Новые требования по защите данных владельцев платежных карт международных платежных систем

Содержание

Введение

В настоящей аналитической записке приводятся основные сведения о "Стандарте безопасности данных Индустрии платежных карт" (Payment Card Industry Data Security Standard — PCI DSS) и краткий обзор изменений, произошедших с момента выпуска стандарта. Анализируются изменения, появившихся в третьей версии стандарта PCI DSS.

Приводятся, изменившиеся с момента выхода второй версии стандарта, требования к лицам, проводящим оценку выполнения требований PCI DSS, а также методология оценки соответствия. На примере платежах систем VISA и MasterCard приводятся сведения об организациях, осуществляющих контроль за выполнением требований PCI DSS.

Описывается деятельность Банка России и Некоммерческого партнерства «АБИСС», направленная на адаптацию требований PCI DSS для российских кредитных организаций и стандартизацию требований по защите данных владельцев платежных карт в отраслевых стандартах Банка России.

Сравниваются и анализируются взаимосвязи требований PCI PSS и требований Положения Банка России №382-П. На примере российской платежной системы ПРО100 отмечаются преимущества соответствия требованиям PCI DSS, и описывается ответственность, которая грозит участникам платежных систем VISA и MasterCard в случае несоответствия требованиям PCI DSS.

Термины, определения и сокращения

Косвенный участник (associate / sponsored / indirect member / participant)	—	Участник платежной системы, с ограниченными правами, членство которого зависит от прямого участника.
Прямой участник (principal / direct member / participant)	—	Участник платежной системы с полными правами.
Спонсирующий участник (sponsoring member / direct participant)	—	Прямой участник платежной системы, который предоставил косвенному участнику возможность проведения расчетов с другими участниками платежной системы и несет ответственность за его деятельность.
Участник (member / participant / affiliate)	—	Участник платежной системы, не зависимо от его статуса в платежной системе.
Организация	—	Участник платежной системы, торгово-сервисное предприятие, поставщик услуг, процессинговый центр или иная организация, которая хранит, обрабатывает или передает данные о владельцах платежных карт или данные аутентификации.
Торгово-сервисное предприятие / точка продаж (merchant)	—	Юридическое лицо или индивидуальный предприниматель, уполномоченное банком участником принимать к оплате платежные карты.
Поставщик услуг (service providers)	—	Организация, которая обрабатывает, хранит или осуществляет передачу данных владельцев платежных карт по поручению участников, торгово-сервисных предприятий или других поставщиков услуг.
Процессинговый центр	—	Организация, осуществляющая обработку транзакций по платежным картам.
Владелец карты	—	Лицо, которому в соответствии с правилами платежной системы изготовлена платежная карта.
Международная платежная система		Система расчетов между банками разных стран, которые используют единые стандарты платежных средств. В настоящем стандарте рассматриваются международные платежные системы Visa и MasterCard, использующие платежные карты и широко распространенные в Российской Федерации.
СКЗИ	—	Средство криптографической защиты информации.
PCI	—	Payment card industry (Индустрия платежных карт).
PCI DSS	—	PCI Data Security Standard (Стандарт по защите данных PCI).
PCI SSC	—	PCI Security Standards Council (Совет по стандартам защиты PCI).
CDE	—	Cardholder Data Environment (Среда данных владельцев карт).
SAD	—	Sensitive authentication data (Конфиденциальные данные аутентификации).

Основные изменения требований по защите данных владельцев платежных карт

Общие сведения

Требования по защите данных владельцев платежных карт определены в Стандарте по защите данных Индустрии платежных карт. Требования и процедуры оценки безопасности (PCI DSS Requirements and Security Assessment Procedures).

Обязанность по соблюдению PCI DSS возлагается на любые организации, участвующие в обработке платежных карт, включая участников платежных систем, торгово-сервисные предприятия, процессинговые центры, поставщиков услуг.

Обязанность по соблюдению стандарта возникает при заключении договора о присоединении к международной платежной системе, а также установлена в правилах платежных систем, разработанных международными платежными системами в соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и «Положения о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» Банка России от 9 июня 2012 г. № 382-П (далее — Положение №382-П).

Хронология изменений

Первая версия стандарта PCI DSS была разработана в 2004 году пятью международными платежными системами American Express, Discover Financial Services, JCB International, MasterCard Worldwide и Visa Inc.

В 2006 году указанные платежные системы сформировали Совет по стандартам защиты индустрии платежных карт (PCI SSC). PCI SSC считается независимым от учредивших его платежных систем и в настоящее время занимается сопровождением и развитием Стандартов защиты PCI.

В ноябре 2013 года PCI SSC опубликовал версию 3.0 стандарта PCI DSS. В таблице 1 приведены краткие сведения о ранее опубликованных версиях стандарта.

Таблица 1 — Основные версии стандарта PCI DSS

Версия стандарта	Год публи-кации	Срок действия	Основные изменения
1.0	2004	01.01.2004 — 31.12.2006	–
1.1	2006	01.01.2007 — 31.12.2008	Добавлена возможность использования компенсационных мер, разъяснения, внесены незначительные изменения
1.2	2008	01.01.2009 — 31.12.2011	Добавлены процедуры проверки выполнения требований стандарта, разъяснения и уточнения требований, в частности ограничение на использование беспроводных сетей, основанных на стандартах безопасности Wired Equivalent Privacy (WEP). Добавлен подзаголовок в наименовании стандарта «Требования и процедуры оценки безопасности»
2.0	2010	01.01.2011 — 31.12.2013[1]	Добавлены разъяснения, уточнения и новые требования: – ранжирование уязвимостей по уровню соответствующего им риска; – идентификация всех уязвимостей с «высокой» оценкой в процессе разработки приложений. Новые требования становятся обязательными с 01.07.2012
3.0	2013	01.01.2014 —	Добавлены разъяснения, уточнения и новые требования, Требования стандарта становятся обязательными с 01.01.2014, за исключением отдельных положений, вступающих в силу с 01.07.2015. Описание новых требований приведено ниже

[1] Отдельные положения стандарта продолжают действовать до 30.06.2015.

