стандартизации ИБ:

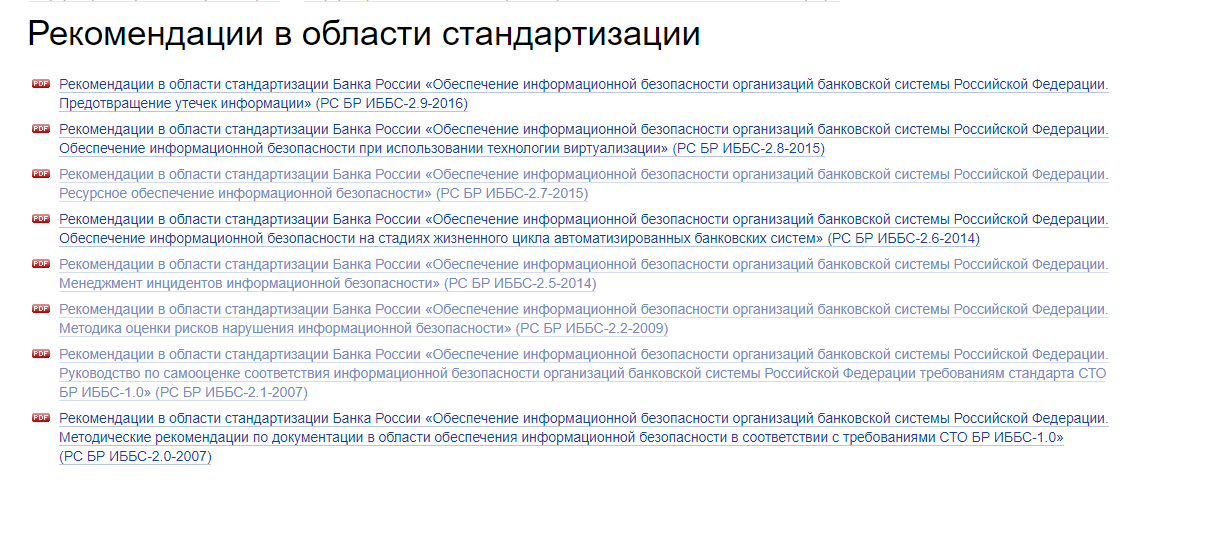
1. [РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0»;](http://www.cbr.ru/credit/gubzi_docs/st20.pdf)
2. [РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.](http://www.cbr.ru/credit/gubzi_docs/st21.pdf)0»;
3. [РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности»;](http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf)
4. [РС БР ИББС-2.5-2014. «Менеджмент инцидентов информационной безопасности»](http://www.cbr.ru/credit/Gubzi_docs/rs-25-14.pdf)



Что еще можно добавить -- достаточно большое внимание уделяется процессам менеджмента системы информационной безопасности, в частности можно выделить **Цикл Деминга**, используемый топ-менеджерами в управлении качеством. Стоит отметить тот факт, что стало значительно больше уделяться внимания документированию процедур безопасности во внутренних нормативных документах банков. Таким образом, даже если процедура фактически не выполняется, но предусмотрена и документирована, -- это повышает результат внутреннего аудита. По сравнению с прошлой редакцией возросло количество частных показателей, а так же изменились весовые значения оценок

Следует сказать еще об одном важном дополнении, касающемся встроенных механизмов защиты в АБС, -- Банк России выпустил рекомендации «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» (РС БР ИББС-2.6-2014)». Суть их заключается в том, что теперь банки могут, ссылаясь на этот документ, выставлять требования разработчикам к функционалу программного обеспечения в части механизмов защиты

3. Защита персональных данных в банках.



По текущему законодательству. Июльская поправка (261-ФЗ) к 152-ФЗ «О персональных данных» наделила Банк России правами на разработку отраслевых нормативных документов по отдельным вопросам, касающимся обработки персональных данных, что узаконило СТО БР ИББС в качестве отраслевого стандарта обеспечения безопасности персональных данных. Кроме того, было так же утверждено право Банка России на разработку отраслевой модели угроз безопасности ПДн (которой являются РС БР ИББС-2.4-2010).

