**Лекция №2 Стандарты ЦБ РФ**

**Введение**

Не секрет, что банки являются краеугольным камнем кредитно-финансовой системы государства и важнейшим финансовым институтом современного общества. В связи с этим на них возлагаются особые требования к обеспечению информационной безопасности. До момента появления отечественных отраслевых стандартов информационной безопасности СТО БР ИББС банки управляли безопасностью, основываясь на положениях внутренних нормативных документов. Но и после принятия этих документов осталось много вопросов, требующих своего решения. Некоторые рассматриваемые в статье вопросы связаны с разрешением «узких мест» системы ИБ банков и адаптации политики безопасности под новые требования с учетом уже имеющегося «багажа» в области защиты информации.

**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), т.е. контролю ситуаций, которые могли бы привести к по несению кредитной организацией потерь и\или ухудшения ее ликвидности вследствие наступления неблагоприятных событий. Таких категорий как *«информационная безопасность»* или *«защита информации»* не существовало в принципе. 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" \l "p803) давал ограниченное право и возможность на защиту конфиденциальных сведений в банковской сфере. Спустя больше чем десятилетие отечественные правотрорцы выпустили в свет 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».

В те же годы в отечественном банковском сообществе 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. Однако и этого было недостаточно -- развитие современных информационных технологий и постоянное стремление предложения новых банковских продуктов на рынок требовали более значительно внимания к данным вопросам.

Следующей эволюционной вехой развития стал 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. Для этого Банк России закрепляет контроль над обращением конфиденциальной информации внутри корпоративной среды. Значительное внимание уделено внешним угрозам: положения стандарта требуют от банков иметь антивирусную защиту с регулярно обновляемыми базам, средства фильтрации спама, управления доступом, регламентировать процедуры внутреннего аудита, использовать шифрование для защиты от несанкционированного доступа и т.п.

Несмотря на все эти очевидные преимущества стандарт носил рекомендательный характер - его положения могли применяться отечественными банками только на добровольной основе. Тем не менее, по результатам исследования респондентов, представленных на [III  межбанковской конференции](http://www.ib-bank.ru/arhiv/05/01/kurilo.rar), прослеживалась явная тенденция к принятию данных документов как обязательной базовой основы для российских банков.

Параллельно с развитием банковских стандартов в середине 2000-х годов в России шел и процесс становления отечественного законодательства в сфере информационной безопасности. Ключевым моментом стало обновление Федерального закона [«Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_165971/), дающего новые актуальные определения информации, информационных технологий и процессов, отдельно заголовком выделена «защита информации». Вслед за ним отдельную категорию в практике защиты информации ознаменовал выход закона [«О Персональных данных»  от 27.07.2006 N 152-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_163964/).

Учитывая все эти нововведения 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 термины и понятия, были уточнены и детализированы некоторые требования по обеспечению безопасности; обновлены требования к системе менеджмента информационной безопасности. Также стандарт обзавелся собственной моделью угроз и нарушителей информационной безопасности организаций БС РФ. Введены новые блоки по требования ИБ в автоматизированных банковских системах, регламентирован процесс банковских платежных и информационных технологических процессов, отдельно сказано про 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). У банковского сообщества появился альтернативный способ выполнения требований по защите персональных данных. В комплексе документов был существенно изменен порядок категорирования ПДн и классификации ИСПДн. Предложенный подход основывался на четких разграничениях специальных, биометрических, обезличенных и общедоступных ПДн и не зависит от объема записей в ИСПДн. Особым приятным моментом для организаций банковской сферы стала разработанная отраслевая модель угроз. Банк вправе ее принять без изменений, что позволяет избежать трудоемкой аналитической работы. Комплекс документов СТО БР ИББС вносит ясность в вопросы аттестации ИСПДн и получения лицензии ФСТЭК России. Значительно упростилась жизнь пункте 9.6 СТО БР ИББС-1.0-2010, в котором снимается необходимость проведения аттестации и лицензирования, если проводятся мероприятия по обеспечению безопасности ИСПДн для собственных нужд банка.

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/), что стало еще одной категорией бизнеса прочно укрепившейся с процессами управлением ИБ. 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/).

На фоне последних мировых событий 2014 года и экономических санкций, введенных западными странами в отношении России, наметилась чёткая тенденция к разработке и переходу на [национальную систему платежных карт](http://ria.ru/economy/20140505/1006613510.html). Это, соответственно, предъявляет дополнительные требования к надежности и безопасности таких систем, что влечет за собой и повышение значения отечественных стандартов ИБ.

