Стандарт безопасности данных платежных приложений (PA-DSS) индустрии платежных карт (PCI)

Требования и процедуры аудита безопасности

Версия 3.0

Ноябрь 2013 г.

Изменения документа

Дата	Версия	Описание	Страницы
1 октября 2008 г.	1.2	*Обеспечено соответствие стандарту PCI DSS версии 1.2 и внедрены незначительные изменения по сравнению с версией 1.1.*	
Июль 2009 г.	1.2.1	*Содержание раздела "Область действия стандарта PA-DSS" согласовано с Руководством по программе PA-DSS версии 1.2.1 для уточнения приложений, на которые распространяется стандарт PA-DSS.*	*v, vi*
		В разделе "Требования 6 к лабораториям" исправлено написание "OWASP".	30
		В разделе "Свидетельство о проверке", часть 2a, изменена глава "Функциональность платежных приложений" с целью соответствия типам приложений, приведенным в Руководстве по программе PA-DSS, и уточнения ежегодных процедур повторной проверки в части 3b.	32, 33
Октябрь 2010 г.	2.0	*Внесены незначительные изменения по сравнению с версией 1.2.1 и выполнено согласование с новым стандартом PCI DSS версии 2.0. Для получения подробной информации см. "PA-DSS: обзор изменений в PA-DSS версии 2.0 по сравнению с версией 1.2.1".*	
Ноябрь 2013 г.	3.0	*Изменение по сравнению с PA-DSS версии 2. Для получения подробной информации см. "PA-DSS: обзор изменений в PA-DSS версии 3.0 по сравнению с версией 2.0".*	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Содержание

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Введение

Назначение документа

Требования и процедуры аудита безопасности стандартов безопасности данных платежных приложений (PA-DSS) индустрии платежных карт (PCI) регламентируют требования к безопасности и процедурам аудита для поставщиков платежных приложений. Настоящий документ предназначен для использования сертифицированными аудиторами платежных приложений (PA-QSA), проводящими аудит платежных приложений с целью подтверждения их соответствия стандарту PA-DSS. Для получения подробной информации о документировании аудита PA-DSS и создании отчета о проверке (ROV) PA-QSA должен изучить *бланк отчета о проверке на соответствие PA-DSS,* доступный на веб-сайте Совета по стандартам безопасности данных индустрии платежных карт (PCI SSC): www.pcisecuritystandards.org.

Дополнительные ресурсы, включая свидетельства о проверке, часто задаваемые вопросы и *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения,* доступны на веб-сайте Совета по стандартам безопасности данных индустрии платежных карт (PCI SSC): www.pcisecuritystandards.org.

Связь между стандартами PCI DSS и PA-DSS

Использование приложения, соответствующего стандарту PA-DSS, не является гарантией соответствия требованиям стандарта PCI DSS, поскольку данное приложение должно быть внедрено в среду, соответствующую стандарту PCI DSS, согласно *Руководству по внедрению PA-DSS*, которое должно быть предоставлено разработчиком платежного приложения (согласно требованию 13 стандарта PA-DSS). Требования стандарта PA-DSS основаны на *требованиях стандарта PCI DSS, а также требованиях и процедурах аудита безопасности*, в которых указаны требования соответствия стандарту PCI DSS (и, следовательно, требования к платежному приложению, способствующие соответствию стандарту PCI DSS). Со стандартом PCI DSS можно ознакомиться на веб-сайте www.pcisecuritystandards.org.

Все приложения, хранящие, обрабатывающие или передающие данные держателя карты, проходят проверку на соответствие стандарту PCI DSS, даже если они уже прошли проверку на соответствие стандарту PA-DSS. Оценка на соответствие стандарту PCI DSS должна подтвердить, что платежное приложение настроено надлежащим образом и надежно защищено в соответствии с требованиями PCI DSS. Если платежное приложение подверглось какой-либо модификации, требуется более тщательная оценка на соответствие стандарту PCI DSS, так как приложение может больше не соответствовать версии, проверенной по PA-DSS

PCI DSS может не распространяться непосредственно на поставщиков платежных приложений, если они не хранят, не обрабатывают или не передают данные держателей карт, или не имеют доступа к данным держателей карт своих клиентов. Тем не менее, так как данные платежные приложения используются клиентами поставщика приложения для хранения, обработки и передачи данных держателей карт, и их клиенты обязаны соответствовать стандарту PCI DSS, платежные приложения должны способствовать, а не препятствовать соответствию клиентов требованиям стандарта PCI DSS. Некоторые примеры случаев, когда небезопасные платежные приложения могут препятствовать достижению соответствия стандарту:

1. хранение данных магнитной полосы и (или) эквивалентной чиповой информации в клиентской сети после авторизации;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

2. наличие приложений, требующих от клиентов отключения различных функциональных возможностей, регламентируемых стандартом PCI DSS, например антивирусного программного обеспечения или межсетевых экранов, требуемых для надлежащей работы платежного приложения;
3. использование разработчиками небезопасных методов подключения для поддержки клиента.

Безопасные платежные приложения при внедрении в среду, соответствующую стандарту PCI DSS, позволят избежать нарушений безопасности и мошеннических действий, которые могут привести к несанкционированному разглашению номера платежной карты (PAN), полных данных магнитной полосы, проверочных кодов и значений (CAV2, CID, CVC2, CVV2), а также PIN-кодов и PIN-блоков.

Интеграторы и реселлеры

Поставщики приложений могут привлекать интеграторов и реселлеров к продаже, установке и (или) поддержке платежных приложений от своего имени. Интеграторы/реселлеры отвечают за обеспечение безопасной установки и эксплуатации платежных приложений, так как они часто предоставляют доступ к услугам клиентам поставщика и помогают с установкой соответствующих стандарту PA-DSS платежных приложений. Неправильные настройка, поддержка или техобслуживание приложения могут привести к появлению уязвимостей в системе безопасности среды данных держателей карт клиента, чем могут воспользоваться злоумышленники. Поставщики приложений должны обучать своих клиентов, интеграторов и реселлеров навыкам установки и настройки платежных приложений в соответствии с требованиями стандарта PCI DSS.

С целью безопасного внедрения платежных приложений квалифицированные интеграторы и реселлеры PCI (QIR) проходят обучение в Совете по стандартам PCI DSS и PA-DSS. Для получения дополнительной информации о программе PCI QIR см. www.pcisecuritystandards.org.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Область применения стандарта PCI DSS

Данный стандарт применяется для всех организаций сферы обработки платежных карт: торговых точек, процессинговых центров, финансовых учреждений и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные.

Данные держателей карт и критичные аутентификационные данные включают следующее.

Данные платежных карт (Account Data)	
Данные держателя карты:	**Критичные аутентификационные данные:**
▪ Основной номер держателя карты (PAN) ▪ Имя держателя карты ▪ Дата истечения срока действия карты ▪ Сервисный код	▪ Полные данные дорожки магнитной полосы или ее эквивалент на чипе ▪ CAV2/CVC2/CVV2/CID ▪ PIN/PIN-блоки

Основной номер держателя карты (PAN) является определяющим фактором для данных держателя карты. Если имя держателя карты, сервисный код и (или) срок действия хранятся, обрабатываются или передаются вместе с номером PAN или иным образом присутствуют в среде данных держателей карт, то они должны быть защищены согласно применимым требованиям PCI DSS.

Таблица на следующей странице иллюстрирует наиболее часто используемые элементы данных держателей карт и критичных аутентификационных данных; в ней показано, разрешено или запрещено их хранение и должен ли быть защищен каждый из этих элементов. Данная таблица не является исчерпывающей, она демонстрирует различные типы требований, которые применяются к каждому элементу данных.

		Элемент данных	***Хранение разрешено***	***Хранение данных в нечитаемом виде в случайном порядке согласно требованию 2.3 PA-DSS***
платежных карт (Account	***Данные держателя карты (Cardholder Data)***	*Основной номер держателя карты (PAN)*	*Да*	*Да*
		Имя держателя карты	*Да*	*Нет*
		Сервисный код	*Да*	*Нет*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

		Дата истечения срока действия карты	*Да*	*Нет*
	Критичные аутентификационные данные (Sensitive Authentication Data)[1]	*Полные данные дорожки* [2]	*Нет*	*Нельзя хранить согласно требованию 1.1 PA-DSS*
		CAV2/CVC2/CVV2/CID[3]	*Нет*	*Нельзя хранить согласно требованию 1.1 PA-DSS*
		PIN/PIN-блок[4]	*Нет*	*Нельзя хранить согласно требованию 1.1 PA-DSS*

Требования 2.2 и 2.3 PA-DSS применяются только к PAN. Если PAN хранится вместе с другими данными держателей карт, то в соответствии с требованием 2.3 PA-DSS хранить в нечитаемом виде необходимо только PAN.

Запрещается хранить критичные аутентификационные данные после авторизации, даже в зашифрованном виде. Данное требование действует, даже если PAN отсутствует в среде.

1 *Критичные аутентификационные данные не должны храниться после авторизации (даже в зашифрованном виде).*

2 *Полные данные на дорожке магнитной полосы, эквивалентные данные на чипе или в ином месте*

3 *Трех- или четырехзначное проверочное значение, изображенное на лицевой или обратной стороне платежной карты*

4 *Персональный идентификационный номер, который вводится держателем карты при выполнении операции с предъявлением карты, и (или) зашифрованный PIN-блок, предоставляемый в сообщении об операции*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Область действия стандарта PA-DSS

Стандарт PA-DSS распространяется на поставщиков приложений и иных разработчиков приложений, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные. Для получения информации, связанной с соответствием приложений различных типов требованиям, см. *Руководство по программе PA-DSS*.

Область оценки на соответствие стандарту PA-DSS должна включать следующее:

- Охват всей функциональности платежного приложения, включая, помимо прочего:
  1) двусторонние платежные функции (авторизация и расчет);
  2) ввод и вывод;
  3) сбойные ситуации;
  4) интерфейсы и подключения к другим файлам, системам и (или) платежным приложениям или компонентам приложений;
  5) все потоки данных держателей карт;
  6) механизмы шифрования;
  7) механизмы аутентификации.
- Охват рекомендаций, которые поставщик платежного приложения должен предоставить клиентам и интеграторам/реселлерам (см. *Руководство по внедрению стандарта PA-DSS* далее в данном документе), чтобы гарантировать, что:
  1) клиент знает, как внедрить платежное приложение в соответствии с требованиями стандарта PCI DSS;
  2) клиент осведомлен о том, что определенные платежные приложения и параметры среды могут препятствовать соответствию стандарту PCI DSS.

  Следует помнить, что поставщик платежного приложения должен предоставить такие рекомендации, даже если конкретный параметр:
  1) не может быть проконтролирован поставщиком платежного приложения после установки приложения клиентом; или
  2) находится под ответственностью клиента, а не поставщика платежного приложения.
- Охват всех выбранных платформ оцениваемой версии платежного приложения (платформы должны быть указаны).
- Охват средств, используемых платежным приложением либо в его рамках для доступа и (или) просмотра данных держателей карт (средства отчетности, средства ведения журнала и т. д.).
- Охват всех программных компонентов, связанных с платежным приложением, включая требования и взаимозависимости стороннего ПО.
- Охват всех остальных типов платежных приложений, необходимых для полного внедрения.
- Охват методологии назначения версии поставщика.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Применимость PA-DSS к платежным приложениям, установленным на аппаратных терминалах

В данном разделе приведены инструкции для поставщиков, желающих провести проверку резидентных платежных приложений и аппаратных терминалов (также известных как отдельные или выделенные платежные терминалы) на соответствие PA-DSS.

Резидентные платежные приложения на аппаратных терминалах могут пройти проверку на соответствие PA-DSS двумя способами:

1. Резидентное платежное приложение соответствует всем требованиям стандарта PA-DSS и получает сертификат согласно стандартным процедурам.

2. Резидентное платежное приложение соответствует не всем требованиям стандарта PA-DSS, но оборудование, на котором установлено приложение, находится в списке устройств, одобренных PCI SSC и обеспечивающих безопасность транзакций с использованием PIN-кода (PTS) в качестве одобренного POI-устройства. В данном случае приложение может соответствовать требованиям стандарта PA-DSS посредством комбинации утвержденных механизмов PA-DSS и PTS.

Информация, приведенная далее в этом разделе, относится только к платежным приложениям, установленным на POI-устройства, прошедшие проверку и получившие одобрение PCI PTS.

Если одно или несколько требований PA-DSS не могут быть выполнены непосредственно платежным приложением, они могут быть удовлетворены косвенно механизмами, протестированными в рамках проверки PCI PTS. Для того, чтобы устройство могло быть включено в проверку PA-DSS, оно ДОЛЖНО быть сертифицировано как POI-устройство, получившее одобрение PCI PTS, и включено в список одобренных PTS-устройств согласно PCI SSC. POI-устройство, получившее PTS-одобрение и обеспечивающее надежную вычислительную среду, станет "***обязательной взаимозависимостью***" для платежного приложения, а комбинация устройства и приложения будет указана в списке сертифицированных платежных приложений PA-DSS.

При проведении оценки на соответствие требованиям PA-DSS PA-QSA должен всесторонне проверить платежное приложение и зависимое оборудование по всем требованиям PA-DSS. Если PA-QSA установит, что одно или несколько требований PA-DSS не может быть выполнено резидентным платежным приложением, но при этом они выполняются механизмами, одобренными согласно PCI PTS, PA-QSA должен:

1. четко указать, какие требования выполнены согласно PA-DSS (как обычно);

2. четко указать, какие требования выполнены согласно PCI PTS в поле "Выполнено" для соответствующего требования;

3. привести подробное объяснение, почему платежное приложение не соответствует требованию PA-DSS;

4. указать процедуры, которые были проведены, чтобы определить, что это требование было полностью выполнено посредством одобренного механизма контроля PCI PTS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

5. указать аппаратный терминал, одобренный согласно PCI PTS, как "обязательную взаимозависимость" в разделе "Краткое описание" отчета о проверке.

После завершения проверки платежного приложения со стороны PA-QSA и его последующего принятия PCI SSC одобренное аппаратное PTS-устройство будет указано как "взаимозависимость" для платежного приложения в списке одобренных приложений PA-DSS.

Резидентные платежные приложения на аппаратных терминалах, одобренные путем комбинации механизмов PA-DSS и PCI PTS, должны соответствовать следующим критериям:

1. должны предоставляться клиенту комплексно (аппаратный терминал и приложение) ИЛИ, в случае раздельного предоставления, поставщик приложения и (или) интегратор/реселлер должны подготовить приложение к поставке таким образом, чтобы оно работало только на аппаратном терминале, для которого оно было одобрено;

2. должны по умолчанию поддерживать соответствие требованиям стандарта PCI DSS клиента;

3. должны иметь текущую поддержку и обновления с целью постоянного соответствия стандарту PCI DSS;

4. если приложение отдельно продается, поставляется или лицензируется для клиентов, поставщик должен предоставить информацию о зависимом оборудовании, необходимом для использования с приложением в соответствии с его включением в список PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Руководство по внедрению стандарта PA-DSS

Одобренные платежные приложения должны иметь возможность внедрения в соответствии с требованиями стандарта PCI DSS. Поставщики ПО должны предоставить *Руководство по внедрению стандарта PA-DSS* для обучения своих клиентов и интеграторов/реселлеров принципам безопасного внедрения продукции, документирования безопасных конфигураций, упоминаемых в настоящем документе, и четкого определения ответственности поставщика, интегратора/реселлера и клиента по выполнению требований стандарта PCI DSS. В нем должно описываться, как клиенту и (или) интегратору/реселлеру следует обеспечивать параметры защиты в сети клиента. Например, *Руководство по внедрению стандарта PA-DSS* должно охватывать обязанности и основные функции парольной защиты по стандарту PCI DSS, даже если она не обеспечивается платежным приложением, чтобы клиент или интегратор/реселлер понимали принципы внедрения безопасных паролей для соответствия требованиям стандарта PCI DSS.

Руководство по внедрению стандарта PA-DSS должно предоставить подробную информацию по настройке платежного приложения в соответствии с требованиями, а не просто повторить требования стандарта PCI DSS или PA-DSS. Во время проверки PA-QSA должен убедиться, что инструкции являются точными и эффективными. PA-QSA также должен убедиться, что *Руководство по внедрению стандарта PA-DSS* передано клиентам и интеграторам/реселлерам.

Платежные приложения, внедряемые согласно *Руководству по внедрению стандарта PA-DSS* в среде, соответствующей стандарту PCI DSS, должны способствовать и поддерживать соответствие клиентов требованиям стандарта PCI DSS.

См. *Приложение A: краткое изложение Руководства по внедрению стандарта PA-DSS* с целью сравнения обязанностей по внедрению механизмов контроля, указанных в *Руководстве по внедрению стандарта PA-DSS*.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования, предъявляемые к сертифицированным аудиторам платежных приложений (PA-QSA)

Только сертифицированные аудиторы платежных приложений (PA-QSA), работающие в компаниях, являющихся сертифицированными аудиторами платежных приложений (PA-QSA), имеют право проводить проверки на соответствие требованиям стандарта PA-DSS. Список QSA платежных приложений см. на веб-сайте www.pcisecuritystandards.org, где перечислены компании, имеющие право на проведение проверок на соответствие требованиям стандарта PA-DSS.

- PA-QSA должны использовать процедуры тестирования, приведенные в настоящем документе по Стандарту безопасности данных для платежных приложений.
- PA-QSA должен иметь доступ к лаборатории, в которой осуществляется процесс проверки.

Лаборатория по тестированию

- Лаборатории по тестированию могут находиться либо по месту работы PA-QSA, либо на территории поставщика приложения.
- Лаборатория по тестированию должна иметь возможности для моделирования практической эксплуатации платежного приложения.
- PA-QSA должен провести "чистую" установку приложения в лабораторной среде, что убедиться, что среда действительно моделирует практическую ситуацию и поставщик не вносил в среду каких-либо изменений и не совершал какие-либо манипуляции.
- См. *Приложение B: подтверждение конфигурации лаборатории по тестированию, предназначенной для проверки на соответствие требованиям стандарта PA-DSS* в настоящем документе, где указаны подробные требования к лаборатории и сопутствующим процессам.
- PA-QSA должен заполнить и отправить *Приложение B* для конкретной лаборатории, используемой для проверки платежного приложения, в рамках заполнения отчета о проверке PA-DSS (ROV).

Инструкции по заполнению и требования к содержанию отчета о проверке

Инструкции по заполнению и требования к содержанию отчета о проверке теперь предоставляются в *бланке отчета о проверке на соответствие стандарту PA-DSS (ROV). Бланк отчета о проверке на соответствие стандарту PA-DSS (ROV)* должен быть использован при создании отчета о проверке. В PCI SSC должны быть отправлены только соответствующие требованиям отчеты о проверке (ROV) платежных приложений. Подробная информация о процессе отправки отчета о проверке (ROV) приведена в *Руководстве по программе PA-DSS*.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Шаги создания отчета о проверке PA-DSS

Настоящий документ содержит таблицу требований и процедур аудита безопасности, а также *Приложение B: конфигурация лаборатории по тестированию для проведения оценки на соответствие требованиям PA-DSS*. В требованиях и процедурах аудита безопасности описываются процедуры, которые должен выполнить PA-QSA.

PA-QSA должен выполнить следующие шаги:

1. подтвердить область применения проверки на соответствие требованиям PA-DSS;
2. выполнить проверку на соответствие требованиям PA-DSS;
3. заполнить отчет о проверке (ROV), используя *бланк отчета о проверке на соответствие стандарту PA-DSS*, включая подтверждение конфигурации лаборатории по тестированию, используемой для проверки;
4. заполнить и подписать свидетельство о проверке (для PA-QSA и поставщика приложения). Свидетельство о соответствии можно получить на веб-сайте PCI SSC (www.pcisecuritystandards.org);
5. после заполнения отправить все вышеперечисленные документы и *Руководство по внедрению стандарта PA-DSS* в PCI SSC согласно *Руководству по программе PA-DSS.*

Примечание.

Отправку следует отложить, пока все требования стандарта PA-DSS не будут подтверждены как выполненные.

Руководство по программе PA-DSS

См. *Руководство по программе PA-DSS* для получения информации об управлении программой PA-DSS, в том числе по следующим вопросам:

- применимость стандарта PA-DSS к различным типам приложений;
- отправка отчета о проверке и процессы приемки;
- ежегодный процесс обновления платежных приложений, включенных в список одобренных платежных приложений;
- обязанности по уведомлению в случае, если приложение, находящееся в списке, будет признано виновным в разглашении конфиденциальной информации.

PCI SSC оставляет за собой право требовать повторной проверки вследствие значительных изменений стандарта безопасности данных платежных приложений и (или) вследствие выявленных уязвимостей в приложении, находящемся в списке.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Стандарт безопасности данных платежных приложений (PA-DSS). Требования и процедуры аудита безопасности

В приведенной ниже таблице поля имеют следующие значения.

- **Требования стандарта PA-DSS** – в данном столбце приведены требования по обеспечению защиты, которым должны соответствовать платежные приложения
- **Процедуры тестирования** – в данном столбце приведены процессы тестирования, которым должен следовать PA-QSA, чтобы подтвердить, что требования стандарта PA-DSS выполнены
- **Пояснение** – в данном столбце описывается назначение или функция безопасности каждого требования PA-DSS с целью содействия в его понимании. Информация в этом столбце не заменяет и не дополняет требования и процедуры тестирования PA-DSS.

Примечание.

Требования стандарта PA-DSS не должны считаться выполненными, если какие-либо механизмы контроля не внедрены либо запланированы на будущее.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 1. Не хранить полные данные магнитной дорожки, код или значение проверки подлинности карты (CAV2, CID, CVC2, CVV2), или данные PIN-блока

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). В случае получения критичных аутентификационных данных все данные должны стать невосстановимыми по завершении процесса авторизации. К критичным аутентификационным данным относятся данные, перечисленные в требованиях 1.1.1 – 1.1.3. ***Согласуется с требованием 3.2 стандарта PCI DSS***	**1.1.a** Если данное платежное приложение хранит критичные аутентификационные данные, следует убедиться, что приложение предназначено исключительно для эмитентов и (или) компаний, предоставляющих услуги эмиссии.	Критичные аутентификационные данные состоят из полных данных на магнитной дорожке, кода или значения подтверждения подлинности карты и данных PIN-кода. Хранение критичных аутентификационных данных запрещается. Эти данные представляют интерес для злоумышленников, поскольку позволяют им генерировать поддельные платежные карты и осуществлять мошеннические операции. Эмитенты платежных карт или компании, предоставляющие услуги эмиссии или поддерживающие этот процесс, часто создают и управляют критичными аутентификационными данными в рамках процесса эмиссии. Эмитенты и компании, обеспечивающие услуги эмиссии, могут иметь обоснованную необходимость хранения критичных аутентификационных данных. Такая необходимость должна иметь обоснование с точки зрения бизнеса, а хранимые данные должны быть надежно защищены. Для неэмитентов сохранение критичных аутентификационных данных после аутентификации запрещено, и приложение должно иметь механизм надежного удаления данных без возможности их восстановления.
	1.1.b Для всех остальных платежных приложений, хранящих критичные аутентификационные данные (см. требования 1.1.1 – 1.1.3) до авторизации, необходимо получить и изучить методологию надежного удаления данных, чтобы устранить возможность ее восстановления.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1.1 После авторизации запрещается хранить полное содержимое дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте). Эти данные также называются "полная дорожка", "дорожка", "дорожка 1", "дорожка 2" и "данные магнитной полосы". ***Примечание.*** *Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы:* • *имя держателя счета;* • *номер платежной карты (PAN);* • *дата истечения срока действия карты;* • *сервисный код.* *Для минимизации рисков разрешается хранить только те указанные элементы данных, которые необходимы для проведения операции.* ***Согласуется с требованием 3.2.1 стандарта PCI DSS***	**1.1.1** Установить платежное приложение и выполнить много тестовых операций, моделирующих все функции платежного приложения, включая создание сбойных ситуаций и записей журнала. Использовать аналитические средства и (или) методы (коммерческие средства, сценарии и т. д.)[5] для проверки всех сообщений, выводимых платежным приложением, и подтверждения того, что полное содержимое любой дорожки магнитной полосы на обратной стороне карты или эквивалентные данные на чипе не хранятся после авторизации. Следует включить как минимум следующие типы файлов (а также все сообщения, созданные платежным приложением): • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • энергонезависимая память, включая энергонезависимый кэш; • схемы баз данных; • содержимое баз данных.	Если сохранены полные данные дорожки, злоумышленник, получивший доступ к этим данным, может использовать их для воспроизведения платежных карт и осуществления мошеннических транзакций.

