Стандарт безопасности данных
индустрии платежных карт (PCI DSS)

Требования и процедуры аудита безопасности

Версия 3.0

Ноябрь 2013 г.

Изменения документа

Дата	Версия	Описание	Страницы
Октябрь 2008 г.	1.2	*В документе "Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности" версии 1.2 содержатся общие и конкретные изменения по сравнению с версией 1.1 под названием "Процедуры аудита безопасности". Для получения подробной информации см. "Обзор изменений стандарта безопасности данных PCI DSS в версии 1.2 по сравнению с версией 1.1".*	
Июль 2009 г.	1.2.1	*Добавлено предложение, которое было неправильно удалено в версиях PCI DSS 1.1 и 1.2.*	5
		Исправлено “then” на “than” в описании процедур проведения тестирования 6.3.7.a и 6.3.7.b.	32
		Удалено выделение серым цветом для столбцов "Выполнено" и "Не выполнено" в описании процедур проведения тестирования 6.5.b.	33
		Для таблицы "Компенсационные меры – Пример заполнения" исправлено предложение в верхней части страницы, которое теперь звучит так: "Пользуйтесь этой таблицей для описания компенсационных мер для требований, имеющих статус "Выполнено" благодаря использованию компенсационных мер".	64
Октябрь 2010 г.	2.0	*Внедрены изменения из версии 1.2.1. См. "PCI DSS: обзор изменений PCI DSS в версии 2.0 по сравнению с версией 1.2.1".*	
Ноябрь 2013 г.	3.0	*Изменение по сравнению с версией 2.0. См. "PCI DSS: обзор изменений PCI DSS в версии 3.0 по сравнению с версией 2.0".*	

Содержание

Введение и обзор стандарта PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан в целях повышения уровня безопасности данных владельцев платежных карт и содействия процессу повсеместного внедрения единообразных мер по защите данных держателей карт. В основе стандарта PCI DSS лежат фундаментальные технические и операционные требования, которые разработаны для защиты данных держателей карт.данный стандарт применяется для всех организаций сферы обработки платежных данных: торгово-сервисных предприятий, процессинговых центров, банков-эквайеров, организаций, выпускающих платежные карты, и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные. Ниже приведен общий обзор 12 требований стандарта PCI DSS.

Стандарт безопасности данных индустрии платежных карт (PCI DSS): подробные сведения

Построение и обслуживание защищенной сети и систем	**1.** Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт **2.** Не использовать пароли и другие системные параметры, заданные производителем по умолчанию
Защита данных держателей карт	**3.** Обеспечить безопасное хранение данных держателей карт **4.** Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования
Программа управления уязвимостями	**5.** Использовать и регулярно обновлять антивирусное программное обеспечение **6.** Разрабатывать и поддерживать безопасные системы и приложения
Внедрение строгих мер контроля доступа	**7.** Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью **8.** Определять и подтверждать доступ к системным компонентам **9.** Ограничить физический доступ к данным держателей карт
Регулярный мониторинг и тестирование сети	**10.** Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт **11.** Регулярно выполнять тестирование систем и процессов обеспечения безопасности.
Поддержание политики информационной безопасности	**12.** Разработать и поддерживать политику информационной безопасности для всего персонала организации

В данном документе, *"Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности"*, приведены 12 требований стандарта и описаны соответствующие процедуры проведения оценки соответствия данному стандарту. Данный документ предназначен для использования в процессе оценки соответствия стандарту PCI DSS как части процедуры аттестации организации. Приведенные ниже разделы содержат детальные рекомендации и описывают оптимальные способы содействия организациям при подготовке, проведении и составлении отчетных материалов по результатам проверки на соответствие

требованиям стандарта PCI DSS. Требования стандарта PCI DSS и процедуры проведения тестирования описываются, начиная со стр. 15.

Стандарт PCI DSS содержит минимальный набор требований для защиты данных держателей карт, который может быть расширен дополнительными регулирующими механизмами и методами сокращения рисков, а также требованиями и распоряжениями местного, регионального и отраслевого законодательства. Кроме того, в соответствии с законодательством или нормативными требованиями может требоваться особая защита данных, идентифицирующих личность, или других элементов данных (например, имени держателя карты). PCI DSS не заменяет собой местные или региональные законы, правительственные распоряжения или иные требования законодательства.

Источники информации о PCI DSS

На сайте Совета PCI SSC (PCI Security Standards Council) (www.pcisecuritystandards.org) имеются дополнительные источники информации, призванные облегчить оценку организаций и подтверждение их соответствия, в том числе следующее.

- Библиотека документов, в том числе:
  - *PCI DSS: обзор изменений PCI DSS в версии 3.0 по сравнению с версией 2.0*
  - *Краткий справочник по PCI DSS*
  - *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения*
  - *Дополнительная информация и рекомендации*
  - *Приоритетный подход к PCI DSS*
  - *Бланк отчета о соответствии требованиям и инструкции по его заполнению*
  - *Анкеты самооценки, рекомендации и инструкции по их заполнению*
  - *Свидетельства о соответствии*
- Часто задаваемые вопросы
- Веб-сайт "PCI для малого бизнеса"
- Курсы обучения и информационные вебинары по PCI
- Список уполномоченных организаций, проводящих аудит безопасности и авторизованных поставщиков услуг сканирования (ASV)
- Список одобренных PTS устройств и платежных приложений, прошедших проверку на соответствие стандарту PA-DSS

***Примечание**. Данная информация дополняет стандарт PCI DSS. Она дает представление о дополнительных аспектах проведения проверки на соответствие стандарту, но не изменяет, не исключает, не заменяет и не дополняет содержание стандарта или какое-либо из его требований.*

Более подробная информация об этих и других ресурсах доступна на сайте *www.pcisecuritystandards.org*.

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

Требования PCI DSS применимы к организациям и средам, в которых осуществляется хранение, обработка или передача банковских данных (данных держателей карт и (или) критичных аутентификационных данных). Некоторые требования PCI DSS также могут быть применены к организациям, передавшим платежные операции или управление информационной средой держателей карт (CDE) третьим лицам[1]. Кроме того, организации, передавшие платежные операции или управление информационной средой держателей карт (CDE) третьим лицам, обязуются гарантировать, что защита банковских данных осуществляется третьими лицами в соответствии с применимыми требованиями 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.

[1] Согласно индивидуальным программам платежных компаний по обеспечению соответствия требованиям

		Элемент данных	Хранение разрешено	Хранение данных в нечитаемом виде согласно требованию 3.4
Данные платежных карт (Account Data)	**Данные держателя карты (Cardholder Data)**	Основной номер держателя карты (PAN)	Да	Да
		Имя держателя карты	Да	Нет
		Сервисный код	Да	Нет
		Дата истечения срока действия карты	Да	Нет
	Критичные аутентификационные данные (Sensitive Authentication Data)[2]	Полные данные дорожки[3]	Нет	Нельзя хранить согласно требованию 3.2
		CAV2/CVC2/CVV2/CID[4]	Нет	Нельзя хранить согласно требованию 3.2
		PIN/PIN-блок[5]	Нет	Нельзя хранить согласно требованию 3.2

Требования 3.3 и 3.4 стандарта PCI DSS применяются только к основному номеру держателя карты (PAN). Если PAN хранится вместе с другими данными, то в соответствии с требованием 3.4 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. Организации должны напрямую связаться со своими эквайерами или отделениями, отвечающими за отдельные торговые марки, чтобы узнать, разрешается ли хранить критичные аутентификационные данные до авторизации и в течение какого срока, а также получить информацию о других требованиях к использованию и защите данных.

2 Критичные аутентификационные данные не должны храниться после авторизации (даже в зашифрованном виде).
3 Полные данные на дорожке магнитной полосы, эквивалентные данные на чипе или в другом месте.
4 Трех- или четырехзначное проверочное значение, изображенное на лицевой или обратной стороне карты.
5 Персональный идентификационный номер, который вводится держателем карты при выполнении операции с предоставлением карты, и (или) зашифрованный PIN-блок, присутствующий в сообщении об операции.

Связь между стандартами PCI DSS и PA-DSS

Применимость стандарта PCI DSS к приложениям, соответствующим стандарту PA-DSS

Использование приложения, соответствующего стандарту безопасности данных платежных приложений (PA-DSS), не является гарантией соответствия требованиям стандарта PCI DSS, поскольку приложение должно быть внедрено в среду, соответствующую стандарту PCI DSS, и в соответствии с Руководством по внедрению PA-DSS, должно быть представлено разработчиком платежного приложения.

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 соответствия стандарту PCI DSS призвана подтвердить, что платежное приложение, соответствующее стандарту PA-DSS, должным образом настроено и надежно защищено в соответствии с требованиями PCI DSS. Если приложение подверглось какой-либо модификации, оценка соответствия стандарту PCI DSS потребует более тщательного изучения, так как приложение может более не соответствовать версии, утвержденной PA-DSS.

Требования стандарта PA-DSS основаны на *Требованиях и процедурах аудита безопасности стандарта PCI DSS* (определенных в данном документе). Стандарт PA-DSS более детально описывает требования к платежному приложению для упрощения достижения соответствия стандарту PCI DSS.