Описание изменений

Структура требований

В целом структура требований в версии 3.0 осталась прежней, за исключением нескольких утонений и дополнений. В стандарте выделяется 6 целей защиты данных владельцев платежных карт, которые достигаются реализацией следующих 12 групп требований.

Построить и поддерживать защищенную сеть ***и системы***[1].

1. Установить и поддерживать конфигурацию межсетевых экранов для защиты данных владельцев платежных карт.

2. Не использовать заданные производителем настройки паролей и других параметров безопасности.

Защитить данные владельцев платежных карт.

3. Обеспечить защиту данных владельцев платежных карт при хранении.

4. Обеспечить шифрование данных владельцев платежных карт при передаче по открытым сетям или сетям общего пользования.

Поддерживать программу по управлению уязвимостями.

5. ***Обеспечить защиту всех систем от вредоносного программного обеспечения***[2] *и регулярно обновлять антивирусное программное обеспечение или программы.*

6. Разработать и поддерживать защищенные системы и приложения.

Внедрить строгие методы контроля доступа.

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

8. ***Осуществлять идентификацию и аутентификацию при доступе к компонентам системы***[3].

9. Ограничить физический доступ к данным владельцев платежных карт.

Регулярно контролировать и тестировать сеть.

10. Отслеживать и контролировать любой доступ к сетевым ресурсам и данным владельцев платежных карт.

11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

Поддерживать политику информационной безопасности.

12. Поддерживать политику, которая определяет вопросы информационной безопасности для всего персонала.

Область распространения требований

В новой версии стандарта вместо области оценки соответствия используется понятие область распространения требований PCI DSS. Согласно стандарту в область распространения требований входят все компоненты системы, являющиеся частью или подключенные к среде данных владельцев платежных карт (CDE). CDE включает людей, процессы и технологии, с использованием которых осуществляется хранение, обработка или передача данных владельцев платежных карт или конфиденциальных данных аутентификации (SAD). К компонентам системы относится сетевое оборудование, серверы, вычислительные устройства и приложения.

Рекомендуемый порядок внедрения требований

Не все требования PCI DSS одинаково эффективны для защиты данных владельцев платежных карт. Для тех организаций, которые в первые внедряют стандарт PCI DSS, PCI SSC разрабатывает документ «PCI DSS. Упорядоченный подход к внедрению PCI DSS». Этот документ призван помочь организациям на пути достижения соответствия требованиям PCI DSS и сначала реализовать наиболее эффективные меры, тем самым максимально сократить риски утечки данных владельцев платежных карт уже на первых этапах внедрения требований стандарта.

---

[1] Дополнение появилось в PCI DSS версии 3.0.

[2] Ранее требовалось обязательное использование антивирусного программного обеспечения или программ.

[3] Ранее требовалось назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре.

В новой версии стандарта впервые приводится ссылка на документ «Упорядоченный подход к внедрению PCI DSS»[1], однако новая версия документа, учитывающая требованияPCI DSS v3.0, пока не вышла.

Следует отметить, что для достижения соответствия PCI DSS, должны быть удовлетворены все требования стандарта, вне зависимости от очередности их внедрения.

Процесс оценки соответствия

Вместо «этапов проведения оценки соответствия» появился «процесс оценки соответствия требованиям PCI DSS». Процесс оценки фактически не изменился и заключается в следующем:

1. Проверить область оценки соответствия требованиям PCI DSS.
2. Провести оценку соответствия требованиям PCI DSS, следуя процедурам проверки для каждого требования.
3. Если требуется, принять корректирующие меры для каждого не выполненного требования.
4. Заполнить Опросный лист самооценки (SAQ) или Отчет об оценке соответствия (ROC), включая документацию по всем компенсационным мерам, в соответствии с руководством и инструкциями PCI.
5. Заполнить Аттестат соответствия (для поставщиков услуг или торгово-сервисных предприятий).
6. Представить SAQ или ROC и Аттестат соответствия с отчетом ASV о сканировании контролирующей организации.

Для оценки соответствия больших организаций и информационных систем, в стандарте приводятся рекомендации по формированию выборки объектов и компонентов информационной системы для обследования. В новой версии стандарта явно указано, что эти требования распространяются только на лиц, проводящих оценку соответствия, — как на внутренних, так и на внешних аудиторов.