Однако ряд положений СТО БР ИББС вступил в конфликт с новой версией закона «О персональных данных»:

* федеральный закон не даёт возможность операторам ПДн использовать не сертифицированные, но одобренные руководством организации, средства защиты информации (п.7.4.2 СТО БР ИББС-1.0-2010);
* под понятие информационной системы персональных данных, приведенное в законе, подпадают все автоматизированные банковские системы, обрабатывающие персональные данные, без исключения (п. 7.10.9 СТО БР ИББС-1.0-2010 исключает из понятия ИСПДн [АБС](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0), реализующие банковские платёжные технологические процессы).

Техническая сторона вопроса защиты персональных данных, согласно 19 статье 152-ФЗ, устанавливается Правительством РФ, а не нормами СТО БР ИББС, что так же противоречит основной идее создания отраслевого стандарта.

В ближайшее время статус СТО БР ИББС будет уточнён подзаконными нормативными актами Правительства, ФСТЭК, ФСБ, а также информационными письмами Банка России.

А так, СТО БР ИББС 2.3, своя модель (спецы брали модель, определяли требования и строили перечень необходимых мероприятий). Потом был конфликт с 1119 и приказом 21 (так как банки решили, что они должны полностью соответствовать СТО БР ИББС). Поэтому строгие треболвания были отменены, упрощена классфифкация, таблица уровня защищенности подогнана под приказ 21. Роскомнадзором отдельно были внесены пояснения в отношении биометрических ПДн??????

4. Информационная безопасность национальной платежной системы.

МИР. Президент подписал закон о создании в России национальной системы платежных карт (НСПК) и обеспечении бесперебойности работы международных платежных систем. Целью проекта обозначено инфраструктурно и информационно замкнуть процесс осуществления денежных переводов внутри России, закрепить территориально внутри страны операционные центры и платежные клиринговые центры. (крч если нас отключат)

НПС дает возможность отслеживает все денежные операции, в том числе финансирование сомнительных сделок и мошеннические операции, которые могут угрожать безопасности граждан или страны в целом.

Для обеспечения безопасности НПС был выпущен целый рад подзаконных актов, серди которых основополагающее [Положение о защите информации в платежной системе» от 13.06.2012 №584](http://www.consultant.ru/law/hotdocs/19153.html). Но в большей мере отвечает выпущенное ответственным департаментом Банком России [Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств…» от 09.06.2012 N 382-П)](http://www.consultant.ru/document/cons_doc_LAW_149221/)

С обновлением П-382 тенденции обеспечения защиты теперь смещены в сторону:

* применением банкоматов и платежных терминалов;
* применения пластиковых платежных карт;
* использования сети Интернет (систем дистанционного банковского обслуживания (ДБО) и мобильного банкинга);
* требований к порядку разработки и распространения специализированного ПО, предназначенного для использования клиентом при переводе денежных средств;
* что очень порадовало, расширение требований по повышению осведомленности клиентов о возможных рисках получения несанкционированного доступа к защищаемой информации и рекомендуемых мерах по их снижению;
* требований о необходимости проведения классификации банкоматов и платежных терминалов, результаты которой должны учитываться при выборе мер защиты;
* процедур приостановления проведения платежа оператором по переводу денежных средств в случае обнаружения признаков мошеннических действий;
* предусмотрены процедуры защиты от современных угроз безопасности, таких как: скимминг (путем использования специализированных средств, препятствующих несанкционированному считыванию треков платежных карт; защита сервисов расположенных в сети Интернет от внешних атак (DoS-атак); защита от фишинга (от фальсифицированных ложных ресурсов сети Интернет).
* требование по применению платежных карт, оснащенных микропроцессором, с 2015 года и запрет выпуска карт, не оснащенных микропроцессором, после 1-го января 2015 года;
* 29 новых показателей оценки.

5. Информационная безопасность платежных систем.

В мировом сообществе признанным стандартом безопасности считается [Payment Card Industry Data Security Standard (PCI DSS)](https://www.pcisecuritystandards.org/), который был разработан советом PCI SSC. В него вошли такие карточные брэнды, как Visa, MasterCard, American Express, JCB и Discovery

Стандарт PCI DSS описывает требования к защите данных о держателях карт, сгруппированные в двенадцать разделов. Основной акцент в стандарте PCI DSS делается на обеспечении безопасности сетевой инфраструктуры и защите хранимых данных о держателях платежных карт, как наиболее уязвимых с точки зрения угроз конфиденциальности местах. Также стандарт регламентирует правила безопасной разработки, поддержки и эксплуатации платежных систем.