[5] *Аналитическое средство или метод: средство или метод для обнаружения, анализа и представления аналитических данных, которое позволяет легко и быстро аутентифицировать, найти и восстановить доказательства из компьютерных ресурсов. Аналитические средства или методы, используемые PA-QSA, должны точно установить местоположение критичных аутентификационных данных, записанных платежным приложением. Этими средствами могут быть приобретенные продукты, продукты с открытым исходным кодом или разработанные PA-QSA внутри организации.*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1.2 После авторизации запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с карты (трех- или четырехзначного числа, изображенного на лицевой или обратной стороне карты). ***Согласуется с требованием 3.2.2 стандарта PCI DSS***	**1.1.2** Установить платежное приложение и выполнить многочисленные тестовые операции, моделирующие все функции платежного приложения, включая создание сбойных ситуаций и записей журнала. Использовать аналитические средства и (или) методы (коммерческие средства, сценарии и т. д.) для проверки всех сообщений, выводимых платежным приложением, и подтверждения того, что трех- или четырехзначное число, изображенное на лицевой или обратной стороне карты (CVV2, CVC2, CID, CAV2), не хранится после авторизации. Следует включить как минимум следующие типы файлов (а также все сообщения, созданные платежным приложением): • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • энергонезависимая память, включая энергонезависимый кэш; • схемы баз данных; • содержимое баз данных.	Назначение кода подтверждения подлинности карты состоит в защите операций без предоставления карты (например, при заказе товаров через Интернет, по почте или по телефону). В случае кражи этих данных, злоумышленник получит возможность совершения мошеннических операций по сети Интернет, по почте или телефону.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1.3 После авторизации запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока. ***Согласуется с требованием 3.2.3 стандарта PCI DSS***	**1.1.3** Установить платежное приложение и выполнить большое число тестовых операций, моделирующих все функции платежного приложения, включая создание сбойных ситуаций и записей журнала. Использовать аналитические средства и (или) методы (коммерческие средства, сценарии и т. д.) для изучения всех сообщений, выводимых платежным приложением, и подтверждения того, что PIN-коды и зашифрованные PIN-блоки не хранятся после авторизации. Следует включить как минимум следующие типы файлов (а также все сообщения, созданные платежным приложением): • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • энергонезависимая память, включая энергонезависимый кэш; • схемы баз данных; • содержимое баз данных.	Данные значения должны быть известны только владельцу карты или банку, который выпустил карту. В случае кражи этих данных злоумышленник получит возможность совершения мошеннических дебетовых операций с использованием PIN-кода (например, для получения наличных через банкомат).

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1.4 Безопасным образом удалить все данные дорожки (содержимое магнитной полосы или его аналог на чипе), коды и значения проверки подлинности карты, PIN-коды и PIN-блоки, сохраненные предыдущими версиями платежного приложения, в соответствии с отраслевыми стандартами безопасного удаления, как определено, к примеру, списком одобренных продуктов, составленным Агентством национальной безопасности или другими национальными стандартами или нормативами, либо стандартами или нормативами штата. ***Примечание.*** *Данное требование действует, только если в предыдущей версии платежного приложения хранились критичные аутентификационные данные.* ***Согласуется с требованием 3.2 стандарта PCI DSS***	**1.1.4.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • накопленные данные должны быть удалены (данные дорожки, коды проверки подлинности карты, PIN-коды или PIN-блоки, сохраненные предыдущими версиями платежного приложения). • инструкции по удалению накопленных данных; • удаление этих данных абсолютно необходимо для соответствия требованиям стандарта PCI DSS; **1.1.4.b** Изучить программные файлы платежного приложения и документацию по конфигурации, чтобы подтвердить, что поставщик предоставляет безопасное средство или процедуру для удаления данных. **1.1.4.c** Подтвердить при помощи аналитических средств и (или) методов, что безопасное средство или процедура удаления, предоставленные поставщиком, надежно удаляют данные в соответствии с отраслевыми стандартами удаления данных.	Все эти элементы критичных аутентификационных данных запрещается хранить после авторизации. Если более старые версии платежного приложения хранили данную информацию, поставщик платежного приложения обязан предоставить инструкции в *Руководстве по внедрению стандарта PA-DSS*, а также безопасное средство или процедуру удаления. Если данные не будут удалены безопасным образом, они могут остаться на торговых точках в скрытом виде, и злоумышленники, получившие доступ к такой информации, смогут создать поддельные платежные карты и (или) совершить мошеннические операции.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
1.1.5 Запрещается хранить критичные аутентификационные данные в системах поставщика. Если какие-либо критичные аутентификационные данные (предавторизационные данные) необходимо использовать в целях отладки или устранения неисправностей, следует гарантировать следующее. • Сбор критичных аутентификационных данных производится, только если это необходимо для решения конкретной проблемы. • Такие данные хранятся в определенном известном месте с ограниченным доступом. • Для решения конкретной проблемы собирается минимальный необходимый объем данных. • Во время хранения критичные аутентификационные данные шифруются при помощи стойких криптографических алгоритмов. • Сразу после использования данные удаляются безопасным образом, в том числе из следующих мест: – файлы журнала; – файлы отладки; – другие источники данных, полученные от клиентов. ***Согласуется с требованием 3.2 стандарта PCI DSS.***	**1.1.5.a** Изучить процедуры *поставщика приложения*, применяемые для решения проблем клиентов, и убедиться, что они удовлетворяют следующим требованиям. • Сбор критичных аутентификационных данных производится, только если это необходимо для решения конкретной проблемы. • Такие данные хранятся в определенном известном месте с ограниченным доступом. • Для решения конкретной проблемы собирается минимальный необходимый объем данных. • Критичные аутентификационные данные шифруются на время хранения. • Данные удаляются безопасным образом сразу после использования. **1.1.5.b** Выбрать несколько недавно полученных запросов на поиск неисправностей от пользователей и убедиться, что в каждом случае выполнялась процедура, приведенная в пункте 1.1.5.a. **1.1.5.c** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров. • Сбор критичных аутентификационных данных производится, только если это необходимо для решения конкретной проблемы. • Такие данные хранятся в определенном известном месте с ограниченным доступом. • Для решения конкретной проблемы собирается минимальный необходимый объем данных. • Критичные аутентификационные данные шифруются на время хранения. • Данные безопасным образом удаляются сразу после использования.	Если поставщик предоставляет клиентам услуги, которые могут привести к сбору критичных аутентификационных данных (например, в целях поиска неисправностей или отладки), поставщик должен свести к минимуму сбор данных и убедиться, что они защищены и удалены безопасным образом, когда в них нет необходимости. Если поиск неисправностей требует, чтобы приложение было временно настроено для сбора критичных аутентификационных данных, то приложение необходимо вернуть к стандартной защищенной конфигурации (а именно отключить сбор критичных аутентификационных данных) немедленно после завершения сбора необходимых данных. Если они больше не требуются, то критичные аутентификационные данные следует удалить в соответствии с отраслевыми стандартами (например, используя программу для удаления таким безопасным образом, который гарантирует невозможность восстановления данных).

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 2. Обеспечить безопасное хранение данных держателей карт

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.1 Поставщик приложения должен предоставить клиентам инструкции в отношении удаления безопасным образом данных держателей карт по истечении указанного клиентом срока хранения. ***Согласуется с требованием 3.1 стандарта PCI DSS.***	**2.1** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров. • Данные держателей карт должны быть удалены безопасным образом по истечении указанного клиентом срока хранения. • Необходимо составить список всех мест, где платежное приложение хранит данные держателей карт (чтобы клиент знал, откуда следует удалить данные). • Клиентам должны быть предоставлены инструкции, согласно которым они должны удалить безопасным образом данные держателей карт, которые более не требуются для юридических, нормативных или деловых целей. • Инструкции в отношении удаления безопасным образом данных держателей карт, сохраненных платежным приложением, включая данные, хранящиеся в базовом ПО или системе, где установлено приложение (т. е. ОС, базы данных и т. д.). • Инструкции по настройке базового ПО или системы, где установлено приложение (т. е. ОС, базы данных и т. д.) с целью предотвращения неумышленного сбора или хранения данных держателей карт, например вследствие резервного копирования или восстановления системы.	Для поддержки требования 3.1 стандарта PCI DSS поставщик должен предоставить подробную информацию обо всех местах, где платежное приложение может хранить данные держателей карт, включая базовое ПО или системы, где установлено приложение (т. е. ОС, базы данных и т. д.), а также инструкции по удалению данных безопасным образом из этих мест по истечении указанного клиентом срока хранения. Клиенты и интеграторы/реселлеры также должны предоставить информацию о конфигурации базового ПО или системы, где установлено и работает приложение, чтобы убедиться, что они не собирают данные держателей карт без ведома клиента. Клиент должен знать, как базовая система, где установлено приложение, может собирать данные из приложения, чтобы предотвратить такой сбор или обеспечить надлежащую защиту данных.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.2 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. ***Примечание.*** *Это требование не заменяет собой иные более строгие требования к отображению данных держателей карт (например, юридические требования или требования к брендированию платежных карт на чеках кассовых терминалов (в местах продаж).* ***Согласуется с требованием 3.3 стандарта PCI DSS.***	**2.2.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • информацию обо всех случаях отображения основного номера держателя карты, включая, помимо прочего, кассовые терминалы, экраны, журналы и чеки; • подтверждение того, что платежное приложение маскирует все случаи отображения основного номера держателя карты по умолчанию; • инструкции по настройке платежного приложения таким образом, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть основной номер держателя карты полностью;	полное отображение основного номера держателя карты на экранах компьютеров, квитанциях об операциях с платежными картами, факсах, в бумажных отчетах и т. п. может привести к тому, что эти данные станут известны неавторизованным лицам и могут быть использованы в мошеннических целях. Это требование касается защиты основного номера держателя карты, отображаемого на экранах, бумажных квитанциях, распечатках и т. д., и его следует отличать от требования 2.3 стандарта PA-DSS, которое касается защиты основного номера держателя карты при его хранении в файлах, базах данных и т. д.
	2.2.b Установить платежное приложение и проверить все случаи отображения данных основного номера держателя карты, включая, помимо прочего, устройства кассовых терминалов, экраны, журналы и чеки. В каждом случае отображения основного номера держателя карты необходимо убедиться, что он замаскирован.	
	2.2.c Платежное приложение должно быть настроено в соответствии с *Руководством по внедрению стандарта PA-DSS*, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть основной номер держателя карты полностью. В каждом случае отображения основного номера держателя карты необходимо проверить параметры настройки приложения и убедиться, что номер должным образом замаскирован, и только сотрудники с обоснованной коммерческой необходимостью могут видеть основной номер держателя карты полностью.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.3 Основной номер держателя карты должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий). Для этого следует использовать любой из следующих методов: • стойкое однонаправленное хеширование (должен быть хеширован весь основной номер держателя карты); • усечение (хеширование не может использоваться для замещения усеченного сегмента основного номера держателя карты); • использование механизмов One-Time-Pad ("одноразовых блокнотов", хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных (токены, index tokens); • стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами. *(Продолжение на следующей странице)*	**2.3a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • информацию о настраиваемых параметрах для каждого метода, используемого приложением для приведения данных держателей карт в нечитаемый вид, и инструкции по настройке каждого метода на всех устройствах, где данные держателей карт хранятся платежным приложением (согласно требованию 2.1 стандарта PA-DSS); • список случаев, когда данные держателей карт могут быть предоставлены торговым точкам для хранения вне платежного приложения, и указания относительно ответственности торгово-сервисных предприятий по приведению основного номера держателя карты в нечитаемый вид в таких случаях. **2.3.b** Изучить метод, используемый для защиты основного номера держателя карты, включая алгоритмы шифрования (если применимо). Убедиться, что основной номер держателя карты представлен в нечитаемом виде при помощи одного из следующих методов: • стойкое однонаправленное хеширование; • усечение (truncation); • использование механизмов One-Time-Pad ("одноразовых блокнотов", хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных (токены, index tokens); • стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами.	Недостаточная защита основных номеров держателей карт может привести к тому, что злоумышленники смогут просматривать или получать эти данные. Для приведения данных держателей карт к нечитаемому виду можно использовать функции одностороннего хеширования на базе криптостойкого шифрования. Их использование целесообразно тогда, когда нет необходимости в восстановлении основного номера держателя карты (так как одностороннее хеширование является необратимым). Цель усечения заключается в том, что хранится только часть (не больше шести первых и четырех последних цифр) основного номера держателя карты. Токен – это криптографический параметр, который заменяет основной номер держателя карты на основе заданного индекса для получения непредсказуемого значения. Одноразовый блокнот – это система, в которой секретный ключ, сгенерированный случайным образом, используется только один раз для шифрования сообщения, которое затем расшифровывается с помощью соответствующего одноразового блокнота и ключа. *(Продолжение на следующей странице)*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
Примечания. • При наличии доступа одновременно к усеченному и хешированному номерам карты для злоумышленника не составит большого труда восстановить данные исходного основного номера держателя карты. Если маскированное и усеченное значение одного и того же основного номера держателя карты создаются платежным приложением, необходимо ввести дополнительные средства контроля для недопущения корреляции между усеченным и хешированным значениями, так как при этом исходный основной номер держателя карты становится легко восстановим. • Независимо от места хранения основной номер держателя карты должен быть нечитаемым, даже если хранится вне платежного приложения (например, в файлах журнала, созданных приложением для хранения в среде торговой точки). ***Согласуется с требованием 3.4 стандарта PCI DSS***	**2.3.c** Изучить несколько таблиц или файлов из нескольких хранилищ данных, созданных приложением, и убедиться, что основной номер держателя карты представлен в нечитаемом виде.	Цель стойкой криптографии (см. определение в документе *"Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения"*) заключается в том, что шифрование основывается на использовании проверенных стандартизованных алгоритмов (а не собственных алгоритмов) со стойкими ключами шифрования.
	2.3.d Если приложение создает файлы для использования вне приложения (например, файлы, созданные для экспорта или резервного копирования), включая хранение на съемных носителях информации, следует изучить несколько созданных файлов, включая сохраненные на съемных носителях (например, резервные копии), чтобы убедиться, что основной номер держателя карты представлен в нечитаемом виде.	
	2.3.e Изучить несколько журналов регистрации событий и убедиться, что основной номер держателя карты из них удален или представлен в нечитаемом виде.	
	2.3.f Если поставщик приложения по какой-либо причине хранит основной номер держателя карты (например, вследствие получения от клиентов файлов журналов и отладки, и из других источников данных в целях отладки и поиска неисправностей), следует убедиться, что основной номер держателя карты представлен в нечитаемом виде согласно требованиям 2.3.a – 2.3.e выше.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.4 Платежное приложение должно защищать ключи шифрования данных держателей карт от их раскрытия или неправильного использования. ***Примечание.*** *Данное требование относится к ключам, используемым для шифрования хранящихся данных держателей карт, а также к ключам для шифрования ключей, используемым для защиты ключей для шифрования данных. Подобные ключи для шифрования ключей должны обладать таким же уровнем защиты, как и ключи для шифрования данных.* ***Согласуется с требованием 3.5 стандарта PCI DSS***	**2.4.a** Изучить документацию по продукту и опросить ответственных лиц, чтобы убедиться, что действуют надлежащие механизмы контроля, ограничивающие доступ к ключам шифрования, используемым приложением. **2.4.b** Изучить файлы конфигурации системы с целью убедиться, что: • ключи хранятся в зашифрованном формате; • ключи для шифрования ключей хранятся отдельно от ключей для шифрования данных; • ключи для шифрования ключей должны обладать таким же уровнем защиты, как и ключи для шифрования данных, которые они защищают. **2.4.c** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что клиенты и интеграторы/реселлеры проинструктированы: • разрешать доступ к ключам шифрования наименьшему возможному количеству сотрудников, ответственных за их хранение и использование; • хранить ключи только в строго определенных защищенных хранилищах и в строго определенном виде.	Ключи шифрования должны быть надежно защищены, поскольку лица, получившие к ним доступ, смогут расшифровать данные. Требование к платежному приложению по защите ключей от раскрытия и неправильного использования применяется как к ключам для шифрования ключей, так и к ключам для шифрования данных. Необходимо максимально уменьшить количество лиц, имеющих доступ к ключам шифрования. Обычно это лица, отвечающие за хранение ключей.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.5 В платежные приложения должны быть полностью внедрены все процессы и процедуры управления ключами шифрования данных держателей карт, включая по крайней мере: ***Согласуется с требованием 3.6 стандарта PCI DSS***	**2.5** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • инструкции по безопасному созданию, распространению, защите, изменению, хранению и изъятию/смене ключей шифрования в случаях, когда в управление ключами вовлечены клиенты или интеграторы/реселлеры; • образец формы для сотрудников по хранению и использованию ключей, в которой они подтверждают, что поняли свою ответственность и принимают свои обязанности.	Способ управления ключами шифрования представляет собой критически важную часть непрерывного обеспечения безопасности платежного приложения. Правильно организованный процесс управления ключами, вне зависимости от того, выполняется ли он вручную или автоматически в составе продукта шифрования, должен соответствовать отраслевым стандартам и всем требованиям с 2.5.1 по 2.5.7. Предоставление потребителям рекомендаций по безопасной передаче, хранению и обновлению ключей шифрования, которые помогут предотвратить неправильное управление или раскрытие неавторизованным сторонам. Данное требование применяется к ключам, которые используются для шифрования данных держателей карт, и соответствующим ключам для шифрования ключей.
2.5.1 Генерация стойких криптографических ключей	**2.5.1.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по безопасной генерации ключей шифрования.	Платежное приложение должно генерировать стойкие ключи, как описано в документе *"Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения"* в определении термина "стойкая криптография".
	2.5.1.b Протестировать приложение, включая методы, использованные при генерации ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют генерации стойких ключей шифрования.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.5.2 Безопасное распространение ключей	**2.5.2.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по безопасному распространению ключей шифрования.	Платежное приложение должно распространять ключи безопасным образом, то есть в зашифрованном виде и только посредством авторизованных процессов.
	2.5.2.b Протестировать приложение, включая методы, использованные для распространения ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют безопасному распространению ключей шифрования.	
2.5.3 Безопасное хранение ключей шифрования	**2.5.3.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по безопасному хранению ключей шифрования.	Платежное приложение должно хранить ключи безопасным образом (например, шифруя их при помощи ключа шифрования ключей).
	2.5.3.b Протестировать приложение, включая методы, использованные для хранения ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют безопасному хранению ключей шифрования.	
2.5.4 Смена ключей шифрования, период действия которых истек (например, когда истек установленный срок, и (или) когда данным ключом было зашифровано определенное количество криптотекста), основана на передовых практических методах индустрии безопасности и указаниях (например, *специальное издание 800-57 Национального института стандартов и технологий*) и должна производиться согласно предписаниям соответствующего производителя или владельца ключа.	**2.5.4.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • определенный период действия для каждого ключа, используемого приложением; • процедуры обеспечения смены ключа по истечении определенного периода действия.	Период действия ключа — это период времени, в течение которого ключ шифрования можно использовать для решения определенной задачи. Аспекты, рассматриваемые при определении криптопериода, включают, но не ограничиваются: надежность базового алгоритма, размер или длина ключа, риск кражи ключа и конфиденциальность данных, зашифрованных с помощью ключа. Периодическая замена ключей шифрования является обязательной для минимизации рисков несанкционированного получения ключей шифрования и последующего дешифрования данных.
	2.5.4.b Протестировать приложение, включая методы, использованные для замены ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют смене ключей по истечении определенного периода действия.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.5.5 Изъятие или смена ключей (например, архивация, уничтожение и (или) аннулирование) при нарушении целостности (например, увольнение сотрудника, обладающего информацией об открытом коде ключа и т. д.), а также ключей, относительно которых существуют подозрения в их компрометации. ***Примечание.*** *Если существует необходимость сохранения изъятых или замененных ключей, они должны быть безопасно заархивированы (например, посредством ключа шифрования ключей). Помещенные в архив криптографические ключи должны использоваться только в целях дешифрования/ верификации.*	**2.5.5.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • инструкции, согласно которым ключи должны быть изъяты либо заменены в случае нарушения целостности или наличия подозрений о компрометации; • процедуры изъятия или смены ключей (например, архивация, уничтожение и (или) аннулирование); • процедуры для проверки того, что изъятые или замененные ключи не используются для шифрования.	Ключи, которые больше не используются или в которых нет необходимости, а также ключи, относительно которых существуют подозрения о компрометации, должны быть изъяты и (или) уничтожены, чтобы устранить возможность их использования. Если требуется хранение таких ключей (например, для поддержки архивированных зашифрованных данных), то они должны быть надежно защищены. Платежное приложение должно обеспечивать возможность смены ключей, которые необходимо заменить или относительно которых существуют подозрения о компрометации.
	2.5.5.b Протестировать приложение, включая методы, использованные для изъятия или смены ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют смене или изъятию ключей (например, путем архивации, уничтожения и (или) аннулирования, если применимо).	
	2.5.5.c Протестировать приложение с использованием изъятых/замененных ключей, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* гарантируют, что приложение не будет использовать изъятые или замененные ключи для шифрования.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.5.6 Если платежное приложение поддерживает ручное управление ключами шифрования в открытом виде, соответствующие процедуры обязаны предусматривать разделение знания и двойной контроль ключей. ***Примечание.*** *Примеры процедур управления ключами вручную включают, в том числе: генерацию ключа, его передачу, загрузку, хранение и уничтожение.*	**2.5.6.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • подробные сведения о процедурах ручного управления ключами шифрования в открытом виде, поддерживаемых приложением; • инструкции по обеспечению разделения знания и двойного контроля для всех таких операций.	Разделение знаний и двойной контроль ключей используются для исключения возможности того, что один человек получит доступ к целому ключу. Данные механизмы контроля применяются к процедурам ручного управления ключами. Разделение знаний – это метод, при использовании которого двое или более лиц владеют отдельными компонентами одного ключа, которые по отдельности не позволяют узнать исходный ключ шифрования; каждое лицо знает только свой компонент ключа, и отдельные компоненты не позволяют узнать исходный ключ шифрования. Двойной контроль требует наличия двух или более людей для выполнения определенной функции, при этом ни один из них не имеет доступа к учетным данным другого.
	2.5.6.b Протестировать приложение, включая все процедуры ручного управления ключами шифрования в открытом виде, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют реализации разделения знаний и двойного контроля ключей, необходимых для всех процедур ручного управления ключами в открытом виде.	
2.5.7 Защита от неавторизованной смены ключей	**2.5.7.a** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по защите от неавторизованной смены ключей шифрования.	Платежное приложение должно определить для пользователей приложения методы, обеспечивающие возможность только авторизованной смены ключей. Конфигурация приложения не должна допускать или принимать подмену ключей, инициированную неавторизованными источниками или неожиданными процессами.
	2.5.7.b Протестировать приложение, включая методы, использованные для смены ключей шифрования, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* препятствуют неавторизованной смене ключей шифрования.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
2.6 Предоставить механизм, делающий невозможным восстановление компонентов ключей шифрования или криптограмм, хранимых платежным приложением, в соответствии в отраслевыми стандартами. Это ключи шифрования, используемые для шифрования или проверки данных держателей карт. ***Примечание.*** *Данное требование применяется, только если платежное приложение использует или предыдущие версии платежного приложения использовали компоненты ключей шифрования или криптограммы для шифрования данных держателей карт.* ***Согласуется с требованием 3.6 стандарта PCI DSS***	**2.6.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и подтвердить, что документация включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • процедуры, описывающие использование средства или процедуры, предназначенных для обеспечения невозможности восстановления компонентов ключей шифрования; • компонент ключа шифрования должен быть лишен возможности восстановления, если ключи больше не используются, в соответствии требованиями PCI DSS к управлению ключами; • процедуры повторного шифрования накопленных данных при помощи новых ключей, включая процедуры обеспечения безопасности данных при их нахождении в открытом виде во время процесса дешифрования/повторного шифрования.	Поставщики должны предоставить своим клиентам механизм, позволяющий удалять безопасным образом устаревшие компоненты ключей шифрования, которые больше не требуются. Следует обратить внимание, что удаление устаревших компонентов ключей шифрования осуществляется по усмотрению клиентов. Компоненты ключей шифрования и (или) криптограммы могут быть лишены возможности восстановления посредством использования средств или процессов, включающих, помимо прочего: • надежное удаление, как определено, к примеру, в списке одобренных продуктов, составленном Управлением национальной безопасности или другими национальными стандартами или нормативами либо стандартами или нормативами штата; • удаление ключа шифрования ключей, при условии, что оставшиеся ключи шифрования данных существуют только в форме, зашифрованной удаленным ключом шифрования ключей.
	2.6.b Изучить финальную версию приложения, чтобы убедиться, что поставщик предоставил средство и (или) процедуру, при помощи которых приложение может предотвратить восстановление компонентов ключей шифрования.	
	2.6.c Протестировать приложение, включая методы предотвращения восстановления ключей шифрования. Убедиться, при помощи аналитических средств и (или) методов, что средство или процедура надежного удаления, предоставленные поставщиком, обеспечивают невозможность восстановления компонентов ключей шифрования в соответствии с отраслевыми стандартами.	
	2.6.d Протестировать методы повторного шифрования накопленных данных при помощи новых ключей, чтобы убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* способствуют успешному повторному шифрованию накопленных данных при помощи новых ключей.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 3. Предоставление функций безопасной аутентификации