Лучшие практики по внедрению PCI DSS

В стандарте появился новый раздел «Лучшие практики по внедрению PCI DSS в обычную деятельность организации», содержащий рекомендации по обеспечению постоянного соответствия требованиям PCI DSS, в том числе:

а) контроль (мониторинг) защитных мер, таких как межсетевые экраны, системы обнаружения и предотвращения вторжений, обеспечения целостности, антивирусной защиты, контроля доступа и др;
б) обнаружение отказов защитных мер и своевременное принятие необходимых действий, включающих:
   - восстановление защитных мер;
   - выявление причин отказа;
   - выявление и устранение инцидентов безопасности, возникших во время отказа защитных мер;
   - принятие мер, направленных на устранение причин отказа защитных мер;
   - возобновление контроля защитных мер, при необходимости в усиленном режиме, чтобы подтвердить эффективность работы защитных мер;
в) предварительный анализ изменений условий функционирования организации и принятие соответствующих мер, в том числе:
   - оценка влияния на область распространения требований PCI DSS;
   - выявление требований PCI DSS, применимых к новым (изменившимся) системам и сетям;
   - обновление области распространения требований PCI DSS и внедрение требуемых защитных мер;
г) документирование результатов анализа воздействия изменений организационной структуры на область распространения и требования PCI DSS;
д) проведение периодических проверок, чтобы подтвердить соблюдение требований PCI DSS и выполнение процедур безопасности персоналом;
е) ежегодная проверка наличия поддержки используемого оборудования и программного обеспечения производителем и того, что они удовлетворяют требованиям безопасности организации и PCI DSS в частности;
ж) разделение обязанностей по обеспечению безопасности и (или) аудиту от других функций.

[1] Prioritized Approach for PCI DSS.

Отчет об оценке соответствия

Раздел «Инструкции по составлению и содержанию отчета об оценке соответствия» в новой версии стандарта был сокращен. Согласно данному разделу при формировании отчетности по результатам оценки соответствия необходимо использовать PCI DSS «Шаблон отчета об оценке соответствия» (PCI DSS ROC Reporting Template) и следовать инструкциям платежных систем. Форма отчета об оценке соответствия из PCI DSS исключена. А «Шаблон отчета об оценке соответствия» в настоящее время не опубликован. Предполагается, что он будет опубликован в документе PCI DSS «Report on Compliance (ROC) Reporting Template and Reporting Instructions», который упоминается в стандарте. Вероятно, этот документ будет разработан на основе опубликованного PCI SSC в 2011 году документа «ROC. Инструкций по формированию отчетности по PCI DSS v2.0»[1].

Изменения требований PCI DSS

В разделе «Детальные требования PCI DSS и процедуры оценки безопасности» в таблицах с требованиями исчезли графы «In Place», «Not In Place» «Target Date/Comments», в место них появилась графа «Guidance», в которой поясняется суть требований.

В группах требований с 1 по 11 добавлены требования, в соответствии с которыми по каждой группе требований должны существовать документированные политики и операционные процедуры, требования которых должны выполняться и доводиться до сведения вовлеченного персонала.

В новой версии стандарта появились или были существенно изменены в общей сложности 19 требований, приведенных в таблице 2.

Таблица 2 — Новые требования PCI DSS

Группа требований	Измененное / новое требование	Дата вступления в силу
1 Установить и поддерживать конфигурацию межсетевых экранов для защиты данных владельцев платежных карт	*(1.1 Разработать и внедрить стандарт конфигурации межсетевых экранов и маршрутизаторов, который включает:)* 1.1.3 Актуальную схему потоков данных владельцев платежных карт в системах и компьютерной сети	01.01.2014
2 Не использовать заданные производителем настройки паролей и других параметров безопасности	2,4 Наличие актуального перечня компонентов системы, входящих в область PCI DSS (с описанием функций/назначения каждого из них)	01.01.2014
5 Обеспечить защиту всех систем от вредоносного программного обеспечения	*(5.1 Установить антивирусное ПО на всех системах, которые подвержены воздействию вредоносного ПО).* 5.1.2 Для систем, которые обычно считаются не подверженными воздействию вредоносного ПО, проводить периодическую оценку, для идентификации и оценки изменяющихся угроз, вызванных вредоносным ПО, чтобы удостовериться, что для данных систем не требуется антивирусная защита	01.01.2014
	5.3 Обеспечить работу антивирусных средств в активном состоянии и невозможность их отключения или изменения пользователем, кроме случаев, когда такое отключение делается на ограниченное время, и санкционировано руководством	01.01.2014
6 Разработать и поддерживать защищенные системы и приложения	*(6.5. В процессе разработки ПО принять меры по недопущению уязвимостей кода, включающие: обучение персонала… и использование инструкций по разработке приложений методами безопасного программирования).* 6.5.10 Обеспечить защиту от ошибок при аутентификации и управлении сессиями *(для веб-приложений и интерфейсов приложений)*	**01.07.2015**

