Стандарт Банка России и PCI DSS. Что общего?

Сычев Артем Михайлович,
заместитель начальника ГУБиЗИ
Банка России

Область применения PCI DSS 3.0 и комплекса документов БР ИББС

К совокупности защитных мер, реализующих обеспечение ИБ организации БС РФ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение

Комплекс документов БР ИББС

Устанавливает общие требования

К совокупности процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов

Назначение и распределение ролей и обеспечение доверия к персоналу

Использование средств антивирусной защиты

Использование средств криптографической защиты информации

Использование ресурсов сети Интернет

Управление доступом и регистрации

Построение и обслуживание защищенной сети и систем

Внедрение строгих мер контроля доступа

Защита данных держателей карт

Определение области действия системы обеспечения информационной безопасности

Оценка рисков нарушения ИБ

Реализация программ по обучению и повышению осведомленности персонала в области ИБ

Разработка/коррекция внутренних документов в области ИБ

Обнаружение и реагирование на инциденты ИБ

Мониторинг и контроль защитных мер

Регулярный мониторинг и тестирование сети

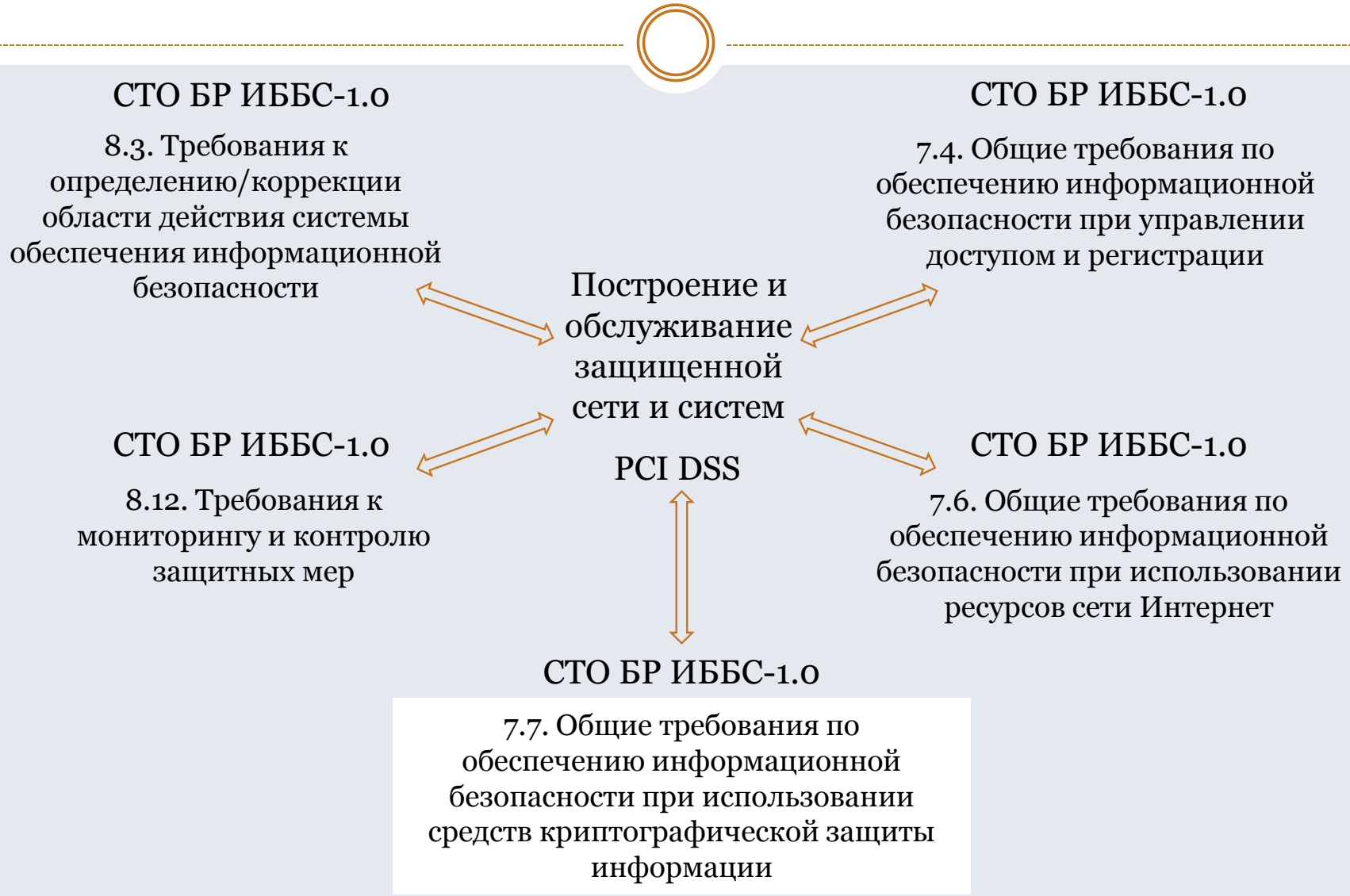
Программа управления уязвимостями

Поддержание политики ИБ

PCI DSS

Устанавливает фундаментальные технические и операционные требования

Построение и обслуживание защищенной сети и систем. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС



Построение и обслуживание защищенной сети и систем. Требование 1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

PCI DSS 3.0	СТО БР ИББС-1.0
1.1 Должны быть разработаны и внедрены стандарты конфигурации брандмауэров и маршрутизаторов. 1.2 Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в среде данных держателей карт. 1.3 Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом информационной среды держателей карт. 1.4 Установить персональные брандмауэры на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети. 1.5 Политики безопасности и процедуры управления брандмауэрами по умолчанию документированы, используются и известны всем заинтересованным лицам.	7.6.4. Рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on line. 7.6.10. При взаимодействии с сетью Интернет должны быть документально определены и использоваться защитные меры противодействия атакам хакеров и распространению спама. 8.12.1. Должны быть документально определены процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры должны проводиться персоналом организации БС РФ, ответственным за обеспечение ИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ. 8.12.3. Должны быть документально определены и выполняться процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер.

Построение и обслуживание защищенной сети и систем. Требование 2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