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
3.1 Платежное приложение должно поддерживать и обеспечивать использование уникальных идентификаторов пользователей и безопасную аутентификацию для административного доступа и доступа к данным держателей карт. Безопасная аутентификация должна быть обеспечена для всех учетных записей, созданных или управляемых приложением, до завершения установки и для последующих изменений после установки. Приложение должно обеспечить выполнение приведенных ниже требований 3.1.1–3.1.11: ***Примечание.*** *Термин "последующие изменения", используемый в тексте требования 3, относится ко всем изменениям приложения, приводящим к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей.* ***Примечание.*** *Данные меры управления паролями не должны применяться к сотрудникам, имеющим доступ только к одному номеру карты в один момент времени для обеспечения проведения единичной операции. Данные меры применяются к доступу, осуществляемому сотрудниками с административными возможностями, доступу к системам, содержащим данные держателей карт, и доступу, контролируемому платежным приложением.* *Данное требование распространяется на платежное приложение и все связанные с ним средства, используемые для просмотра или доступа к данным держателей карт.* ***Согласуется с требованиями 8.1 и 8.2 стандарта PCI DSS***	**3.1.a** *Изучить Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что клиенты и интеграторы/реселлеры: • получили четкие и недвусмысленные разъяснения в отношении того, как платежное приложение обеспечивает надежную аутентификацию для всех учетных данных для аутентификации, которые приложение генерирует или которыми управляет, посредством: – обеспечения безопасных изменений учетных данных для аутентификации до завершения установки в соответствии с требованиями 3.1.1–3.1.11; – обеспечения безопасности всех последующих (после установки) изменений учетных данных для аутентификации в соответствии с требованиями 3.1.1–3.1.11. • осведомлены, что в целях выполнения требований стандарта PCI DSS все изменения аутентификационных конфигураций должны пройти проверку на соответствие строгости методов аутентификации требованиям стандарта PCI DSS; • получили рекомендации, что учетным записям по умолчанию (даже если они не будут использоваться) рекомендуется назначить надежную аутентификацию, а затем отключить либо не использовать эти учетные записи; • получили четкие и недвусмысленные разъяснения в отношении того, как учетные данные для аутентификации (не созданные и не управляемые приложением) используются платежным приложением; как изменить учетные данные для аутентификации до или после завершения установки и обеспечить надежную аутентификацию в соответствии с требованиями 3.1.1–3.1.11 на всех уровнях приложения и для всех пользовательских учетных записей с административным доступом или доступом к данным держателей карт.	Уникально идентифицируя каждого пользователя – вместо использования одного идентификатора для нескольких сотрудников – приложение поддерживает индивидуальную ответственность сотрудников за свои действия и эффективно отслеживает все действия, выполняемые каждым сотрудником, регламентируемые требованиями стандарта PCI DSS. Это поможет ускорить разрешение и предотвращение происходящих инцидентов, связанных с информационной безопасностью. Надежная аутентификация при использовании совместно с уникальными идентификаторами помогает защитить уникальные идентификаторы пользователей от раскрытия, поскольку для этого злоумышленнику потребуется знать и уникальный идентификатор, и пароль (или другой элемент аутентификации).

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
3.1.1 Платежное приложение не должно использовать (или требовать использования) административные учетные записи по умолчанию для другого необходимого программного обеспечения (например, платежное приложение не должно использовать административную учетную запись базы данных по умолчанию). ***Согласуется с требованием 2.1 стандарта PCI DSS***	**3.1.1** Платежное приложение должно быть установлено и настроено в соответствии с *Руководством по внедрению стандарта PA-DSS*, включая настройку административных учетных записей для всего необходимого программного обеспечения. Следует протестировать платежное приложение, чтобы убедиться, что оно не использует (и не требует использования) административные учетные записи по умолчанию для другого необходимого программного обеспечения.	Административные учетные записи (и пароли), установленные по умолчанию, известны широкому кругу лиц, их знают все лица, знакомые с платежным приложением или системой, где оно установлено. Если используются административные учетные записи или пароли, заданные по умолчанию, неавторизованное лицо может получить доступ к приложению и данным, просто войдя в систему под известными широкому кругу лиц учетными данными.
3.1.2 Приложение должно обеспечить изменение всех паролей приложения, установленных по умолчанию для всех учетных записей, созданных или управляемых приложением, до завершения установки и в случае последующих изменений. Это относится ко всем учетным записям, включая учетные записи пользователей, приложений и сервисов, а также к учетным записям, используемым поставщиком с целью техподдержки. ***Примечание.*** *Данное требование нельзя выполнить посредством регламентирования процесса, выполняемого пользователем, или инструкций из Руководства по внедрению стандарта PA-DSS. После завершения установки и в случае внесения последующих изменений приложение должно препятствовать использованию учетных записей, настроенных по умолчанию или встроенных в систему, пока не будет изменен пароль, заданный по умолчанию.*	**3.1.2** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением. **3.1.2.a** Необходимо установить приложение в соответствии с *Руководством по внедрению стандарта PA-DSS*, проверить настройки учетной записи и пароля и попытаться ввести все пароли, используемые по умолчанию, чтобы убедиться, что приложение обеспечивает изменение всех установленных по умолчанию паролей по завершении процесса установки. **3.1.2.b** Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и пароля и попытаться ввести все пароли по умолчанию, чтобы убедиться, что приложение обеспечивает изменение всех паролей, установленных по умолчанию, после внесения изменения.	Если приложение не обеспечивает смену паролей, заданных по умолчанию, к нему может быть осуществлен неавторизованный доступ со стороны любого лица, знакомого с настройками, устанавливаемыми по умолчанию.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
Согласуется с требованием 2.1 стандарта PCI DSS		
3.1.3 Платежное приложение назначает уникальный идентификатор для пользовательских учетных записей. ***Согласуется с требованием 8.1.1 стандарта PCI DSS***	**3.1.3** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	После назначения уникального идентификатора пользователя его доступ и деятельность в рамках приложения можно отследить.
	3.1.3.a Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и попытаться создать разные учетные записи приложения с одинаковым идентификатором пользователя, чтобы убедиться, что платежное приложение назначает только уникальные идентификаторы пользователей по завершении процесса установки.	
	3.1.3.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что уникальные идентификаторы пользователей назначаются всем учетным записям после внесения изменения.	
3.1.4 Платежное приложение должно использовать как минимум один из следующих методов для 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,	**3.1.4** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Данные методы аутентификации при использовании совместно с уникальными идентификаторами помогают защитить уникальные идентификаторы пользователей от разглашения, поскольку злоумышленнику потребуется знать и уникальный идентификатор, и пароль (или другой элемент аутентификации).
	3.1.4.a Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и протестировать методы аутентификации, чтобы убедиться, что приложение использует как минимум один из определенных методов для всех учетных записей по завершении процесса установки.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
биометрические параметры); ***Согласуется с требованием 8.2 стандарта PCI DSS***	**3.1.4.b** Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо протестировать методы аутентификации, чтобы убедиться, что приложение использует как минимум один из определенных методов для всех учетных записей после внесения изменения.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
3.1.5 Платежное приложение **не** должно запрашивать или использовать групповые, общие или стандартные учетные записи и пароли. ***Согласуется с требованием 8.5 стандарта PCI DSS***	**3.1.5** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением. **3.1.5.a** Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS*, проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что по завершении процесса установки приложение не запрашивает и не использует групповые, общие и стандартные учетные записи и пароли. **3.1.5.b** Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что приложение не запрашивает и не использует групповые, общие и стандартные учетные записи и пароли после внесения изменения.	При использовании несколькими пользователями одних и тех же учетных данных (например, учетной записи и пароля) становится невозможным назначить ответственность за действия, выполненные отдельным пользователем, или эффективно регистрировать события, связанные с этими действиями, поскольку эти действия могут быть совершены любым лицом, которому известны эти учетные данные.
3.1.6 Платежное приложение должно применять следующие требования в отношении паролей: • наличие в пароле не менее семи символов; • наличие в пароле и цифр, и букв. Как вариант, пароли и (или) кодовая фраза должны иметь сложность и стойкость, сравнимые с указанными выше параметрами.	**3.1.6** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением. **3.1.6.a** Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS*и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение требует, чтобы пароль соответствовал следующим требованиям в отношении сложности и надежности: • использование в пароле не менее семи символов; • наличие в пароле и цифр, и букв.	Злоумышленники часто пытаются найти учетные записи со слабыми или отсутствующими паролями, чтобы получить доступ к приложению или системе. Злоумышленнику относительно просто найти слабозащищенные учетные записи и получить доступ к конфиденциальной информации приложения или базовой системы под видом настоящего пользователя, если используются короткие или легко угадываемые пароли. *(Продолжение на следующей странице)*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	3.1.6.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение требует, чтобы пароль соответствовал следующим требованиям в отношении сложности и надежности: • использование в пароле не менее семи символов; • наличие в пароле и цифр, и букв.	В соответствии с данным требованием пароли должны насчитывать не менее семи символов и содержать цифры и буквы. В случае, если данное требование не может быть выполнено в силу технических ограничений, организации могут использовать принцип "эквивалентной надежности" для оценки альтернатив. NIST SP 800-63-1 определяет "энтропию", как "степень сложности угадывания или подбора пароля или ключа". Настоящий и иные документы, в которых обсуждается "энтропия пароля", можно использовать для получения дополнительной информации о величинах энтропии и эквивалентной надежности пароля для паролей с другими минимальными требованиями.
	3.1.6.c Если приложение использует другой минимальный набор символов и длину паролей, необходимо рассчитать энтропию паролей, требуемых приложением, и убедиться, что она как минимум эквивалентна указанным выше параметрам (а именно не менее 7 букв и цифр).	
3.1.7 Платежное приложение требует изменения пароля пользователя не реже одного раза в 90 дней. ***Согласуется с требованием 8.2.4 стандарта PCI DSS***	**3.1.7** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Пароли и (или) кодовые фразы, не изменяемые в течение длительного времени, дают злоумышленникам больше возможностей для их взлома.
	3.1.7.a Необходимо установить приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение требует, чтобы пароль был изменен не реже одного раза в 90 дней.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	3.1.7.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение требует, чтобы пароль был изменен не реже одного раза в 90 дней.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
3.1.8 Платежное приложение должно хранить историю паролей и требовать, чтобы новый пароль отличался от любого из последних четырех использованных паролей. ***Согласуется с требованием 8.2.5 стандарта PCI DSS***	**3.1.8** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Если история паролей не ведется, эффективность смены паролей снижается, так как предыдущие пароли могут быть использованы повторно снова и снова. Запрет повторного использования паролей в течение определенного периода времени снижает вероятность того, что угаданные или подобранные пароли будут использованы в будущем.
	3.1.8.a Необходимо установить приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение хранит историю паролей и требует, чтобы новый пароль отличался от любого из последних четырех использованных паролей.	
	3.1.8.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение хранит историю паролей и требует, чтобы новый пароль отличался от любого из последних четырех использованных паролей.	
3.1.9 Платежное приложение блокирует учетную запись после шести неудачных попыток входа. ***Согласуется с требованием 8.1.6 стандарта PCI DSS***	**3.1.9** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Без реализованного механизма блокировки учетных записей злоумышленник может непрерывно пытаться подобрать пароль или вручную, или с использованием автоматизированных средств (программ взлома паролей) до достижения успеха и получения доступа к пользовательской учетной
	3.1.9.a Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение блокирует учетную запись после шести неудачных попыток входа.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	3.1.9.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа выполненных изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение блокирует учетную запись после шести неудачных попыток входа.	записи.
3.1.10 Платежное приложение устанавливает период блокировки учетной записи равный 30 минутам или до разблокировки учетной записи администратором. ***Согласуется с требованием 8.1.7 стандарта PCI DSS***	**3.1.10** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Если учетная запись пользователя блокируется в результате непрекращающихся попыток подбора пароля, защитные меры в виде задержки активации заблокированных учетных записей помогут остановить злоумышленника от непрерывного подбора пароля (он будет вынужден остановиться по крайней мере на 30 минут до автоматической активации учетной записи). Кроме того, если будет запрошена повторная активация, администратор может установить, действительно ли владелец учетной записи запросил ее.
	3.1.10.a Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение устанавливает период блокировки учетной записи равный 30 минутам или до разблокировки учетной записи администратором.	
	3.1.10.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение устанавливает период блокировки учетной записи равный 30 минутам или до разблокировки учетной записи администратором.	
3.1.11 Если сеанс платежного приложения находится в состоянии простоя в течение более 15 минут, приложение должно	**3.1.11** Приложение должно быть протестировано следующим образом по отношению ко всем учетным записям, созданным или управляемым приложением.	Когда пользователи отлучаются от открытого сеанса, имеющего доступ к платежному приложению, это

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
требовать ввода пароля для разблокировки или повторной активации сеанса. ***Согласуется с требованием 8.1.8 стандарта PCI DSS***	**3.1.11.a** Необходимо установить приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки учетной записи, чтобы убедиться, что по завершении процесса установки приложение устанавливает время простоя сеанса равное 15 минутам или меньше.	соединение может использоваться кем-нибудь в их отсутствие, что приведет к несанкционированному доступу к учетной записи и (или) ненадлежащему ее использованию.
	3.1.11.b Протестировать все функции приложения, приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки учетной записи и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения приложение устанавливает время простоя сеанса равное 15 минутам или меньше.	
3.2 Поставщик приложения должен сообщить клиентам, что любой доступ к компьютерам, серверам и базам данных, содержащим платежные приложения, должен требовать уникального идентификатора пользователя и безопасной аутентификации. ***Согласуется с требованиями 8.1. и 8.2 стандарта PCI DSS***	**3.2** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что клиенты и интеграторы/реселлеры проинструктированы в отношении контроля доступа к компьютерам, серверам и базам данных, содержащим платежные приложения и данные держателей карт, посредством уникального идентификатора пользователя и безопасной аутентификации, соответствующей требованиям стандарта PCI DSS.	Если приложение установлено или используется системами, которые не обеспечивают надежных механизмов идентификации и аутентификации, надежную идентификацию, предоставляемую приложением, можно будет обойти, что приведет к небезопасному доступу.
3.3 Необходимо обеспечить безопасность всех паролей платежных приложений (включая пароли учетных записей пользователя и приложения) во время передачи и хранения. ***Согласуется с требованием 8.2.1 стандарта PCI DSS***	**3.**3 Выполнить следующее.	Если пароли платежного приложения хранятся или передаются по сети без шифрования, злоумышленники могут легко перехватить пароли, используя анализатор пакетов, или получить непосредственный доступ к паролям в файлах в месте их хранения и использовать украденные данные для получения неавторизованного доступа. Соединение уникальной вводной переменной с каждым паролем перед применением алгоритма хэширования
3.3.1 Следует использовать надежную криптографию, чтобы привести все пароли платежного приложения в нечитаемый вид на время передачи.	**3.3.1.a** Изучить документацию поставщика и конфигурации приложения, чтобы убедиться, что надежная криптография используется для приведения всех паролей в нечитаемый вид на время передачи.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	3.3.1.b Необходимо проверить передачу всех типов паролей приложения (например, войти в приложение из другой системы и пройти аутентификацию для другой системы), чтобы убедиться, что надежная криптография используется для приведения всех паролей в нечитаемый вид на время передачи.	
3.3.2 Необходимо использовать надежный односторонний криптографический алгоритм, основанный на утвержденных стандартах, для приведения всех паролей в нечитаемый вид на время хранения. Каждый пароль должен быть соединен с уникальной вводной переменной перед применением криптографического алгоритма.	**3.3.2.a** Изучить документацию поставщика и конфигурации приложения, чтобы убедиться, что**:** • хранящиеся пароли приведены в нечитаемый вид при помощи надежного одностороннего криптографического алгоритма, основанного на утвержденных стандартах; • каждый пароль соединен с уникальной вводной переменной перед применением криптографического алгоритма.	
Примечание. *Вводная переменная не обязана быть непредсказуемой или храниться в секрете*	**3.3.2.b** Для каждого типа паролей приложения необходимо определить все возможные места хранения, включая само приложение, системы, на которых оно установлено, файлы журнала, параметры реестра и т. д. Необходимо проверить все хранящиеся файлы паролей, чтобы убедиться, что пароли приведены в нечитаемый вид при помощи надежного одностороннего криптографического алгоритма с постоянным использованием уникальной вводной переменной во время хранения.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
3.4 Платежное приложение должно ограничивать доступ к необходимым функциям и (или) ресурсам и назначать встроенным учетным записям приложения минимальные права доступа: • по умолчанию все учетные записи приложения/сервисов имеют доступ только к тем функциям и (или) ресурсам, которые необходимы для их работы; • по умолчанию все учетные записи приложения/сервисов имеют минимальные права доступа к каждой функции и (или) ресурсу, необходимым учетной записи. ***Согласуется с требованием 7 стандарта PCI DSS***	**3.4.a** Необходимо установить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и проверить настройки встроенных учетных записей, чтобы убедиться, что по завершении процесса установки: • все учетные записи приложения/сервисов имеют доступ только к тем функциям и (или) ресурсам, которые необходимы для их работы; • все учетные записи приложения/сервисов имеют минимальные права доступа к каждой функции и (или) ресурсу, необходимым учетной записи.	Чтобы ограничить доступ к данным держателей карт и конфиденциальным функциям только теми учетными записями, которым необходим такой доступ, необходимо определить уровни и права доступа для каждой встроенной учетной записи, чтобы могли выполняться назначенные функции, но отсутствовали дополнительные или необязательные права и возможности доступа. Назначение минимальных прав доступа помогает предотвратить ошибочное или случайное изменение конфигурации приложения или настроек безопасности со стороны пользователей, не обладающих достаточными знаниями о приложении. Обеспечение минимальных прав доступа также поможет свести к минимуму ущерб в случае, если неавторизованное лицо получит доступ к идентификатору пользователя.
	3.4.b Протестировать все функции приложения, приводящие к изменениям встроенных учетных записей, в том числе приводящие к возврату настроек учетных записей пользователей к значениям по умолчанию, изменениям существующих конфигураций учетных записей и изменениям, приводящим к созданию новых или повторному созданию существующих учетных записей. Для каждого типа изменений необходимо проверить настройки встроенных учетных записей и протестировать функциональность приложения, чтобы убедиться, что после внесения изменения: • все учетные записи приложения/сервисов имеют доступ только к тем функциям и (или) ресурсам, которые необходимы для их работы; • все учетные записи приложения/сервисов имеют минимальные права доступа к каждой функции и (или) ресурсу, необходимым учетной записи.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 4. Следует вести журнал активности платежного приложения

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
4.1 После завершения процесса установки по умолчанию должен вестись журнал доступа всех пользователей и должна присутствовать возможность соотнести действия с конкретными пользователями. ***Согласуется с требованием 10.1 стандарта PCI DSS***	**4.1.a** Необходимо установить платежное приложение. Следует протестировать приложение, чтобы убедиться, что протоколирование событий платежного приложения автоматически включено после установки.	Крайне важно, чтобы в платежном приложении присутствовал процесс или механизм, соотносящий пользователей с ресурсами приложения, к которым был осуществлен доступ, генерирующий журналы аудита и предоставляющий возможность отслеживать подозрительную деятельность конкретного пользователя. Группы, расследующие инциденты, полагаются на подобные журналы для начала проведения расследования.
	4.1.b Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что оно включает в себя следующие инструкции: • инструкции по установке приложения таким образом, чтобы ведение журналов было включено и настроено по умолчанию после завершения процесса установки; • инструкции по настройке доступных клиенту параметров журнала после установки в соответствии в требованиями стандарта PCI DSS согласно приведенным ниже требованиям 4.2, 4.3 и 4.4 стандарта PA-DSS. • Журналы не должны быть отключены, так как это приведет к несоответствию требованиям стандарта PCI DSS. • Инструкции по настройке доступных клиенту параметров журнала сторонних программных компонентов, поставляемых совместно либо требуемых платежным приложением, после установки в соответствии в требованиями стандарта PCI DSS.	
4.2 Платежное приложение должно предоставлять автоматический механизм протоколирования следующих событий. ***Согласуется с требованием 10.2 стандарта PCI DSS***	**4.2** Протестировать платежное приложение, изучив настройки и файлы журнала аудита платежного приложения, и выполнить следующее:	регистрация событий согласно пунктам 4.2.1 – 4.2.7 позволяет организации выявить и отследить потенциально вредоносную активность.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
4.2.1 Любой доступ пользователя к данным держателей карт при помощи приложения	**4.2.1** Убедиться в том, что факты доступа пользователя к данным держателей карт при помощи приложения регистрируются.	Злоумышленники могут получить информацию об учетной записи пользователя с доступом к данным держателей карт при помощи приложения или создать новую неавторизованную учетную запись для получения доступа к данным держателей карт. Регистрация всех событий доступа к данным держателей карт позволяет выявить, какие учетные записи могут быть взломаны или неправильно использованы.
4.2.2 Любые действия, совершенные с использованием административных полномочий в отношении приложения	**4.2.2** Убедиться в том, что любые действия, совершенные с использованием административных полномочий в отношении приложения, регистрируются.	Учетные записи с расширенными правами доступа, такие как "administrator", могут влиять на безопасность или функционирование приложения. Если не регистрировать события, организация не сможет отслеживать проблемы, связанные с ошибками администрирования или ненадлежащим использованием прав доступа.
4.2.3 Доступ к журналам аудита приложения должен управляться самим приложением либо посредством его функций	**4.2.3** Убедиться в том, что доступ к журналам аудита приложения, управляемый самим приложением либо посредством его функций, регистрируется.	Злоумышленники часто пытаются изменить записи в журнале, чтобы скрыть свои действия. Регистрация событий доступа позволяет организации определять несоответствия или факт подмены записей в журнале.
4.2.4 Неуспешные попытки логического доступа	**4.2.4** Убедиться в том, что неуспешные попытки логического доступа регистрируются.	Злоумышленники часто предпринимают многочисленные попытки доступа к целевым системам. Несколько неуспешных попыток входа в систему могут свидетельствовать о том, что неавторизованный пользователь пытается войти в систему путем подбора паролей.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
4.2.5 Использование и изменение механизмов идентификации и аутентификации приложения (включая, помимо прочего, создание новых учетных записей, расширение прав доступа и т. д.), а также все изменения, добавления, удаления учетных записей с правами суперпользователя ("root") или администратора	**4.2.5** Убедиться в том, что использование и изменение механизмов идентификации и аутентификации приложения (включая, помимо прочего, создание новых учетных записей, расширение прав доступа и т. д.), а также все изменения, добавления, удаления учетных записей с правами суперпользователя ("root") или администратора регистрируются.	Без знания того, кто входил в систему на момент возникновения инцидента, невозможно установить, какие учетные записи были использованы. Злоумышленники могут также предпринимать попытки обхода механизмов аутентификации. Действия, включающие, помимо прочего, создание новых учетных записей, расширение или изменение прав доступа, могут свидетельствовать о неавторизованном использовании механизмов аутентификации.
4.2.6 Инициализация, остановка или приостановка ведения журналов аудита	**4.2.6** Убедиться в том, что следующие события регистрируются: • инициализация журналов аудита приложения; • остановка или приостановка ведения журналов аудита приложения.	Выключение (или приостановка ведения) журналов протоколирования событий перед выполнением подозрительных действий является распространенной практикой среди злоумышленников, которые стремятся избежать обнаружения. Инициализация записей в журнале может свидетельствовать о том, что функции журнала были отключены пользователем в целях сокрытия действий.
4.2.7Создание и удаление объектов системного уровня приложением либо посредством его функций	**4.2.7**Убедиться в том, что создание и удаление объектов системного уровня приложением либо посредством его функций регистрируется.	Злоумышленники часто создают или заменяют объекты системного уровня на целевой системе, чтобы получить контроль над определенной функцией или операцией этой системы. Регистрация создания или замены объектов системного уровня, таких как таблицы баз данных или запрограммированные процедуры, упростит процесс установления правомочности таких изменений.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
4.3 Платежное приложение должно регистрировать как минимум следующие параметры для каждого события. ***Согласуется с требованием 10.3 стандарта PCI DSS***	**4.3** Протестировать платежное приложение, изучив настройки и файлы журнала аудита платежного приложения, и выполнить следующее для каждого контролируемого события (из 4.2):	записывая элементы, указанные в пунктах 4.3.1 – 4.3.6, для контролируемых событий, перечисленных в п. 4.2, можно быстро идентифицировать потенциальную компрометацию и получить достаточно сведений о том, кто, что, когда, где и как сделал.
4.3.1 Идентификатор пользователя	**4.3.1** Убедиться в том, что идентификатор пользователя включен в записи журнала.	
4.3.2 Тип события	**4.3.2** Убедиться в том, что тип события включен в записи журнала.	
4.3.3 Дата и время	**4.3.3** Убедиться в том, что дата и время включены в записи журнала.	
4.3.4 Успешным или неуспешным было событие	**4.3.4** Убедиться в том, что в журнале указано, успешным или неуспешным было событие.	
4.3.5 Источник события	**4.3.5** Убедиться в том, что источник события включен в записи журнала.	
4.3.6 Идентификатор или название данных, системного компонента или ресурса	**4.3.6** Убедиться в том, что идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие, включены в записи журнала.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
4.4. Платежное приложение должно обеспечивать централизованное ведение журнала. ***Примечание.*** *Примеры данной функции включают, помимо прочего:* • ведение журнала при помощи стандартных отраслевых механизмов, таких как Common Log File System (CLFS), Syslog, текст с разделителями и т. д.; • предоставление функций и документации для конвертации собственного формата журнала приложения в стандартные отраслевые форматы для быстрой централизованный регистрации. ***Согласуется с требованием 10.5.3 стандарта PCI DSS***	**4.4.**a Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что клиентам и интеграторам/реселлерам предоставлено следующее: • описание поддерживаемых механизмов ведения журнала; • инструкции и процедуры внедрения журналов платежного приложения в централизованную среду ведения журналов. **4.4.b** Установить и настроить платежное приложение в соответствии с *Руководством по внедрению стандарта PA-DSS*, чтобы убедиться, что инструкции являются точными и функции, обеспечивающие возможность торговой точки внедрять журналы в централизованный сервер журналов, работают.	При недостаточной защите журналов гарантировать их полноту, точность и целостность будет невозможно, и они будут бесполезны в качестве средства расследования после компрометации. Включение журналов платежного приложения в централизованную систему ведения журналов позволяет клиенту интегрировать и сопоставлять свои журналы, а также последовательно обеспечивать их безопасность в своей среде.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 5. Необходимо разработать безопасные платежные приложения