[1] PCI DSS. ROC Reporting Instructions for PCI DSS v2.0

Группа требований	Измененное / новое требование	Дата вступления в силу
8. Осуществлять идентификацию и аутентификацию при доступе к компонентам системы	*(8.2 В дополнение к присвоению уникального идентификатора обеспечить надлежащее управление аутентификацией пользователей для пользователей не являющихся клиентами и администраторов ...)* 8.2.3 Пароли / ключевые фразы должны удовлетворять следующим критериям: – минимальная длина не менее 7 символов; – содержат как цифровые, так и буквенные символы. Либо пароли / ключевые фраз должны обладать сложностью и стойкостью эквивалентной указанным выше параметрам	01.01.2014
	(8.5 Не использовать групповые, совместно используемые или общие идентификаторы, пароли или другие средства (методы) аутентификации ...) 8.5.1 Дополнительное требование к поставщикам услуг: Поставщики услуг с удаленным доступом к активам клиентов (например, для поддержки POS систем или серверов) должны использовать уникальные аутентификационные данные (такие как пароли/ ключевые фразы) для каждого клиента	**01.07.2015**
	8.6 При использовании других механизмов аутентификации данные механизмы должны быть назначены с учетом следующего: – механизм аутентификации должен быть назначен отдельной учетной записи и не должен использоваться для доступа к нескольким учетным записям; – механизмы физического и/или логического контроля должны использоваться, чтобы обеспечить возможность использования такого механизма аутентификации для получения доступа только для соответствующей учетной записи	01.01.2014
9. Ограничить физический доступ к данным владельцев платежных карт	9.3 Обеспечить контроль физического доступа персонала в области с ограниченным доступом, с учетом следующих требований: – доступ должен быть разрешен и предоставляться на основе должностных обязанностей субъекта; – доступ прекращается незамедлительно при прекращении выполнения должностных обязанностей и физические средства для доступа, такие как ключи, карты доступа, и т.д., возвращены или заблокированы	01.01.2014
	9.9 Защитить устройства, которые считывают данные платежных карт при непосредственном физическом взаимодействии с картой, от внесения в них изменений или подмены, в том числе: 9.9.1 иметь и поддерживать в актуальном состоянии перечень таких устройств; 9.9.2 осуществлять периодический осмотр устройств, с целью выявления следов внесения в них изменений или подмены; 9.9.3 проводит обучение персонала с целью информирования о возможности внесения изменения или подмены устройств	**01.07.2015**
10 Отслеживать и контролировать любой доступ к сетевым ресурсам и данным владельцев платежных карт	*(10.2. Обеспечить автоматическое ведение журналов аудита и возможность реконструкции следующих событий:)* 10.2.5 Использование или изменение механизма идентификации и аутентификации, включая создание новой учетной записи, повышение привилегий, а также всех изменение, добавление, удаление учетных записей с правами администратора; 10.2.6 Инициализация, выключение или остановка протоколирования событий	01.01.2014

Группа требований	Измененное / новое требование	Дата вступления в силу
11 Регулярно выполнять тестирование систем и процессов обеспечения безопасности	11.1 Внедрить процесс обнаружения беспроводных точек доступа и осуществлять ежеквартальное обнаружение и идентификацию авторизованных и неавторизованных точек доступа. В том числе: 11.1.1 вести перечень авторизованных точек доступа, включая документальное подтверждение требований бизнеса; 11.1.2 внедрить процедуру реагирования на инциденты, для случая обнаружения несанкционированных точек доступа	01.01.2014
	11.3 Внедрить методологию тестирования на проникновение, которая включает: – принятые в отрасли методы тестирования на проникновение (например, NIST SP 800-115); – все критические и пограничные системы, входящие в CDE; – тестирование как снаружи, так и изнутри сети; – тестирование для подтверждения корректности сегментации сети и механизмов, использованных для сокращения области распространения требований PCI DSS; – определять тесты на проникновение на уровне приложений, с учетом как минимум уязвимостей, перечисленных в требовании 6.5; – определять тесты на проникновение на сетевом уровне, включая компоненты, которые обеспечивают функционирование сети, а также операционных систем; – включать анализ и рассмотрение угроз и уязвимостей, которые были обнаружены за последние 12 месяцев; – устанавливать сроки хранения результатов тестирования и результатов внедрения корректирующих мер	**01.07.2015**[1]
	(11.3 Внедрить методологию тестирования на проникновение). 11.3.4 В случае использования сегментации для изоляции CDE от других сетей проводить тестирование на проникновение как минимум ежегодно и после любых изменений в методах/механизмах сегментации, чтобы обеспечить работоспособность и эффективность сегментации для изоляции систем, входящих в область требований PCI DSS, от других систем	01.01.2014
	(11.5 Внедрить механизмы обнаружения изменений … и настроить ПО для контроля изменений на контроль критичных файлов как минимум раз в неделю). 11.5.1 Внедрить процесс реагирования на все уведомления, сформированные системой обеспечения целостности	01.01.2014
12 Поддерживать политику, которая определяет вопросы информационной безопасности для всего персонала	12.2 Внедрить процесс оценки рисков, который: – проводится как минимум ежегодно и в случае существенных изменений условий функционирования (например, изменение собственника, слияние, переезд и т.д.); – предусматривает идентификацию критичных активов, угроз и уязвимостей; – предусматривает наличие документированных результатов	01.01.2014
	(12.8 Разработать и внедрить политики и процедуры управления отношениями с поставщиками услуг …, в том числе:) 12.8.5 Вести информацию о том, какие требования PCI DSS реализуются каждым из поставщиками услуг, а какие — организацией	01.01.2014

[1] До вступления в силу требования 11.3 должны соблюдаться требования к тестированию на проникновение, установленные в PCI DSS v2.0.

Группа требований	Измененное / новое требование	Дата вступления в силу
	12.9 Дополнительное требование к поставщикам услуг: Поставщики услуг должны в письменной форме подтверждать своим клиентам, что они несут ответственность за безопасность данных владельцев платежных карт, которыми они обладают или иных образом хранят, обрабатывают или передают по поручению клиентов, или с учетом того, что они могут повлиять на безопасность CDE клиента	**01.07.2015**

Кроме того, в новой версии стандарта содержится 65 уточнений и дополнений существующих требований.

Требования к оценщикам безопасности

Оценка соответствия требованиям стандарта, как и ранее, должна проводиться ежегодно и может быть проведена либо в форме самооценки, либо в форме внешней оценки соответствия.

Самооценка проводится самой организацией, при этом рекомендуется, чтобы оценщик прошел обучение по программе PCI SSC «Внутренний оценщик безопасности» — ISA (Internal Security Assessor).