При внедрении в среду, соответствующую стандарту PCI DSS, безопасные платежные приложения позволят избежать нарушений безопасности и мошеннических действий, которые могут привести к компрометации основного номера держателя карты, полных данных дорожки, проверочных кодов и значений (CAV2, CID, CVC2, CVV2), а также PIN-кодов и PIN-блоков.

Для определения того, применим ли стандарт PA-DSS к тому или иному платежному приложению, обратитесь к документу "Руководство по программе PA-DSS", который доступен на сайте www.pcisecuritystandards.org.

Область применения стандарта PCI DSS для поставщиков платежных приложений

PCI DSS может распространяться на поставщиков платежных приложений, если они хранят, обрабатывают или передают данные держателей карт или имеют доступ к данным держателей карт своих клиентов (например, в качестве поставщика услуг).

Область действия требований PCI DSS

Требования PCI DSS предъявляются ко всем системным компонентам, входящим или подключенным к информационной среде держателей карт (CDE). Информационная среда держателей карт (CDE) – это совокупность людей, процессов и технологий, которые хранят, обрабатывают или передают данные держателей карт или критичные аутентификационные данные. Системные компоненты включают в себя сетевые устройства, серверы, вычислительные устройства и приложения. Вот неполный список примеров системных компонентов:

- системы, обеспечивающие безопасность (например, серверы аутентификации), способствующие сегментации (например, внутренние брандмауэры) или влияющие на безопасность информационной среды держателей карт;
- виртуализованные компоненты, такие как виртуальные машины, виртуальные коммутаторы и маршрутизаторы, виртуальные приложения/компьютеры и гипервизоры;
- сетевые компоненты, включая, помимо прочего, брандмауэры, коммутаторы, маршрутизаторы, беспроводные точки доступа, устройства сетевой безопасности и другие устройства безопасности;
- типы серверов включая, помимо прочего, веб-серверы, серверы приложений, серверы баз данных, серверы аутентификации, почтовые серверы, прокси-серверы, серверы протокола NTP (Network Time Protocol – протокола сетевого времени) и серверы DNS (Domain Name System – системы доменных имен);
- приложения, включая все приобретенные или самостоятельно разработанные приложения, в том числе внутренние и внешние (например, веб-приложения);
- любой компьютер или устройство, расположенное или подключенное к информационной среде держателей карт (CDE).

Первым этапом выполнения оценки соответствия требованиям PCI DSS должно быть определение области аудита. Как минимум один раз в год и перед каждой ежегодной оценкой соответствия оцениваемая организация должна проверять корректность определения области применения PCI DSS, идентифицируя все места хранения и потоки данных держателей карт и проверяя, все ли они включены в область применения PCI DSS. Для того чтобы проверить корректность области применения PCI DSS, следует выполнить следующие действия:

- оцениваемая организация идентифицирует и документирует присутствие всех данных держателей карт в своей инфраструктуре, чтобы убедиться в том, что данные держателей карт отсутствуют вне установленной на текущий момент информационной среды держателей карт;
- когда все места нахождения данных определены, организация использует эту информацию, чтобы убедиться в том, что область применения PCI DSS определена корректно (например, результаты могут быть представлены в виде схемы или перечня мест расположения данных);
- любые обнаруженные данные держателей карт входят в область проверки PCI DSS и в информационную среду держателей карт; в случае обнаружения данных, не входящих в информационную среду держателей карт, такие данные следует удалить надлежащим образом, переместить в установленную на данный момент информационную среду держателей карт или изменить толкование информационной среды держателей карт так, чтобы оно включало эти данные;

- организация сохраняет документы, описывающие процесс определения области проверки на соответствие требованиям PCI DSS; документы сохраняются для их проверки аудитором и (или) для использования в рамках следующей ежегодной оценки области проверки на соответствие требованиям PCI DSS.

При каждой проверке на соответствие требованиям PCI DSS аудитор должен подтвердить, что область проверки точно определена и документирована.

Сегментация сети (Network Segmentation)

Выделение среды обработки данных держателей карт в отдельный сегмент не является требованием PCI DSS. Однако сегментация рекомендована как средство, позволяющее уменьшить:

- область действия PCI DSS;
- затраты на оценку соответствия PCI DSS;
- стоимость и сложность реализации технических мер соответствия PCI DSS;
- риск для организации (за счет размещения данных в сегменте, которым легче управлять).

В случае отсутствия адекватной сегментации (т.н. "плоская сеть") под область действия PCI DSS попадает вся сеть. Сегментация сети может быть выполнена путем настройки межсетевых экранов, маршрутизаторов со списками контроля доступа или при помощи другой технологии, которая ограничивает доступ к определенному сегменту сети. Системные компоненты, не входящие в область проверки на соответствие требованиям PCI DSS, должны быть изолированы (сегментированы) от информационной среды держателей карт (CDE) так, чтобы даже в случае взлома таких компонентов это не повлияло бы на безопасность информационной среды держателей карт.

Важной предпосылкой к сокращению области среды данных держателей карт является понимание бизнес-потребностей и процессов, связанных с хранением, обработкой или передачей этих данных. Размещение этих данных в обособленном сегменте и удаление из него ненужной информации может потребовать пересмотра устоявшейся практики ведения бизнеса.

Визуализация потоков данных на диаграмме помогает изучить все потоки данных и демонстрирует, насколько эффективна сегментация при изолировании среды данных держателей карт.

Если сегментация сети используется для уменьшения области применения PCI DSS, аудитор должен удостовериться в том, что сегментация адекватно уменьшает область оценки. На высоком уровне адекватная сегментация сети изолирует системы, которые хранят, обрабатывают или передают данные держателей карт, от остальных систем. Адекватность реализации сегментации зависит от конфигурации сети, используемых технологий и других мер, которые могут быть реализованы.

Приложение D. "Сегментация и выборка бизнес-объектов и системных компонентов" содержит дополнительную информацию о влиянии сегментации и выборки на определение границ области оценки PCI DSS.

Беспроводные технологии

Если в организации используются беспроводные технологии для хранения, обработки или передачи данных держателей карт (например, применение беспроводных кассовых терминалов) или если беспроводная локальная сеть (WLAN) подключена или является частью информационной среды держателей карт, в силу вступают и должны быть выполнены требования и процедуры проведения проверки PCI DSS для беспроводных сред (например, требования 1.2.3, 2.1.1 и 4.1.1). Перед внедрением беспроводных технологий организация должна тщательно проанализировать необходимость их внедрения и оценить связанные с этим риски. Рекомендуется использовать беспроводные технологии только для передачи некритичных данных.

Привлечение сторонних поставщиков услуг (аутсорсинг)

Для тех поставщиков услуг, которым необходимо проходить ежегодную процедуру аудита на месте, оценка соответствия должна проводиться в отношении всех системных компонентов, которые входят в среду ДДК.

Поставщики услуг и торгово-сервисные предприятия могут воспользоваться услугами сторонних организаций по обработке, хранению и передаче данных держателей карт или управлению маршрутизаторами, межсетевыми экранами, серверами, системами физической безопасности. Однако это может оказать негативное влияние на безопасность данных держателей карт.

Стороны должны четко определить, какие службы и системные компоненты входят в область проверки поставщика услуг на соответствие требованиям PCI DSS, какие требования предъявляются к поставщику услуг, а какие – к клиентам поставщика услуг и должны быть отражены в отчете у них. Например, хостинг-провайдер должен четко указать, какие IP-адреса просканированы в рамках ежеквартального сканирования на наличие уязвимостей, и за какие адреса ответственны клиенты.

Поставщик услуг (третья сторона) может подтвердить соответствие требованиям двумя способами:

1) пройти оценку PCI DSS и представить доказательство соответствия своим клиентам, или
2) не проводить собственную оценку соответствия PCI DSS и предоставить возможность оценки своих услуг в ходе проверки соответствия каждого из своих клиентов.

Если третье лицо проводит собственную оценку соответствия стандарту PCI DSS, оно должно представить своим клиентам достаточные доказательства того, что область проверки поставщика услуг включает услуги, относящиеся к клиенту, и что соответствующие требования PCI DSS были изучены, а соответствие им – подтверждено. Конкретные виды доказательств, которые поставщик услуг должен предоставить своим клиентам, зависят от действующих соглашений/контрактов между этими сторонами. Например, свидетельство о соответствии требованиям и (или) соответствующие разделы отчета поставщика услуг о соответствии (отредактированного для защиты конфиденциальной информации) могут содержать всю или некоторую необходимую информацию.