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.1 Поставщик программного обеспечения должен определить и внедрить формальный процесс безопасной разработки платежных приложений, включающий в себя следующие положения: • платежные приложения должны разрабатываться согласно требованиям PCI DSS (например, в отношении безопасной аутентификации и ведения журнала); • в процессе разработки должны применяться промышленные стандарты и (или) передовые технологии; • требования к информационной безопасности должны учитываться в течение всего цикла разработки; • перед выпуском приложения или обновлением приложения необходимо проводить проверки на безопасность. ***Согласуется с требованием 6.3 стандарта PCI DSS***	**5.1.a** Изучить документированные процессы разработки программного обеспечения и убедиться, что в их основу положены промышленные стандарты и (или) передовые технологии.	Если не уделять должного внимания защите информации на этапах разработки программного обеспечения (определения требований, проектирования, анализа и тестирования), в код приложения непреднамеренно или сознательно могут быть введены уязвимости для системы безопасности.
	5.1.b Убедиться, что документированные процессы разработки программного обеспечения включают процедуры для обеспечения следующих требований: • вопросы информационной безопасности должны учитываться в течение всего цикла разработки; • разработка платежных приложений должна вестись в соответствии с требованиями стандартов PCI DSS и PA-DSS.	
	5.1.c Убедиться, что документированные процессы разработки программного обеспечения включают: • проверки на безопасность перед выпуском приложения или обновлением приложения; • процедуры для проверок на безопасность, которые необходимо выполнить, чтобы убедиться, что требования PCI DSS и PA-DSS в отношении безопасности выполнены.	
	5.1.d Опросить разработчиков программного обеспечения, чтобы подтвердить, что документированные процессы выполняются. В частности: • требования к информационной безопасности учитываются в течение всего цикла разработки; • разработка платежных приложений ведется в соответствии с требованиями стандартов PCI DSS и PA-DSS; • проверки на безопасность проводятся через установленные интервалы в ходе всего процесса разработки и перед выпуском для гарантии того, что требования стандартов PCI DSS и PA-DSS в отношении безопасности будут выполнены.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.1.1 Убедиться в том, что действующие основные номера держателей карт не используются для тестирования и разработки. ***Согласуется с требованием 6.4.3 стандарта PCI DSS***	**5.1.1.a** Изучить процессы разработки программного обеспечения, чтобы убедиться, что они включают процедуры, обеспечивающие неприменение действующих основных номеров держателей карт в целях тестирования и разработки.	Эмитенты платежных карт и многие банки-эквайеры могут предоставлять номера, пригодные для тестирования, в случае, если требуются реалистичные основные номера держателей карт для тестирования функциональности системы перед выпуском.
	5.1.1.b Изучить процессы проведения проверки и опросить сотрудников, чтобы убедиться в том, что действующие основные номера держателей карт не используются для целей тестирования и разработки.	
	5.1.1.c Изучить выборку тестовых данных и убедиться в том, что действующие основные номера держателей карт не используются для целей тестирования и разработки.	
5.1.2 Убедиться в том, что тестовые данные и платежные счета удалены до передачи приложения потребителям. ***Согласуется с требованием 6.4.4 стандарта PCI DSS***	**5.1.2.a** Изучить процессы разработки программного обеспечения, чтобы убедиться, что они включают процедуры проверки того, что тестовые данные и платежные счета удалены до передачи приложения потребителям.	Тестовые данные и платежные счета должны быть удалены из приложения до его передачи потребителям, так как наличие этих элементов может раскрыть информацию о ключевых структурных компонентах приложения.
	5.1.2.b Изучить процессы проведения тестирования и опросить персонал, чтобы убедиться в том, что все тестовые данные и платежные счета удаляются до передачи приложения потребителям.	
	5.1.2.c Изучить финальную версию платежного приложения, чтобы убедиться в том, что все тестовые данные и платежные счета удалены до передачи приложения потребителям.	
5.1.3 Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей платежных приложений потребителям	**5.1.3.a** Изучить процессы разработки программного обеспечения, чтобы убедиться, что они включают процедуры проверки того, что индивидуальные учетные записи, имена пользователей и пароли удалены до передачи приложения потребителям.	Настроенные предварительно индивидуальные учетные записи, имена пользователей и пароли могут быть использованы в качестве "черного хода" разработчиками или другими

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
Согласуется с требованием 6.3.1 стандарта PCI DSS	**5.1.3.b** Изучить процессы проведения тестирования и опросить персонал, чтобы убедиться в том, что индивидуальные учетные записи, имена пользователей и пароли удалены до передачи платежного приложения потребителям.	лицами, обладающими знанием об этих учетных записях, для получения доступа к приложению, что может привести к компрометации приложения и связанных с ним данных держателей карт.
	5.1.3.c Изучить финальную версию платежного приложения, чтобы убедиться в том, что индивидуальные учетные записи, имена пользователей и пароли удалены до передачи платежного приложения потребителям.	
5.1.4 Проверить программный код платежного приложения на наличие потенциальных уязвимостей после внесения значительных изменений (вручную или автоматически) перед передачей потребителям с соблюдением следующих минимальных требований: • изменения программного кода контролируются лицами, иными, чем создавший его автор, и лицами, знакомыми с методиками контроля кода (code review techniques) и методами безопасного программирования (secure coding practices); • контроль программного кода обеспечивает его разработку в соответствии с основными принципами безопасного программирования*;* (см. требование 5.2 стандарта PA-DSS); • все необходимые корректировки вносятся до выпуска программного обеспечения; • результаты контроля кода	**5.1.4.a** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что поставщик выполняет контроль кода в отношении всех изменений программного кода (вручную или автоматически) следующим образом: • изменения программного кода контролируются лицами, иными, чем создавший его автор, и лицами, знакомыми с методиками контроля кода (code review techniques) и методами безопасного программирования (secure coding practices); • контроль программного кода обеспечивает его разработку в соответствии с основными принципами безопасного программирования*;* (см. требование 5.2 стандарта PA-DSS); • все необходимые корректировки вносятся до выпуска программного обеспечения; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска программного обеспечения; • документированные результаты контроля кода включают в себя одобрение руководства, имена автора и лица, проверяющего код, а также список изменений, внесенных перед выпуском;	Уязвимости безопасности в коде приложения обычно используются злоумышленниками для получения доступа к сети и кражи данных держателей карт. Для защиты от подобных типов атак необходимо использовать соответствующие методики контроля кода. Методики контроля кода должны подтвердить, что в ходе процесса разработки применялись передовые методы безопасного программирования. Поставщик приложения должен использовать соответствующие методы безопасного программирования, применимые к используемым технологиям. Контроль кода должны выполнять опытные специалисты, знакомые с методиками контроля кода и способные обнаружить потенциальные проблемы в коде. Для обеспечения объективной и независимой оценки контроль кода

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
рассматриваются и утверждаются руководством до выпуска программного обеспечения; • документированные результаты контроля кода включают в себя одобрение руководства, имена автора и лица, проверяющего код, а также список изменений, внесенных перед выпуском. ***Примечание.*** *Данное требование по осуществлению контроля кода применимо ко всем компонентам платежного приложения (как внутренних так и общедоступных веб-приложений) как составная часть жизненного цикла разработки системы. Контроль кода может проводиться компетентным внутренним персоналом или третьими сторонами.* ***Согласуется с требованием 6.3.2 стандарта PCI DSS***	**5.1.4.b** Изучить результаты контроля нескольких изменений кода, и убедиться в том, что: • контроль кода выполнялся опытным специалистом, не являющимся автором кода; • контроль кода проводился в соответствии с основными принципами безопасного программирования; • все необходимые корректировки вносились до выпуска программного обеспечения; • результаты контроля кода были проверены и утверждены руководством до выпуска программного обеспечения.	следует поручать лицам, которые не являются создателями кода. Исправление ошибок в коде перед передачей программного обеспечения потребителям позволяет предотвратить потенциальное использование небезопасного кода злоумышленниками. Исправлять ошибки в коде после передачи программного обеспечения потребителям гораздо сложнее и дороже. Проведение официальной проверки и утверждение кода руководством до выпуска позволяет гарантировать, что код одобрен и разработан в соответствии с политиками и процедурами.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.1.5 Надежные методики контроля исходного кода должны быть внедрены с целью проверки целостности исходного кода в ходе процесса разработки.	**5.1.5.a** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться в том, что поставщик использует надежные методики контроля исходного кода для проверки целостности исходного кода в ходе процесса разработки.	Передовые методики контроля исходного кода помогают гарантировать, что все изменения кода являются намеренными и авторизованными и выполняются только лицами, имеющими для этого обоснованную потребность. В качестве примеров таких методик можно привести процедуры контроля по входам/выходам для кода со строгим контролем доступа и сравнения сразу после изменения кода с целью подтверждения того, что последняя одобренная версия не была изменена (например, с использованием контрольных сумм).
	5.1.5.b Изучить механизмы и процедуры обеспечения безопасности исходного кода, чтобы убедиться в том, что целостность исходного кода обеспечивается в ходе процесса разработки.	
5.1.6 Платежные приложения должны разрабатываться с использованием передовых методов безопасного программирования, включая: • разработку с минимальными правами доступа для среды приложения; • разработку с отказоустойчивыми значениями по умолчанию (по умолчанию запрещено выполнение любого кода, кроме указанного изначально);	**5.1.6.a** Изучить процессы разработки ПО, чтобы убедиться в том, что методики безопасного программирования определены и включают следующее: • разработку с минимальными правами доступа для среды приложения; • разработку с отказоустойчивыми значениями по умолчанию (по умолчанию запрещено исполнение любого кода, кроме указанного изначально); • разработку для всех видов точек доступа, включая такие разновидности ввода, как многоканальный ввод в приложение.	Разработка с минимальными правами доступа является наиболее эффективным способом предотвращения внесения небезопасных условий в приложение. Включение отказоустойчивых значений по умолчанию может помешать злоумышленнику получить конфиденциальную информацию о сбое приложения, которую затем можно использовать для совершения атаки. Обеспечение защиты для всех случаев

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
• разработку для всех видов точек доступа, включая такие разновидности ввода, как многоканальный ввод в приложение.	**5.1.6** Опросить разработчиков, чтобы убедиться, что приложения разрабатываются с использованием передовых методов безопасного программирования, включая: • разработку с минимальными правами доступа для среды приложения; • разработку с отказоустойчивыми значениями по умолчанию (по умолчанию запрещено выполнение любого кода, кроме указанного изначально); • разработку для всех видов точек доступа, включая такие разновидности ввода, как многоканальный ввод в приложение.	доступа и ввода данных в приложение устраняет вероятность того, что канал ввода будет подвержен компрометации. Несоблюдение данных принципов в ходе разработки кода может привести к выпуску небезопасного приложения и дополнительным затратам на устранение проблем в будущем.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.1.6.1 Методики программирования должны включать документацию, разъясняющую способ хранения основных номеров держателей карт и (или) критичных аутентификационных данных в памяти.	**5.1.6.1** Изучить методики программирования, чтобы убедиться, что они включают документацию, разъясняющую способ хранения основных номеров держателей карт и (или) критичных аутентификационных данных в памяти.	Злоумышленники используют вредоносные программы для сбора конфиденциальных данных из памяти. Минимизация рисков для основных номеров держателей карт и (или) критичных аутентификационных данных, хранящихся в памяти, поможет снизить вероятность того, что они будут собраны злоумышленником или сохранены на диск в файле дампа памяти и оставлены без защиты. Данное требование призвано акцентировать внимание на способе хранения основных номеров держателей карт и (или) критичных аутентификационных данных в памяти. Знание о том, когда и как долго конфиденциальные данные присутствуют в памяти, и их формата поможет поставщикам приложения обнаружить потенциальные уязвимости в своих приложениях и определить, требуется ли дополнительная защита. Приведут ли методики программирования к таким действиям, зависит от конкретного разрабатываемого приложения и используемых технологий.
	5.1.6.1.b Опросить разработчиков, чтобы убедиться, что они обращают внимание на способ хранения основных номеров держателей карт и критичных аутентификационных данных в памяти во время процесса разработки приложения.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.1.7 Обучить разработчиков приложения методикам безопасной разработки, применимым к обязанностям разработчика и используемым технологиям, например: • проектированию безопасных приложений; • методикам безопасного программирования с целью устранения распространенных уязвимостей (например, инструкции поставщика, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding и т. д.); • управлению конфиденциальными данными в памяти; • контролю кода; • тестированию защиты (например, методикам теста на проникновение); • методикам оценки рисков. ***Примечание.*** *Обучение разработчиков приложения может осуществляться как самой организацией, так и третьими лицами. Обучение может осуществляться на рабочем месте, под руководством инструктора либо электронным образом.*	**5.1.7a** Убедиться, что документированные процессы разработки программного обеспечения требуют обучить разработчиков приложения методикам безопасной разработки, применимым к обязанностям разработчика и используемым технологиям.	Если разработчики будут знакомы с методами безопасной разработки, это поможет снизить количество уязвимостей в системе безопасности вследствие использования ненадежных с точки зрения безопасности методик программирования. Обученный персонал с большей долей вероятности обнаружит уязвимости в структуре и коде приложения. Платформы и методология разработки ПО часто меняются, так же как угрозы и риски, стоящие перед приложениями. Обучение методам безопасной разработки должно соответствовать меняющимся методам разработки.
	5.1.7.b Опросить несколько сотрудников, чтобы убедиться, что они знакомы с безопасными методами разработки и методиками программирования, применимыми к используемым технологиям.	
	5.1.7.c Изучить документацию о ходе обучения и убедиться, что все разработчики приложения прошли обучение, соответствующее их обязанностям и используемым технологиям.	
5.1.7.1 По мере необходимости дополнить программу обучения, чтобы охватить новые технологии разработки и используемые методы.	**5.1.7.1** Изучить обучающие материалы и опросить несколько разработчиков, чтобы убедиться, что программа обучения обновляется с целью охвата новых технологий разработки и используемых методов.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2 В процессе разработки всех платежных приложений должны быть устранены все распространенные уязвимости в коде. ***Примечание.*** *Уязвимости, перечисленные в требованиях 5.2.1 – 5.2.9 стандарта PA-DSS и требованиях 6.5.1 – 6.5.9 PCI DSS соответствовали передовым практическим методам индустрии безопасности на момент публикации данной версии стандарта PA-DSS. По мере развития передовых методик управления уязвимостями (таких как руководство OWASP Top 10, SANS CWE Top 25, CERT Secure Coding и т. д.) следует использовать их актуальную версию.* ***Согласуется с требованием 6.5 стандарта PCI DSS***	**5.2** Убедиться, что платежные приложения не подвержены распространенным уязвимостям кода, выполнив ручной или автоматизированный тест на проникновение, нацеленный на выявление следующих уязвимостей.	Прикладной уровень подвержен высокому риску и может являться объектом как внутренних, так и внешних угроз. Без надлежащей защиты данные держателей карт и другая конфиденциальная информация компании могут быть раскрыты. Требования 5.2.1 – 5.2.9 являются минимальными требованиями, которые необходимо соблюдать. Этот список состоит из наиболее распространенных уязвимостей кода на момент публикации данной версии стандарта PA-DSS. В случае обновления списка распространенных уязвимостей кода, методики программирования, используемые поставщиком, должны изменяться соответственно.
Примечание. *Требования 5.2.1 – 5.2.6, приведенные ниже, распространяются на все платежные приложения (внешние или внутренние).*		

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2.1 Возможности для внедрения кода, в особенности, внедрение SQL-кода. Также следует учесть инъекции OS Command, LDAP и Xpath.	**5.2.1** Внедрения кода, в особенности внедрение SQL-кода, могут быть предотвращены при помощи следующих методик программирования: • проверка того, что введенная пользователями информация не может изменить существующие команды и запросы; • использование параметризованных запросов.	Внедрения кода, в особенности внедрения SQL-кода, являются распространенным способом взлома приложений. Внедрение происходит, когда предоставленные пользователем данные передаются интерпретатору вместе с командой или запросом. Злоумышленнику удается обмануть интерпретатор, запустить вредоносные команды или изменить данные, что открывает компоненты внутри приложения для таких атак, как переполнение буфера. Приложению необходимо проверять все вводимые данные перед обработкой (например, посредством проверки всех буквенных символов, сочетания буквенных и цифровых символов и т. д.).
5.2.2 Переполнение буфера	**5.2.2** Переполнение буфера можно предотвратить при помощи следующих методик программирования: • подтверждение границ буфера; • усечение строк ввода.	Переполнение буфера происходит, когда приложение не имеет соответствующих ограничений при проверке буферного пространства. Это может привести к тому, что информация, содержащаяся в буфере, вытесняется за пределы пространства буферной памяти в пространство исполняемой памяти. Когда это происходит, злоумышленник получает возможность внедрить в буфер вредоносный код и затем поместить этот вредоносный код в пространство исполняемой памяти посредством переполнения буфера. Затем вредоносный код выполняется, что позволяет злоумышленнику получить удаленный доступ к приложению и (или) зараженной системе.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2.3 Небезопасное криптографическое хранилище	**5.2.3** Небезопасное криптографическое хранилище можно защитить при помощи следующих методик программирования: • защита от криптографических ошибок; • использование стойких криптографических алгоритмов и ключей.	Приложения, которые не используют для хранения данных стойкие криптографические алгоритмы надлежащим образом, подвергаются риску компрометации и утечки учетных данных для проверки подлинности и (или) данных держателей карт.
5.2.4 Небезопасная передача данных	**5.2.4** Небезопасную передачу данных можно предотвратить, используя методики программирования, которые должным образом аутентифицируют и шифруют все конфиденциальные данные при передаче.	Приложения, которые не шифруют надлежащим образом конфиденциальный сетевой трафик с применением стойких криптографических алгоритмов, подвергаются повышенному риску компрометации и утечки данных держателей карт.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2.5 Некорректная обработка ошибок	**5.2.5** Некорректную обработку ошибок можно предотвратить, используя методики программирования, исключающие утечку информации через сообщения об ошибках (например, отображая общие, а не конкретные сведения об ошибке).	Вследствие некорректной обработки ошибок может происходить утечка информации о конфигурации и информационировании приложения или разглашение информации о правах доступа. Злоумышленники используют эти уязвимости для кражи критичных данных или для полного взлома системы. Если злоумышленник сможет вызвать появление ошибок, которые приложение не сможет правильно обработать, существует возможность получения злоумышленником подробной информации о системе, возникновения ситуации отказа в обслуживании, нарушения работы системы безопасности или сбоя приложения или системы. Например, сообщение "введен неправильный пароль" сообщает злоумышленнику о том, что использовалось верное имя пользователя и необходимо сфокусировать свои усилия только на подборе пароля. Следует использовать сообщения об ошибках более общего характера, например: "данные не могут быть подтверждены".
5.2.6 Все уязвимости, имеющие "высокую" степень риска, найденные в процессе обнаружения уязвимостей в соответствии с требованием 7.1 стандарта PA-DSS.	**5.2.6** При программировании должны приниматься меры по предотвращению уязвимостей с высокой степенью риска, которые могут повлиять на работу приложения (в соответствии с требованием 7.1 стандарта PA-DSS).	Все уязвимости, которым была присвоена высокая степень риска (в соответствии с требованием 7.1 стандарта PA-DSS) и которые могут повлиять на работу приложения, должны быть выявлены и устранены во время разработки приложения.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
Примечание. *Требования 5.2.7 – 5.2.10, приведенные ниже, распространяются на веб-приложения и интерфейсы приложений (внешние или внутренние).*		Веб-приложениям свойственны уникальные риски для безопасности, основанные на их архитектуре, а также в связи с их относительной доступностью для компрометации наряду с частыми случаями проявления последней.
5.2.7 Межсайтовый скриптинг (XSS)	**5.2.7** Межсайтовый скриптинг (XSS) можно предотвратить при помощи следующих методик программирования: • проверка всех параметров перед их включением в код; • использование контекстно-зависимого изолирования.	Межсайтовый скриптинг XSS происходит, когда приложение отправляет предоставленные пользователем данные в веб-браузер без предварительной проверки или шифрования этого содержимого. Межсайтовый скриптинг позволяет злоумышленникам выполнять сценарии в браузере для захвата сеансов пользователя, изменения вида веб-сайтов, внедрения червей и т. д.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2.8 Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий)	**5.2.8** Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий) можно предотвратить при помощи следующих методик программирования: • надлежащая аутентификация пользователей; • проверка введенных данных; • отсутствие доступа пользователей к прямым ссылкам на внутренние объекты; • пользовательские интерфейсы, ограничивающие доступ к неразрешенным функциям.	Проблемы, связанные с контролем доступа, возникают, когда разработчик предоставляет ссылку на внутренний объект, такой как файл, каталог, запись в базе данных или ключ, в виде URL-адреса или параметра формы. Злоумышленники могут использовать эти ссылки для доступа к другим объектам без авторизации. Злоумышленник может просканировать структуру каталогов веб-сайта (обход директорий), чтобы получить неавторизованный доступ к данным или информации о функционировании сайта для ее последующего использования в мошеннических целях. Если пользовательские интерфейсы не ограничивают доступ к запрещенным функциям, это может позволить злоумышленникам получить доступ к учетным данным с широкими полномочиями или данным держателей карт. Ограничение доступа к ресурсам данных поможет предотвратить передачу данных держателей карт на неавторизованные ресурсы.
5.2.9 Подделка межсайтовых запросов (CSRF)	**5.2.9** Подделку межсайтовых запросов (CSRF) можно предотвратить при помощи методик программирования, при использовании которых приложения не полагаются на учетные данные для проверки подлинности и токены, автоматически отправляемые браузерами.	В случае подделки межсайтовых запросов (CSRF) браузер жертвы отправляет предварительно авторизованный запрос в уязвимое веб-приложение, что позволяет злоумышленнику совершить любые действия, которые может совершить жертва (например, обновление сведений о счете, совершение покупок или даже вход в приложение).