Внешняя оценка соответствия может проводиться только организаций, имеющей статус сертифицированного оценщика безопасности — QSA (Qualified Security Assessor). Перечень организаций, имеющих статус QSA опубликован на сайте PCI SSC.

Возможность проведения самооценки для подтверждения соответствия требованиям PCI DSS определяется правилами платежной системы, в соответствии с рекомендациями PCI SSC, и зависит от характера участия организации в платежной системе и количества транзакций с использованием платежных карт в год.

В настоящее время установлены ограничения на проведение самооценки, приведенные в таблице 3.

Таблица 3 — Критерии допустимости проведения самооценки

Характер участия в платежной системе	Критерий проведения самооценки[1]
Торгово-сервисное предприятие	Level 2-4 (менее 6 млн. транзакций в год[2])
Поставщик услуг	Level 2 (менее 300 тыс. транзакций в год)
Процессинговый центр	Категория 3 (Client Acquiring VNPs[3])
Косвенный участник	По требованию спонсирующего участника (как правило, в соответствии Level 2 поставщика услуг – менее 300 тыс. транзакций в год)
Прямой участник	—[4]

Вместо самооценки любая организация, вне зависимости от характера ее участия в платежной системе или количества транзакций с использованием платежных карт, может провести внешнюю оценку соответствия.

Кроме того, участники[5] платежной системы должны выполнять как минимум ежеквартальное внешнее сканирование на выявление уязвимостей, проводимое одобренным PCI SSC поставщиком услуг по сканированию — ASV (Approved Scanning Vendor). Перечень организаций, имеющих статус ASV опубликован на сайте PCI SSC.

[1] Количество транзакций определяется отдельно для каждой платежной системы.

[2] Уровень торгово-сервисного предприятия может быть повышен платежной системой для организации индивидуально.

[3] Процессинговый центр, принадлежащий банку, обслуживающему торгово-сервисному предприятию, или другому клиенту, который обрабатывает только транзакции от своих клиентов и использует только разрешенные номера банков (BIN).

[4] Для прямых участников платежных систем предусмотрена только процедура внешней оценки соответствия, которая проводится ежегодно.

[5] Необходимость предоставления результатов сканирования для торгов сервисных предприятий Level 4 (менее 20 тыс. транзакций от электронной коммерции или менее 1 млн. транзакций по всем другим каналам), определяется банком, обслуживающим соответствующее торгово-сервисное предприятие.

Методология оценки соответствия

Как упоминалось в предыдущем подразделе, проверка выполнения требований PCI DSS может проводиться в форме самооценки или оценки соответствия.

В обоих случаях проверяется выполнение всех требований PCI DSS, в соответствии с процедурами, установленными в стандарте.

При проведении самооценки следует использовать «Self-assessment Questionnaires (SAQs) and SAQ Instructions and Guidelines»[1]. По результатам самооценки необходимо заполнить соответствующий лист самооценки — SAQ (Self-assessment Questionnaires), при необходимости описать компенсационные меры, пояснить причину неприменимости отдельных требований стандарта, представить план устранения недостатков, заполнить аттестат соответствия — AOC (Attestation of Compliance)[2].

При проведении оценки соответствия необходимо следовать документу PCI SSC «Report on Compliance (ROC) Reporting Template and Reporting Instructions»[3]. По результатам оценки соответствия должен быть сформирован отчет об оценке соответствия (ROC), а для торгово-сервисных предприятий и поставщиков услуг так же аттестат соответствия (AOC).

SAQ/ROC и AOC с приложенными результатами сканирования ASV являются достаточными документами для подтверждения соответствия требованиям PCI DSS. Данные документы должны быть переданы в контролирующую организацию. В таблице 4 приведены, организации, контролирующие выполнение требований PCI DSS участниками платежной системы.

Кроме указанных документов, организация должна располагать документами, подтверждающими выполнение требований PCI DSS участниками платежной системы, которых она контролирует.

Таблица 4 — Организации, контролирующие выполнение требований PCI DSS

Участник платежной системы	Контролирующая организация
Прямой участник	Платежная система
Косвенный участник	Спонсирующий участник
Торгово-сервисное предприятие	Участник, с которым торгово-сервисное предприятие заключило договор на осуществление расчетов с использованием платежных карт
Поставщик услуг	Участник, заключивший договор с поставщиком услуг
Процессинговый центр, подключенный напрямую Visa Net	Платежная система
Иной процессинговый центр	Участник, заключивший договор с процессинговым центром

[1] Размещенные на сайте версии данных документ не учитывают изменения, появившиеся в PCI DSS v3.0.

[2] Размещенные на сайте версии данных документ не учитывают изменения, появившиеся в PCI DSS v3.0.

[3] На момент написания аналитической записки данный документ не опубликован.

Защита данных владельцев платежных карт при обеспечении информационной безопасности организаций банковской системы Российской Федерации

Стандарты Банка России не содержат требований об обязательном соответствии PCI DSS. Несмотря на то, что требования стандартов частично пересекаются, в настоящее время они не гармонизированы.

В 2011 был создан Технический комитет №122 «Стандарты финансовых операций» в состав, которого вошел Подкомитет №1 «Безопасность финансовых (банковских) операций», одной из целей которого является гармонизация профессиональных стандартов обеспечения информационной безопасности банковской и платежной индустрий, в том числе, со стандартами PCI DSS.

В 2013 году при поддержке Центрального банка Российской Федерации и НП «АБИСС», был разработан официальный перевод PCI DSS v2.0 на русский язык и PCI SSC был запущен минисайт, содержащий русскоязычную версию стандарта, а также ряд сопутствующих документов.