Международные платежные системы обязывают организации, на которые распространяются требования стандарта, проходить регулярную проверку соответствия этим требованиям, что рано или поздно может затронуть и НСПК. Однако сертификация российских банков по зарубежному PCI DSS стандарту шла довольно медленно, а отечественного аналога на сегодняшний день нет (тем не меннее приводится таблица сравнения с СТО БР и ФЗ о НПС).

В отличие от всех зарубежных стандартов, российский 382-П призван стимулировать отечественных разработчиков и производителей средств защиты информации (СЗИ), так, например, обязывая субъекты НПС обеспечить применение некриптографических СЗИ от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия. При этом, применение решений иностранного производства явно разрешено.

Более того, Банк России усиливает свой контроль за соблюдением установленных правил. В своем документе [Указание № 2831-У от  09.06.2012  «Об отчетности по обеспечению защиты информации в платежных системах…»](http://www.cbr.ru/PSystem/P-sys/2831-U.pdf)

PCI PA-DSS (Payment Card Industry Payment Application Data Security Standard) определяющий требования к приложениям, обрабатывающим данные о держателях карт и процессу их разработки. И, второй - стандарт Payment Card Industry PIN Transaction Security (PCI PTS), ранее PCI PED, касаются производителей, которые задают и реализуют технические параметры и систему управления для устройств, поддерживающих набор ПИН-кода и использующихся для проведения платежных операций по картам.

6. Определения PCI DSS.

ASV (Approved Scanning Vendor) – поставщик услуг сканирования, имеющий официальный статус от Совета стандартов безопасности (PCI SSC).

On-site аудит – аудит инфраструктуры Заказчика, проводимый аудитором непосредственно на реально функционирующих компонентах.

QSA (Qualified Security Assessor) — компания, сотрудники которой индивидуально прошли тренинги и экзамены, проводимые Советом стандартов безопасности (PCI SSC).

Аудитор (консультант) — лицо, занимающееся аудитом по стандарту PCI DSS (проверкой соответствия требованиям стандарта) и консультационной деятельностью, связанной с оценкой соответствия требованиям стандарта PCI DSS.

Заказчик – юридическое лицо, заинтересованное в выполнении исполнителем услуги проверки на соответствие требованиям стандарта PCI DSS.

Эквайер – член ассоциации эмитентов банковских карт, который устанавливает и поддерживает взаимодействие с предприятиями торгово-сервисной сети, принимающей платежные карты. [2]

7. Стандарт PCI DSS.

Стандарт безопасности данных индустрии платежных карт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационной инфраструктуре торгово-сервисных предприятий, сервис-провайдеров и других организаций

1) Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности. Версия 2.0 (Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures v2.0).

В документе детально описаны 12 требований стандарта, область их применимости, основные сведения по подготовке к аудиту соответствия требованиям стандарта и проведению аудита, а также сведения по написанию отчетных материалов. Документ разработан преимущественно для использования аудиторами, проводящими onsite-аудит на соответствие требованиям стандарта.

2) Глоссарий. Версия 2.0 (Glossary v2.0).

Перечень терминов и сокращений, используемых в нормативной документации PCI DSS. Предназначен для понимания терминов, используемых в других поддерживающих документах и поэтому рекомендуется Заказчику для ознакомления.

3) Ориентирование в PCI DSS. Версия 2.0 (Navigating the PCI DSS. Version 2.0).

Документ, в котором описываются 12 требований стандарта с пояснением их значений в целях улучшения понимания требований стандарта предприятиями торгово-сервисной сети, сервис-провайдерами и другими финансовыми учреждениями.

4) Приоритезированный подход к достижению соответствия PCI DSS. Версия 1.2 (Prioritized Approach for PCI DSS v1.2).

Правила работ для уменьшения рисков на ранних стадиях мероприятий по достижению соответствия стандарту. Приоритезированный подход состоит из 6 этапов, которые в порядке приоритета помогут распределить усилия по достижению соответствия, снизят риск компрометации данных о платежных картах в процессе выполнения. Подход не заменяет требования стандарта PCI DSS v2.0.