Дополнительно торгово-сервисные предприятия и поставщики услуг должны контролировать статус соответствия PCI DSS всех сторонних организаций, которые имеют доступ к данным держателей карт. *Подробная информация приведена в требовании 12.8.*

Рекомендации по внедрению стандарта PCI DSS в традиционные бизнес-процессы

Чтобы гарантировать надлежащую реализацию механизмов обеспечения безопасности, стандарт PCI DSS должен быть внедрен в традиционные бизнес-процессы в рамках общей стратегии безопасности организации. Это позволит организации следить за эффективностью механизмов обеспечения безопасности на постоянной основе и обеспечивать соответствие стандарту PCI DSS между проверками на соответствие PCI DSS. Примеры внедрения PCI DSS в традиционные бизнес-процессы включают, помимо прочего:

1. мониторинг механизмов обеспечения безопасности (например, брандмауэры, системы обнаружения и предотвращения вторжений, мониторинг целостности файлов, антивирус, управление доступом и т.д.), чтобы гарантировать их эффективную и надлежащую работу;
2. своевременное обнаружение и реагирование на любые отказы механизмов обеспечения безопасности. Процессы реагирования на отказы механизмов обеспечения безопасности должны включать:
    - восстановление механизма обеспечения безопасности;
    - определение причины отказа;
    - определение и решение любых проблем с безопасностью, возникших во время отказа механизма обеспечения безопасности;
    - внедрение нового средства безопасности (например, процесса или технического механизма) во избежание повторного возникновения причины отказа;
    - возобновление мониторинга механизма безопасности, желательно с временным его усилением для проверки эффективности работы механизма;
3. оценка изменений окружения (например, добавление новых систем, внесение изменений в систему или конфигурацию сети) до окончательного внесения изменений, а также:
    - определение потенциального воздействия на область проверки PCI DSS (например, новое правило брандмауэра, разрешающее подключение между системой в информационной среде держателей карт и другой системой, может привести к включению других систем или сети в область проверки PCI DSS);
    - определение требований PCI DSS, применимых к системам и сетям, на которые распространяются изменения (например, если новая система входит в область проверки PCI DSS, ее необходимо настроить согласно стандартам системной конфигурации, включая мониторинг целостности файлов, антивирус, исправления безопасности, ведение журнала аудита и т.д., и включить в план ежеквартального сканирования на наличие уязвимостей);
    - обновление области проверки PCI DSS и внедрение необходимых механизмов обеспечения безопасности;
4. внесение изменений в организационную структуру (например, слияние или приобретение компаний) должно привести к официальной проверке изменений области проверки и требований PCI DSS.

5. Необходимо проводить регулярную оценку и опрос с целью подтверждения того, что требования PCI DSS выполняются, а сотрудники следуют процессам обеспечения безопасности. Такая регулярная оценка должна распространяться на все отделения и филиалы, в том числе торговые точки, центры обработки данных и т.д., и включать оценку системных компонентов (или их образцов) с целью подтверждения того, что требования PCI DSS выполняются (например, применены конфигурационные стандарты, используются последние исправления безопасности и версии антивирусных баз, проводится мониторинг журнала аудита и т.д.). Частота проведения регулярной оценки определяется организацией в зависимости от размера и сложности окружения.

   Оценка также может использоваться для проверки ведения учета соответствующих данных – например, журналов аудита, отчетов о результатах сканирования на наличие уязвимостей, журналов брандмауэра и т.д. – и облегчения подготовки организации к следующей оценке на соответствие требованиям.

6. Оценка аппаратных и программных технологий проводится не реже одного раза в год для подтверждения продолжения их технической поддержки поставщиком и соответствия требованиям организации к безопасности, включая PCI DSS. Если будет установлено, что технологии более не поддерживаются поставщиком или не соответствуют требованиям организации к безопасности, организация должна подготовить план решения проблемы, при необходимости включающий замену технологий.

Кроме вышеуказанных мер организациям также рекомендуется внедрить разделение обязанностей по обеспечению безопасности, чтобы сотрудники, обеспечивающие безопасность и (или) аудит, не участвовали в деятельности предприятия. В средах, где один сотрудник выполняет несколько обязанностей (например, администрирование и выполнение действий по обеспечению безопасности), обязанности могут быть распределены таким образом, чтобы ни один сотрудник не обладал полным контролем над процессом без независимого надзора. Например, ответственными за настройку и утверждение изменений можно назначить разных сотрудников.

Примечание. *Эти рекомендации по внедрению PCI DSS в традиционные бизнес-процессы предоставлены исключительно в консультативных целях и не заменяют и не дополняют какое-либо требование PCI DSS.*

Для аудиторов: выборочная оценка бизнес-объектов и системных компонентов

Выборочная оценка позволяет аудиторам ускорить процесс оценки при наличии большого количества бизнес-объектов и (или) системных компонентов.

Хотя аудитору разрешается проводить выборочную оценку бизнес-объектов и системных компонентов в рамках проверки на соответствие требованиям PCI DSS, организациям запрещается применять требования PCI DSS только к части окружения (например, требования о проведении ежеквартального сканирования на наличие уязвимостей распространяются на все системные компоненты). Аудитору также запрещается проводить проверку на соответствие только некоторым требованиям PCI DSS.

После рассмотрения общего масштаба и уровня сложности оцениваемой среды аудитор, выполняющий оценку соответствия организации требованиям PCI DSS, может выбрать несколько бизнес-объектов и системных компонентов для проверки. Размер выборки должен быть определен сначала для бизнес-объектов, а затем для системных компонентов внутри каждого из них. Выборка должна быть репрезентативной как для всех типов и местоположений бизнес-объектов, так и для типов системных компонентов внутри бизнес-объектов. Выборка должна быть достаточно обширной, чтобы аудитор мог удостовериться в выполнении всех требований.

Примеры бизнес-объектов включают, но не ограничиваются: офисами организации, магазинами, франчайзинговыми предприятиями, центрами обработки данных и другими объектами в разных местоположениях. Необходимо проверить на соответствие системные компоненты в каждом выбранном бизнес-объекте. Например, операционные системы, функции и приложения, в отношении которых может быть выполнена проверка.

Так, аудитор может определить, что выборка внутри бизнес-объекта включает в себя сервера Sun, на которых функционирует веб-сервер Apache, Windows-серверы, на которых функционирует СУБД Oracle, мейнфреймы, на которых функционируют устаревшие платежные приложения, серверы передачи данных под управлением HP-UX и Linux-серверы с MySQL. Если все приложения работают на базе одной операционной системы (например, Windows 7 или Solaris 10), проверке подлежат множество различных приложений (например, серверы базы данных, веб-серверы, серверы передачи данных).

При выборе бизнес-объектов и системных компонентов для оценки аудитор должен учесть следующее:

- при наличии стандартизированных по PCI DSS процессов и механизмов безопасности, которые должны соблюдаться всеми бизнес-объектами или системными компонентами, выборка может быть меньше, чем в случае отсутствия таких процессов и мер безопасности; выборка должна быть достаточно большой, чтобы аудитор мог быть уверен в том, что все бизнес-объекты и системные компоненты настроены и функционируют в соответствии со стандартными процессами; аудитор должен убедиться, что стандартизированные и централизованные механизмы безопасности внедрены и работают эффективно;
- в случае наличия более одного процесса (например, для разных типов бизнес-объектов/системных компонентов) выборка должна быть достаточно большой, чтобы включать объекты, привязанные к каждому процессу;
- в случае отсутствия стандартизированных процессов размер выборки должен быть достаточно большим, чтобы аудитор мог убедиться, что каждый бизнес-объект и системный компонент корректно понимает и выполняет требования PCI DSS;

- выборка системных компонентов должна включать каждый используемый тип и сочетание; например, выборка приложений должна включать все версии и платформы для каждого типа приложений.

Для каждого случая применения выборки аудитор должен:

- документировать обоснование примененного метода выборки и ее размера;
- документировать и утвердить стандартизованные процессы, рассматриваемые при определении размера выборки;
- объяснить, насколько сделанная выборка репрезентативна.

Также см.: Приложение D: "Сегментация и выборка бизнес-объектов и системных компонентов".

Аудитор должен проверять корректность выборки при каждом проведении оценки соответствия требованиям стандарта PCI DSS. При применении выборки в рамках каждой оценки должны выбираться разные бизнес-объекты и системные компоненты.

Компенсационные меры (Compensating Controls)

Все компенсационные меры должны быть ежегодно документированы, проанализированы и утверждены аудитором и включены в Отчет о соответствии согласно *Приложению B: "Компенсационные меры"* и *Приложению C: "Компенсационные меры – Форма для заполнения"*.

Для каждой компенсационной меры в обязательном порядке должна быть заполнена форма "Компенсационные меры" *(Приложение C)* . Кроме того, результаты компенсационных мер должны быть отражены в Отчете о соответствии в разделе соответствующего требования PCI DSS.

Подробнее о компенсационных мерах см. в *Приложении B* и *C*.

Инструкции по заполнению и требования к содержанию отчета о соответствии требованиям

Инструкции по заполнению и требования к содержанию отчета о соответствии требованиям теперь указаны в *бланке отчета о соответствии стандарту PCI DSS*.

Бланк отчета о соответствии стандарту PCI DSS следует использовать как шаблон для создания *отчета о соответствии требованиям*. Проверяемая организация должна выполнять требования каждой платежной системы по заполнению отчета для подтверждения статуса соответствия. За подробностями следует обращаться к представителям соответствующей платежной системы или эквайеру.

Процесс проведения проверки на соответствие стандарту PCI DSS

1. *Подтвердить область проверки на соответствие требованиям PCI DSS.*
2. *Провести проверку среды на соответствие PCI DSS, следуя процедурам проведения проверки на соответствие каждому требованию.*
3. *При необходимости восполнить все отсутствующие элементы.*
4. *Заполнить соответствующий отчет о проведении проверки (анкету самооценки* или отчет о соответствии требованиям), указав все компенсационные меры согласно применимым рекомендациям и инструкциям PCI.
5. *Заполнение Свидетельства о соответствии (Attestation of Compliance). Свидетельства о соответствии доступны на сайте PCI SSC.*
6. *Направление отчетного листа для самооценки или отчета о соответствии и Свидетельства о соответствии вместе со всей требуемой документацией – например, результатами ASV-сканирования – банку-эквайеру (для торгово-сервисных предприятий) или платежной системе, или другой уполномоченной организации (для поставщиков услуг).*

Детальные требования PCI DSS и процедуры проведения аудита

В приведенной ниже таблице требований и процедур оценки безопасности PCI DSS столбцы означают следующее.