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.2.10Противодействие взлому механизмов аутентификации и управления сессией	**5.2.10**Противодействие взлому механизмов аутентификации и управления сессией осуществляется при помощи следующих методик программирования: • сеансовые токены (например, cookies) помечаются как "безопасные"; • отсутствие идентификатора сеанса в URL-адресе; • внедрение соответствующих ограничений по длительности сеанса и ротации идентификаторов после успешного входа.	Безопасная аутентификация и управление сессией не позволят злоумышленнику взломать подлинные учетные данные, ключи или сеансовые токены, с помощью которых можно выдать себя за авторизованного пользователя.
5.3 Поставщик ПО должен выполнять процедуры контроля изменений при всех изменениях приложения. Процедуры контроля изменений должны следовать тем же процессам разработки ПО, что и новые версии (в соответствии в требованием 5.1 стандарта PA-DSS) и включать следующее. ***Согласуется с требованием 6.4.5 стандарта PCI DSS***	**5.3.a** Изучить процедуры контроля изменений ПО, используемые поставщиком, и: • убедиться, что процедуры соответствуют документированным процессам разработки программного обеспечения, определенным в требовании 5.1; • убедиться, что процедуры требуют выполнения приведенных ниже требований 5.3.1 – 5.3.4.	Без надлежащего контроля обновления ПО и обновления безопасности могут не оказать надлежащего воздействия.
	5.3.b Опросить разработчиков, чтобы определить недавние изменения в платежном приложении. Изучить недавние изменения в платежном приложении и отследить связанную с ними документацию по контролю изменений. В отношении каждого изученного изменения необходимо установить документирование следующей информации в соответствии с процедурами контроля изменений.	
5.3.1 Документирование влияния изменений	**5.3.1** Убедиться, что влияние изменений, внесенных клиентом, задокументировано по каждому из изменений.	Последствия изменений должны документироваться, чтобы все вовлеченные стороны могли надлежащим образом запланировать все изменения в обработке данных.
5.3.2 Документированное согласование изменения уполномоченными лицами	**5.3.2** Убедиться, что для каждого изменения присутствует документированное согласование уполномоченными лицами.	Утверждение уполномоченными лицами указывает на то, что изменение является легитимным, утвержденным и санкционированным руководством.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.3.3 Тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы	**5.3.3.a** Для каждого изменения необходимо проверить, что производственная функциональность была протестирована, чтобы убедиться, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы. **5.3.3.b** Убедиться, что все изменения (включая обновления) протестированы в соответствии с требованием 5.2 до передачи приложения клиентам.	Следует выполнять тщательное тестирование для проверки того, что внедрение изменения не оказывает негативного влияния на уровень безопасности платежного приложения. Цель тестирования состоит в подтверждении работоспособности всех существующих механизмов защиты и того, что эти механизмы работают надлежащим образом после внедрения изменений в платежное приложение.
5.3.4 Процедуры отмены изменения или удаления продукта	**5.3.4** Убедиться, что для каждого изменения подготовлены процедуры отмены или удаления продукта.	Для каждого изменения должна существовать процедура отмены, которая позволит вернуть приложение в первоначальное состояние в случае сбоя или неблагоприятного воздействия изменения на приложение.
5.4 Поставщик платежного приложения должен задокументировать и использовать методологию назначения версий ПО в рамках жизненного цикла разработки системы. Методология должна соответствовать процедурам, приведенным в *Руководстве по программе PA-DSS* и касающимся изменений в платежном приложении, и включать как минимум следующее.	**5.4** }Изучить документированные процессы разработки программного обеспечения и убедиться, что они включают методологию назначения версий ПО и что эта методология соответствует требованиям Руководства по программе PA-DSS. Убедиться, что документированная методология назначения версий является обязательной для соблюдения платежным приложением, включая все изменения платежного приложения.	Без четко определенной методологии назначения версий изменения приложения могут остаться незамеченными, и клиенты и интеграторы/реселлеры могут не увидеть воздействие изменения версии на приложение.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.4.1 Методология назначения версий должна давать определение конкретным использованным элементам версии, как описано ниже: • подробная информация о том, как элементы схемы нумерации версий соответствуют требованиям *Руководства по программе PA-DSS*; • формат схемы нумерации версий, включая количество элементов, разделительные знаки, набор символов и т. д. (состоящий и буквенных, цифровых и (или) буквенно-цифровых знаков). *(Продолжение на следующей странице)*	**5.4.1.a** Изучить документированную методологию назначения версий и убедиться, что она включает следующее: • подробную информацию о том, как элементы схемы нумерации версий соответствуют требованиям *Руководства по программе PA-DSS;* • формат схемы нумерации версий, включая количество элементов, разделительные знаки, набор символов и т. д. (например, 1.1.1.N, состоящий и буквенных, цифровых и (или) буквенно-цифровых знаков); • определение того, что каждый элемент обозначает в схеме нумерации версий (например, тип изменения, существенное, незначительное или отладочное изменение версии, подстановочный знак и т. д.); • определение элементов, которые указывают на использование подстановочных знаков.	Методология назначения версий поставщика платежного приложения должна включать в себя четкую схему нумерации версий, которая определяет используемые элементы, формат версии, иерархию различных элементов версий и т.д. для конкретного платежного приложения. Схема нумерации версий должна четко указывать, как каждый из элементов используется в номере версии. *(Продолжение на следующей странице)*
• определение того, что каждый элемент обозначает в схеме нумерации версий (например, тип изменения, существенное, незначительное или отладочное изменение версии, подстановочный знак и т. д.); • определение элементов, которые указывают на использование подстановочных знаков. ***Примечание.*** *Подстановочные знаки могут быть заменены только элементами номера версии, которые обозначают изменения, не затрагивающие вопросы безопасности. В требовании 5.5.3 приведены дополнительные требования в отношении использования подстановочных знаков.*	**5.4.1.b** Убедиться, что элементы схемы нумерации версий соответствуют типам изменений, указанным в Руководстве по программе PA-DSS. **5.4.1.c** Изучить недавние изменения платежного приложения, назначенные номера версий и документацию по контролю изменений, определяющую тип изменения, и убедиться, что элементы номера версии совпадают с соответствующим изменением и параметрами, определенными документированной методологией назначения версий. **5.4.1.d** Опросить несколько разработчиков и убедиться, что они знакомы со схемой нумерации версий, включая допустимое использование подстановочных знаков в номере версии.	Схема версий может быть представлена по-разному, например, как N.NN.NNA, где "N" обозначает цифровой элемент, а "A" – буквенный. Схема нумерации версий должна содержать данные о наборе символов (например, 0-9, A-Z и т. д.), который можно использовать для каждого элемента версии. Без четко обозначенной схемы нумерации версий изменения в приложении могут быть неточно отображены форматом номера версии.
5.4.2 Методология назначения версий должна указывать тип и воздействие изменения приложения в соответствии с	**5.4.2.a** Изучить документированную методологию назначения версий поставщика ПО и убедиться, что данная методология включает:	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
Руководством по программе PA-DSS, в том числе: • описание всех типов и воздействий изменений приложения; • конкретное определение изменений, которые: – не оказывают воздействия на функциональность приложения или его взаимозависимости; – оказывают воздействие на функциональность приложения, но не затрагивают функции, связанные с безопасностью или требованиями PA-DSS; – оказывают воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • связь каждого типа изменений с конкретным номером версии.	• описание всех типов и воздействий изменений приложения (например, изменение не оказывает воздействия, оказывает незначительное или значительное воздействие на приложение); • конкретное определение изменений, которые: – не оказывают воздействия на функциональность приложения или его взаимозависимости; – оказывают воздействие на функциональность приложения, но не затрагивают функции, связанные с безопасностью или требованиями PA-DSS; – оказывают воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • связь каждого типа изменений с конкретным номером версии.	
	5.4.2.b Убедиться, что методология назначения версий соответствует требованиям *Руководства по программе PA-DSS*.	
	5.4.2.c Опросить сотрудников и изучить процессы для каждого типа изменений, чтобы убедиться, что документированная методология соблюдается для всех типов изменений.	
	5.4.2.d Выбрать несколько недавних изменений платежного приложения и изучить документацию по контролю изменений, в которой описаны типы изменений приложения, чтобы убедиться, что назначенная версия соответствует типу изменения согласно документированной методологии.	
5.4.3 Методология назначения версий должна конкретно определять, используются ли подстановочные знаки и методы их применения. Должна присутствовать следующая информация: • подробная информация об использовании подстановочных знаков в	**5.4.3.a** Изучить документированную методологию назначения версий поставщика ПО, чтобы убедиться, что она включает подробную информацию об использовании подстановочных знаков, в том числе: • подробную информацию об использовании подстановочных знаков в методологии назначения версий;	подстановочный знак PA-DSS может использоваться в схеме нумерации версий для обозначения нескольких изменений, не влияющих на функции безопасности; подстановочный знак является единственным переменным элементом

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
методологии назначения версий; • подстановочные знаки никогда не используются для изменений, оказывающих воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • любой элемент номера версии, обозначающий изменение, не влияющее на функции безопасности (включая подстановочные знаки), не должен использоваться для обозначения изменения, влияющего на функции безопасности; • подстановочные знаки не должны стоять перед элементами версии, которые могут обозначать изменения, влияющие на функции безопасности; никакие элементы версии, стоящие после подстановочного знака, не должны использоваться для обозначения изменения, влияющего на функции безопасности. ***Примечание.*** *Подстановочные знаки могут использоваться только в соответствии с Руководством по программе PA-DSS.*	• подстановочные знаки никогда не используются для изменений, оказывающих воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • любой элемент номера версии, обозначающий изменение, не влияющее на функции безопасности (включая подстановочные знаки), не должен использоваться для обозначения изменения, влияющего на функции безопасности; • никакие элементы, стоящие справа от подстановочного знака, не должны использоваться для обозначения изменения, влияющего на функции безопасности; • изменения, влияющие на функции безопасности, требуют изменения другого элемента номера версии, стоящего слева от первого подстановочного знака; **5.4.3.b** Убедиться, что использование подстановочных знаков соответствует требованиям *Руководства по программе PA-DSS*. Например, элементы, стоящие после подстановочного знака, не должны использоваться для обозначения изменения, влияющего на функции безопасности. **5.4.3.c** Опросить сотрудников и изучить процессы для каждого типа изменений, чтобы убедиться, что: • подстановочные знаки никогда не используются для изменений, оказывающих воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • элементы номера версии, обозначающие изменение, не влияющее на функции безопасности (включая подстановочные знаки), не должны использоваться для обозначения изменения, влияющего на функции безопасности.	схемы нумерации версий и используется для обозначения незначительных изменений, не влияющих на функции безопасности, между каждой версией, обозначаемой подстановочным знаком; например, номер версии 1.1.x может обозначать версии 1.1.2, 1.1.3 и т. д., информируя клиента о том, что кодовая база остается неизменной, за исключением поверхностных или других незначительных типов изменений; все случаи использования подстановочных знаков должны быть предопределены методологией назначения версий поставщика, и использование должно соответствовать *Руководству по программе PA-DSS*. ***Примечание.*** *Использование подстановочных знаков является необязательным.*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	5.4.3.d Выбрать несколько недавних изменений платежного приложения и изучить документацию по контролю изменений, в которой описаны типы изменений приложения. Убедиться в том, что: • подстановочные знаки не используются для изменений, оказывающих воздействие на функции, связанные с безопасностью или требованиями PA-DSS; • элементы номера версии, обозначающие изменение, не влияющее на функции безопасности (включая подстановочные знаки), не используются для обозначения изменения, влияющего на функции безопасности.	
5.4.4 Опубликованная методология назначения версий поставщика должна быть передана клиентам и интеграторам/реселлерам.	**5.4.4** Убедиться, что *Руководство по внедрению стандарта PA-DSS* включает описание методологии назначения версий поставщика для клиентов и интеграторов/реселлеров, а также следующее: • информацию о схеме нумерации версий, включая формат схемы нумерации версий (количество элементов, разделительные знаки, набор символов и т. д.); • информацию об обозначении изменений, влияющих на функции безопасности, на схеме версий; • информацию о том, как другие типы изменений отражаются на версии; • информацию об используемых подстановочных знаках, включая подтверждение того, что они никогда не будут использованы для обозначения изменения, влияющего на функции безопасности.	Включение методологии назначения версий поставщика в *Руководство по внедрению стандарта PA-DSS* предоставит клиентам и интеграторам/реселлерам информацию, необходимую для понимания того, какую версию платежного приложения они используют, а также типов изменений, внесенных в каждую версию платежного приложения.
5.4.5 Если используется сопоставление внутренних версий с опубликованной схемой нумерации версий, методология назначения версий должна включать сопоставление	**5.4.5.a** Изучить документированную методологию назначения версий, чтобы убедиться, что она включает сопоставление внутренних версий с выпущенными общедоступными версиями.	Некоторые поставщики платежных приложений применяют методологии назначения версий для внутреннего пользования или справки, которые

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
внутренних версий с общедоступными.	**5.4.5.b** Изучить недавние изменения, чтобы подтвердить, что внутренняя методология назначения версий согласуется с общедоступной схемой по типу изменения.	отличаются от методологии, используемой для общедоступных версий. В таких случаях важно, чтобы обе методологии назначения версий были четко определены и документированы, равно как и их взаимосвязь.
5.4.6 У поставщика ПО должен действовать процесс проверки обновлений приложения на соответствие методологии назначения версий до выпуска приложения.	**5.4.6.a** Изучить документированные процессы разработки программного обеспечения и методологию назначения версий, чтобы убедиться в том, что существует процесс проверки обновлений приложения на соответствие методологии назначения версий перед выпуском приложения.	Крайне важно, чтобы у поставщиков платежного приложения действовал процесс обеспечения соответствия обновления ПО области применения и назначению запланированной версии, а также процесс информирования клиентов о таких изменениях. В противном случае в приложение могут быть внесены изменения, оказывающие негативное воздействие на безопасность приложения клиента без его ведома.
	5.4.6.b Опросите разработчиков ПО и проследите за процессами, чтобы убедиться, что обновления приложения проверяются на соответствие методологии назначения версий перед выпуском приложения.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.5 Методики оценки рисков (например, моделирование угроз для приложения) используются для выявления потенциальных конструктивных ошибок и уязвимостей в системе безопасности приложения в процессе разработки приложения. Процедуры оценки рисков могут включать следующее: • охват всех функций платежного приложения, включая, помимо прочего, функции, влияющие на безопасность приложения, и функции, нарушающие границы доверия; • оценку точек решения, последовательности процессов, потоков данных, хранения данных и границ доверия; • определение всех областей приложения, взаимодействующих с основным номером держателя карты и (или) критичными аутентификационными данными или информационной средой держателей карт (CDE), а также любыми процессно-ориентированными результатами, которые могут привести к раскрытию данных держателей карт. • список потенциальных угроз и уязвимостей, составленный по результатам анализов потоков данных держателей карт, с назначенными категориями риска (например, высокий, средний или низкий приоритет); • внесение соответствующих исправлений и защитных мер в процессе разработки; • документация результатов оценки рисков для изучения и утверждения руководством.	**5.5** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться в том, что поставщик использует методики оценки риска в рамках процесса разработки ПО, в том числе: • охват всех функций платежного приложения, включая, помимо прочего, функции, влияющие на безопасность приложения, и функции, нарушающие границы доверия; • оценку точек решения, последовательности процессов, потоков данных, хранения данных и границ доверия; • определение всех областей приложения, взаимодействующих с основным номером держателя карты / критичными аутентификационными данными или информационной средой держателей карт (CDE), а также любыми процессно-ориентированными результатами, которые могут привести к раскрытию данных держателей карт; • список потенциальных угроз и уязвимостей, составленный по результатам анализов потоков данных держателей карт, с назначенными категориями риска (например, высокий, средний или низкий приоритет); • внесение соответствующих исправлений и защитных мер в процессе разработки; • документация результатов оценки рисков для изучения и утверждения руководством.	В целях поддержания качества и безопасности платежных приложений поставщики приложений должны использовать методики оценки рисков в процессе разработки ПО. Моделирование угроз является методом оценки рисков, который можно использовать для анализа структур и потоков данных приложения на наличие возможностей раскрытия конфиденциальной информации неавторизованным пользователям. Данные процессы позволяют разработчикам ПО выявлять и устранять потенциальные проблемы с безопасностью на ранних стадиях разработки, повышать безопасность приложения и минимизировать затраты на разработку.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
5.6 Поставщик ПО должен внедрить процесс документирования и авторизации финальной версии приложения и его обновлений. Документация должна включать: • подпись уполномоченной стороны, официально утверждающую выпуск приложения или его обновления; • подтверждение того, что поставщик использовал процессы безопасной разработки.	**5.6.a** Изучить документированные процессы, чтобы убедиться в том, что финальная версия приложения и его обновления должны быть официально утверждены и задокументированы, включая подпись уполномоченной стороны, официально утверждающую выпуск приложения, и подтверждение того, что использовались процессы жизненного цикла разработки ПО.	В организации поставщика платежного приложения необходимо назначить лицо, ответственное за проверку и полное выполнение процессов безопасной разработки (в соответствии с требованиями 5.1 – 5.5). Без официальной проверки и подтверждения ответственной стороны важные процессы обеспечения безопасности могут быть пропущены или исключены, что приведет к выпуску некачественного или недостаточно безопасного приложения.
	5.6.b Изучить утвердительную документацию нескольких недавно вышедших приложений и обновлений и убедиться, что она содержит: • официальное утверждение и подпись ответственной стороны; • подтверждение того, что были использованы процессы безопасной разработки.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 6. Защита беспроводной передачи данных

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
6.1 В платежных приложениях, использующих беспроводные технологии, необходимо изменить параметры беспроводной связи по умолчанию, установленные поставщиком, включая, помимо прочего, ключи шифрования, пароли, строки доступа протокола SNMP. Беспроводные технологии должны использоваться безопасным образом. ***Согласуется с требованиями 1.2.3 и 2.1.1 стандарта PCI DSS***	**6.1** Если платежные приложения разрабатывались для использования с беспроводными технологиями или поставляются в комплекте с приложениями для беспроводной связи, необходимо убедиться, что ни одно из приложений для беспроводной связи не использует параметры по умолчанию, установленные поставщиком. **6.1.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • платежное приложение при установке должно требовать изменения ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию для всех беспроводных компонентов, управляемых приложением; • процедуры изменения ключей шифрования и паролей, включая строки доступа протокола SNMP, в случае увольнения из компании любого сотрудника, имеющего доступ к ключам/паролям; • инструкции по изменению ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию на любом беспроводном компоненте, предоставленном, но не контролируемом платежным приложением; • инструкции по установке брандмауэра между беспроводными сетями и системами, в которых хранятся данные держателей карт; • подробные данные о беспроводном трафике (включая информацию о конкретных портах), который будет использовать функция беспроводной связи платежного приложения; • инструкции по настройке брандмауэра для запрета или – если такой трафик необходим в целях совершения операций – разрешения только авторизованного трафика между беспроводной средой и средой данных держателей карт.	Злоумышленники часто используют уязвимости беспроводных технологий для получения доступа к сети и данным держателей карт. Если беспроводные сети недостаточно защищены (например, если настройки безопасности, заданные по умолчанию, не изменяются), существует возможность прослушивания трафика анализаторами беспроводных пакетов, извлечения паролей и данных и проникновения в сеть. По этим причинам платежные приложения не должны требовать использования параметров беспроводной связи по умолчанию либо небезопасных параметров. Если брандмауэры не запрещают доступ к среде данных держателей карт из беспроводной сети, злоумышленники, которые имеют несанкционированный доступ к беспроводной сети, могут без труда подключиться к среде данных держателей карт и получить доступ к банковским данным.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	6.1.b Установить приложение в соответствии с *Руководством по внедрению стандарта PA-DSS* и протестировать приложение и настройки беспроводной связи, чтобы убедиться в выполнении следующих требований всеми функциями беспроводной связи, управляемыми платежным приложением: • заданные по умолчанию ключи шифрования были изменены при установке; • заданные по умолчанию строки доступа протокола SNMP были изменены при установке; • заданные по умолчанию пароли/кодовые фразы точек доступа были изменены при установке; • микропрограммы беспроводных устройств обновлены до актуальной версии с поддержкой стойкого шифрования для аутентификации и передачи данных через беспроводные сети; • прочие настройки безопасности беспроводных устройств, установленные производителем по умолчанию, были изменены (если применимо).	
	6.1.c В отношении всех функций беспроводной связи, управляемых платежным приложением, необходимо выполнить инструкции из *Руководства по внедрению стандарта PA-DSS*, касающиеся изменения ключей шифрования, паролей/кодовых фраз и строк доступа протокола SNMP. Убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* являются точными и способствуют изменению ключей шифрования, паролей и строк доступа протокола SNMP.	
	6.1.d В отношении всех беспроводных компонентов, предоставляемых, но не управляемых платежным приложением, необходимо выполнить инструкции из *Руководства по внедрению стандарта PA-DSS*, касающиеся изменения ключей шифрования, паролей/кодовых фраз и строк доступа протокола SNMP. Убедиться, что инструкции из *Руководства по внедрению стандарта PA-DSS* являются точными и способствуют изменению ключей шифрования, паролей и строк доступа протокола SNMP.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	6.1.e Установить приложение и протестировать функции беспроводной связи, чтобы убедиться, что беспроводной трафик и порты, используемые приложением, соответствуют указанным в *Руководстве по внедрению стандарта PA-DSS*.	
6.2 Платежные приложения, использующие беспроводные технологии, должны применять используемые в отрасли передовые методы (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных. ***Примечание.*** *Использование протокола WEP в качестве протокола защиты запрещено.* ***Согласуется с требованием 4.1.1 стандарта PCI DSS***	**6.2.a** В платежных приложениях, разработанных для использования с беспроводными технологиями, необходимо протестировать все функции беспроводной связи, чтобы убедиться, что приложение применяет используемые в отрасли передовые методы (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных.	Злоумышленники используют свободно распространяемые и широкодоступные средства для прослушивания беспроводного трафика. Использование стойкого шифрования может предотвратить раскрытие критичной информации, передаваемой по беспроводной сети. Стойкое шифрование для аутентификации и передачи данных держателей карт помогает предотвратить доступ злоумышленников к беспроводным сетям или использование беспроводных сетей для получения доступа к другим системам и данным.
	6.2.b В приложениях для беспроводной связи, поставляемых в комплекте с платежным приложением, необходимо протестировать все функции беспроводной связи, чтобы убедиться, что применяются используемые в отрасли передовые методы (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных.	
	6.2.c Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • инструкции по настройке приложения таким образом, чтобы оно применяло передовые отраслевые методы (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных, и (или) • инструкции по настройке приложений для беспроводной связи, поставляемых в комплекте с платежным приложением, таким образом, чтобы применялись передовые отраслевые методы по обеспечению стойкого шифрования при аутентификации и передаче данных.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
6.3 Предоставить клиентам инструкции по безопасному использованию беспроводных технологий. ***Примечание.*** *Данное требование распространяется на все платежные приложения, независимо от того, разрабатываются ли они для использования с беспроводными технологиями.* ***Согласуется с требованиями 1.2.3, 2.1.1 и 4.1.1 стандарта PCI DSS***	**6.3** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что клиенты и интеграторы/реселлеры осведомлены о настройке беспроводной связи в соответствии с требованиями стандарта PCI DSS, включая изменение настроек, установленных поставщиком по умолчанию, и применение используемых в отрасли передовых методов по обеспечению стойкого шифрования при аутентификации и передаче данных держателей карт, как описано ниже: • инструкции по изменению при установке всех ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию; • инструкции по изменению ключей шифрования, паролей и строк доступа протокола SNMP в случае увольнения из компании любого сотрудника, имеющего доступ к ключам/паролям; • инструкции по установке брандмауэра между беспроводными сетями и системами, в которых хранятся данные держателей карт, и настройке брандмауэра для запрета или – если такой трафик необходим для выполнения операций – разрешения только авторизованного трафика между беспроводной средой и средой данных держателей карт; • инструкции по применению передовых практических методов индустрии безопасности (например, IEEE 802.11i) для обеспечения стойкого шифрования при аутентификации и передаче данных.	Поставщики платежного приложения должны предоставить клиентам инструкции по настройке приложения для работы с беспроводными технологиями, даже если приложение непосредственно не предназначено для использования в беспроводной среде. Беспроводные сети широко распространены, и клиенты должны быть осведомлены о стандартных настройках безопасности, которые необходимо произвести для обеспечения безопасности платежного приложения.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 7. Необходимо тестировать платежные приложения с целью устранения уязвимостей и регулярного обновления приложений