5) Требования, предъявляемые к квалифицированным экспертам безопасности (PCI DSS Validation Requirements for Qualified Security Assessors).

Приложение, в котором содержатся требования, предъявляемые Советом по стандартам безопасности платежных карт экспертам безопасности, получающим или уже имеющим статус квалифицированного эксперта безопасности (QSA).

6) Требования, предъявляемые к поставщикам услуг сканирования (PCI DSS Validation Requirements for Approved Scanning Vendors).

Приложение, в котором содержатся требования, предъявляемые Советом по стандартам безопасности платежных карт экспертам безопасности, получающим или уже имеющим поставщика услуг сканирования (ASV).

7) Листы самооценки. Версия 2.0 (PCI DSS Self-Assessment Questionnaire v2.0).

Листы самооценки предназначены для организации проведения самооценки торгово-сервисными предприятиями и сервис-провайдерами их соответствия стандарту и представляют собой средства проверки соответствия финансовой организации стандарту PCI DSS согласно документу «Стандарт безопасности данных индустрии платежных карт. Требования и процедуры аудита безопасности. Версия 2.0» («Payment Card Industry Data Security Standard. Requirements and Security Assessment Procedures v2.0»). Существуют несколько вариантов листа самоооценки, которые используются в том или ином случае.

8) Аттестация соответствия PCI DSS – торговые организации. Версия 2.0 (PCI DSS Attestation of Compliance – Merchants v2.0).

Шаблон документа, который заполняется QSA или торговой организацией (в случае, если торговая организация осуществляет внутренний аудит), и в результате является официальным документом о соответствии данной организации стандарту PCI DSS.

9) Аттестация соответствия PCI DSS – сервис-провайдеры. Версия 2.0 (PCI DSS Attestation of Compliance – Service Providers v2.0).

Шаблон документа, который должны заполнить QSA и сервис-провайдер в качестве официального документа о соответствии данного сервис-провайдера стандарту PCI DSS.

8. Дополнительные документы PCI DSS.

1) Дополнительные документы – ASV (Additional Documents — ASV).

Набор документации для поставщиков услуг сканирования (ASV): руководство по программе ASV, список требований ASV, проверка соответствия статусу ASV.

2) Дополнительные документы – QSA (Additional Documents — QSA).

Набор документации для квалифицированных экспертов безопасности (QSA): соглашение QSA, список требований QSA.

3) Дополнительные документы – PFI (Additional Documents — PFI).

Набор документации для экспертов-криминалистов в индустрии платежных карт (PFI): руководство по программе PFI, список требований PFI, проверка соответствия статусу PFI. Статус эксперта-криминалиста в платежной индустрии введен Советом PCI SSC со второй версией стандарта PCI DSS.

4) Требование 11.3 Тестирование на проникновение (Requirement 11.3 Penetration Testing).

Подробное описание требования 11.3 стандарта PCI DSS к проведению тестирований на проникновение.

5) Требование 6.6 Защита веб-приложений (Requirement 6.6 Application Reviews and Web Application Firewalls Clarified).

Уточнение к требованию 6.6 стандарта PCI DSS к обеспечению защиты веб-приложений.

6) Руководство по беспроводным сетям. Версия 1.2 (Wireless Guidelines v1.2)

Документ содержит предложения и рекомендации для развертывания и тестирования беспроводных сетей в контексте требований стандарта PCI DSS.

9. Ключевые требования по организации защиты данных.

1) Требование 1. «Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт».

2) Требование 2. «Не использовать пароли и другие системные параметры, заданные производителем по умолчанию».

3) Требование 3. «Обеспечить безопасное хранение данных о держателях карт».

4) Требование 4. «Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования».

5) Требование 5. «Использовать и регулярно обновлять антивирусное программное обеспечение».

6) Требование 6. «Разрабатывать и поддерживать безопасные системы и приложения».

7) Требование 7. «Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью».

8) Требование 8. «Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре».

9) Требование 9. «Ограничить физический доступ к данным о держателях карт».

10) Требование 10. «Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт».

11) Требование 11. «Регулярно выполнять тестирование систем и процессов обеспечения безопасности».

12) Требование 12. «Разработать и поддерживать политику информационной безопасности».

10. Программы обеспечения безопасности Visa и MasterCard.