- **Требования PCI DSS** – в данном столбце описываются требования стандарта безопасности данных; соответствие PCI DSS проверяется на базе этих требований.
- **Процедуры проведения тестирования** – в данном столбце описываются действия, которые должен выполнить аудитор для проверки выполнения требований PCI DSS (и наличия отметки "Выполнено").
- **Пояснение** – в данном столбце описывается назначение или функция безопасности каждого требования PCI DSS. В данном столбце описываются только рекомендации, что призвано помочь понять назначение каждого требования. Информация в этом столбце не заменяет и не дополняет требования и процедуры проведения тестирования PCI DSS.

Примечание. *Требования стандарта PCI DSS не считаются выполненными, если механизмы контроля не были внедрены либо запланированы на будущее. После того как все невыполненные требования будут выполнены организацией, аудитор должен убедиться, что проблемы устранены и все требования выполнены.*

Ознакомьтесь со следующими информационными материалами (доступными на веб-сайте PCI SSC), в которых описывается процедура документального оформления оценки PCI DSS.

- *См. инструкции по заполнению отчета о соответствии в* бланке отчета о соответствии стандарту PCI DSS.
- *См. инструкции и рекомендации по заполнению анкет самооценки в документе* "Инструкции и рекомендации по заполнению анкет самооценки соответствия стандарту PCI DSS".
- *См. инструкции по подаче отчета о соответствии стандарту PCI DSS в* свидетельствах о соответствии стандарту PCI DSS.

Построение и обслуживание защищенной сети и систем

Требование 1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

Межсетевые экраны – это средства вычислительной техники, контролирующие сетевой трафик между локальной сетью организации и внешней средой, а также между сегментами локальной сети разного уровня критичности. Среда данных держателей карт является примером области повышенной критичности внутри доверенной локальной сети организации.

Межсетевой экран анализирует проходящий через него трафик и блокирует соединения, которые не удовлетворяют определенным критериям безопасности.

Все системы должны быть защищены от неавторизованного доступа из недоверенных сетей, будь то подключение через Интернет систем электронной коммерции, доступ сотрудников к Интернету посредством браузеров, доступ сотрудников к электронной почте, выделенные подключения business-to-business, подключения по беспроводным сетям или иным технологиям. Зачастую кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – основные механизмы обеспечения безопасности любой компьютерной сети.

Иные системные компоненты могут использоваться для обеспечения функциональности брандмауэра, если они отвечают минимальным требованиям к брандмауэрам, приведенным в Требовании 1. Системные компоненты, использующиеся для обеспечения функциональности межсетевого экранирования внутри среды данных держателей карт, должны быть включены в определение и область действия Требования 1.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.1 Должны быть разработаны и внедрены стандарты конфигурации брандмауэров и маршрутизаторов, которые должны включать в себя следующее:	**1.1** изучение стандартов конфигурации брандмауэров и маршрутизаторов, а также иной нижеуказанной документации для проверки того, что стандарты включают в себя все необходимые требования и внедряются следующим образом.	Межсетевые экраны и маршрутизаторы – это ключевые компоненты архитектуры, которые используются для контроля входа в сеть и выхода из нее. Это программное обеспечение или оборудование, которое блокирует несанкционированный доступ к сети и управляет входом в сеть и выходом из нее. Стандарты и процедуры конфигурации помогают обеспечить надежную защиту данных.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.1.1 Формальный процесс утверждения и тестирования всех сетевых соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов.	**1.1.1.a** Ознакомиться с документированными процедурами и убедиться, что существует формальный процесс тестирования и утверждения всех: • сетевых соединений и • изменений в конфигурациях брандмауэров и маршрутизаторов.	Документированный и внедренный процесс утверждения и тестирования всех подключений и изменений брандмауэров и маршрутизаторов поможет не допустить возникновения проблем безопасности, связанных с неправильной настройкой сети, маршрутизатора или брандмауэра. Без формального утверждения и тестирования изменений записи об изменениях могут не обновляться, что может привести к несоответствию между сетевой документацией и реальной конфигурацией.
	1.1.1.b Для проведения выборочной проверки сетевых соединений следует опросить ответственных сотрудников и изучить записи, чтобы удостовериться, что сетевые соединения прошли утверждение и тестирование.	
	1.1.1.c Сделать выборку реальных изменений в конфигурации брандмауэра и маршрутизатора, сравнить их с записями об изменениях и опросить ответственных сотрудников, чтобы удостовериться, что изменения прошли утверждение и тестирование.	
1.1.2 Актуальная схема сети с указанием всех подключений к среде данных держателей карт из других сетей, включая все беспроводные сети	**1.1.2.a** Изучить схему (схемы) и конфигурации сети и проверить наличие актуальной схемы сети, а также то, что в схеме отмечены все подключения к данным держателей карт, в том числе беспроводные.	Схемы сети описывают конфигурацию сети и расположение всех сетевых устройств. Без актуальной схемы сети устройства могут быть проигнорированы при внедрении стандарта PCI DSS, и на них не будут распространяться меры безопасности, что сделает их уязвимыми к взлому.
	1.1.2.b Опросить ответственных сотрудников, чтобы проверить актуальность схемы сети.	
1.1.3 Актуальная схема, отображающая потоки данных держателей карт во всех системах и сетях	**1.1.3** Изучить схему потоков данных и опросить сотрудников, чтобы убедиться, что схема соответствует следующим требованиям: • отображение потоков данных держателей карт во всех системах и сетях; • актуальность и обновление в случае внесения изменений в среду данных держателей карт.	на схемах потоков данных держателей карт указано расположение всех данных держателей карт, которые хранятся, обрабатываются или передаются внутри сети. Схемы сети и потоков данных держателей карт помогают организации получить представление об области среды данных и отслеживать ее путем

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
		сопоставления потока данных держателей карт по всей сети и между отдельными системами и устройствами.
1.1.4 Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью организации	**1.1.4.a** Проверить стандарты конфигурации брандмауэра на наличие требований о необходимости межсетевого экранирования каждого Интернет-соединения, а также между демилитаризованной зоной (DMZ) и внутренней сетью.	Использование брандмауэра на каждом входящем и исходящем подключении, а также между демилитаризованной зоной (DMZ) и внутренней сетью позволяет организации отслеживать и контролировать доступ и свести к минимуму шансы злоумышленников на получение доступа к внутренней сети через незащищенное соединение.
	1.1.4.b Убедиться, что стандарты конфигурации брандмауэра не противоречат схеме сети.	
	1.1.4.c Изучить конфигурации сети для проверки наличия межсетевого экранирования каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью согласно документированным стандартам конфигурации и схемам сети.	
1.1.5 Описание групп, ролей и обязанностей по управлению сетевыми компонентами	**1.1.5.a** Убедиться, что стандарты конфигурации брандмауэров и маршрутизаторов содержат описание ролей, групп и обязанностей по управлению сетевыми компонентами.	Описание ролей и определение сфер ответственности гарантирует осведомленность персонала о том, кто отвечает за безопасность всех компонентов сети, и осведомленность лиц, ответственных за управление компонентами, о своих обязанностях. Без формального назначения ролей и обязанностей можно потерять контроль над устройствами.
	1.1.5.b Опросить сотрудников, ответственных за управление компонентами сети, чтобы подтвердить, что роли и обязанности назначены в соответствии с документацией.	
1.1.6 Обоснованный документированный перечень всех разрешенных для использования сервисов, протоколов и портов, необходимых для работы бизнес-приложений, включающий документальное описание внедренных механизмов защиты небезопасных протоколов. Примеры небезопасных сервисов, протоколов или портов включают,	**1.1.6.a** Убедиться, что стандарты конфигурации брандмауэров и маршрутизаторов содержат документированный перечень всех служб, протоколов и портов и обоснование коммерческой необходимости для каждого из них (например, HTTP, SSL, SSH, VPN).	Взлом часто происходит из-за наличия неиспользуемых и небезопасных служб и портов, поскольку они часто содержат известные уязвимости, и многие организации не устанавливают исправления уязвимостей для служб, протоколов и портов, которые они не используют (даже при наличии уязвимостей). Четкое определение и документальное оформление служб, протоколов и портов, необходимых для осуществления деятельности,
	1.1.6.b Выявить разрешенные небезопасные сервисы, протоколы и порты и проверить документальное оформление механизмов защиты для каждой службы.	
	1.1.6.c Изучить конфигурацию брандмауэров и маршрутизаторов и убедиться, что механизмы защиты документированы и внедрены	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
помимо прочих, FTP, Telnet, POP3, IMAP и SNMP версии 1 и 2.	для каждой небезопасной службы, протокола и порта.	позволяет организациям обеспечить отключение или удаление всех остальных служб, протоколов и портов. Если небезопасные службы, протоколы или порты необходимы для ведения бизнеса, нужно четко понимать риск, связанный с их использованием, обосновать необходимость их использования, а также задокументировать и внедрить механизмы защиты, которые позволят безопасно использовать эти протоколы. Если эти небезопасные службы, протоколы и порты не являются необходимыми для ведения бизнеса, их следует отключить или удалить.
1.1.7 Требование пересмотра наборов правил брандмауэров и маршрутизаторов не реже одного раза в полгода	**1.1.7.a** Убедиться, что стандарты конфигурации брандмауэров и маршрутизаторов требуют пересмотра наборов правил как минимум раз в полгода. **1.1.7.b** Проверить документацию, относящуюся к пересмотру наборов правил и опросить ответственных сотрудников, чтобы убедиться, что наборы правил пересматриваются как минимум раз в полгода.	Пересмотр наборов правил дает организации возможность ежеквартального удаления всех ненужных, устаревших или некорректных правил и гарантирует, что все наборы правил разрешают доступ только авторизованным службам и портам, которые соответствуют документированному коммерческому обоснованию. Организациям, часто изменяющим большие наборы правил брандмауэров и маршрутизаторов, рекомендуется проводить пересмотр чаще, чтобы гарантировать, что наборы правил все еще соответствуют требованиям бизнеса.
1.2 Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в	**1.2** Изучить конфигурацию брандмауэров и маршрутизаторов, убедиться, что соединения между незащищенными сетями и системными компонентами, находящимися в среде данных держателей карт, ограничены.	Важно обеспечить защиту сети между внутренней защищенной сетью и любыми незащищенными внешними сетями или сетями, которые не находятся под контролем организации;