Стандарт PCI DSS версии 3.0 в настоящее время официально не переведен на русский язык.

Защита данных владельцев платежных карт в национальной платежной системе

В соответствии с требованиями Положения №382-П оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств.

В соответствии с требованиями Положения №382-П оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Кроме того, оператор по переводу денежных средств обеспечивает выполнение банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к обеспечению защиты информации при осуществлении переводов денежных средств, а также контроль соблюдения этих требований.

В платежной системеVisa обязанность по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств возложена на участников платежной системы и расчетные центры. При этом Участник платежной системы должен обеспечить выполнение требований стандарта PCI DSS.

В платежной системе MasterCard требования по защите информации не раскрываются в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

Поскольку соблюдение требований PCI DSS стало фактически частью требований национальной платежной системы, в ходе проверок выполнения требований Положения №382-П следует проверять наличие свидетельств выполнения требований PCI DSS — наличие SAQ/ROC, AOC, и результатов сканирования ASV. В приложении А приведены результаты сравнительного анализа требований PCI DSS и Положения №382-П.

В соответствии с правилами платежной системы «Универсальная электронная карта» («ПРО100») наличие подтверждения соответствия стандарту PCI DSS может стать основанием для освобождения субъекта платежной системы от проверки со стороны ее оператора (либо внешнего аудита), проводимого не реже одного раза в два года.

Ответственность за нарушение

Ответственность за несоблюдение требований PCI DSS устанавливается системой управления рисками и штрафными санкциями, установленными в платежной системе. В таблице 5 приведены величины штрафных санкций за нарушение требований платежных систем по защите данных[1].

Таблица 5 — Штрафные санкции за нарушение требований по защите данных платежных систем

Платежная система	Нарушение	Участник	Торгово-сервисное предприятие		Поставщики услуг
			1, 2 уровень	3 уровень	
Visa[2]	Первое	$50 000	—	—	—
	Второе	$100 000	—	—	—
	Третье и последующее	$200 000	—	—	—
MasterCard	Первое	$25 000	$25 000	$10 000	$25 000
	Второе	$50 000	$50 000	$20 000	$50 000
	Третье	$75 000	$100 000	$40 000	$100 000
	Четвертое и последующее	$100 000	$200 000	$80 000	$200 000

Кроме того, невыполнение требований PCI DSS может рассматриваться как нарушение правил защиты информации и законодательства о национальной платежной системе и наказываться в соответствии с Кодексом РФ об административных правонарушениях.

Статья 13.12. Нарушение правил защиты информации

6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных частями 1, 2 и 5 настоящей статьи, -

влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от одной тысячи до двух тысяч рублей; на юридических лиц - от десяти тысяч до пятнадцати тысяч рублей.

Статья 15.36. Неисполнение предписания Банка России, направленного им при осуществлении надзора в национальной платежной системе

Повторное в течение года неисполнение оператором платежной системы, операционным центром, платежным клиринговым центром предписания Банка России, направленного им при осуществлении надзора в национальной платежной системе, -

влечет наложение административного штрафа на должностных лиц в размере от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от ста тысяч до пятисот тысяч рублей.

[1] Приведенные значения не учитывают штрафные санкции в случае компрометации данных владельцев платежных карт.
[2] Величина штрафных санкций к торгово-сервисным предприятиям и поставщикам услуг определяется прямым участником платежной системы и (или) иным участником, ответственным за их соответствие требованиям платежной системы.

Приложение А
Сравнительный анализ требований PCI DSS и Положения №382-П

Наименование группы требований из PCI DSS v3.0	***Соответствующие требования Положения №382-П***		
	Краткое описание группы требований	***Номер подпункта (требования) и краткое описание требования***	***Несоответствия***
1. Установить и поддерживать конфигурацию межсетевых экранов для защиты данных владельцев платежных карт	Пункт 2.8 регламентирует требования по защите информации при использовании информационно-телекоммуникационной сети Интернет	2.8.1 (П.56) регламентирует использование фильтрации сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры	Не определены обязательные параметры конфигурации межсетевых экранов и маршрутизаторов
2. Не использовать заданные производителем настройки паролей и других параметров безопасности	—	—	Данная группа требований не отражена в Положении № 382-П
3. Обеспечить защиту данных владельцев платежных карт при хранении	Пункт 2.5 регламентирует требования по защите информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры	2.5.6 (П.15) устанавливает запрет несанкционированного копирования защищаемой информации. 2.5.6 (П.16) определяет необходимость защиты резервных копий защищаемой информации. 2.5.6 (П.17 - П.18) регламентирует уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, способом, обеспечивающим невозможность ее восстановления	Не установлены требования к хранению PAN (номера платежной карты)
	Пункт 2.6 регламентирует требования по защите информации от несанкционированного доступа	2.6.3 (П.29, П.29.1-П.29.4) определяет порядок хранения и регистрации информации о владельцах платежных карт	
	Пункт 2.10 регламентирует требования по защите информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технологических мер защиты информации	2.10.4 (П.76) регламентирует контроль соблюдения технологии хранения защищаемой информации. 2.10.4 (П.79) регламентирует восстановление данных держателей карт в случае умышленного (случайного) разрушения (искажения)	