PCI DSS 3.0	СТО БР ИББС-1.0
2.1 Всегда изменяйте значения параметров и пароли, заданные поставщиками по умолчанию, и отключайте или удаляйте учетные записи по умолчанию перед подключением систем к сети. 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. 2.3 При использовании неконсольного административного доступа к системе следует всегда шифровать канал с использованием стойких криптографических алгоритмов. Следует использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа. 2.4 Вести учет системных компонентов, на которые распространяется действие стандарта PCI DSS. 2.5 Политики безопасности, процедуры управления учетными данными поставщиков по умолчанию и другие параметры безопасности документированы, используются и известны всем заинтересованным лицам. 2.6 Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон.	7.4.2. В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД. 7.6.2. В организации БС РФ должен быть документально определен порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственного за обеспечение ИБ. 7.7.1. Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России. 8.3.1. Должна быть документально определена опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации). Классификацию информационных активов рекомендуется проводить на основании оценок ценности информационных активов для интересов (целей) организации БС РФ, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов. 8.12.1. Должны быть документально определены процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры должны проводиться персоналом организации БС РФ, ответственным за обеспечение ИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ. 8.12.3. Должны быть документально определены и выполняться процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер.

Защита данных держателей карт. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС

СТО БР ИББС-1.0

7.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

СТО БР ИББС-1.0

7.6. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет

Защита данных держателей карт

PCI DSS

СТО БР ИББС-1.0

7.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов

Защита данных держателей карт. Требование 3. Обеспечить безопасное хранение данных держателей карт

PCI DSS 3.0

3.1 Хранение данных держателей карт должно быть ограничено только необходимым минимумом. Должны быть разработаны политики, процедуры и процессы хранения и уничтожения данных.

3.2 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). В случае получения критичных аутентификационных данных все данные невозможно будет восстановить по завершении процесса авторизации.

3.3 Следует маскировать основной номер держателя карты при его отображении (максимально возможное количество знаков для отображения – первые шесть и последние четыре), чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь основной номер держателя карты.