Результатом всех этих событий стало очередное переиздание стандарта. 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). В новой редакции исправили огрехи прошлых выпусков и, что очень важно, требования и рекомендации СТО привели в соответствие с вышеописанным 382-П. Так, например, уточнен список требующих регистрации операций в ДБО, , расширен список защищаемой информации, исходя из П-382, приведена таблица соответствия частных показателей оценки из СТО и показателей из текущей редакции 382-П.

Не менее значимым достижением стала актуализированная база нормативных требований с учетом последних изменений законодательства в сфере защиты Персональных данных, а именно добавлены ссылки на [Постановление Правительства №1119](http://www.consultant.ru/document/cons_doc_LAW_137356/) и [Приказ ФСТЭК России №21](http://fstec.ru/normotvorcheskaya/akty/53-normotvorcheskaya/akty/prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21).

Все это сформировало единую методическую и нормативную платформу для обеспечения комплексной информационной безопасности с учетом банковской специфики. Пакет документов СТО БР ИББС обособил российские банки выстроив в них систему безопасности с отраслевой точки зрения, но в то же время впитал лучшую мировую практику и опыт зарубежных коллег по обеспечению информационной безопасности.

**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:

1. [СТО БР ИББС-1.0-2014. «Общие положения (5 редакция)»](http://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf);
2. [СТО БР ИББС-1.1-2007. «Аудит информационной безопасности»;](http://www.cbr.ru/credit/gubzi_docs/st11.pdf)
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)

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)

Первые три документа являются обязательными для всех банков, которые приняли указанный стандарт в качестве своей базовой политики. Документ «Общие положения» являются основой 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. (см. таблица 1)

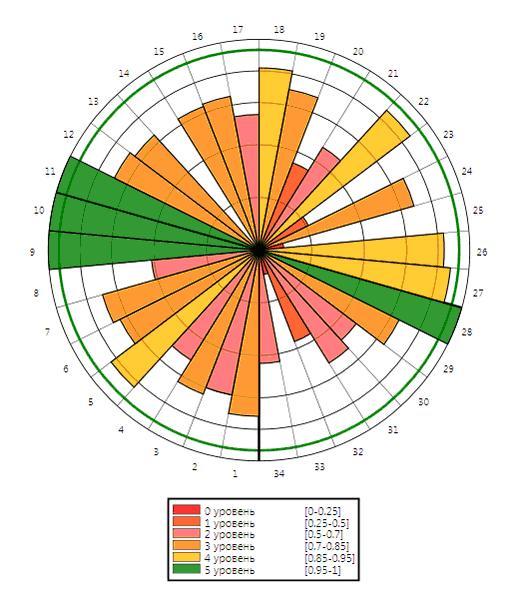
**Таблица 1. Требования к обеспечению информационной безопасности**

|  |
| --- |
| - при назначении и распределении ролей и обеспечении доверия к персоналу; |
| - в автоматизированных банковских систем (АБС) на стадиях жизненного цикла; |
| - при управлении доступом и регистрацией пользователей; |
| - к средствам антивирусной защиты; |
| - при использовании ресурсов сети Интернет; |
| - при использовании средств криптографической защиты информации; |
| - в банковских платежных технологических процессах; |
| - по обработке персональных данных; |
| - отельным заголовком вынесены требования к системе менеджмента информационной безопасности. |

Документ «Аудит информационной безопасности»  самый мало страничный из всех, 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.

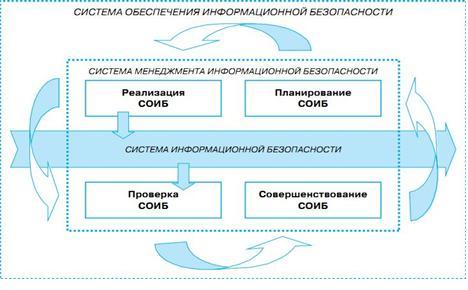
И последний из рассматриваемых документ «Методика оценки соответствия требованиям ИБ» -- это свод методик оценки и таблиц с соответствующими полями для заполнения. Каждое мероприятие и мера защиты дают определенное весовое значение в оценке называемый групповой показатель. По результатам групповых показателей выстраивается круговая диаграмма соответствия требованием СТО БР ИББС (см. рисунок 2). Все значений групповых показателей лежат в диапазоне от **0** до **1**, в котором для определения итога выделены еще 6 уровней соответствия стандарту, начиная с нулевого. Банком России рекомендованы уровни 4 и 5 (см. рисунок 2). Соответственно чем выше значение, тем более считается защищенной система. На круговой диаграмме эти сектора имеют зеленый цвет, красный же -- показатель критического уровня.