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
7.1 Поставщики ПО должны установить процесс выявления и устранения уязвимостей, как описано ниже. ***Примечание.*** *В данный процесс должны быть включены все системы и ПО, требуемые приложением либо поставляемые вместе с ним (например, веб-серверы, сторонние библиотеки и программы).* ***Согласуется с требованием 6.1 стандарта PCI DSS***	**7.1.a** Изучить документацию по процессам устранения уязвимостей и подтвердить наличие процедур для: • выявления новых уязвимостей в системе безопасности с использованием для этого надежных источников информации; • присвоения уровня риска выявленным уязвимостям; • тестирования платежных приложений и их обновлений на наличие уязвимостей перед выпуском. **7.1.b** Убедиться в том, что процессы выявления новых уязвимостей и внесения исправлений в платежное приложение распространяются на все ПО, требуемое платежным приложением или поставляемое вместе с ним (например, веб-серверы, сторонние библиотеки или программы).	Поставщики должны быть в курсе новых уязвимостей, которые могут оказать воздействие на их приложения, включая уязвимости компонентов, лежащих в основе приложения, или ПО, требуемого для работы приложения или поставляемого вместе с ним. Поставщики, знающие об уязвимостях своих платежных приложений или лежащих в их основе компонентов, должны устранить эти уязвимости перед выпуском либо внедрить иной механизм для снижения вероятности того, что уязвимость может быть использована злоумышленником в случае, если обновление безопасности не будет доступно немедленно.
7.1.1 Выявить новые уязвимости в системе безопасности с использованием надежных источников информации.	**7.1.1** Опросить ответственных сотрудников и изучить процессы, чтобы убедиться, что новые уязвимости в системе безопасности обнаружены: • в платежном приложении и лежащих в его основе системах или ПО, требуемых платежным приложением или поставляемых вместе с ним; • с использованием надежных источников информации (таких как веб-сайты поставщика ПО/систем, Национальная база данных уязвимостей Национального института стандартов и технологий (NIST NVD), список уязвимостей и угроз компании MITRE (MITRE CVE) и веб-сайты US-CERT Министерства национальной безопасности США).	Надежные источники следует использовать для получения информации об уязвимостях и (или) обновлениях сторонних программных компонентов. Источники информации об уязвимостях должны быть достоверными (например, веб-сайты поставщиков, отраслевые новостные группы, почтовые рассылки или RSS-потоки). Примерами отраслевых источников информации могут служить Национальная база данных уязвимостей Национального института стандартов и технологий (NIST NVD), список уязвимостей и угроз компании MITRE (MITRE CVE) и веб-сайты US-CERT Министерства национальной безопасности США.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
7.1.2 Назначить уровень риска всем выявленным уязвимостям, включая затрагивающие лежащие в основе приложения системы или ПО, требуемые для работы платежного приложения или поставляемые вместе с ним. ***Примечание.*** *Ранжирование рисков должно быть основано на общепринятых отраслевых рекомендациях с учетом потенциального воздействия. Например, критерии уровня риска могут основываться на уровне риска по шкале CVSS, и (или) классификации поставщика, и (или) воздействию на функциональность приложения.* *Уровень риска должен быть присвоен как минимум всем уязвимостям с высоким уровнем риска для приложения. Уязвимости считаются критическими, если они представляют неотвратимую угрозу, влияют на работу важнейших компонентов приложения или могут привести к компрометации, если не будут устранены.*	**7.1.2** Опросить ответственных сотрудников или изучить процессы, чтобы убедиться, что уровень риска назначен всем выявленным уязвимостям, включая затрагивающие лежащие в основе приложения системы или ПО, требуемые для работы платежного приложения или поставляемые вместе с ним.	Как только поставщик выявляет уязвимость, которая может оказать негативное влияние на его приложение, необходимо оценить и ранжировать риск, которые представляет эта уязвимость. Для этого необходим процесс, позволяющий активно следить за отраслевыми источниками информации на предмет появления сведений об уязвимостях. Оценка уровня риска (например, по шкале "высокий", "средний" или "низкий") позволяет поставщикам быстрее выявлять и устранять проблемы с высоким приоритетом (например, срочным выпуском важных обновлений) и минимизировать вероятность использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для среды клиентов.
7.1.3 Протестировать платежные приложения и их обновления на наличие уязвимостей перед выпуском	**7.1.3** Опросить ответственных сотрудников или изучить процессы, чтобы убедиться, что платежные приложения тестируются на наличие уязвимостей перед выпуском.	Поставщик должен включить в процесс управления уязвимостями платежного приложения надлежащее тестирование, чтобы гарантировать, что все выявленные уязвимости будут устранены перед выпуском. *В качестве примеров методов тестирования можно привести тест на проникновение и (или) методики фаззинга для выявления потенциальных уязвимостей, например путем внедрения искаженных или неожидаемых данных или изменения битного размера данных.*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
7.2 Поставщики ПО должны организовать процесс своевременной разработки и развертывания обновлений безопасности.	**7.2** Изучить документацию по процессам разработки и распространения обновлений безопасности, чтобы убедиться, что процесс включает процедуры, соответствующие требованиям 7.2.1 – 7.2.2:	Обновления ПО, призванные устранить уязвимости в системе безопасности должны разрабатываться и передаваться клиентам в кратчайшие сроки после обнаружения критической уязвимости, чтобы свести к минимуму вероятность использования уязвимости злоумышленниками.
7.2.1 Обновления ПО и исправления безопасности должны доставляться клиентам безопасным образом с известной цепочкой сертификатов.	**7.2.1** Опросить ответственных сотрудников и изучить процессы, чтобы убедиться, что обновления ПО и исправления безопасности доставляются клиентам безопасным образом с известной цепочкой сертификатов.	Исправления для системы безопасности должны распространяться таким образом, при котором злоумышленники не могли бы перехватить обновления в момент передачи, изменить их и повторно отправить ничего не подозревающим клиентам.
7.2.2 Обновления ПО и исправления для системы безопасности должны доставляться клиентам таким образом, при котором обеспечивается целостность кода обновлений.	**7.2.2.a** Опросить ответственных сотрудников и изучить процессы, чтобы убедиться, что обновления ПО и исправления системы безопасности доставляются клиентам таким образом, при котором обеспечивается целостность кода обновлений.	Процесс установки обновлений безопасности должен содержать механизм проверки кода на изменения (т. е. на отсутствие несанкционированных замен или вмешательств). Проверки целостности включают, помимо прочего, использование контрольных сумм, сертификаты с цифровой подписью и т. д.
	7.2.2.b Опросить ответственных сотрудников и изучить процессы обновления приложений, чтобы убедиться, что обновления ПО и исправления безопасности тестируются на целостность на целевой системе перед установкой.	
	7.2.2.c Убедиться в том, что целостность кода обновлений и исправлений поддерживается, запустив процесс обновления с произвольным кодом и подтвердив, что система не допускает обновления.	
7.3 Предоставить сведения о выпуске каждого обновления приложения, включая подробную информацию о воздействии обновления и изменении номера версии для обозначения обновления.	**7.3.a** Изучить процессы выпуска обновлений и опросить сотрудников, чтобы убедиться, что для всех обновлений подготовлены сведения о выпуске, включая подробную информацию о воздействии обновления и изменении номера версии для обозначения обновления.	Сведения о выпуске предоставляют клиентам подробную информацию об обновлениях ПО, включая список измененных файлов или функций приложения, а также функций

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
	7.3.b Изучить сведения о выпуске нескольких обновлений и убедиться, что они прилагались к обновлению.	обеспечения безопасности, которые могли быть затронуты. Сведения о выпуске также должны указывать, как конкретное обновление влияет на общий номер версии, связанный с выпуском обновления.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 8. Необходимо обеспечить возможность внедрения в безопасные сетевые среды

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
8.1 Платежное приложение должно иметь возможность внедрения в безопасную сетевую среду. Приложение не должно препятствовать использованию устройств, приложений или конфигураций, необходимых для соответствия требованиям стандарта PCI DSS. *Например, платежное приложение не должно препятствовать установке обновлений, защите от вредоносного ПО, конфигурации брандмауэра или любым другим устройствам, приложениям или конфигурациям, необходимым для соответствия требованиям стандарта PCI DSS.* ***Согласуется с требованиями 1, 3, 4, 5 и 6 стандарта PCI DSS***	**8.1.a** Установить приложение в лабораторных условиях, соответствующих требованиям PCI DSS, согласно *Руководству по внедрению стандарта PA-DSS.* Протестировать платежное приложение, чтобы убедиться, что оно может работать в сети, полностью соответствующей требованиям стандарта PCI DSS. **8.1.b** Протестировать приложение и лежащие в его основе системы, чтобы убедиться, что платежное приложение не препятствует работе и использованию функций PCI DSS на лежащих в его основе системах, например приложение не мешает установке обновлений программ защиты от вредоносного ПО или работе других функций PCI DSS.	Платежное приложение должно быть спроектировано и разработано таким образом, чтобы его установка и работа не препятствовали внедрению в организации других механизмов контроля, необходимых для соответствия требованиям стандарта PCI DSS. Например, платежное приложение должно быть способно работать в среде с антивирусными программами (то есть не должно требовать выключения или удаления таких программ).
8.2 Платежное приложение должно использовать или требовать использования в целях своего функционирования только необходимых и безопасных устройств, протоколов, управляющих программ, компонентов и зависимого программного обеспечения и оборудования, включая предоставленные третьими сторонами. *Например, если приложению требуется NetBIOS, совместный доступ к файлам, Telnet, FTP и т. д., то они должны быть защищены при помощи SSH, S-FTP, SSL, IPSec или других технологий.* ***Согласуется с требованием 2.2.2***	**8.2.a** Изучить системные службы, протоколы, управляющие программы, компоненты и зависимое программное обеспечение и оборудование, задействованные платежным приложением или требуемые для его работы. Подтвердить, что только необходимые и безопасные системные службы, протоколы, управляющие программы, компоненты и зависимое программное обеспечение и оборудование включены по умолчанию. **8.2.b** Установить приложение и протестировать его функции, чтобы убедиться, что если приложение поддерживает использование небезопасных протоколов, служб, управляющих программ или компонентов, то они имеют безопасную конфигурацию по умолчанию.	Существует много протоколов, которые необходимы для выполнения операций (или они включены по умолчанию) и которые часто используются злоумышленниками для компрометации системы или сети. Платежное приложение не должно требовать использования небезопасных протоколов, служб, управляющих программ и т. д. Если приложение поддерживает использование небезопасных протоколов, служб, управляющих программ или компонентов, они должны быть

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
стандарта PCI DSS	**8.2.c** Убедиться, что в *Руководстве по внедрению стандарта PA-DSS* задокументированы все необходимые протоколы, службы, компоненты и зависимое программное обеспечение и оборудование, требуемые для выполнения функций платежного приложения, включая предоставленные третьими сторонами.	защищены по умолчанию.
8.3 Платежное приложение не должно требовать использования любых служб или протоколов, препятствующих использованию или нормальному функционированию технологий двухфакторной аутентификации для обеспечения безопасного удаленного доступа (доступ на сетевом уровне производится из внешней сети) к сетевых ресурсам, расположенным в среде данных держателей карт. ***Примечание.*** *Двухфакторная*	**8.3.a** Изучить функциональность платежного приложения, чтобы убедиться, что она не требует использования каких-либо служб или протоколов, препятствующих использованию или нормальному функционированию технологий двухфакторной аутентификации для обеспечения удаленного доступа.	Платежные приложения должны проектироваться и разрабатываться таким образом, чтобы при установке и работе приложение не требовало от организации использования служб или протоколов, которые помешают организации внедрить и использовать решения по двухфакторной аутентификации для обеспечения удаленного доступа. К примеру, приложение не должно по умолчанию

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
аутентификация требует использования двух из трех методов аутентификации (см. ниже). Использование одного метода дважды (например, использование двух различных паролей) не считается двухфакторной аутентификацией. Методы аутентификации, или факторы, включают следующее: • то, что вы знаете (например, пароль или парольная фраза); • то, что у вас есть (например, ключи или смарт-карты); • то, что вы есть (например, биометрические параметры). *К примерам технологий двухфакторной аутентификации относятся такие технологии, как RADIUS с токенами, TACACS с токенами и другие технологии, способствующие двухфакторной аутентификации.* ***Согласуется с требованием 8.3 стандарта PCI DSS***	**8.3.b** Определить механизмы удаленного доступа, поддерживаемые приложением, и убедиться, что они не препятствуют двухфакторной аутентификации.	использовать порт 1812 (который, как известно, назначается RADIUS согласно RFC 2865), если RADIUS рассматривается в качестве поддерживаемой технологии аутентификации и авторизации.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 9. Данные держателей карт ни в коем случае не должны храниться на сервере, подключенном к Интернету

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
9.1 Платежное приложение должно быть разработано таким образом, чтобы любой веб-сервер и любой компонент системы хранения данных держателей карт (например, сервер базы данных) не были должны находиться на одном сервере, и компонент системы хранения данных не был должен находиться в одной зоне сети (такой как демилитаризованная зона (DMZ)) с веб-сервером. ***Согласуется с требованием 1.3.7 стандарта PCI DSS***	**9.1.a** Определить все компоненты системы хранения данных платежного приложения (например, базы данных) и все веб-серверы. Установить компоненты системы хранения данных и веб-серверы на различных серверах и протестировать функциональность приложения. Убедиться, что платежное приложение не требует для функционирования установки какого-либо компонента системы хранения данных (например, базы данных) на том же сервере, где установлен веб-сервер.	Любой компонент веб-сервера платежного приложения подвержен значительному риску компрометации вследствие открытой структуры общедоступных сетей (Интернет, общественная беспроводная сеть и т. д.), а также природы и количества атак, которые могут поступить из таких сетей. Компоненты системы хранения данных держателей карт требуют более высокого уровня защиты, чем общедоступные компоненты приложения. Если данные расположены в демилитаризованной зоне (DMZ), задача получения доступа к этой информации для злоумышленника упрощается, поскольку ему нужно будет
	9.1.b Установить компоненты системы хранения данных и веб-серверы в разные зоны сети. Протестировать все функции приложения в различных зонах сети, чтобы убедиться в том, что платежное приложение не требует для функционирования установки какого-либо компонента системы хранения данных (например, базы данных) в той же зоне сети, где установлен веб-сервер.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

	9.1.c Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • указания не хранить данные держателей карт в общедоступных системах (например, веб-сервер и сервер базы данных не должны находиться на одном сервере); • инструкции по настройке платежного приложения для использования демилитаризованной зоны (DMZ) с целью разграничения Интернета и систем, в которых хранятся данные держателей карт (например, можно установить веб-сервер в DMZ, а компонент системы хранения данных в другой внутренней зоне сети); • список служб/портов, которые приложение должно использовать для передачи данных между двумя зонами сети (чтобы торговая точка могла открыть в брандмауэре только необходимые порты).	преодолеть меньшее количество уровней защиты. По этой же причине никогда не следует держать веб-серверы на том же сервере, где расположен компонент системы хранения данных. Если злоумышленнику удастся получить доступ к учетной записи на веб-сервере, в его распоряжении без дополнительных усилий также окажется база данных держателей карт.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 10. Необходимо обеспечить безопасный удаленный доступ к платежному приложению

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
10.1 При осуществлении удаленного доступа к платежному приложению из-за пределов среды клиента всегда должна использоваться двухфакторная аутентификация. ***Примечание.*** *Для двухфакторной аутентификации требуется применение двух из трех методов аутентификации (описание методов аутентификации см. в требовании 3.1.4 стандарта PA-DSS).* ***Согласуется с требованием 8.3 стандарта PCI DSS***	**10.1.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя следующие инструкции для клиентов и интеграторов/реселлеров: • сведения о том, что для соответствия требованиям стандарта PCI DSS при удаленном доступе к платежному приложению из сети, внешней по отношению к сети клиента, всегда должна использоваться двухфакторная аутентификация. • Описание механизмов двухфакторной аутентификации, поддерживаемых приложением. • Инструкции по настройке поддержки двухфакторной аутентификации в приложении (два из трех методов аутентификации, описанных в требовании 3.1.4 стандарта PA-DSS).	Двухфакторная аутентификация требует два метода аутентификации для доступа с более высоким уровнем риска, например доступа, инициируемого из внешней сети. Поставщики платежных приложений должны предоставить клиентам инструкции по настройке поддержки указанных механизмов двухфакторной аутентификации в приложении с целью надлежащего внедрения таких механизмов и выполнения соответствующих требований стандарта PCI DSS. Данное требование в отношении двухфакторной аутентификации применяется лишь в том случае, когда удаленный доступ осуществляется из сети, являющейся внешней для среды клиента.
	10.1.b Если поставщик приложения может осуществлять удаленный доступ к платежному приложению клиента вне пределов среды клиента, необходимо изучить политику поставщика, чтобы убедиться, что он соблюдает требования клиента в отношении двухфакторной аутентификации при таком доступе.	
10.2 Удаленный доступ к платежному приложению должен осуществляться безопасным образом, как описано ниже.	**10.2** Убедиться, что удаленный доступ осуществляется, как описано ниже:	все механизмы удаленного доступа, используемые поставщиком платежного приложения и (или)

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
10.2.1 Если обновления платежного приложения доставляются посредством удаленного доступа к системам клиента, поставщики ПО должны проинформировать клиентов о включении возможностей удаленного доступа только на время загрузки обновления и немедленном их выключении после завершения загрузки. В случае доставки через виртуальную частную сеть (VPN) или посредством другого высокоскоростного соединения поставщики ПО должны рекомендовать клиентам должным образом настроить брандмауэр (общий либо персональный), чтобы обеспечить защиту постоянного подключения. ***Согласуется с требованиями 1 и 12.3.9 стандарта PCI DSS***	**10.2.1.a** Если обновления платежного приложения доставляются посредством удаленного доступа к системам клиента, необходимо изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно содержит: • инструкции для клиентов и интеграторов/реселлеров в отношении безопасного использования технологий удаленного доступа с указанием того, что возможности удаленного доступа, используемые поставщиками и деловыми партнерами, должны включаться только на время загрузки обновления и немедленно выключаться после завершения загрузки; • рекомендации для клиентов и интеграторов/реселлеров по использованию должным образом настроенного брандмауэра (общего либо персонального), если компьютер использует виртуальную частную сеть (VPN) или другое высокоскоростное соединение, для защиты постоянного подключения в соответствии в требованием 1 стандарта PCI DSS.	интеграторами/реселлерами (к примеру, для техподдержки услуг, оказываемых поставщиками), должны соответствовать применимым требованиям стандарта PCI DSS.
	10.2.1.b Если поставщик доставляет платежное приложение и (или) обновления посредством удаленного доступа к сетям клиента, необходимо изучить методы доставки и убедиться, что они включают в себя следующее: • включение возможностей удаленного доступа к сетям клиента только при необходимости и немедленное выключение после использования; • если удаленный доступ осуществляется посредством виртуальной частной сети или другого высокоскоростного соединения, подключение должно быть защищено в соответствии с требованием 1 стандарта PCI DSS.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
10.2.2 Если поставщики или интеграторы/реселлеры могут получить доступ к платежным приложениям клиентов удаленно, необходимо использовать уникальные учетные данные (такие как пароль/кодовая фраза) для каждой среды клиента. ***Согласуется с требованием 8.5.1 стандарта PCI DSS***	**10.2.2** Если поставщики или интеграторы/реселлеры могут получить доступ к платежным приложениям клиентов удаленно, необходимо изучить процессы поставщика и опросить сотрудников, чтобы убедиться в том, что для каждой среды клиента, к которой они имеют доступ, используется уникальный пароль.	Чтобы предотвратить взлом сред нескольких клиентов при помощи единых учетных данных, поставщики, осуществляющие удаленный доступ к средам клиентов должны использовать разные аутентификационные учетные данные для каждого клиента. При создании пароля следует избегать повторяющихся легкоугадываемых шаблонов. Такие учетные данные со временем становятся общедоступными и могут быть использованы неавторизованными лицами для компрометации клиентов поставщика.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
10.2.3 Удаленный доступ к платежным приложениям клиентов со стороны поставщиков, интеграторов/реселлеров или клиентов должен осуществляться безопасным образом. Для этого следует: • изменить настройки по умолчанию в ПО для удаленного доступа (например, изменить пароли по умолчанию и использовать уникальные пароли для каждого клиента); • разрешать подключения только с конкретных (известных) IP- и (или) MAC-адресов; • использовать надежную аутентификацию и сложные пароли для входа (см. требования 3.1.1 – 3.1.11 стандарта PA-DSS); • обеспечить зашифрованную передачу данных в соответствии с требованием 12.1 стандарта PA-DSS; • настроить блокировку учетной записи после определенного количества неудачных попыток входа (см. требования 3.1.9 – 3.1.10 стандарта PA-DSS); • установить VPN-соединения через брандмауэр перед разрешением доступа; • активировать функцию регистрации событий; • разрешить доступ к средам клиентов только авторизованным интеграторам/реселлерам. ***Согласуется с требованиями 2, 8 и 10 стандарта PCI DSS***	**10.2.3.a** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что клиенты и интеграторы/реселлеры проинформированы о том, что удаленный доступ к платежному приложению должен осуществляться безопасным образом, для чего следует: • изменить настройки по умолчанию в ПО для удаленного доступа (например, изменить пароли по умолчанию и использовать уникальные пароли для каждого клиента); • разрешать подключения только с конкретных (известных) IP- и (или) MAC-адресов; • использовать надежную аутентификацию и сложные пароли для входа (см. требования 3.1.1 – 3.1.11 стандарта PA-DSS); • обеспечить зашифрованную передачу данных в соответствии с требованием 12.1 стандарта PA-DSS; • настроить блокировку учетной записи после определенного количества неудачных попыток входа (см. требование 3.1.8 стандарта PA-DSS); • установить VPN-соединения через брандмауэр перед разрешением доступа; • активировать функцию регистрации событий; • разрешить доступ к средам клиентов только авторизованным сотрудникам. **10.2.3.b** Если поставщик приложения может получить доступ к платежным приложениям клиентов удаленно, необходимо изучить процессы поставщика и опросить сотрудников, чтобы убедиться в том, что удаленный доступ осуществляется безопасным образом.	Поставщики платежных приложений должны предоставить клиентам и интеграторам/реселлерам инструкции по настройке поддержки безопасного удаленного доступа в приложении с целью надлежащего внедрения таких механизмов и выполнения соответствующих требований стандарта PCI DSS. Данное требование распространяется на все типы удаленного доступа к среде клиента.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 11. Необходимо шифровать конфиденциальный трафик в общедоступных сетях

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
11.1 Если платежное приложение отправляет или обеспечивает отправку данных держателей карт через общедоступные сети, оно должно поддерживать использование стойких методов шифрования и протоколов безопасности (например, SSL/TLSIPSEC, SSH и т. д.) для защиты конфиденциальных данных держателей карт, передаваемых через общедоступные сети, включая следующее: • прием только доверенных ключей и сертификатов; • используемый протокол должен поддерживать только безопасные версии и конфигурации; • стойкость шифрования должна соответствовать используемой методологии шифрования. *Примеры общедоступных сетей включают, помимо прочего:* • Интернет; • беспроводные технологии, включая, помимо прочего, стандарты 802.11 и Bluetooth; • технологии сотовой связи, например, GSM, CDMA;	**11.1.a** Если платежное приложение отправляет или обеспечивает отправку данных держателей карт через общедоступные сети, необходимо убедиться, что приложение обеспечивает стойкое шифрование и протоколы безопасности или определяет методы их использования.	Критичные данные должны шифроваться при передаче по общедоступным сетям, потому что злоумышленник может перехватить и (или) изменить их маршрут при передаче.
	11.1.b Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по использованию стойкого шифрования и протоколов безопасности, предоставляемых или указанных приложением, в том числе: • инструкции, указывающие, что стойкое шифрование и протоколы безопасности должны использоваться в случае передачи данных держателей карт через общедоступные сети; • инструкции по проверке приема только доверенных ключей и (или) сертификатов; • инструкции по настройке платежного приложения таким образом, чтобы использовались только безопасные версии, и по внедрению протоколов безопасности; • инструкции по настройке платежного приложения таким образом, чтобы применялось шифрование достаточной стойкости для используемой методологии.	Безопасная передача данных держателей карт требует использования доверенных ключей/сертификатов, безопасного протокола передачи и шифрования достаточной стойкости для шифрования данных держателей карт. Обратите внимание на то, что некоторые версии протоколов (например, SSL 2.0, SSH 1.0 и TLS 1.0) содержат документированные уязвимости, такие как переполнение буфера, которые могут быть использованы злоумышленником для получения контроля над системой. Независимо от того, какой протокол используется платежным приложением, следует убедиться, что он настроен для использования только безопасных конфигураций и версий, для предотвращения установки