3.4 PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий).

3.5 Задокументировать и внедрить процедуры для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования следующим образом.

3.6 Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных держателей карт, в том числе следующие.

СТО БР ИББС-1.0

7.7.6. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем рекомендуется реализовать процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

7.7.7. Порядок применения СКЗИ определяется руководством организации БС РФ на основании указанных выше в данном разделе документов и должен включать:

— порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС;
— порядок эксплуатации;
— порядок восстановления работоспособности в аварийных случаях;
— порядок внесения изменений;
— порядок снятия с эксплуатации;
— порядок управления ключевой системой;
— порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

7.8.8. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать в том числе:

— защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;
— доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
— контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
— аутентификацию входящих электронных платежных сообщений;
— двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
— возможность ввода платежной информации в АБС только для авторизованных пользователей;
— контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
— восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
— сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;
— доставку электронных платежных сообщений участникам обмена.

Кроме того, в организации БС РФ рекомендуется организовать авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип “двойного управления”).

Защита данных держателей карт. Требование 4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования

PCI DSS 3.0	СТО БР ИББС-1.0
4.1 Для защиты данных держателей карт во время их передачи через общедоступные сети следует использовать надежные криптографические алгоритмы и протоколы защиты (например, SSL/TLS, IPSEC, SSH и т.д.) 4.2 Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты и т.д.). 4.3 Убедиться, что политики безопасности и процедуры шифрования передаваемых данных держателей карт документированы, используются и известны всем заинтересованным лицам.	7.6.3. В организациях БС РФ, осуществляющих дистанционное банковское обслуживание клиентов, в связи с повышенными рисками нарушения ИБ при взаимодействии с сетью Интернет должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии. 7.8.2. Банковский платежный технологический процесс должен быть документирован в организации БС РФ. 7.8.8. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать в том числе: — защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений; — доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации; — контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации; — аутентификацию входящих электронных платежных сообщений; — двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями; — возможность ввода платежной информации в АБС только для авторизованных пользователей; — контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.); — восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники; — сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов; — доставку электронных платежных сообщений участникам обмена. Кроме того, в организации БС РФ рекомендуется организовать авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип “двойного управления”).

Программа управления уязвимостями. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС

СТО БР ИББС-1.0

7.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

СТО БР ИББС-1.0

7.3. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла

Программа управления уязвимостями PCI DSS

СТО БР ИББС-1.0

8.12. Требования к мониторингу и контролю защитных мер

РС БР ИББС-2.6-2014

Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем

Программа управления уязвимостями. Требование 5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО

PCI DSS 3.0

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

5.2 Убедится, что все антивирусные механизмы:

• актуальны;

• выполняют периодическое сканирование;

• создают журналы регистрации событий.

5.3 Необходимо убедиться, что антивирусные программы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени.

5.4 Убедиться, что политики безопасности и процедуры защиты систем от вредоносного ПО документированы, используются и известны всем заинтересованным лицам.

СТО БР ИББС-1.0

7.5.1. На всех автоматизированных рабочих местах и серверах АБС организации БС РФ, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты.

Процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС должны быть документированы и осуществляться администраторами АБС или иными официально уполномоченными лицами Рекомендуется организовать автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ.

7.5.2. В организации БС РФ рекомендуется организовать функционирование постоянной антивирусной защиты в автоматическом режиме.

7.5.6. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

7.5.7. Должны быть документально определены процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

— необходимые меры по отражению и устранению последствий вирусной атаки;

— порядок официального информирования руководства;

— порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

7.5.8. Должны быть документально определены и выполняться процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС. Результаты контроля должны документироваться.