**Рисунок 2. Круговая диаграмма соответствия требованиям СТО БР ИББС**



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 (рисунок 3).

**Рисунок 3. Цикл Деминга для СОИБ СТО БР ИББС**



В новой редакции Банк России актуализировал методику оценки соответствия информационной безопасности. Основные изменения коснулись подхода к оценке:

* все требования теперь отнесены к одному из трех классов (документирование, выполнение, документирование и выполнение);
* оценка групповых показателей определяется как среднее арифметическое (отсутствуют весовые коэффициенты частных показателей);
* вводится понятие корректирующих коэффициентов, влияющих на оценки по направлениям и зависящих от количества полностью не реализованных требований Стандарта;
* значение показателя М9 (Общие требования по обработке персональных данных) рассчитывается по общей схеме (а не как минимальное из значений входящих частных показателей в предыдущей версии стандарта).

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 (см. рисунок 4).

**Рисунок 4. Изменения в прошлой и текущей редакции СТО БР ИББС (по данным ИнфоКонстал Менеджмент, www. km-ltd.com, 2014)**



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)»](http://www.cbr.ru/credit/Gubzi_docs/rs-26-14.pdf). Суть их заключается в том, что теперь банки могут, ссылаясь на этот документ, выставлять требования разработчикам к функционалу программного обеспечения в части механизмов защиты. Нельзя забывать, что это именно рекомендации, а не требования, и сам Банк России навязывать ничего не может, однако он позволяет транслировать эти рекомендации от имени банковского сообщества, а это уже изменение в лучшую сторону.

**Защита персональных данных в банках**

До выхода 5 редакции СТО БР ИББС–2014, защита персональных данных в банках базировалась на [двух документах](http://bankir.ru/tehnologii/s/sravnenie-podhodov-k-zaschite-personalnih-dannih-dlya-bankov-8091939/): БР ИББС-2.3-2010. «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» и РС БР ИББС-2.4-2010. «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации».

На практике это выглядело так: брали в неизменном виде предложенную Центральным Банком частную отраслевую модель угроз, по методическим рекомендациям определяли требований к защите каждой ИСПДн, исходя из и количества и списка обрабатываемых данных, и в дальнейшем выстраивали по ним перечень необходимых мероприятий.

Главной головной болью специалистов до сегодняшнего дня было то, что настоящие требований действовали вплоть до очередной редакции СТО БР ИББС – 2014, хотя на тот момент защита ПДн уже выстраивалась в соответствии с ПП-1119 и приказом ФСТЭК №21. В виду того, что банки должны соответствовать принятому пакету СТО БР ИББС, многие из них пользовались не актуальными методиками и, как следствие, не соответствовали новым реалиям обеспечения безопасности.

С выходом этих двух упомянутых нормативных документов ситуация изменилась к лучшему - были отменены некоторые строгие требования по лицензированию, упрощены процедуры классификации ИСПДн, оператору ПДн дано больше прав на выбор защитных мер. Требования к защите ИСПДн определяясь таблицей соответствия «уровня защищенности» и применяемых к ним процедур безопасности, детализациях которых была представлена приказом ФСТЭК № 21. Это позволило нивелировать различия в методике защиты ПДн в отраслевом стандарте ЦБ и общего российского законодательства.

В обновленном стандарте появился новый термин «Ресурс ПДн», для которого сформированы требования к документированности отдельных процедур, связанных с обработкой персональных данных (раздел 7.10). Отдельно рассмотрены вопросы, связанные с уничтожением персональных данных: организациям предоставлена возможность уничтожать ПДн не сразу, а на периодической основе, но не реже одного раза в полгода.

Роскомнадзором отдельно были внесены [пояснения в отношении биометрических ПДн](http://legion-info.ru/разъяснение-роскомнадзора-про-биоме/), например фотографии сотрудников, если таковые используются в целях осуществления контрольно-пропускного режима или выставлены на сайте компании в качестве общедоступной информации о руководстве, не попадают под режим специальных требованиям к защите.

Банкам же, которые ранее уже выполнили требования по защите ПДн по старому стандарту, для соответствия новым требованиям нужно скорректировать свои внутренние нормативные документы, провести заново классификацию и пере адресацию ИСПДн и, в соответствии с уровнем защищенности, определить для себя новый перечень защитных мероприятий. Хочется отметить, что сейчас у банков появилось больше свободы в выборе средств и методов защиты, однако применение именно сортированных ФСТЭК средств защиты информации по-прежнему является обязательным.