Наименование группы требований из PCI DSS v3.0	***Соответствующие требования Положения №382-П***		
	Краткое описание группы требований	***Номер подпункта (требования) и краткое описание требования***	***Несоответствия***
	Пункт 2.9 регламентирует требования по защите информации при использовании СКЗИ	2.9.1-2.9.5 (П.58-П.70) определяют порядок использования СКЗИ	
4. Обеспечить шифрование данных владельцев платежных карт при передаче по открытым сетям или сетям общего пользования	Пункт 2.8 регламентирует требования по защите информации при использовании информационно-телекоммуникационной сети Интернет	2.8.1 (П.53) регламентирует использование технических средств защиты информации для предотвращения несанкционированного доступа при передаче по сети Интернет	—
	Пункт 2.9 регламентирует требования по защите информации при использовании СКЗИ	2.9 (П.58, П.70) определяют порядок применения СКЗИ	
5. Обеспечить защиту всех систем от вредоносного программного обеспечения и регулярно обновлять антивирусное программное обеспечение или программы	Пункт 2.7 регламентирует требования по защите информации от воздействия вредоносного кода	2.7.1. (П.40, П.42) определяет необходимость использования технических средств защиты информации от воздействия вредоносного кода. 2.7.1. (П.41) определяет необходимость регулярно обновлять версии технических средств защиты информации от воздействия вредоносного кода	—
6. Разработать и поддерживать защищенные системы и приложения	Пункт 2.7 регламентирует требования по защите информации от воздействия вредоносного кода	2.7.1 (П.41) определяет необходимость регулярно обновлять версии технических средств защиты информации от воздействия вредоносного кода. 2.7.4 (П.46) регламентирует проведение проверок на наличие вредоносного кода после установки или изменения программного обеспечения	Не регламентирована регулярная установка критических обновлений безопасности на все системные компоненты и программное обеспечение. Не определены требования к разрабатываемым приложениям. Не регламентирована разработка и внедрение процедур управления изменениями системных компонентов. Не приводятся рекомендаций по разработке и внедрению приложений и системных процедур
	Пункт 2.8 регламентирует требования по защите информации при использовании информационно-телекоммуникационной сети Интернет	2.8.1. (П.56) регламентирует использование фильтрации сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры	
	Пункт 2.16 регламентирует требования к доведению до оператора платежной системы информации об обеспечении защиты	2.16.2 (П.120) устанавливает, что для анализа обеспечения защиты необходимо направлять оператору платежной системы информацию о выявленных угрозах и уязвимостях в защите	

Наименование группы требований из PCI DSS v3.0	*Соответствующие требования Положения №382-П*		
	Краткое описание группы требований	*Номер подпункта (требования) и краткое описание требования*	*Несоответствия*
	Пункт 2.17 регламентирует требования к совершенствованию защиты информации	2.17.2 (П.126) регламентирует порядок принятия мер, направленных на совершенствование защиты информации, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации	
7. Ограничить доступ к данным владельцев платежных карт в соответствии со служебной необходимостью	Пункт 2.4 регламентирует требования по защите информации при назначении и распределении функциональных прав и обязанностей лиц	2.4.1 (П.1-П.4) определяют необходимость регистрации лиц, имеющих доступ к защищаемой информации. 2.4.3 (П.7) устанавливает контроль и регистрацию действий лиц, имеющих доступ к защищаемой информации	—
	Пункт 2.6 регламентирует требования по защите информации от несанкционированного доступа	2.6.4. (П.31-П.32) устанавливает требование по назначению работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации и запрет на несанкционированное расширение прав доступа	
8. Осуществлять идентификацию и аутентификацию при доступе к компонентам системы	Пункт 2.6 регламентирует требования по защите информации от несанкционированного доступа	2.6.3 (П.21-П.28) регламентирует процедуры идентификации, аутентификации, авторизации лиц, осуществляющих доступ к компонентам системы	Не регламентирован удаленный доступ к сети. Не регламентирована парольная политика
9. Ограничить физический доступ к данным владельцев платежных карт	Пункт 2.5 регламентирует требования по защите информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры	2.5.6 (П.17 - П.18) регламентирует уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, способом, обеспечивающим невозможность ее восстановления	Не определен порядок доступа посетителей в помещения. Не регламентировано ведение журнала учета посетителей

Наименование группы требований из PCI DSS v3.0	*Соответствующие требования Положения №382-П*		
	Краткое описание группы требований	*Номер подпункта (требования) и краткое описание требования*	*Несоответствия*
	Пункт 2.6 регламентирует требования по защите информации от несанкционированного доступа	2.6.5 (П.33) регламентирует использование технических средств защиты информации, предназначенных для контроля физического доступа к объектам инфраструктуры. 2.6.5 (П.34) регламентируют необходимость применения организационных мер или технических средств защиты, предназначенных для предотвращения физического воздействия на средства вычислительной техники и телекоммуникационное оборудование. 2.6.5 (П.35) определяет использование технических средств защиты информации, предназначенных для регистрации физического доступа к банкоматам. 2.6.8 (П.38) устанавливает необходимость принятия мер, направленных на предотвращение хищений носителей защищаемой информации	
10. Отслеживать и контролировать любой доступ к сетевым ресурсам и данным владельцев платежных карт	Пункт 2.6 регламентирует требования по защите информации от несанкционированного доступа	2.6.3 (П.24-П.25, П.28-П.30) устанавливает необходимость регистрации следующих действий: – при осуществлении доступа работников к защищаемой информации; – связанных с назначением и распределением прав доступа к защищаемой информации; – клиентов с использованием автоматизированной системы; – связанных с назначением и распределением прав клиентов; – с банковскими счетами. 2.6.5 (П.35) регламентирует регистрацию доступа к банкоматам. 2.6.7 (П.37) регламентирует контроль отсутствия на платежных терминалах и банкоматах технических средств, предназначенных для несанкционированного получения информации. 2.6.3 (П.29.2) устанавливает требования к порядку хранения и срокам хранения журналов регистрации	Не регламентированы требования по защите и анализу журналов аудита. Нет требования об использовании технологии синхронизации часов