Программа управления уязвимостями. Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

PCI DSS 3.0	СТО БР ИББС-1.0
6.1 Должен быть внедрен процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также ранжирования риска (например, "высокий", "средний" или "низкий") недавно обнаруженных уязвимостей. 6.2 Все системные компоненты и программное обеспечение должны быть защищены от известных уязвимостей путем установки необходимых обновлений системы безопасности, выпущенных поставщиком. Критичные обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем. 6.3 Разработать безопасные внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс). 6.4 Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов. 6.5 Предотвращать распространенные уязвимости программного кода в процессе разработки ПО. 6.6 Следует обеспечить защиту общедоступных веб-приложений от известных атак (а также регулярно учитывать новые угрозы и уязвимости). 6.7 Убедиться, что политики безопасности и процедуры разработки для обеспечения безопасности систем и приложений документированы, используются и известны всем заинтересованным лицам.	7.3.2. Разработка технических заданий и приемка АБС должны осуществляться по согласованию и при участии подразделения (лиц) в организации БС РФ, ответственного за обеспечение ИБ. 7.3.3. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС должны осуществляться под контролем подразделения (лиц) в организации, ответственного за обеспечение ИБ. На стадии эксплуатации АБС должны быть документально определены и выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер. Результаты выполнения контроля должны документироваться. 7.3.4. Привлекаемые для разработки и (или) производства средств и систем защиты АБС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ. 7.3.5. Разрабатываемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации БС РФ. Приобретаемые организацией БС РФ готовые АБС и (или) их компоненты рекомендуется снабжать указанной документацией. Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки. В договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов организациям БС РФ должны включаться положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости или позиции фирмы-поставщика (разработчика), руководство организации БС РФ должно оценить и документально оформить допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов. 7.3.8. На стадии эксплуатации АБС должны быть документально определены и выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер. Результаты выполнения контроля должны документироваться. 7.3.9. На стадии сопровождения (модернизации) должны быть документально определены и выполняться процедуры контроля. Результаты выполнения контроля должны документироваться. 7.3.10. На стадии сопровождения (модернизации) при любом внесении изменения в АБС должны проводиться процедуры проверки функциональности, результаты которой должны документально фиксироваться. 8.12.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

Внедрение строгих мер контроля доступа. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС

СТО БР ИББС-1.0

7.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации

СТО БР ИББС-1.0

7.2. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу

Внедрение строгих мер контроля доступа

PCI DSS

СТО БР ИББС-1.0

7.1. Общие положения

Внедрение строгих мер контроля доступа. Требование 7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью

PCI DSS 3.0	СТО БР ИББС-1.0
7.1 Доступом к вычислительным ресурсам и данным держателей карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями. 7.2 Следует установить систему контроля доступа к системным компонентам, основанную на принципе необходимых полномочий и применить принцип "запрещено все, что явно не разрешено" ("deny all"). 7.3 Убедиться, что политики безопасности и процедуры ограничения доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	7.1.4. При распределении прав доступа работников и клиентов к информационным акт вам организации БС РФ следует руководствоваться принципами: — “знать своего клиента”; — “знать своего служащего”; — “необходимо знать”, а также рекомендуется использовать принцип “двойное управление”. 7.2.1. В организации БС РФ должны быть выделены и документально определены роли ее работников. Формирование ролей, связанных с выполнением деятельности по обеспечению ИБ среди прочего должно осуществляться на основании требований 7 и 8 разделов настоящего стандарта. 7.2.2. Роли следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть документально зафиксирована в должностных инструкциях.

Внедрение строгих мер контроля доступа. Требование 8. Определять и подтверждать доступ к системным компонентам