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
среде данных держателей карт. ***Примечание.*** *Недоверенной является любая сеть, внешняя по отношению к сетям, принадлежащим проверяемой организации и (или) сеть, которая не контролируется проверяемой организацией.*		при несоблюдении данной меры организация будет подвержена риску несанкционированного доступа злоумышленников или вредоносного программного обеспечения к данным; для обеспечения эффективности брандмауэра он должен иметь соответствующие конфигурации, которые позволяют контролировать и (или) ограничивать входящий и исходящий трафик в сети организации.
1.2.1 Входящий и исходящий трафик должен быть ограничен только соединениями, необходимыми для информационной среды держателей карт, а весь остальной трафик должен быть запрещен.	**1.2.1.a** Проверить, что в стандартной конфигурации брандмауэра и маршрутизатора указан входящий и исходящий трафик, необходимый для информационной среды держателей карт.	Это требование направлено на предотвращение доступа злоумышленников к сети организации через неавторизованные IP-адреса или использования служб, протоколов и портов несанкционированным образом (например, для отправки данных, которые они получили из вашей сети на недоверенный сервер). Установка запрета на весь входящий и исходящий трафик, кроме необходимого, помогает предотвратить проникновение несанкционированного и потенциально вредоносного трафика через неочевидные бреши в системе безопасности.
	1.2.1.b Убедиться, что в конфигурации брандмауэра и маршрутизатора разрешен только входящий и исходящий трафик, необходимый для среды данных держателей карт.	
	1.2.1.c Убедиться, что весь прочий входящий и исходящий трафик явно запрещен, например, путем явного запрета "deny all" или неявного запрета по умолчанию после разрешающих правил.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.2.2 Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов маршрутизаторов.	**1.2.2.a** Убедиться, что конфигурационные файлы маршрутизаторов защищены от несанкционированного доступа. **1.2.2.b** Убедиться, что конфигурации маршрутизаторов синхронизированы, например, рабочая (или активная) конфигурация и стартовая конфигурация (используемая при загрузке устройств) совпадают.	Хотя рабочие (или активные) конфигурационные файлы обычно включают текущие безопасные настройки, в файлах стартовой конфигурации (используемых маршрутизаторами при перезапуске или загрузке) необходимо вручную указать те же безопасные настройки для их применения при каждом перезапуске. Поскольку они выполняются только время от времени, о файлах стартовой конфигурации часто забывают и не обновляют их. Если маршрутизатор выполняет перезапуск и загружает стартовую конфигурацию без использования рабочих настроек безопасности, этим могут воспользоваться злоумышленники для проникновения в сеть.
1.2.3 Установить брандмауэры между каждой беспроводной сетью и информационной средой держателей карт и настроить их на блокирование любого трафика из беспроводной сети либо разрешение только авторизованного трафика между беспроводной сетью и информационной средой данных держателей карт в том случае, если такой трафик необходим в целях совершения операций.	**1.2.3.a** Изучить конфигурации брандмауэров и маршрутизаторов и убедиться, что брандмауэры установлены между каждой беспроводной сетью и информационной средой держателей карт. **1.2.3.b** Убедиться, что брандмауэры настроены на блокирование любого трафика из беспроводной сети, либо разрешение только авторизованного трафика между беспроводной сетью и информационной средой держателей карт в том случае, если такой трафик необходим в целях совершения операций.	Злоумышленники часто используют уязвимости беспроводных технологий для получения доступа к сети и данным о держателях карт. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может просто и незаметно проникнуть в сеть. 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. Межсетевые экраны должны быть установлены между всеми

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
		беспроводными сетями и CDE независимо от назначения среды, к которой подключена беспроводная сеть. Помимо прочего, это могут быть корпоративные сети, розничные магазины, гостевые сети, склады и т.д.
1.3 Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом информационной среды держателей карт**.**	**1.3** Проверить конфигурацию брандмауэров и маршрутизаторов, включая, помимо прочего, маршрутизатор на границе с сетью Интернет, маршрутизатор и брандмауэр демилитаризованной зоны (DMZ), сегмент DMZ, пограничный маршрутизатор и внутренний сегмент сети данных держателей карт, чтобы убедиться в отсутствии прямого доступа из сети Интернет к системным компонентам внутреннего сегмента сети данных держателей карт.	Назначение брандмауэра состоит в управлении и контроле всех соединений между общедоступными системами и внутренними системами, особенно теми, которые используются для хранения, обработки или передачи данных держателей карт. Если разрешен прямой доступ между общедоступными системами и средой данных о держателях карт, межсетевой экран удается обойти, и системные компоненты, которые используются для хранения данных о держателях карт, становятся уязвимыми для злоумышленников.
1.3.1 Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным сервисам, протоколам и портам.	**1.3.1** Проверить конфигурации брандмауэров и маршрутизаторов и убедиться, что демилитаризованная зона (DMZ) применяется для ограничения входящего и исходящего трафика только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным службам, протоколам и портам.	Демилитаризованная зона (DMZ) – это часть сети, которая управляет соединениями между сетью Интернет (или другими недоверенными сетями) и общедоступными службами (такими как веб-сервер). Эта функция позволяет предотвратить доступ злоумышленников к внутренней сети организации из Интернета и использование служб, протоколов или портов несанкционированным образом.
1.3.2 Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.	**1.3.2** Убедиться, что входящие Интернет-соединения в конфигурации брандмауэра и маршрутизатора ограничены только IP-адресами, находящимися в демилитаризованной зоне (DMZ).	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.3.3 Должны быть запрещены любые прямые входящие или исходящие соединения между сетью Интернет и средой данных о держателях карт.	**1.3.3** Убедиться, что в конфигурации брандмауэров и маршрутизаторов запрещены прямые входящие и исходящие соединения между сетью Интернет и информационной средой держателей карт.	Изучение всех входящих и исходящих соединений обеспечивает возможность проверки и ограничения трафика по источнику и (или) назначению, а также проверки и блокирования нежелательного содержимого, что позволяет предотвратить несанкционированное соединение между недоверенными и доверенными средами. Это помогает предотвратить отправку данных злоумышленниками, которые они получили из вашей сети, на внешний недоверенный сервер в недоверенной сети.
1.3.4 Примите меры по противодействию подмене IP-адреса, позволяющие определить фальшивые исходные IP-адреса и заблокировать им доступ в сеть (например, заблокировать Интернет-трафик с внутренним исходным адресом).	**1.3.4** Изучить конфигурации брандмауэров и маршрутизаторов и проверить наличие мер по противодействию подмене IP-адреса (например, пакеты с внутренними адресами не могут достигнуть демилитаризованной зоны (DMZ) от источника из сети Интернет).	Обычно пакет содержит IP-адрес компьютера, который его отправил. Это позволяет другим компьютерам в сети узнать, откуда был отправлен пакет. Злоумышленники часто пытаются подменить (или имитировать) IP-адрес отправителя, чтобы система-получатель сочла, что пакет пришел из доверенного источника. Фильтрация входящего трафика позволяет, помимо прочего, предотвратить подмену IP-адресов (имитацию для пакета адреса внутренней сети организации).
1.3.5 Необходимо запретить неавторизованный исходящий трафик из среды данных держателей карт в сеть Интернет.	**1.3.5** Изучить конфигурации брандмауэров и маршрутизаторов и убедиться, что весь исходящий трафик из информационной среды держателей карт в сеть Интернет явно санкционирован.	Весь трафик, исходящий из среды данных держателей карт, следует оценить на соответствие установленным правилам. Необходимо проверить соединения, чтобы ограничить трафик только авторизованными соединениями (например, посредством ограничения исходных/целевых адресов или портов и (или) блокирования содержимого).