VISA AIS

Требования программы Visa AIS, которые должны быть выполнены организацией, зависят от числа ежегодно хранимых, обрабатываемых и передаваемых ею учетных данных Visa. В соответствии с этими данными эквайер присваивает определенный уровень торгово-сервисному предприятию. Ниже представлен список требований программы для торгово-сервисных предприятий и сервис провайдеров.

Требования к торгово-сервисным предприятиям (merchants):

1) ежегодный аудит на соответствие требованиям PCI DSS (любое ТСП, обрабатывающее более 6 млн. транзакций по Visa в год или интернациональные ТСП, которым был присвоен 1 уровень Visa в другом регионе или стране);

2) ежегодное самостоятельное заполнение опросного листа (SAQ) (ТСП, обрабатывающие от 1 млн. до 6 млн. транзакций по Visa в год по всем платежным каналам или ТСП, обрабатывающие от 20 000 до 1 млн. транзакций электронной торговли по Visa в год);

3) ежеквартальное сканирование сети поставщиком услуг сканирования (ASV);

4) наличие аттестата соответствия (для всех уровне ТСП);

5) проверка соответствия требованиям, выполняемая эквайером (ТСП, обрабатывающие менее 20 000 транзакций электронной торговли по Visa в год, или все другие ТСП, обрабатывающие до 1 млн. транзакций в год).

Требования, предъявляемые Visa к сервис-провайдерам (Service Providers):

1) ежегодный аудит на соответствие требованиям PCI DSS;

2) ежегодное заполнение SAQ (любой поставщик услуг, обрабатывающий менее 300 000 транзакций по Visa в год);

3) ежеквартальное сканирование сети в соответствии со стандартом PCI DSS;

4) наличие аттестата соответствия.

Программа MasterCard SDP

Программа MasterCard Site Data Protection (SDP), утвержденная MasterCard, предназначена для обеспечения безопасного хранения ТСП и сервис-провайдерами данных учетных записей MasterCard в соответствии со стандартом PCI DSS. Ниже представлен список требований программы для торгово-сервисных предприятий и сервис провайдеров.

Требования, предъявляемые MasterCard торгово-сервисным предприятиям (merchants):

а) ТСП уровня 1 (все ТСП, с ежегодным оборотом более 6 миллионов транзакций ежегодно по картам MasterCard и Maestro; все ТСП, пострадавшие от взлома или атаки, результатом которого была утечка данных; любое ТСП, которое было отнесено к уровню 1, по усмотрению MasterCard) должны выполнять следующие требования:

1) ежегодный аудит, выполняемый QSA;

2) ежеквартальное сканирование сети, выполняемое ASV;

3) обязательное выполнение процедур подтверждения соответствия.

б) ТСП уровня 2 (все ТСП с оборотом более 1 миллиона, но менее либо равным 6 миллионам транзакций ежегодно по картам MasterCard и Maestro; все ТСП, соответствующие уровню 2 другой платежной системы) должны выполнять следующие требования:

1) ежегодный аудит, проводимый QSA;

2) ежегодное заполнение опросного листа SAQ (до 31 декабря 2010 года);

3) ежеквартальное сканирование сети, проводимое ASV;

4) выполнение начальных процедур проверки соответствия (до 31 декабря 2010 года).

в) ТСП уровня 3 (все ТСП, количество транзакций электронной торговли по MasterCard и Maestro превышает 20 000 в год, но общее количество транзакций электронной торговли по MasterCard и Maestro не превышает 1 миллиона; все ТСП, соответствующие уровню 3 другой платежной системы) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;

2) ежеквартальное сканирование сети, проводимое ASV;

3) обязательное выполнение процедур подтверждения соответствия.

г) ТСП уровня 4 (все ТСП, не относящиеся к первым трем уровням) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;

2) ежеквартальное сканирование сети, проводимое ASV;

3) консультация с эквайером о дате выполнения процедур проверки соответствия.

Требования, предъявляемые MasterCard сервис-провайдерам (Service Providers):

а) Сервис-провайдеры уровня 1 (все сторонние процессинги; все организации хранения данных, которые хранят, передают или обрабатывают ежегодно более 300 000 транзакций MasterCard и Maestro) должны выполнять следующие требования:

1) ежегодный аудит, проводимый QSA;

2) ежеквартальное сканирование сети, проводимое ASV.