PCI DSS 3.0	СТО БР ИББС-1.0
8.1 Определить и внедрить политики и процедуры управления идентификацией сотрудников (не клиентов) и администраторов на всех системных компонентах, регламентирующие следующие требования. 8.2 Помимо назначения уникального идентификатора, для обеспечения надлежащего управления аутентификацией сотрудников (не пользователей) и администраторов на уровне всех системных компонентов должен применяться хотя бы один из следующих методов аутентификации всех пользователей: • то, что вы знаете (например, пароль или парольная фраза); • то, что у вас есть (например, ключи или смарт-карты); • то, чем вы обладаете (например, биометрические параметры). 8.3 Для средств удаленного доступа сотрудников (включая пользователей и администраторов) и любых третьих лиц (включая доступ поставщиков для поддержки или техобслуживания) во внутреннюю сеть из внешней сети должен быть реализован механизм двухфакторной аутентификации. 8.4 Задокументировать и проинформировать всех пользователей о процедурах и политиках аутентификации 8.5 Не использовать групповые, общие и стандартные учетные записи и пароли, а также прочие подобные методы аутентификации. 8.6 В случае использования других механизмов аутентификации (например, физических или логических токенов безопасности, смарт-карт, сертификатов и т.д.). 8.7 Любой доступ к базе данных держателей карт (включая доступ со стороны приложений, администраторов и любых других пользователей) должен быть ограничен. 8.8 Убедиться, что политики безопасности и процедуры идентификации и аутентификации документированы, используются и известны всем заинтересованным лицам.	7.4.1. В организации БС РФ должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий. Процедуры управления доступом должны исключать возможность “самосанкционирования”. Результаты контроля процедур должны документироваться. 7.4.2. В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД. 7.4.12. Работа всех пользователей АБС должна осуществляться под уникальными учетными записями.

Внедрение строгих мер контроля доступа. Требование 9. Ограничить физический доступ к данным держателей карт

PCI DSS 3.0	СТО БР ИББС-1.0
9.1 Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные держателей карт. 9.2 Разработать процедуры, позволяющие легко различать персонал организации и посетителей. 9.3 Контролировать физический доступ сотрудников к критичным помещениям. 9.4 Внедрить процедуры идентификации и авторизации посетителей. 9.5 Должна быть обеспечена физическая безопасность всех видов носителей. 9.6 Должен быть обеспечен строгий контроль за передачей всех видов носителей информации внутри организации и вне ее. 9.7 Должен быть обеспечен строгий контроль хранения носителей и управление доступом к ним. 9.8 Носители, хранение которых более не требуется для выполнения бизнес- задач или требований законодательства, должны быть уничтожены. 9.9 Обеспечить защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой, от подделки и подмены. 9.10 Убедиться, что политики безопасности и процедуры ограничения физического доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	7.4.2. В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД. 7.4.5. Порядок доступа работников организации БС РФ в помещения, в которых размещаются объекты среды информационных активов, должен быть регламентирован во внутренних документах организации БС РФ, а его выполнение должно контролироваться. Результаты контроля выполнения порядка доступа должны оформляться документально. 7.4.11. В организации БС РФ должны применяться защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ. Все попытки НСД и НРД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа.

Регулярный мониторинг и тестирование сети. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС