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.3.6 Необходимо включить динамическую пакетную фильтрацию с сохранением состояния (разрешение прохождения пакетов только для установленных соединений).	**1.3.6** Изучить конфигурации брандмауэров и маршрутизаторов и убедиться, что брандмауэры осуществляют проверку состояния соединения (динамическую фильтрацию пакетов) (должны быть разрешены прохождения пакетов только для установленных соединений и только в пределах предварительно установленного сеанса).	Брандмауэр, который выполняет динамическую фильтрацию пакетов, хранит информацию о состоянии каждого соединения. Благодаря сохранению информации о состоянии брандмауэр знает, являются ли пакеты, которые выглядят как ответ на предыдущее соединение, действительным авторизованным ответом (поскольку он хранит информацию о состоянии каждого соединения) или же это попытка обойти брандмауэр, чтобы он разрешил соединение.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
1.3.7 Необходимо размещать системные компоненты (например, базы данных), в которых хранятся данные держателей карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей.	**1.3.7** Изучить конфигурации брандмауэров и маршрутизаторов и убедиться, что системные компоненты, в которых хранятся данные держателей карт, располагаются во внутренней сети, отделенной от демилитаризованной зоны (DMZ) и иных недоверенных сетей.	Если данные расположены в DMZ, задача получения доступа к этой информации для злоумышленника упрощается, поскольку ему нужно будет преодолеть меньшее количество уровней защиты. Размещение системных компонентов, в которых хранятся данные держателей карт, во внутренней сети, отделенной от демилитаризованной зоны (DMZ) и иных недоверенных сетей брандмауэром, не позволит неавторизованному сетевому трафику дойти до системного компонента. ***Примечание.*** *Это требование не распространяется на временное хранение данных держателей карт в энергозависимой памяти.*
1.3.8 Должно быть запрещено раскрытие частных IP-адресов и данных о маршрутах третьим сторонам, не имеющим авторизованного доступа. ***Примечание.*** *Методы сокрытия IP-адресации включают, но не ограничиваются:* • *технология Network Address Translation (NAT);* • *расположение серверов, содержащих данные держателей карт за прокси-серверами/брандмауэрами;*	**1.3.8.a** Изучить конфигурации брандмауэров и маршрутизаторов и убедиться, что применяются методы, обеспечивающие предотвращение раскрытия частных IP-адресов и перенаправления данных из внутренней сети в сеть Интернет.	Запрет передачи внутренних или частных IP-адресов является действенным способом предотвращения получения злоумышленником информации об IP-адресе внутренней сети и использования им этой информации для проникновения в сеть. Средства, используемые для соблюдения этого требования, зависят от используемой сетевой технологии. Например, средства контроля могут быть разными для сетей IPv4 и сетей IPv6.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
• *удаление или фильтрация объявлений маршрутов для частных сетей, требующих зарегистрированной адресации;* • *внутреннее использование адресного пространства RFC1918 вместо зарегистрированных адресов.*	**1.3.8.b** Опросить сотрудников и изучить документацию, чтобы убедиться в отсутствии неавторизованного раскрытия частных IP-адресов и перенаправления данных внешним сторонам.	
1.4 Установить персональные брандмауэры на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети. Требования к конфигурации брандмауэров: • определены конкретные настройки конфигурации для персональных брандмауэров; • персональные брандмауэры активно работают; • настройки персональных брандмауэров не могут быть изменены пользователями мобильных и (или) принадлежащих сотрудникам компьютеров.	**1.4.a** Изучить политики и стандартные конфигурации и убедиться, что: • требуется установка персональных брандмауэров на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети из внешних сетей; • определены конкретные настройки конфигурации для персональных брандмауэров; • персональные брандмауэры настроены на активную работу; • настройки персональных брандмауэров не могут быть изменены пользователями мобильных и (или) принадлежащих сотрудникам компьютеров. **1.4.b** Провести выборочную проверку мобильных устройств и (или) устройств, принадлежащих сотрудникам, и убедиться, что: • персональные брандмауэры установлены и настроены согласно конкретным конфигурационным настройкам организации; • персональные брандмауэры активно работают; • настройки персональных брандмауэров не могут быть изменены пользователями мобильных и (или) принадлежащих сотрудникам компьютеров.	Мобильные устройства с прямым доступом в Интернет вне зоны действия защиты брандмауэра компании более уязвимы перед веб-угрозами. Использование персонального брандмауэра помогает защитить устройства от веб-атак с целью получения доступа к системам и данным организации после повторного подключения устройства к сети. Конкретные настройки конфигурации для персональных брандмауэров определяются организацией. ***Примечание.*** *Это требование применяется к компьютерам, принадлежащим сотрудникам или компании. Системы, которыми невозможно управлять с помощью корпоративных процедур, создают уязвимости периметра сети, которыми могут воспользоваться злоумышленники. Разрешение недоверенных подключений к сети организации может привести к предоставлению доступа хакерам и другим злоумышленникам.*
1.5 Убедиться, что политики безопасности и процедуры управления брандмауэрами по умолчанию документированы,	**1.5** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры управления брандмауэрами:	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения постоянного контроля над

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
используются и известны всем заинтересованным лицам.	• документированы; • используются; • известны всем заинтересованным лицам.	брандмауэрами с целью предотвращения несанкционированного доступа к сети.