Наименование группы требований из PCI DSS v3.0	*Соответствующие требования Положения №382-П*		
	Краткое описание группы требований	*Номер подпункта (требования) и краткое описание требования*	*Несоответствия*
	Пункт 2.10 регламентирует требования по защите информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технологических мер защиты информации	2.10.4 (П.81) регламентирует выявление фальсифицированных электронных сообщений	
	Пункт 2.14 Требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств	2.14.5 (П.111-П.112) регламентирует контроль применения организационных и технических мер защиты информации	
11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности	Пункт 2.9 регламентирует требования по защите информации при использовании СКЗИ	2.9.2 (П.62) регламентирует необходимость использования СКЗИ, которые обеспечивают контроль целостности программного обеспечения для среды функционирования СКЗИ	Не регламентирован процесс выявления беспроводных точек доступа к сети. Не регламентировано проведение тестирований на проникновение на уровне сети и на уровне приложений. Не определена методологию тестирования на проникновение. Не регламентировано проведение контроля целостности критичных системных файлов
	Пункт 2.13 регламентирует требования к выявлению инцидентов и реагированию на них	2.13.2 (П.101, П.103-П.104) определяет необходимость: – использования технических средств защиты информации, предназначенных для выявления инцидентов; – реагирования на выявленные инциденты; – проведения анализа причин возникновения выявленных инцидентов	
	Пункт 2.15 регламентирует требования к оценке выполнения требований к обеспечению защиты информации	2.15.2 (П.113-П.113.1), 2.15.3 (П.113.2) устанавливают требования к проведению регулярной оценки соответствия	
	Пункт 2.16 регламентирует требования к доведению до оператора платежной системы информации об обеспечении защиты	2.16.2 (П.120) устанавливает, требование об уведомлении оператора платежной системы о выявленных угрозах и уязвимостях в защите	

Наименование группы требований из PCI DSS v3.0	***Соответствующие требования Положения №382-П***		
	Краткое описание группы требований	***Номер подпункта (требования) и краткое описание требования***	***Несоответствия***
	Пункт 2.17 регламентирует требования к совершенствованию защиты информации	2.17.2 (П.126) регламентирует порядок принятия мер, направленных на совершенствование защиты информации, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации	
12. Поддерживать политику, которая определяет вопросы информационной безопасности для всего персонала	Все группы требований положения 382-П должны быть документированы, выполняться и контролироваться в процессе оценки соответствия, в том числе: – пункт 2.6 – требования по защите информации от несанкционированного доступа; – пункт 2.8 – требования по защите информации при использовании информационно-телекоммуникационной сети Интернет; – пункт 2.9 – требования по защите информации при использовании СКЗИ; – пункт 2.10 – требования по использованию взаимосвязанной совокупности организационных мер защиты информации и технологических мер защиты информации; – пункт 2.13 – требования к выявлению инцидентов и реагированию на них; – пункт 2.17 – требования к совершенствованию защиты информации	В состав организационных и технических мер, которые должны быть отражены в нормативных документах оператора по переводу денежных средств, входят: – 2.6.5 (П.33) технические средств защиты информации, предназначенные для предотвращения физического воздействия; – 2.6.5 (П.33) технические средства защиты информации, предназначенные для предотвращения физического воздействия; – 2.6.5 (П.34) организационные меры защиты информации и (или) технические средства защиты информации, предназначенные для регистрации доступа к банкоматам; – 2.6.8 (П.38) меры, направленные на защиту носителей защищаемой информации; – 2.6.3 (П.21-П.29.4) процедуры идентификации и аутентификации; – 2.8.1 (П.56) фильтрация сетевых пакетов; – 2.8.1 (П.52-П.53) организационные меры, предназначенные для предотвращения несанкционированного доступа; – 2.9.3 (П.63-П.69) СКЗИ; – 2.10.2 (П.72) организационные меры, используемые при обмене электронными сообщениями и другой информацией; – 2.10.4 (П.80-П.81) выявление фальсифицированных электронных сообщений; – 2.13.2 (П.101), 2.13.2 (П.103), 2.13.4 (П.106.1-П.106.2) организационные меры, предназначенные для выявления, реагирования и хранения сведений об инцидентах; – 2.17.2 (П.126) меры, направленные на совершенствование защиты информации, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации	Не установлены требования по проверке кандидатов на работу

Наименование группы требований из PCI DSS v3.0	***Соответствующие требования Положения №382-П***		
	Краткое описание группы требований	***Номер подпункта (требования) и краткое описание требования***	***Несоответствия***
	Пункт 2.11 регламентирует требования к организации и функционированию службы информационной безопасности	2.11.1 (П.82) устанавливает необходимость формирования службы информационной безопасности	Требования по распределению обязанностей в области управления информационной безопасностью не полностью соответствуют требованиям стандарта
	Пункт 2.12 регламентирует требования к повышению осведомленности работников в области обеспечения защиты информации	2.12.1 (П.93-П.94), 2.12.2 (П.95) устанавливают необходимость повышения осведомленности работников в области обеспечения защиты информации	—