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
• GPRS; • спутниковые средства связи. ***Согласуется с требованием 4.1 стандарта PCI DSS***	**11.1.c** Если платежное приложение обеспечивает стойкое шифрование и протоколы безопасности, необходимо установить и протестировать приложение в соответствии с инструкциями из *Руководства по внедрению стандарта PA-DSS* и убедиться, что: • протокол по умолчанию использует только доверенные ключи и (или) сертификаты; • протокол по умолчанию использует только безопасные конфигурации без поддержки незащищенных версий и конфигураций; • для шифрования данных применяются соответствующие стойкие алгоритмы.	небезопасных соединений.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
11.2 Если платежное приложение обеспечивает отправку основных номеров держателей карт посредством использования пользовательских технологий передачи данных (например, электронной почты, систем мгновенной отправки сообщений, чатов), оно должно предоставить решение для приведения этих номеров в нечитаемый вид или внедрения стойкого шифрования, либо указать метод стойкого шифрования основных номеров держателей карт. ***Согласуется с требованием 4.2 стандарта PCI DSS***	**11.2.a** Если платежное приложение допускает и (или) обеспечивает отправку основных номеров держателей карт посредством использования пользовательских технологий передачи данных, следует убедиться в наличии решения, которое приводит номера в нечитаемый вид или внедряет стойкое шифрование, либо указывает метод его использования.	Сообщения, передаваемые по электронной почте, с помощью систем мгновенного обмена сообщениями или в чате, могут быть перехвачены в процессе доставки с помощью анализаторов пакетов как во внутренней, так и во внешней общедоступной сети. Запрещается использовать такие средства передачи данных для отправки основных номеров держателей карт, если платежное приложение не обеспечивает использования стойкого шифрования или приведения номеров в нечитаемый вид.
	11.2.b Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, чтобы убедиться, что оно содержит инструкции для клиентов и интеграторов/реселлеров по использованию решения, предоставленного или указанного приложением, в том числе: • процедуры использования указанного решения для приведения основных номеров держателей карт в нечитаемый вид или защиты таких номеров при помощи стойкого шифрования; • инструкции, указывающие, что основной номер держателя карты должен передаваться в нечитаемом виде или быть защищен посредством стойкого шифрования при использовании пользовательских технологий передачи сообщений.	
	11.2.c Если решение предоставляется вместе с платежным приложением, необходимо установить и протестировать приложение, чтобы убедиться, что решение приводит основной номер держателя карты в нечитаемый вид или внедряет стойкое шифрование.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 12. Необходимо шифровать неконсольный административный доступ

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
12.1 Если платежное приложение обеспечивает неконсольный административный доступ, необходимо шифровать такой доступ посредством стойкого шифрования при помощи таких технологий, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа. ***Примечание.*** *Открытые протоколы, такие как Telnet или rlogin, никогда не должны использоваться для административного доступа.* ***Согласуется с требованием 2.3 стандарта PCI DSS***	**12.1.a** Установить платежное приложение в лаборатории и протестировать неконсольные административные соединения, чтобы убедиться, что перед запросом пароля администратора применяется метод стойкого шифрования.	Если при удаленном администрировании не используются безопасная аутентификация и шифрование, существует возможность перехвата злоумышленником конфиденциальной информации (например, паролей администратора). Злоумышленник может воспользоваться такой информацией для получения доступа к приложению и (или) сети, изменения разрешений и кражи данных.
	12.1.b Изучить настройки конфигурации платежного приложения, чтобы убедиться, что открытые протоколы, такие как Telnet или rlogin, не используются платежным приложением для неконсольного административного доступа.	
	12.1.c Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя инструкции для клиентов и интеграторов/реселлеров по настройке стойкого шифрования в приложении с использованием таких технологий, как SSH, VPN или SSL/TLS для шифрования неконсольного административного доступа.	
12.2 Проинструктировать клиентов шифровать неконсольный административный доступ посредством стойкого шифрования при помощи таких технологий, как SSH, VPN или SSL/TLS, для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа. ***Примечание.*** *Открытые протоколы, такие как Telnet или rlogin, никогда не должны использоваться для административного доступа.* ***Согласуется с требованием 2.3 стандарта PCI DSS***	**12.2** Изучить *Руководство по внедрению стандарта PA-DSS*, подготовленное поставщиком, и убедиться, что оно включает в себя инструкции для клиентов и интеграторов/реселлеров по внедрению стойкого шифрования с использованием таких технологий, как SSH, VPN или SSL/TLS, для шифрования неконсольного административного доступа.	Поставщики платежных приложений должны будут предоставить клиентам и интеграторам/реселлерам инструкции по настройке использования в приложении стойкого шифрования для неконсольного административного доступа. Это поможет обеспечить надлежащее внедрение механизмов обеспечения безопасности, соответствующих требованиям стандартов PCI DSS и PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 13. Необходимо составить Руководство по внедрению стандарта PA-DSS для клиентов, реселлеров и интеграторов

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
13.1 Разработать, составить и распространить *Руководство по внедрению стандарта PA-DSS* для клиентов, интеграторов и реселлеров, которое соответствует следующим требованиям.	**13.1** Изучить *Руководство по внедрению стандарта PA-DSS* и соответствующие процессы поставщика, и опросить сотрудников, чтобы убедиться, что: • *руководство по внедрению стандарта PA-DSS* предоставлено всем клиентам, реселлерам и интеграторам вместе с приложением; • у поставщика действует механизм предоставления *Руководства по внедрению стандарта PA-DSS* клиентам, реселлерам и интеграторам по запросу.	Продуманное и подробное *Руководство по внедрению стандарта PA-DSS* помогает клиентам и интеграторам/реселлерам при внедрении надлежащих мер обеспечения безопасности и конфигурации платежного приложения и лежащих в его основе компонентов с целью соответствия требованиям стандартов PCI DSS и PA-DSS по защите данных держателей карт.
13.1.1 Руководство должно предоставлять клиентам, интеграторам и реселлерам актуальную информацию, относящуюся к приложению.	**13.1.1** Изучить *Руководство по внедрению стандарта PA-DSS* и убедиться, что оно: • четко указывает название и версию рассматриваемого платежного приложения; • предоставляет информацию о взаимозависимостях приложений, необходимых для его настройки в соответствии с требованиями PCI DSS;	
13.1.2 Соответствует всем требованиям, приведенным в данном документе, независимо от того, упоминается ли *Руководство по внедрению стандарта PA-DSS* напрямую.	**13.1.2** Изучить *Руководство по внедрению стандарта PA-DSS* и, консультируясь с Приложением А, убедиться, что *Руководство* охватывает все требования, приведенные в настоящем документе.	
13.1.3 Руководство необходимо проверять не реже раза в год и после изменений в приложении либо требованиях стандарта PA-DSS и обновлять по мере необходимости в целях поддержания актуальности документации по отношению к требованиям,	**13.1.3.a** Изучить *Руководство по внедрению стандарта PA-DSS* и опросить сотрудников, чтобы убедиться в том, что *Руководство* проходит проверку: • не реже одного раза в год; • после внесения изменений в приложение; • после изменения требований стандарта PA-DSS.	После каждого обновления приложения изменяются функциональные возможности системы и, в некоторых случаях, критичные механизмы обеспечения безопасности. Если не поддерживается актуальность *Руководства по внедрению стандарта*

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
приведенным в настоящем документе.	**13.1.3.b** Убедиться, что *Руководство по внедрению стандарта PA-DSS* обновляется по мере необходимости и соответствует: • изменениям требований стандарта PA-DSS; • изменениям в приложении или его взаимозависимостях.	*PA-DSS* по отношению к последним версиям платежного приложения, клиенты и интеграторы/реселлеры могут пропустить и неправильно настроить критичные механизмы контроля безопасности приложения, что может в итоге позволить злоумышленнику обойти защиту и получить доступ к конфиденциальным данным.
	13.1.3.c Изучить *Руководство по внедрению стандарта PA-DSS* и соответствующие процессы поставщика и опросить сотрудников, чтобы убедиться, что у поставщика действует механизм информирования клиентов, реселлеров и интеграторов об обновлениях и передачи обновленных версий.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование 14. Необходимо назначить сотрудникам обязанности по стандарту PA-DSS и обеспечить программы обучения сотрудников, реселлеров и интеграторов

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
14.1 Проводить обучение по информационной безопасности и стандарту PA-DSS среди сотрудников поставщика, имеющих обязанности по стандарту PA-DSS, не реже раза в год.	**14.1** Изучить обучающие материалы и опросить ответственных сотрудников поставщика, чтобы убедиться, что сотрудники, имеющие обязанности по стандарту PA-DSS, проходят обучение по информационной безопасности и стандарту PA-DSS не реже раза в год.	Чтобы платежное приложение было разработано эффективно и в соответствии с требованиями стандарта PA-DSS, сотрудники поставщика платежного приложения должны быть осведомлены о требованиях стандарта PA-DSS и своих обязанностях в отношении текущих проверок на соответствие требованиям стандарта PA-DSS. Поставщик платежного приложения несет ответственность за надлежащее обучение своих сотрудников в этих областях.
14.2 Распределить роли и обязанности среди сотрудников поставщика, включая следующее: • общая ответственность за соответствие всем требованиям стандарта PA-DSS; • информирование об изменениях в руководстве по программе PA-DSS PCI SSC; • обеспечение использования методов безопасного программирования; • обучение и предоставление вспомогательных материалов интеграторам/реселлерам; • обеспечение обучения всех сотрудников поставщика, имеющих обязательства по	**14.2.a** Изучить документированные обязательства, чтобы убедиться, что обязанности по следующим ролям официально назначены: • общая ответственность за соответствие всем требованиям стандарта PA-DSS; • информирование об изменениях в Руководстве по программе PA-DSS PCI SSC; • обеспечение использования методов безопасного программирования; • обучение и предоставление вспомогательных материалов интеграторам/реселлерам; • обеспечение обучения всех сотрудников поставщика, имеющих обязанности по стандарту PA-DSS, включая разработчиков.	В каждой организации-поставщике платежного приложения необходимо назначить ответственной стороне (отдельному лицу или группе) официальную обязанность по стандарту PA-DSS, чтобы гарантировать должное соответствие требованиям стандарта PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
стандарту PA-DSS, включая разработчиков.	**14.2.b** Опросить сотрудников, исполняющих обязанности по следующим ролям, чтобы убедиться, что роли и обязанности четко определены и поняты: • общая ответственность за соответствие всем требованиям стандарта PA-DSS; • информирование об изменениях в Руководстве по программе PA-DSS PCI SSC; • обеспечение использования методов безопасного программирования; • обучение и предоставление вспомогательных материалов интеграторам/реселлерам; • обеспечение обучения всех сотрудников поставщика, имеющих обязанности по стандарту PA-DSS, включая разработчиков.	
14.3 Разработать и внедрить программы обучения и коммуникаций для интеграторов и реселлеров платежного приложения. Обучение должно включать как минимум следующую информацию: • инструкции по внедрению платежного приложения и связанных с ним систем и сетей в соответствии с требованиями стандарта PCI DSS; • охват всех требований, затрагивающих *Руководство по внедрению стандарта PA-DSS* в настоящем документе (и Приложении A).	**14.3.a** Изучить обучающие материалы и убедиться, что они включают следующее: • инструкции по внедрению платежного приложения и связанных с ним систем в соответствии с требованиями стандарта PCI DSS; • охват всех требований, затрагивающих *Руководство по внедрению стандарта PA-DSS* в настоящем документе (и Приложении A).	Неправильная настройка, поддержка или техобслуживание приложения может привести к появлению уязвимостей в системе безопасности среды данных держателей карт клиента, чем могут воспользоваться злоумышленники. Поставщики приложений должны обучить интеграторов/реселлеров безопасной установке и настройке приложения, чтобы гарантировать, что после установки на торговой точке приложение будет соответствовать стандарту PCI DSS. Поставщик платежного приложения несет ответственность за обучение интеграторов и реселлеров по данным вопросам.
	14.3.b Изучить программы обмена данными и соответствующие процессы поставщика и опросить сотрудников, чтобы убедиться, что: • интеграторам и реселлерам предоставлены обучающие материалы; • у поставщика действует механизм предоставления обновленных материалов интеграторам и реселлерам по запросу.	
	14.3.c Опросить несколько интеграторов и реселлеров, чтобы убедиться, что они прошли обучение и получили обучающие материалы от поставщика приложения.	
	14.3.d Изучить доказательства получения интеграторами и реселлерами обучающих материалов от поставщика.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Процедуры проведения тестирования	Пояснение
14.3.1 Пересматривать обучающие материалы не реже раза в год и после изменений в платежном приложении или требованиях стандарта PA-DSS. Обновлять обучающие материалы по мере необходимости, чтобы поддерживать актуальность документации по отношению к новым версиям платежного приложения и изменениям требований стандарта PA-DSS.	**14.3.1.a** Изучить обучающие материалы и убедиться, что они: • пересматриваются не реже раза в год и после изменений в платежном приложении или требованиях стандарта PA-DSS; • обновляются по мере необходимости, чтобы поддерживать актуальность документации по отношению к новым версиям платежного приложения и изменениям требований стандарта PA-DSS.	Обучающие материалы для сотрудников поставщика платежного приложения, интеграторов и реселлеров следует обновлять не реже одного раза в год, чтобы обеспечить их актуальность по отношению к новым версиям платежного приложения и изменениям требований стандарта PA-DSS. Использование устаревших обучающих материалов может снизить эффективность программ обучения, что, в свою очередь, может привести к некачественно разработанным функциям обеспечения безопасности в приложении или неверной настройке приложения интеграторами и реселлерами.
	14.3.1.b Изучить процессы распространения новых версий платежного приложения и убедиться, что обновленная документация предоставляется интеграторам и реселлерам вместе с обновленным платежным приложением.	
	14.3.1.c Опросить несколько интеграторов и реселлеров, чтобы убедиться, что они получили обновленные обучающие материалы от поставщика приложения.	

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Приложение A. Краткое изложение *Руководства по внедрению стандарта PA-DSS*