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

Злоумышленники (внешние и внутренние) при атаке на систему часто пробуют использовать пароли и иные параметры, заданные производителем по умолчанию. Эти пароли хорошо известны, и их легко получить из открытых источников информации.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
2.1 Всегда изменяйте значения параметров и пароли, заданные поставщиками по умолчанию, и отключайте или удаляйте учетные записи по умолчанию **перед** подключением систем к сети. Это требование относится ко ВСЕМ паролям по умолчанию, включая, в том числе, пароли к операционным системам, программам защиты, приложениям и системным учетным записям, *кассовым (*в точках продаж*)* терминалам, а также строки доступа SNMP и т.д.	**2.1.a** Сделать выборку системных компонентов и с помощью системного администратора попытаться осуществить вход в устройства и приложения, используя аутентификационные данные, устанавливаемые поставщиком по умолчанию, чтобы убедиться, что ВСЕ установленные поставщиком пароли (включая пароли к операционным системам, программам защиты, приложениям и системным учетным записям, кассовым (в точках продаж) терминалам и строки доступа SNMP) были изменены (следует использовать руководства пользователя и Интернет-ресурсы, чтобы узнать аутентификационные данные, устанавливаемые поставщиком по умолчанию).	Злоумышленники (находящиеся внутри и вне организации) часто используют настройки, учетные записи и пароли, заданные по умолчанию, для получения доступа к операционным системам, приложениям и устройствам, на которых они установлены. Поскольку эти стандартные настройки хорошо известны и часто публикуются в хакерских сообществах, их изменение сделает вашу систему менее уязвимой для злоумышленников. Даже если учетная запись по умолчанию не предназначена для использования, изменение пароля по умолчанию на надежный уникальный пароль и последующее отключение учетной записи не позволит злоумышленнику повторно включить ее и получить доступ с помощью пароля по умолчанию.
	2.1.b При выборочной проверке системных компонентов следует убедиться, что все ненужные учетные записи по умолчанию (включая учетные записи к операционным системам, программам защиты, приложениям, устройствам, кассовым (в точках продаж) терминалам, а также строки доступа SNMP и т.д.) были удалены или отключены.	
	2.1.c Опросить сотрудников и изучить сопроводительную документацию для подтверждения того, что: • все учетные данные по умолчанию, предоставленные поставщиком (включая пароли по умолчанию к операционным системам, программам защиты, приложениям и системным учетным записям, кассовым (в точках продаж) терминалам, а также строки доступа SNMP и т.д.) изменяются перед подключением систем к сети; • ненужные учетные записи, настроенные по умолчанию, (включая учетные записи к операционным системам, программам защиты, приложениям, устройствам, кассовым (в точках продаж) терминалам, строки доступа SNMP и т.д.) удаляются или отключаются перед подключением систем к сети.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
2.1.1 Для беспроводных сетей, подключенных к информационной среде держателей карт либо передающих данные держателей карт, необходимо изменить ВСЕ параметры по умолчанию, установленные поставщиком, включая, помимо прочего, ключи шифрования для беспроводного доступа, пароли, строки доступа SNMP.	**2.1.1.a** Опросить ответственных сотрудников и изучить сопроводительную документацию для подтверждения того, что: • установленные по умолчанию ключи шифрования были изменены при установке; • ключи шифрования изменяются всякий раз, когда какое-либо лицо, обладающее данными о ключах, уходит из компании либо переходит на другую должность.	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. Кроме того, протокол обмена ключами для ранних версий протокола шифрования 802.11x (Wired Equivalent Privacy, WEP) был взломан и стал сейчас бесполезным для защиты. Микропрограммное обеспечение для устройств следует обновить для поддержки более защищенных протоколов.
	2.1.1.b Опросить сотрудников и изучить политики и процедуры для подтверждения того, что: • при установке по умолчанию требуется изменение строк доступа SNMP; • при установке по умолчанию требуется изменение паролей/кодовых фраз к точкам доступа.	
	2.1.1.c Изучить документацию поставщика и выполнить вход на беспроводные устройства при содействии системного администратора для подтверждения того, что: • строки доступа SNMP по умолчанию не используются; • пароли/кодовые фразы к точкам доступа по умолчанию не используются.	
	2.1.1.d Изучить документацию поставщика и настройки беспроводной конфигурации, чтобы убедиться, что программное обеспечение беспроводных устройств обновлено до актуальной версии и поддерживает стойкие криптографические алгоритмы для: • аутентификации по беспроводной сети; • передачи данных по беспроводной сети.	
	2.1.1.e Изучить документацию поставщика и настройки беспроводной конфигурации, чтобы убедиться, что прочие настройки безопасности беспроводных устройств, установленные поставщиком по умолчанию, были изменены, если применимо.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
2.2 Должны быть разработаны стандарты конфигурации для всех системных компонентов. Стандарты должны учитывать все известные проблемы безопасности, а также положения общепринятых отраслевых стандартов в области безопасности. Примеры источников общепринятых отраслевых стандартов в области безопасности включают, но не ограничиваются: • Центр Интернет-безопасности (CIS); • Международная организация по стандартизации (ISO); • Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS); • Национальный институт стандартов и технологий.	**2.2.a** Изучить стандарты системных конфигураций всех системных компонентов. Убедиться, что стандарты конфигурации учитывают положения общепринятых отраслевых стандартов. **2.2.b** Изучить политики и опросить сотрудников для подтверждения того, что стандарты системной конфигурации обновляются по мере обнаружения новых угроз безопасности, как описывается в требовании 6.1. **2.2.c** Изучить политики и опросить сотрудников для подтверждения того, что стандарты системной конфигурации применяются при настройке новых систем и проверяются перед подключением системы к сети. **2.2.d** Проверить стандарты системной конфигурации на наличие следующих процедур для всех типов системных компонентов: • изменение всех параметров, заданных поставщиками, и удаление ненужных учетных записей по умолчанию; • каждый сервер должен выполнять одну основную функцию, поскольку необходимо исключить совмещение на одном и том же сервере функций, требующих различных уровней защиты; • должны быть включены только необходимые службы, протоколы, управляющие программы и т.д., требующиеся для функционирования системы; • необходимо настроить параметры безопасности для всех указанных служб, протоколов и управляющих программ, которые могут быть небезопасными; • следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы; • из системы должен быть удален весь неиспользуемый функционал: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.	У многих операционных систем, баз данных и корпоративных приложений существуют известные уязвимости, а также известные способы настройки данных систем для устранения этих уязвимостей. Чтобы помочь лицам, которые не являются экспертами в области безопасности, многие организации, специализирующиеся на защите информации, предоставляют рекомендации по повышению уровня безопасности и устранению уязвимостей. Вот некоторые из источников, где вы можете найти рекомендации по стандартам конфигурации: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org, а также веб-сайты поставщиков изделий. Стандарты системной конфигурации должны быть актуальными, чтобы обеспечить устранение вновь обнаруженных слабых мест в системе безопасности до подключения системы к сети.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
2.2.1 Каждый сервер должен выполнять одну основную функцию, поскольку необходимо исключить совмещение на одном и том же сервере функций, требующих различных уровней защиты (например, веб-серверы, серверы СУБД и DNS-серверы следует размещать на разных компьютерах). ***Примечание.*** *При использовании технологии виртуализации необходимо внедрять только одну основную функцию для каждого виртуального системного компонента.*	**2.2.1.a** Сделать выборку системных компонентов, проверить системные конфигурации и убедиться, что выполняется правило "одна основная функция – один сервер". **2.2.1.b** При использовании технологии виртуализации необходимо изучить системные конфигурации и убедиться, что выполняется правило "одна основная функция – один виртуальный системный компонент или устройство".	Если функции, для которых необходим разный уровень безопасности, расположены на одном сервере, уровень безопасности функций с более высокими требованиями к безопасности будет понижен. Кроме того, функции с более низким уровнем безопасности могут создавать угрозы для безопасности других функций того же сервера. Учет требований к безопасности разных функций сервера в стандартах конфигурирования системы и процессах позволяет предотвратить наличие функций с разным уровнем безопасности на одном сервере.
2.2.2 Должны быть включены только необходимые службы, протоколы, управляющие программы и т.д., требующиеся для функционирования системы.	**2.2.2.a** Сделать выборку системных компонентов, проверить включенные службы, управляющие программы и протоколы, и убедиться, что включены только необходимые службы и протоколы. **2.2.2.b** Выявить включенные незащищенные службы, управляющие программы и протоколы, и опросить персонал для подтверждения того, что их использование оправданно согласно документированным стандартам конфигурации.	Как указано в требовании 1.1.6, существует много служб, протоколов или портов, которые необходимы для ведения бизнеса (или включены по умолчанию) и которые часто используются злоумышленниками для компрометации сети. Это требование должно быть частью стандартов конфигурирования систем и связанных процессов организации для обеспечения того, что включены только необходимые службы и протоколы.
2.2.3 Необходимо обеспечить дополнительные механизмы защиты для всех необходимых служб, протоколов и управляющих программ, которые могут быть небезопасными. Например, следует использовать такие технологии защиты, как SSH, S-FTP, SSL или IPSec VPN для защиты таких незащищенных сервисов как NetBIOS,	**2.2.3** Изучить стандарты конфигурации и убедиться, что механизмы защиты для каждой небезопасной службы, управляющей программы и протокола документированы и внедрены.	Включение механизмов защиты до развертывания новых серверов позволит предотвратить установку серверов в среду с небезопасной конфигурацией. Обеспечение надлежащих механизмов защиты для всех небезопасных служб, протоколов и управляющих программ затруднит злоумышленникам использование распространенных уязвимостей в сети.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
совместное использование файлов, Telnet, FTP и т.д.		
2.2.4 Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.	**2.2.4.a** Опросить системных администраторов и (или) администраторов по безопасности с целью проверки того, что им известны настройки основных параметров защиты системных компонентов.	Стандарты конфигурирования систем и связанные с этим процессы должны предусматривать применение настроек и параметров безопасности с известными последствиями для каждого используемого типа системы. *(Продолжение на следующей странице)*
	2.2.4.b Изучить стандарты конфигурации системы и убедиться, что они включают основные параметры безопасности.	
	2.2.4.c Сделать выборку системных компонентов и убедиться, что основные параметры безопасности установлены соответствующим образом и согласно стандартам конфигурации.	Для обеспечения безопасности системной конфигурации сотрудники, ответственные за настройку и (или) администрирование системных компонентов, должны быть осведомлены о конкретных параметрах безопасности и настройках, применимых к системе.
2.2.5 Из системы должен быть удален весь неиспользуемый функционал: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, не нужные для работы веб-серверы.	**2.2.5.a** Сделать выборку системных компонентов, изучить конфигурации и убедиться, что неиспользуемый функционал (например, сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы и т.д.) удален.	Ненужные функции могут облегчить злоумышленникам взлом системы. Избавление от ненужного функционала позволит организации сконцентрироваться на защите нужных функций и снизить риск использования неизвестных функций злоумышленниками. Включение в стандарты и процессы повышения защищенности серверов избавление от ненужного функционала (например, удаление/отключение FTP или веб-сервера, если сервер не будет выполнять свои функции) позволит устранить риски для безопасности, связанные с ненужными функциями.
	2.2.5.b. Изучить документацию и параметры безопасности и проверить, что включенные функции документированы и поддерживают безопасную конфигурацию.	
	2.2.5.c Изучить документацию и параметры безопасности и убедиться, что в выборке системных компонентов присутствует только документированная функциональность.	
2.3 При использовании неконсольного административного доступа к системе следует всегда шифровать канал с	**2.3** Сделать выборку системных компонентов, изучить конфигурации и убедиться, что канал неконсольного административного доступа зашифрован следующим образом.	Если при неконсольном (включая удаленное) администрировании не используются безопасная аутентификация и шифрование, существует возможность перехвата
	2.3.a Наблюдать за входом администратора в каждую систему	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
использованием стойких криптографических алгоритмов. Следует использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа.	и изучить системные конфигурации для того, чтобы подтвердить активизацию механизмов шифрования до запроса пароля администратора.	злоумышленником конфиденциальной информации (например, имен и паролей администратора). Эту информацию злоумышленник может использовать для проникновения в сеть, получения прав администратора и кражи данных. Открытые протоколы (например, HTTP, Telnet и т.д.) не используют шифрование трафика или учетных данных, упрощая перехват этой информации злоумышленником. Чтобы криптографический алгоритм считался стойким, он должен использовать зарекомендовавшие себя протоколы с соответствующей стойкостью ключей и возможностью управления ключами в зависимости от используемого типа технологии (см. определение термина "стойкий криптографический алгоритм" в документе *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения*).
	2.3.b Проверить сервисы и файлы параметров на системах и убедиться, что Telnet и другие небезопасные протоколы удаленного доступа к системе не доступны для неконсольного доступа.	
	2.3.c Просмотреть административный журнал на каждой системе и убедиться, что административный доступ к веб-системам управления подвергается шифрованию с использованием стойких криптографических алгоритмов.	
	2.3.d Ознакомиться с документацией поставщика и убедиться, что используются надежные криптографические алгоритмы в соответствии с последними отраслевыми стандартами и (или) рекомендациями поставщиков.	
2.4 Вести учет системных компонентов, на которые распространяется действие стандарта PCI DSS.	**2.4.a** Проверить системный журнал учета на наличие списка программных и аппаратных компонентов и описания функции/применения для каждого из них.	Наличие текущего списка системных компонентов позволяет организации точно и эффективно определить область внедрения механизмов контроля PCI DSS. Без журнала учета есть риск того, что некоторые системные компоненты будут забыты или случайно исключены из конфигурационных стандартов организации.
	2.4.b Опросить сотрудников для подтверждения того, что журнал учета регулярно обновляется.	
2.5 Убедиться, что политики безопасности, процедуры управления учетными данными поставщиков по умолчанию и другие параметры безопасности документированы, используются и известны всем заинтересованным лицам.	**2.5** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности, процедуры управления учетными данными поставщиков по умолчанию и другие параметры безопасности: • документированы; • используются; • известны всем заинтересованным лицам.	Сотрудники должны быть ознакомлены со следующими политиками безопасности и повседневными рабочими процедурами, чтобы гарантировать постоянный контроль над учетными данными поставщиков, настроенными по умолчанию, и другими параметрами безопасности и предотвратить ненадежные конфигурации.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
2.6 Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным *в Приложении A: "Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)".*	**2.6** Выполните процедуры проведения тестирования **A.1.1**–**A.1.4**, описанные в *Приложении A: "Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)"* для оценки того, обеспечивают ли провайдеры защиту среды и данных для каждой из обслуживаемых сторон (торгово-сервисные предприятия и поставщики услуг).	Данное требование предназначено для хостинг-провайдеров, которые предоставляют общую среду размещения данных для нескольких клиентов на одном и том же сервере. Когда все данные находятся на одном и том же сервере и управление ими осуществляется из единой среды, отдельные клиенты обычно не управляют настройками этих совместно используемых серверов. Добавление клиентами небезопасных функций и скриптов влияет на защищенность данных всех других сред клиента. Поэтому злоумышленник может, получив доступ к данным одного клиента, без труда получить доступ к данным других клиентов. См. подробные сведения о требованиях в *Приложении A*.