**Информационная безопасность национальной платежной системы**

Национальная платежная система (НПС), в виду последних событий, становится все более приоритетным направлением во внутренней политике государства. Президент России Владимир Путин подписал закон о создании в России национальной системы платежных карт (НСПК) и обеспечении бесперебойности работы международных платежных систем. Оператор НСПК создается в форме ОАО, 100% активов которого принадлежит Банку России. Целью проекта обозначено инфраструктурно и информационно замкнуть процесс осуществления денежных переводов внутри России, закрепить территориально внутри страны операционные центры и платежные клиринговые центры.

Фактически, до выхода закона деньги могли появляться из «ниоткуда» и исчезать в «никуда». С выходом закона ситуация меняется, 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. Кроме того, уход от наличного оборота, по мнению правительства,  является еще одним шагом в борьбе со взяточничеством.

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.

**Информационная безопасность платежных систем**

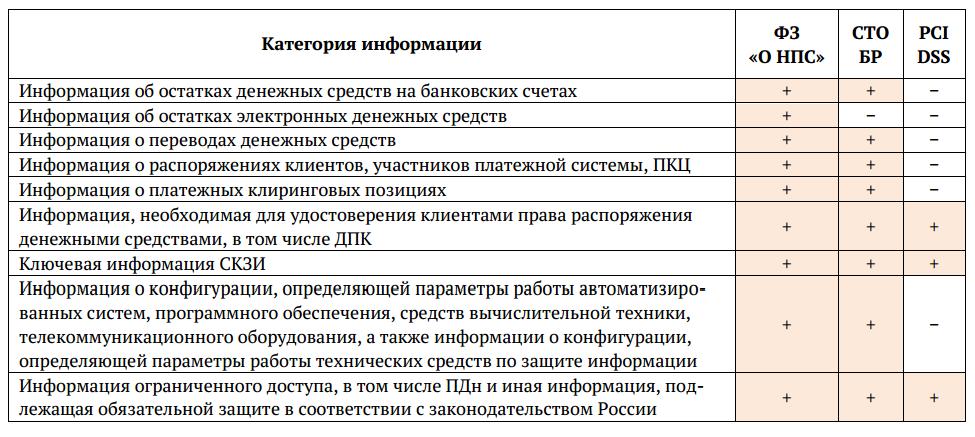
Аналогичная ситуация складывается с использованием пластиковых карт. В мировом сообществе признанным стандартом безопасности считается [Payment Card Industry Data Security Standard (PCI DSS)](https://www.pcisecuritystandards.org/), который был разработан советом PCI SSC. В него вошли такие карточные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

Стандарт PCI DSS описывает требования к защите данных о держателях карт, сгруппированные в двенадцать тематических 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 следует отметить, что стандарт регламентирует правила безопасной разработки, поддержки и эксплуатации платежных систем, в том числе процедуры их мониторинга. Не менее важную роль стандарт отводит разработке и поддержке базы нормативных документов системы менеджмента информационной безопасности.

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.

Однако, выполняя требования П-382 и последней редакции СТО БР ИББС-2014, можно во многом подготовиться к прохождению сертификации по PCI DSS, ведь многие его положения пересекаются с требованиями из отечественного документа: антивирусная безопасность, шифрование, фильтрация с помощью межсетевых экранов, разграничение доступа, отслеживании сеансов связи, а также мониторинг, аудит и менеджмент системы ИБ (см. рисунок 5).

**Рисунок 5. Сравнение категорий защищаемой информации различными стандартами (по данным Уральский центр Систем безопасности,** [**www.usssc.ru**](http://www.usssc.ru/)**, 2014)**



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) явно указывает, в какой форме, и с какой периодичностью субъекты платежных систем должны отчитываться о состоянии информационной безопасности в платежных системах.

Несмотря на популярность и широкое распространение PCI DSS существуют и другие международных стандарты безопасности падежных систем, о которых тоже хотелось бы немного сказать. Один из них стандарт 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.

**Заключение**

СТО БР ИББС является очень важной вехой эволюционного пути развития отечественной системы обеспечения информационной безопасности. Это один из первых отраслевых и адаптированных под российскую действительность стандартов. Конечно, это не панацея от всех бед, остается еще много проблем, над которыми бьются специалисты, но это первый и весьма успешный опыт, приближающий нас к эталонам лучшей зарубежной практики.

Выполняя требования стандарта, многие банки готовят себя к международной сертификации обеспечения безопасности платежных систем PCI DSS. Обеспечивают защиту персональных данных в соответствии с последними требованиями регуляторов. Проводимый ежегодный внутренний аудит позволяет объективно проверить защищенность банков от существенных рисков и угроз ИБ, а руководителям эффективнее спланировать построение и управление комплексной системой защиты.