СТО БР ИББС-1.0

7.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации

СТО БР ИББС-1.0

7.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов

Регулярный мониторинг и тестирование сети

PCI DSS

СТО БР ИББС-1.0

8.12. Требования к мониторингу и контролю защитных мер

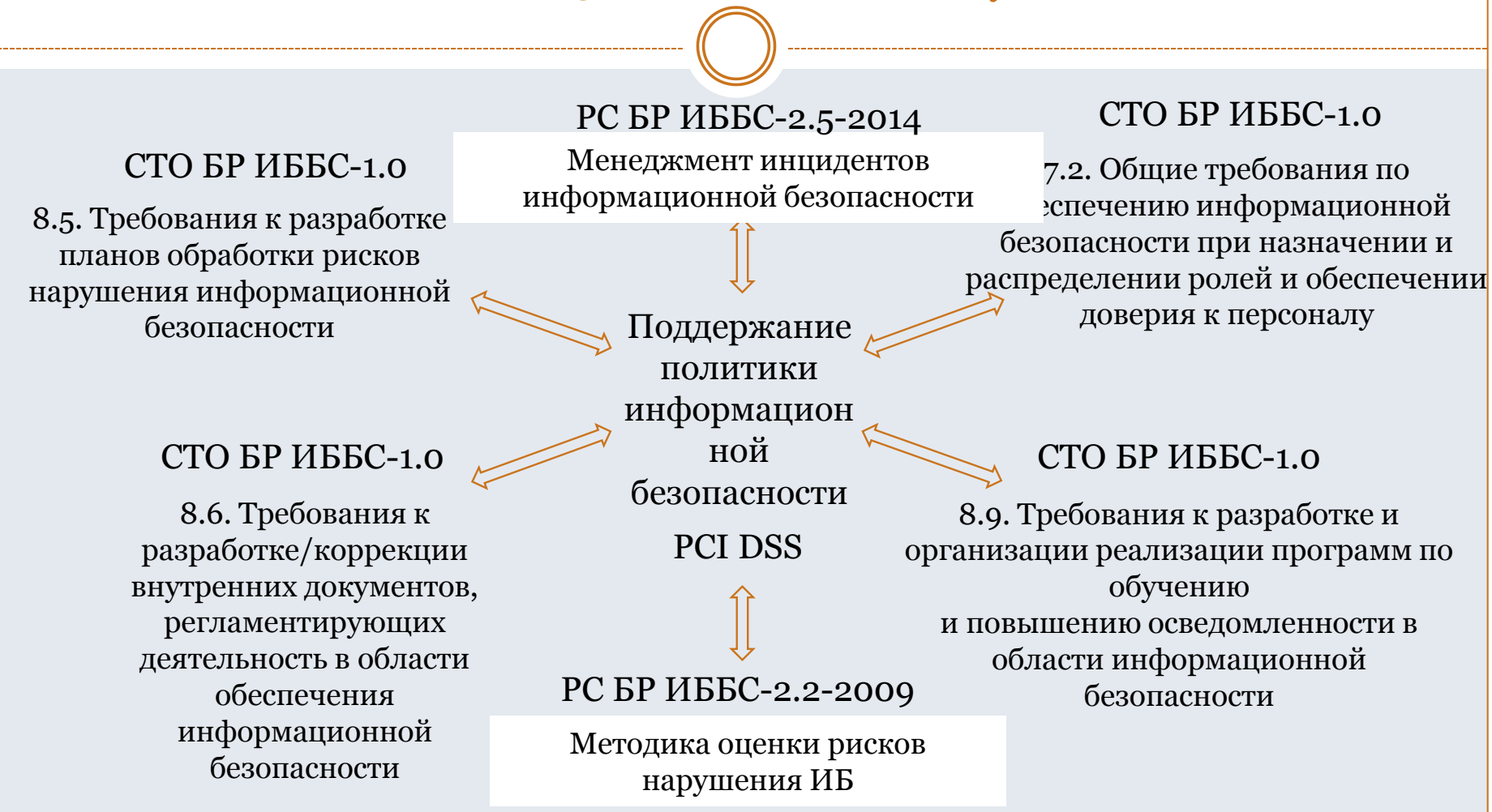
Регулярный мониторинг и тестирование сети. Требование 10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

PCI DSS 3.0	СТО БР ИББС-1.0
10.1 Внедрить журнал регистрации событий, связывающий любой доступ к системным компонентам с конкретным пользователем. 10.2 Для каждого системного компонента должен быть включен механизм протоколирования следующих событий. 10.3 Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры. 10.4 Все системные часы и системное время на критичных системах должны быть синхронизированы, необходимо убедиться в исполнении данного требования для получения, распространения и хранения данных о времени. 10.5 Журналы протоколирования событий должны быть защищены от изменений. 10.6 Изучать журналы протоколирования событий и события безопасности всех системных компонентов с целью обнаружения аномалий или подозрительной активности. 10.7 Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев (например, они могут находиться в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии). 10.8 Убедиться, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт документированы, используются и известны всем заинтересованным лицам.	7.4.3. В организации БС РФ должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий. Процедуры управления доступом должны исключать возможность “самосанкционирования”. Результаты контроля процедур должны документироваться. 7.4.4. В организации БС РФ необходимо документально определить процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций рекомендуется использовать специализированные программные и (или) технические средства. Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга и анализа должны применяться на регулярной основе, например, ежедневно, ко всем выполненным операциям и транзакциям. 7.4.11. В организации БС РФ должны применяться защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ. Все попытки НСД и НРД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа. 7.8.8. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать в том числе: — защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений; — доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации; — контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации; — аутентификацию входящих электронных платежных сообщений; — двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями; — возможность ввода платежной информации в АБС только для авторизованных пользователей; — контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.); — восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники; — сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов; — доставку электронных платежных сообщений участникам обмена.