б) Сервис-провайдеры уровня 2 (все организации хранения данных, которые хранят, передают или обрабатывают ежегодно менее 300 000 транзакций MasterCard и Maestro) должны выполнять следующие требования:

1) ежегодное заполнение опросного листа SAQ;

2) ежеквартальное сканирование сети, проводимое ASV.

**11. Схема взаимодействия МПС с финансовыми организациями.**

Международные платежные системы( МПС)

торгово-сервисные предприятия (ТСП)

Уровень ТСП определяется непосредственно эквайером, к которому подключено ТСП. В свою очередь, МПС два раза в год требует от эквайеров предоставление отчетов о соответствии ТСП уровней 1, 2 и 3 требованиям стандарта PCI DSS. Таким образом, эквайер выполняет роль посредника между торгово-сервисными предприятиями и МПС. В случае нарушения торгово-сервисными предприятиями правил МПС, Visa применит соответствующие меры по контролю рисков, которые могут выражаться в наложении штрафов на эквайеров [5].

Сервис-провайдеры, которые удовлетворяют критерию Уровня 1 проходят необходимые процедуры соответствия и включаются в список PCI DSS Compliant Service Providers. Сервис-провайдеры Уровня 2 не включаются в указанный список и контролируются соответствующими эквайерами (контроль представляет собой мониторинг результатов самоопросника).

12. Аудит ИБ по стандарту PCI DSS.

1) Аудит на соответствие требованиям стандарта PCI DSS

2) Подготовка инфраструктуры Заказчика для проведения аудита на соответствие требованиям стандарта PCI DSS

3) Сканирование уязвимостей в соответствии с требованиями стандарта PCI DSS

4) Тест на проникновение в соответствии с требованиями стандарта PCI DSS

5) Курсы повышения квалификации в области информационной безопасности сотрудников организации-заказчика

Среди подходов к проведению аудитов ИБ различают два принципиально разных методики:

1) тесты на проникновение;

2) технологический аудит информационной безопасности.

Основные этапы проведения аудита

1. Этап первый. Анализ и систематизация.
2. 2) Этап второй. Оценка соответствия требованиям стандарта.
3. 3) Этап третий. Формирование отчета.

13. Основные характеристики технологии NFC.

Технология NFC - следующее поколение технологий беспроводной связи, основанных на физическом принципе взаимной индукции. Создана на основе существующих стандартов и технологий бесконтактных смарт-карт.

* несущая частота 13,56 Мгц
* дальность действия до 10 см
* скорость передачи данных 106, 212, и 424 кбит/с
* автоматическая инициация сеанса связи
* конфигурирование канала связи менее 0,1 секунды

Технология NFC в настоящее время главным образом нацеливается на использование в мобильных телефонах и планшетах.

14. Области применения NFC.

Три основных области применения NFC:

1. эмуляция карт: устройство NFC ведет себя как существующая бесконтактная карта;
2. режим считывания: устройство NFC является активным и считывает пассивную RFID-метку, например, для интерактивной рекламы;
3. режим P2P: два устройства NFC вместе связываются и обмениваются

информацией.

15. Стандарты по NFC.

NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092-2003. Эти стандарты определяют схемы модуляции, кодирование, скорости передачи и радиочастотную структуру интерфейса устройств NFC, а также схемы инициализации и условия, требуемые для контроля за конфликтными ситуациями во время инициализации — и для пассивных и для активных режимов NFC. Кроме того, они также определяют протокол передачи, включая протокол активации и способ обмена данными. Радиоинтерфейс для NFC стандартизирован в: ISO/IEC 18092 / ECMA-340 : Near Field Communication Interface and Protocol-1 (NFCIP-1)[3]

ISO/IEC 21481 / ECMA-352 : Near Field Communication Interface and Protocol-2 (NFCIP-2)[4]

NFC объединяет множество ранее существовавших стандартов, включая ISO 14443, ISO 15693. Таким образом, телефоны, снабженные NFC, способны к взаимодействию с существующей ранее инфраструктурой считывателей. В «режиме эмуляции карты» устройство NFC должно по крайней мере передать уникальный идентификационный номер существующему ранее считывателю