Цель данного Приложения заключается в обобщении требований стандарта PA-DSS, имеющих отношение к разделам *Руководства по внедрению стандарта PA-DSS,* разъяснении содержимого *Руководства по внедрению стандарта PA-DSS*, предоставляемого клиентам и интеграторам/реселлерам (см. "Руководство по внедрению стандарта PA-DSS" на стр. 11) и описании обязанностей по внедрению соответствующих механизмов контроля.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
1.1.4	Удаление критичных аутентификационных данных, сохраненных предыдущими версиями платежного приложения.	Клиентам и интеграторам/реселлерам необходимо предоставить следующие инструкции: ▪ накопленные данные должны быть удалены (данные дорожки, коды проверки подлинности карты, PIN-коды или PIN-блоки, сохраненные предыдущими версиями платежного приложения); ▪ инструкции по удалению накопленных данных; ▪ удаление этих данных абсолютно необходимо для соответствия требованиям стандарта PCI DSS.	**Поставщик приложения**: предоставить клиентам средство или процедуру для надежного удаления критичных аутентификационных данных, сохраненных предыдущими версиями приложения, в соответствии с требованием 1.1.4 PA-DSS. **Клиенты и интеграторы/реселлеры**: удалить все накопленные данные в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 1.1.4 PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
1.1.5	Удаление конфиденциальных аутентификационных (предавторизационных) данных, собранных в результате поиска неисправностей платежного приложения.	Клиентам и интеграторам/реселлерам необходимо предоставить следующие инструкции: ▪ сбор критичных аутентификационных (предавторизационных) данных производится, только если это необходимо для решения конкретной проблемы; ▪ такие данные должны храниться только в определенных известных местах с ограниченным доступом; ▪ для решения конкретной проблемы следует собирать минимальный необходимый объем данных; ▪ конфиденциальные аутентификационные данные должны шифроваться на время хранения; ▪ такие данные должны удаляться безопасным образом сразу после использования.	**Поставщик приложения**: не хранить конфиденциальные аутентификационные данные; осуществлять поиск решения проблем клиента в соответствии с требованием 1.1.5.a стандарта PA-DSS. **Клиенты и интеграторы/реселлеры:** не хранить конфиденциальные аутентификационные данные; осуществлять поиск решения проблем клиента в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 1.1.5.a стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
2.1	Удаление данных держателей карт безопасным образом по истечении указанного клиентом срока хранения.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ данные держателей карт должны быть удалены безопасным образом по истечении указанного клиентом срока хранения; ▪ необходимо составить список всех мест, где платежное приложение хранит данные держателей карт (чтобы клиент знал, откуда следует удалить данные); ▪ клиентам должны быть предоставлены инструкции, согласно которым они должны безопасным образом удалить данные держателей карт, которые более не требуются для юридических, нормативных или деловых целей; ▪ инструкции в отношении надежного удаления данных держателей карт, сохраненных платежным приложением, включая данные, хранящиеся в базовом ПО или системе, где установлено приложение (т. е. ОС, базы данных и т. д.); ▪ инструкции по настройке базового ПО или системы, где установлено приложение (т. е. ОС, базы данных и т. д.) с целью предотвращения неумышленного сбора или хранения данных держателей карт.	**Поставщик приложения**: сообщить клиентам, что данные держателей карт по истечении указанного клиентом срока хранения должны быть удалены безопасным образом из мест, где их хранит платежное приложение, а также из базового ПО или систем, где оно установлено; предоставить инструкции по надежному удалению данных держателей карт, сохраненных платежным приложением. **Клиенты и интеграторы/реселлеры**: удалить безопасным образом данные держателей карт по истечении указанного клиентом срока хранения в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.1 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
2.2	Маскировка основного номера держателя карты при его отображении, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь номер.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ информацию обо всех случаях отображения основного номера держателя карты, включая, помимо прочего, кассовые терминалы, экраны, журналы и чеки; ▪ подтверждение того, что платежное приложение маскирует все случаи отображения основного номера держателя карты по умолчанию; ▪ инструкции по настройке платежного приложения таким образом, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь основной номер держателя карты.	**Поставщик приложения**: предоставить клиентам инструкции по маскировке основного номера держателя карты при его отображении, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь номер. **Клиенты и интеграторы/реселлеры**: маскировать отображение основного номера держателя карты, чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь номер, в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.2 стандарта PA-DSS;
2.3	Представление основного номера держателя карты в нечитаемом виде во всех местах хранения (включая данные на съемных цифровых носителях, резервных копиях и журналах протоколирования событий).	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ информацию о настраиваемых параметрах для каждого метода, используемого приложением для приведения данных держателей карт в нечитаемый вид, и инструкции по настройке каждого метода на всех устройствах, где данные держателей карт хранятся платежным приложением (согласно требованию 2.1 стандарта PA-DSS); ▪ список случаев, когда данные держателей карт могут быть предоставлены торговым точкам для хранения вне платежного приложения, и указания относительно ответственности торгово-сервисных предприятий по приведению основного номера держателя карты в нечитаемый вид в таких случаях.	**Поставщик приложения**: предоставить клиентам инструкции по приведению основного номера держателя карты в нечитаемый вид во всех местах хранения или отображения приложением. **Клиенты и интеграторы/реселлеры**: привести основной номер держателя карты в нечитаемый вид во всех местах хранения в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.3 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
2.4	Защита ключей, используемых для защиты данных держателей карт от раскрытия или неправомерного использования.	Клиентам и интеграторам/реселлерам необходимо предоставить следующие инструкции: ▪ разрешать доступ к ключам шифрования наименьшему возможному количеству сотрудников, ответственных за их хранение и использование; ▪ хранить ключи только в строго определенных защищенных хранилищах и в строго определенном виде.	**Поставщик приложения**: проинформировать клиентов о том, что ключи, используемые для защиты данных держателей карт, должны храниться в безопасном виде и в минимально возможном количестве мест, и доступ к ключам шифрования должен быть ограничен минимально возможным количеством сотрудников, ответственных за их хранение и использование. **Клиенты и интеграторы/реселлеры**: хранить ключи в безопасном виде и в минимально возможном количестве мест, ограничить доступ к ключам шифрования минимально возможным количеством сотрудников, ответственных за их хранение и использование, в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.4 стандарта PA-DSS;
2.5	Внедрение процессов и процедур управления ключами шифрования данных держателей карт.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ инструкции по безопасному созданию, распространению, защите, изменению, хранению и изъятию/смене ключей шифрования в случаях, когда в управление ключами вовлечены клиенты или интеграторы/реселлеры; ▪ образец формы для сотрудников по хранению и использованию ключей, в которой они подтверждают, что поняли свою ответственность и принимают свои обязанности.	**Поставщик приложения**: предоставить клиентам, имеющим доступ к ключам шифрования данных держателей карт, инструкции по внедрению процессов и процедур управления ключами. **Клиенты и интеграторы/реселлеры**: внедрить процессы и процедуры управления ключами, которые используются для шифрования данных держателей карт в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.5 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
2.5.1 – 2.5.7	Внедрение безопасных функций управления ключами.	Предоставить клиентам и интеграторам/реселлерам инструкции по выполнению функций управления ключами, включая: ▪ генерацию стойких ключей шифрования; ▪ безопасное распространение ключей шифрования; ▪ безопасное хранение ключей шифрования; ▪ замену ключей, у которых истек период действия; ▪ изъятие или замену ключей в случае необходимости, если целостность ключа нарушена или существуют подозрения в его компрометации; ▪ разделение знаний и двойной контроль процедур ручного управления ключами шифрования в открытом виде, поддерживаемых платежным приложением; ▪ защиту от неавторизованной смены ключей шифрования.	**Поставщик приложения**: предоставить клиентам инструкции по внедрению безопасных функций управления ключами. **Клиенты и интеграторы/реселлеры**: внедрить безопасные функции управления ключами шифрования в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованиями 2.5.1 – 2.5.7 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
2.6	Обеспечение механизма приведения в нечитаемый вид компонентов ключей шифрования или криптограмм, сохраняемых платежным приложением.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ процедуры, описывающие использование средства или процедуры, предназначенных для обеспечения невозможности восстановления компонентов ключей шифрования; ▪ инструкции, гласящие, что компонент ключа шифрования должен быть приведен в нечитаемый вид без возможности восстановления, если ключи больше не используются, в соответствии требованиями PCI DSS к управлению ключами; ▪ инструкции по повторному шифрованию накопленных данных при помощи новых ключей, включая процедуры поддержания безопасности данных в открытом виде во время процесса дешифрования/повторного шифрования.	**Поставщик приложения**: предоставить средство или процедуру для надежного удаления компонентов ключей шифрования или криптограмм, сохраняемых приложением, и предоставить средство или процедуру для повторного шифрования накопленных данных при помощи новых ключей. **Клиенты и интеграторы/реселлеры**: удалить все накопленные компоненты ключей шифрования согласно требованиям к управлению ключами в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.6 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
3.1	Использование уникального идентификатора пользователя и надежной аутентификации для административного доступа и доступа к данным держателей карт.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ разъяснения в отношении того, как платежное приложение обеспечивает надежную аутентификацию для всех учетных данных для аутентификации (например, имена пользователей, пароли), которые приложение генерирует или которыми управляет, посредством: – обеспечения безопасных изменений учетных данных для аутентификации до завершения установки в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS; – обеспечения безопасности всех последующих (после установки) изменений учетных данных для аутентификации в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS; ▪ информацию, что в целях выполнения требований стандарта PCI DSS, все изменения аутентификационных конфигураций должны пройти проверку на соответствие строгости методов аутентификации требованиям PCI DSS; ▪ рекомендации, что учетным записям по умолчанию (даже если они не будут использоваться) рекомендуется назначить надежную аутентификацию, а затем отключить либо не использовать эти учетные записи; ▪ инструкции по созданию и изменению учетных данных для аутентификации, если такие данные не генерируются и не управляются платежным приложением, в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS, до завершения установки и для последующих изменений после установки, для всех учетных записей уровня приложения с административным доступом или доступом к данным держателей карт.	**Поставщик приложения**: если приложение генерирует или управляет учетными данными для аутентификации, убедиться, что платежное приложение обеспечивает использование клиентами уникальных идентификаторов и надежной аутентификации для учетных записей/паролей в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS; если приложение не генерирует и не управляет учетным данными для аутентификации, убедиться, что *Руководство по внедрению стандарта PA-DSS* содержит четкие и недвусмысленные инструкции для клиентов и интеграторов/реселлеров по изменению и созданию безопасных учетных данных для аутентификации в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: создать и поддерживать уникальные идентификаторы пользователя и надежную аутентификацию в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованиями 3.1.1–3.1.11 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
3.2	Использование уникальных идентификаторов пользователя и надежной аутентификации для доступа к компьютерам, серверам и базам данных, содержащим платежные приложения.	Проинструктировать клиентов и интеграторов/реселлеров в отношении использования уникальных имен и надежной аутентификации для доступа к компьютерам, серверам и базам данных, содержащим платежные приложения и (или) данные держателей карт, в соответствии с требованиями 3.1.1–3.1.11 стандарта PA-DSS.	**Поставщик приложения**: убедиться, что платежное приложение поддерживает использование клиентом уникальных идентификаторов и надежной аутентификации для учетных записей/паролей, в случае настройки поставщиком, для доступа к компьютерам, серверам и базам данных в соответствии с требованиями 3.1.2–3.1.9 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: создать и поддерживать уникальные идентификаторы пользователя и надежную аутентификацию в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованиями 3.1.1–3.1.11 стандарта PA-DSS;
4.1	Внедрение автоматических механизмов протоколирования.	Предоставить инструкции по внедрению автоматических механизмов протоколирования, включающие: ▪ инструкции по установке приложения таким образом, чтобы ведение журналов было включено и настроено по умолчанию после завершения процесса установки; ▪ инструкции по настройке доступных клиенту параметров журнала согласно стандарту PCI DSS после установки в соответствии с требованиями 4.2, 4.3 и 4.4 стандарта PA-DSS; ▪ журналы не должны быть отключены, так как это приведет к несоответствию требованиям стандарта PCI DSS; ▪ инструкции по настройке доступных клиенту параметров журнала сторонних программных компонентов, поставляемых совместно либо требуемых платежным приложением, после установки в соответствии с требованиями стандарта PCI DSS.	**Поставщик приложения**: убедиться, что платежное приложение поддерживает использование клиентом соответствующих стандарту журналов в соответствии с требованиями 4.2, 4.3 и 4.4 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры:** создать и поддерживать журналы, соответствующие стандарту PCI DSS, в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованиями 4.2, 4.3 и 4.4 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
4.4	Обеспечение централизованного ведения журналов.	Предоставить описание поддерживаемых механизмов централизованного ведения журналов, а также инструкции и процедуры внесения журналов платежного приложения в центральный сервер ведения журналов.	**Поставщик приложения**: обеспечить в приложении поддержку централизованного ведения журналов в средах клиентов в соответствии с требованием 4.4 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры:** организовать и поддерживать централизованное ведение журналов в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 4.4 стандарта PA-DSS;
5.4.4	Внедрение и информирование о методологии назначения версий приложения.	Предоставить описание опубликованной методологии назначения версий поставщика и включить пояснения в отношении следующего: ▪ информации о схеме нумерации версий, включая формат схемы нумерации версий (количество элементов, разделительные знаки, набор символов и т. д.); ▪ информации об обозначении изменений, влияющих на функции безопасности, на схеме версий; ▪ информации о том, как другие типы изменений отражаются на версии; ▪ информации об используемых подстановочных знаках, включая подтверждение того, что они никогда не будут использованы для обозначения изменений, не влияющих на функции безопасности.	**Поставщик приложения**: задокументировать и внедрить методологию назначения версий ПО в рамках жизненного цикла разработки системы; методология должна соответствовать процедурам, приведенным в *Руководстве по программе PA-DSS* и касающимся изменений в платежном приложении, в соответствии с требованием 5.5 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры:** понимать, какую версию платежного приложения они используют, и обеспечить использование одобренных версий;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
6.1	Безопасное внедрение беспроводных технологий.	Если платежные приложения разрабатывались для использования с беспроводными технологиями, клиентам и интеграторам/реселлерам должно быть предоставлено следующее: ▪ инструкции, согласно которым платежное приложение при установке должно требовать изменения ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию для всех беспроводных компонентов, управляемых приложением; ▪ процедуры изменения ключей шифрования и паролей, включая строки доступа протокола SNMP, в случае увольнения из компании любого сотрудника, имеющего доступ к ключам/паролям; ▪ инструкции по изменению ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию на любом беспроводном компоненте, предоставленном, но не контролируемом платежным приложением; ▪ инструкции по установке брандмауэра между беспроводными сетями и системами, в которых хранятся данные держателей карт; ▪ подробные данные о беспроводном трафике (включая информацию о конкретных портах), который будет использовать функция беспроводной связи платежного приложения; ▪ инструкции по настройке брандмауэра для запрета или – если такой трафик необходим в целях проведения операций – разрешения только авторизованного трафика между беспроводной средой и средой данных держателей карт.	**Поставщик приложения**: проинструктировать клиентов и интеграторов/реселлеров, что в случае использования беспроводной технологии с платежным приложением необходимо изменить параметры по умолчанию, установленные поставщиком, в соответствии с требованием 6.1 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: если беспроводные технологии были внедрены в платежную среду клиентами или интеграторами/реселлерами, изменить параметры по умолчанию, установленные поставщиком, в соответствии с требованием 6.1 стандарта PA-DSS и установить брандмауэр в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 2.1.1 стандарта PCI DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
6.2	Безопасная передача данных держателей карт через беспроводные сети.	Для платежных приложений, разработанных для использования с беспроводными технологиями, следует приложить инструкции по применению передовых отраслевых методов (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных держателей карт. Сюда входят: ▪ инструкции по настройке приложения таким образом, чтобы оно применяло передовые отраслевые методы (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных, и (или) ▪ инструкции по настройке приложений для беспроводной связи, поставляемых в комплекте с платежным приложением, таким образом, чтобы применялись передовые отраслевые методы по обеспечению стойкого шифрования при аутентификации и передаче данных.	**Поставщик приложения**: проинструктировать клиентов и интеграторов/реселлеров, что в случае использования беспроводной технологии с платежным приложением необходимо обеспечить шифрование передаваемых данных в соответствии с требованием 6.2 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: если беспроводные технологии были внедрены в платежную среду клиентами или интеграторами/реселлерами, использовать безопасную зашифрованную передачу данных в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 6.2 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
6.3	Предоставление инструкций по безопасному использованию беспроводных технологий.	Предоставить инструкции по настройке беспроводной связи в соответствии со стандартом PCI DSS, в том числе: ▪ инструкции по изменению при установке всех ключей шифрования, паролей и строк доступа протокола SNMP по умолчанию; ▪ инструкции по изменению ключей шифрования, паролей и строк доступа протокола SNMP в случае увольнения из компании любого сотрудника, имеющего доступ к ключам/паролям; ▪ инструкции по установке брандмауэра между беспроводными сетями и системами, в которых хранятся данные держателей карт, и настройке брандмауэра для запрета или контроля – если такой трафик необходим в целях совершения операций – всего трафика между беспроводной средой и средой данных держателей карт; ▪ инструкции по применению передовых практических методов индустрии безопасности (например, IEEE 802.11i) для обеспечения стойкого шифрования при аутентификации и передаче данных.	**Поставщик приложения**: проинструктировать клиентов и интеграторов/реселлеров в отношении обеспечения безопасности беспроводных технологий в соответствии с требованием 6.3 PA-DSS. **Клиенты и интеграторы/реселлеры**: обеспечить безопасность беспроводных технологий в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 6.2 стандарта PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
8.2	Использование только необходимых и защищенных служб, протоколов, компонентов и зависимого программного обеспечения и оборудования, включая предоставленные третьими сторонами.	Задокументировать все протоколы, службы, компоненты и зависимое программное обеспечение и оборудование, необходимые для функционирования платежного приложения.	**Поставщик приложения:** убедиться, что платежное приложение обеспечивает использование клиентом только необходимых и защищенных протоколов, служб и т. д. посредством: 1) наличия только необходимых и защищенных протоколов, служб и т. д. по умолчанию, 2) безопасной настройки этих необходимых и защищенных протоколов, служб и т. д. по умолчанию и 3) документирования необходимых протоколов, служб и т. д. для получения справки клиентами и интеграторами/реселлерами. **Клиенты и интеграторы/реселлеры:** использовать документированный список из *Руководства по внедрению стандарта PA-DSS*, чтобы убедиться, что в системе используются только необходимые и защищенные протоколы, службы и т. д. в соответствии с требованием 5.4 стандарта PA-DSS;
9.1	Хранение данных держателей карт только на серверах, не подключенных к Интернету.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ указания не хранить данные держателей карт в общедоступных системах (например, веб-сервер и сервер базы данных не должны находиться на одном сервере); ▪ инструкции по настройке платежного приложения для использования демилитаризованной зоны (DMZ) с целью разграничения Интернета и систем, в которых хранятся данные держателей карт; ▪ список служб/портов, которые приложение должно использовать для передачи данных между двумя зонами сети (чтобы торговая точка могла открыть в брандмауэре только необходимые порты).	**Поставщик приложения**: убедиться, что платежное приложение не требует хранения данных держателей карт в демилитаризованной зоне (DMZ) или доступных через Интернет системах и позволяет использовать DMZ в соответствии с требованием 9 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: настроить платежные приложения таким образом, чтобы данные держателей карт не хранились в доступных через Интернет системах в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 9 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
10.1	Внедрение двухфакторной аутентификации для удаленного доступа к платежному приложению извне среды клиента.	Клиентам и интеграторам/реселлерам необходимо предоставить следующее: ▪ инструкции, согласно которым для соответствия требованиям стандарта PCI DSS при удаленном доступе к платежному приложению извне сети клиента всегда должна использоваться двухфакторная аутентификация; ▪ описание механизмов двухфакторной аутентификации, поддерживаемых приложением; ▪ инструкции по настройке поддержки двухфакторной аутентификации в приложении (два из трех методов аутентификации, описанных в требовании 3.1.4 стандарта PA-DSS).	**Поставщик приложения**: убедиться, что платежное приложение поддерживает использование двухфакторной аутентификации для удаленного доступа к платежному приложению извне среды клиента в соответствии с требованием 10.2 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: организовать и поддерживать двухфакторную аутентификацию для удаленного доступа к платежному приложению извне среды клиента в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 10.2 стандарта PA-DSS;
10.2.1	Безопасная доставка обновлений платежного приложения.	Если обновления платежного приложения доставляются посредством удаленного доступа к системам клиента, необходимо предоставить следующее: ▪ инструкции по включению удаленного доступа для обновления платежного приложения, когда это необходимо для загрузки, и по выключению доступа сразу после завершения загрузки в соответствии с требованием 12.3.9 стандарта PCI DSS; ▪ инструкции, согласно которым, если компьютер использует виртуальную частную сеть (VPN) или другое высокоскоростное соединение, для получения обновлений платежного приложения необходим должным образом настроенный брандмауэр (общий или личный) в соответствии в требованием 1 стандарта PCI DSS.	**Поставщик приложения**: безопасно доставлять обновления платежного приложения в соответствии в требованием 10.3 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: безопасно получать обновления платежного приложения от поставщика в соответствии с *Руководством по внедрению стандарта PA-DSS*, требованием 10.3 стандарта PA-DSS и требованием 1 стандарта PCI DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
10.2.3	Безопасное внедрение ПО для удаленного доступа.	Проинструктировать, что удаленный доступ к платежному приложению должен осуществляться безопасным образом, например следует: ▪ изменить настройки по умолчанию в ПО для удаленного доступа (например, изменить пароли по умолчанию и использовать уникальные пароли для каждого клиента); ▪ разрешать подключения только с конкретных (известных) IP- и (или) MAC-адресов; ▪ использовать надежную аутентификацию и сложные пароли для входа (см. требования 3.1.1 – 3.1.11 стандарта PA-DSS); ▪ обеспечить зашифрованную передачу данных в соответствии с требованием 12.1 стандарта PA-DSS; ▪ настроить блокировку учетной записи после определенного количества неудачных попыток входа (см. требования 3.1.9 – 3.1.10 стандарта PA-DSS); ▪ установить соединение по виртуальной частной сети (VPN) через брандмауэр перед разрешением доступа; ▪ активировать функцию регистрации событий; ▪ разрешить доступ к средам клиентов только авторизованным интеграторам/реселлерам.	**Поставщик приложения**: (1) если поставщик может получить удаленный доступ к платежным приложениям клиента, обеспечить безопасный удаленный доступ, как описано в требовании 10.3.2 стандарта PA-DSS; (2) обеспечить поддержку использования функций защиты удаленного доступа в приложении. **Клиенты и интеграторы/реселлеры**: применять функции защиты удаленного доступа во всех случаях удаленного доступа к приложению в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 10.3.2 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
11.1	Безопасная передача данных держателей карт через общедоступные сети.	Если платежное приложение отправляет или обеспечивает отправку данных держателей карт через общедоступные сети, необходимо предоставить инструкции по внедрению и использованию стойкого шифрования и протоколов безопасности для защиты данных держателей карт при передаче через общедоступные сети, включая: ▪ инструкции, указывающие, что стойкое шифрование и протоколы безопасности должны использоваться в случае передачи данных держателей карт через общедоступные сети; ▪ инструкции по проверке приема только доверенных ключей и (или) сертификатов; ▪ инструкции по настройке платежного приложения таким образом, чтобы использовались только безопасные версии, и по внедрению протоколов безопасности; ▪ инструкции по настройке платежного приложения таким образом, чтобы применялось шифрование достаточной стойкости для используемой методологии.	**Поставщик приложения**: убедиться, что платежное приложение поддерживает использование клиентом стойкого шифрования и протоколов безопасности при передаче данных держателей карт через общедоступные сети в соответствии с требованием 11.1 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: организовать и поддерживать стойкое шифрование и протоколы безопасности при передаче данных держателей карт через общедоступные сети в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 11.1 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
11.2	Шифрование данных держателей карт, отправленных при помощи пользовательских технологий передачи сообщений.	Если платежное приложение обеспечивает отправку основных номеров держателей карт, включить инструкции по внедрению и использованию решения, которое приводит эти номера в нечитаемый вид или внедрить стойкое шифрование, включая: ▪ процедуры использования указанного решения для приведения основных номеров держателей карт в нечитаемый вид или защиты таких номеров при помощи стойкого шифрования; ▪ инструкции, указывающие, что основной номер держателя карты должен передаваться в нечитаемом виде или быть защищен посредством стойкого шифрования при использовании пользовательских технологий передачи сообщений.	**Поставщик приложения**: предоставить или указать метод использования решения, которое приводит основные номера держателей карт в нечитаемый вид, или внедрить стойкое шифрование и обеспечить поддержку приложением шифрования основных номеров держателей карт или приведения их в нечитаемый вид при использовании пользовательских технологий передачи сообщений в соответствии с требованием 11.2 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: зашифровать или привести в нечитаемый вид все основные номера держателей карт, отправленные с использованием пользовательских технологий передачи сообщений, в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 11.2 стандарта PA-DSS;
12.1	Шифрование неконсольного административного доступа.	Если платежное приложение обеспечивает неконсольный административный доступ, включить инструкции по настройке стойкого шифрования в приложении с использованием таких технологий, как SSH, VPN или SSL/TLS для шифрования неконсольного административного доступа к платежному приложению или серверам в среде данных держателей карт.	**Поставщик приложения**: если платежное приложение обеспечивает неконсольный административный доступ, убедиться, что платежное приложение использует стойкое шифрование для неконсольного административного доступа в соответствии с требованием 12.1 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: шифровать неконсольный административный доступ в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 12.1 стандарта PA-DSS;

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требования PA-DSS	Раздел PA-DSS	Требуемые материалы Руководства по внедрению	Обязанность по контролю внедрения
12.2	Шифрование неконсольного административного доступа.	Включить инструкции для клиентов и интеграторов/реселлеров по внедрению стойкого шифрования с использованием таких технологий, как SSH, VPN или SSL/TLS для шифрования неконсольного административного доступа.	**Поставщик приложения**: убедиться, что платежное приложение поддерживает шифрование неконсольного административного доступа в соответствии с требованием 12.2 стандарта PA-DSS. **Клиенты и интеграторы/реселлеры**: шифровать неконсольный административный доступ в соответствии с *Руководством по внедрению стандарта PA-DSS* и требованием 12.2 стандарта PA-DSS.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Приложение B. Конфигурация лаборатории по тестированию для проведения оценки на соответствие требованиям стандарта PA-DSS

В отношении каждой проведенной оценки на соответствие требованиям стандарта PA-DSS, PA-QSA должен подтвердить состояние и возможности лаборатории, использованной для проведения проверки. Данное подтверждение необходимо подать вместе с заполненным *отчетом о проверке (ROV)*.

В отношении каждой лабораторной процедуры проверки PA-QSA должен указать, кому принадлежит лаборатория, в которой проводилась проверка и процедуры – PA-QSA или поставщику приложения. PA-QSA должен убедиться, что лаборатория по тестированию соответствует всем требованиям, приведенным ниже, и по возможности использовать собственную лабораторию. Лабораторию поставщика приложения следует использовать только при необходимости (например, если у PA-QSA отсутствует мейнфрейм, AS400 или Tandem, на котором работает приложение), убедившись, что она соответствует требованиям.

PA-QSA должен проверить все пункты из таблицы ниже, а также:

- **местоположение и владельца лаборатории (лабораторий), используемой для проверки на соответствие требованиям стандарта PA-DSS;**
- **описание тестовой архитектуры лаборатории и среды проведения проверки на соответствие стандарту PA-DSS;**
- **описание метода симуляции практического использования платежного приложения в лаборатории для проверки на соответствие требованиям стандарта PA-DSS.**

В *бланке отчета (ROV) о проверке на соответствие стандарту PA-DSS* приведена информация о проверке лаборатории, которую необходимо приводить при каждой оценке.

Требование к лаборатории	Процедура проверки лаборатории
1. Установить платежное приложение в соответствии с инструкциями поставщика или информацией, полученной в процессе обучения, проведенного для клиента.	**1.** Убедиться, что инструкции поставщика или информация, полученная в процессе обучения, проведенного для клиента, использовалась при установке платежного приложения на всех платформах, перечисленных в отчете о проверке на соответствие требованиям PA-DSS, для моделирования хода практического использования клиентом.
2. Установить и протестировать все версии платежного приложения, перечисленные в отчете о проверке на соответствие требованиям PA-DSS.	**2.a** Убедиться, что все распространенные версии платежного приложения (включая специальные, выпущенные для региона/страны), подлежащие проверке, были установлены.
	2.b Убедиться, что были протестированы все версии платежного приложения и платформы, включая все необходимые системные компоненты и взаимозависимости.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование к лаборатории	Процедура проверки лаборатории
	2.c Убедиться, что в каждой версии платежного приложения были протестированы критичные функции.
3. Установить и внедрить все требуемые стандартом PCI DSS устройства защиты.	**3.** Убедиться, что все требуемые стандартом PCI DSS устройства защиты (например, брандмауэры и антивирусы) были установлены на тестовых системах.
4. Установить и (или) настроить все требуемые стандартом PCI DSS параметры безопасности.	**4.** Убедиться, что все требуемые стандартом PCI DSS параметры безопасности, исправления и т. д. были установлены на тестовых системах (ОС, системном ПО и приложениях), используемых платежным приложением.
5. Смоделировать практическое использование платежного приложения.	**5.a** Лаборатория моделирует практическое использование платежного приложения, в том числе все системы и приложения, где внедрено платежное приложение. Например, к стандартному внедрению платежного приложения может относится среда "клиент–сервер" на торговой точке с кассовым аппаратом и служебный офис или корпоративная сеть. Лаборатория моделирует ситуацию полного внедрения.
	5.b Лаборатория использует только тестовые номера карт для тестирования/моделирования. Действующие основные номера держателей карт использовать запрещается. ***Примечание.*** *Как правило, тестовые номера можно получить у поставщика, эквайера или в процессинговой системе.*
	5.c Лаборатория запускает процесс авторизации платежного приложения и (или) функции расчета, и все результаты проверяются согласно пункту 6 ниже.
	5.d Лаборатория регистрирует все результаты, полученные платежным приложением по каждому возможному сценарию: временные, постоянные, ошибки обработки, режим отладки, файлы журнала и т. д.
	5.e Лаборатория моделирует и проверяет все функции платежного приложения, чтобы выявить все сбойные состояния и записи журнала с использованием как реальных, так и недействительных данных.
6. Предоставить возможности и провести тестирование с использованием следующих методологий тестов на проникновение.	**6.a Использование аналитических средств/методов:** аналитические средства/методы были использованы для проверки всех полученных результатов на наличие конфиденциальных аутентификационных данных (коммерческие средства, сценарии и т. д.) в соответствии с требованием 1.1.1–1.1.3 стандарта PA-DSS.[6]

[6] Аналитическое средство или метод: средство или метод для обнаружения, анализа и представления аналитических данных, которое позволяет легко и быстро аутентифицировать, найти и восстановить доказательства из компьютерных ресурсов. Аналитические средства или методы,

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование к лаборатории	Процедура проверки лаборатории
	6.b Попытка использовать уязвимости приложения: распространенные уязвимости (например, согласно руководству OWASP Top 10, SANS CWE Top 25, CERT Secure Coding и т. д.) были использованы для попытки получения доступа к приложению в соответствии с требованием 5.2 стандарта PA-DSS.
	6.c Лаборатория попыталась исполнить произвольный код в ходе процесса обновления платежного приложения: запустить процесс обновления с произвольным кодом в соответствии с требованием 7.2.2 стандарта PA-DSS.
7. Использовать лабораторию поставщика ТОЛЬКО после подтверждения того, что все требования выполнены.	Если использование лаборатории поставщика является необходимым (например, у PA-QSA отсутствует мейнфрейм, AS400 или Tandem, на котором работает приложение), PA-QSA может (1) использовать предоставленное на время оборудование поставщика или (2) использовать саму лабораторию поставщика при условии, что это отражено в отчете вместе с местом проведения тестов. В любом случае PA-QSA должен подтвердить, что оборудование и лаборатории поставщика соответствуют следующим требованиям.
	7.a PA-QSA подтверждает, что лаборатория поставщика соответствует всем требованиям, перечисленным выше в настоящем документе и документах, указанных в отчете.
	7.b PA-QSA должен провести чистую установку в лабораторной среде, чтобы убедиться, что среда действительно моделирует практическую ситуацию и поставщик не вносил каких-либо изменений и модификаций в среду.
	7.c Все тестирование выполняет PA-QSA (поставщик не должен тестировать собственное приложение).
	7.d Все тестирование (1) выполняется в помещениях поставщика или (2) выполняется удаленно посредством сетевого соединения через защищенный канал (например, VPN).
	7.e Использовать только тестовые номера карт для тестирования/моделирования. Действующие номера держателей карт использовать запрещается. Как правило, тестовые номера можно получить у поставщика, эквайера или в процессинговой системе.
8. Поддерживать эффективный процесс обеспечения качества.	**8.a** Персонал по обеспечению качества PA-QSA подтверждает, что все версии и платформы, указанные в отчете о проверке, прошли тестирование на соответствие стандарту PA-DSS.

используемые PA-QSA, должны точно установить местоположение критичных аутентификационных данных, записанных платежным приложением. Этими средствами могут быть приобретенные продукты, продукты с открытым исходным кодом или разработанные PA-QSA внутри организации.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.

Требование к лаборатории	Процедура проверки лаборатории
	8.b Персонал по обеспечению качества PA-QSA подтверждает, что была проведена проверка на соответствие всем требованиям стандарта PA-DSS.
	8.c Персонал по обеспечению качества PA-QSA подтверждает, что лабораторные конфигурации и процессы PA-QSA соответствуют требованиям и были точно задокументированы в отчете.
	8.d Персонал по обеспечению качества PA-QSA подтверждает, что отчет точно отражает результаты тестирования.

© PCI Security Standards Council, LLC, 2006–2013. Все права защищены.