Регулярный мониторинг и тестирование сети. Требование 11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

PCI DSS 3.0	СТО БР ИББС-1.0
11.1 Внедрить процессы для проведения ежеквартальной проверки наличия беспроводных точек доступа (802.11) и для обнаружения авторизованных и неавторизованных беспроводных точек доступа. 11.2 Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов). 11.3 Внедрить методологию проведения тестирования на проникновение. 11.4 Следует использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Следует осуществлять мониторинг сетевого трафика по периметру среды данных держателей карт и в критичных точках внутри среды данных держателей карт, и оповещать сотрудников о подозрительных действиях. Системы обнаружения и предотвращения вторжений и их сигнатуры должны поддерживаться в актуальном состоянии 11.5 Следует внедрить механизм защиты от изменений (например, мониторинг целостности файлов) для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных; сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю. 11.6 Убедиться, что политики безопасности и процедуры мониторинга и проверки безопасности документированы, используются и известны всем заинтересованным лицам.	8.12.1. Должны быть документально определены процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры должны проводиться персоналом организации БС РФ, ответственным за обеспечение ИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ. 8.12.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

Поддержание политики информационной безопасности. Соответствие PCI DSS 3.0 и комплекса документов БР ИББС



Поддержание политики информационной безопасности. Требование 12. Разработать и поддерживать политику информационной безопасности для всего персонала организации

PCI DSS 3.0	СТО БР ИББС-1.0
12.1 Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности. 12.2 Внедрить процесс оценки рисков. 12.3 Разработать правила эксплуатации критичных технологий и определить надлежащее применение для этих технологий. 12.4 Политика и процедуры обеспечения безопасности должны однозначно определять обязанности всего персонала организации, относящиеся к информационной безопасности. 12.5 Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью. 12.6 Должна быть внедрена официальная программа повышения осведомленности персонала по вопросам безопасности с целью донести до них важность обеспечения безопасности данных держателей карт. 12.7 Следует тщательно проверять кандидатов (будущий персонал) при приеме на работу для минимизации риска внутренних атак.	7.2.5. В организации БС РФ должны быть документально определены процедуры приема на работу, влияющую на обеспечение ИБ, включающие: — проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; — проверку в части профессиональных навыков и оценку профессиональной пригодности. Указанные процедуры должны предусматривать документальную фиксацию результатов проводимых проверок. 8.5.1. По каждому из рисков нарушения ИБ, который является недопустимым, должен быть документально определен план, определяющий один из возможных способов его обработки: — перенос риска на сторонние организации (например, путем страхования указанного риска); — уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска); — осознанное принятие риска; — формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирования планов по их реализации. 8.6.2. В организации БС РФ должны разрабатываться/корректироваться следующие внутренние документы: — политика ИБ организации БС РФ; — частные политики ИБ организации БС РФ; — документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ организации БС РФ. Кроме того, должны быть определены перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ в организации БС РФ. Политика ИБ организации БС РФ должна быть утверждена руководством. 8.6.5. Совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна содержать требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ организации БС РФ 8.6.7. В случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ, в организации БС РФ должен быть утвержден руководством порядок взаимодействия (координирования работы) службы ИБ с указанными работниками. 8.9.1. Должна быть организована документально оформленная и утвержденная руководством работа с персоналом организации БС РФ в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

Заключение

1. Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (комплекс документов БР ИББС) описывает единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства в том числе в части защиты данных держателей карт. Таким образом положения комплекса документов БР ИББС не противоречат фундаментальным техническим и операционным требованиям стандарта безопасности данных индустрии платежных карт (PCI DSS).
2. Гармонизацию комплекса документов БР ИББС и положений PCI DSS возможно осуществлять путем развития рекомендаций в области стандартизации Банка России.