Защита данных держателей карт

Требование 3. Обеспечить безопасное хранение данных держателей карт

Методы защиты данных, такие как шифрование, усечение, маскирование и хеширование, являются критичными компонентами защиты данных держателей карт. Если взломщик обойдет остальные средства управления безопасностью сети и получит доступ к зашифрованным данным, не зная ключа шифрования, то эти данные останутся для него нечитаемыми и практически бесполезными. Иные способы защиты хранимых данных должны рассматриваться как средства уменьшения риска. Методы минимизации риска включают в себя запрет сохранения данных держателей карт, кроме случаев крайней необходимости, хранение обрезанного PAN, если не требуется хранение полного PAN, и избежание пересылки PAN с использованием пользовательских технологий передачи сообщений, таких как электронная почта и системы мгновенной отправки сообщений.

См. *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения* для определения термина “стойкий криптографический алгоритм” и других терминов.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.1 Хранение данных держателей карт должно быть ограничено только необходимым минимумом. Должны быть разработаны политики, процедуры и процессы хранения и уничтожения данных, соответствующие следующим минимальным требованиям к хранению данных держателей карт: • количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований; • процессы безопасного удаления данных, хранение которых более не является необходимым;	**3.1.a** Изучить политики, процедуры и процессы хранения и уничтожения данных и проверить их на наличие следующих минимальных требований: • юридических, нормативных и коммерческих требований к хранению данных, включая • конкретные требования к хранению данных держателей карт (например, данные держателей карт может требоваться хранить в течение срока X по причинам Y); • положение о необходимости безопасного уничтожения данных, если их хранение более не является необходимым по юридическим, нормативным и коммерческим причинам; • действие политик и процедур должно распространяться на все места хранения данных держателей карт; • ежеквартальные процессы обнаружения и безопасного удаления данных держателей карт, которые превышают определенные политикой сроки хранения данных;	политика хранения данных определяет, какие данные необходимо хранить и где находятся эти данные, чтобы их можно было безопасно удалить, как только они станут не нужны; после авторизации разрешается хранить только номер платежной карты (PAN) (в нечитаемом виде), дату истечения срока действия, имя держателя карты и сервисный код. Знание мест хранения данных держателей карт необходимо для их надлежащего хранения или удаления, как только они станут не нужны. Чтобы определить требования к хранению, необходимо понимать потребности бизнеса, а также знать нормативные положения, которые

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
• специфические требования к хранению данных держателей карт; • ежеквартальные процессы обнаружения и безопасного удаления данных держателей карт, которые превышают определенные политикой сроки хранения данных.	**3.1.b** Опросить сотрудников для подтверждения того, что: • все места хранения данных держателей карт включены в процесс хранения и удаления данных; • реализован ежеквартальный процесс обнаружения и безопасного удаления данных держателей карт, проводимый вручную или автоматически; • этот процесс реализуется во всех местах хранения данных держателей карт.	относятся к соответствующей отрасли и применяются к тому типу данных, которые хранятся. *(Продолжение на следующей странице)*
	3.1.c Для нескольких системных компонентов, хранящих данные держателей карт, необходимо: • провести осмотр файлов и системных записей и убедиться, что сроки хранения данных не превышают определенные политикой хранения данных; • соблюдать механизм удаления, чтобы гарантировать, что данные удалены безопасным образом.	Обнаружение и удаление хранящихся данных с истекшим сроком хранения позволяет предотвратить хранение ненужных данных. Данный процесс может проводиться автоматически, вручную или полуавтоматически. Например, можно проводить процедуру обнаружения и удаления данных по расписанию (автоматически или вручную) и (или) проверку мест хранения данных вручную. Внедрение методов безопасного удаления данных гарантирует, что данные невозможно будет восстановить, когда они больше не нужны. ***Если данные вам не нужны, не храните их!***
3.2 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). В случае получения критичных аутентификационных данных все данные невозможно будет восстановить по завершении процесса авторизации. *Эмитенты и компании, обеспечивающие услуги эмиссии, могут*	**3.2.a** Убедиться, что эмитенты и (или) компании, предоставляющие услуги эмиссии и осуществляющие хранение критичных аутентификационных данных имеют на то документированное коммерческое обоснование путем ознакомления с политиками и опроса сотрудников.	Критичные аутентификационные данные состоят из полных данных на магнитной дорожке, кода или значения подтверждения подлинности карты и данных PIN-кода. Хранить критичные аутентификационные данные запрещается! Эти данные представляют интерес для злоумышленников, поскольку позволяют им генерировать поддельные платежные карты и осуществлять мошеннические операции.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
хранить критичные аутентификационные данные, если: • на то есть коммерческое обоснование и • данные хранятся защищенным образом. К критичным аутентификационным данным относятся данные, перечисленные в требованиях 3.2.1 – 3.2.3.	**3.2.b** При проверке эмитентов и (или) компаний, предоставляющих услуги эмиссии и осуществляющих хранение критичных аутентификационных данных, следует провести проверку центров обработки данных и системных конфигураций, чтобы убедиться, что критичные аутентификационные данные надежно защищены.	Эмитенты платежных карт или компании, предоставляющие услуги эмиссии или поддерживающие этот процесс, часто создают и управляют критичными аутентификационными данными в рамках процесса эмиссии. Компании, которые занимаются выпуском платежных карт или поддерживают этот процесс, могут хранить критичные аутентификационные данные, но ТОЛЬКО В ТОМ СЛУЧАЕ, если у них есть обоснованная потребность в хранении таких данных. Важно отметить, что все требования стандарта PCI DSS применяются к эмитентам, и единственное исключение для эмитентов и процессинговых организаций заключается в том, что они могут хранить критичные аутентификационные данные, если у них есть обоснованная потребность в этом. Под обоснованной потребностью понимается необходимость выполнения определенной функции, а не удобство. Такие данные должны храниться с защитой, с соответствием требованиям стандарта PCI DSS и используемой платежной системы.
	3.2.c В других случаях получения критичных аутентификационных данных следует ознакомиться с политиками и процедурами, и проверить системные конфигурации, чтобы убедиться, что данные не сохраняются после авторизации.	
	3.2.d В других случаях получения критичных аутентификационных данных следует ознакомиться с процедурами и убедиться, что процессы безопасного удаления данных гарантируют невозможность восстановления данных.	Для неэмитентов сохранение критичных аутентификационных данных после аутентификации запрещено.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.2.1 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 карты;* • *номер платежной карты (PAN);* • *дата истечения срока действия карты;* • *сервисный код.* *Для минимизации рисков разрешается хранить только указанные элементы данных.*	**3.2.1** Проверить источники данных для нескольких системных компонентов, включая, в том числе, перечисленные ниже, и убедиться, что полные данные любой дорожки магнитной полосы, находящейся на обратной стороне карты (или ее аналог на чипе), ни при каких обстоятельствах не сохраняются после авторизации: • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • несколько схем 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.
3.2.2 Запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с кредитной карты (трех- или четырехзначного числа, изображенного на лицевой или обратной стороне карты).	**3.2.2** Проверить источники данных для нескольких системных компонентов, включая, в том числе, перечисленные ниже, и убедиться, что трех- или четырехзначный проверочный код или значение, изображенное на лицевой стороне карты или на месте для подписи (данные CVV2, CVC2, CID, CAV2), ни при каких обстоятельствах не сохраняются после авторизации: • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • несколько схем 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.2.3 Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.	**3.2.3** Проверить источники данных для нескольких системных компонентов, включая, в том числе, перечисленные ниже, и убедиться, что персональные идентификационные номера (PIN), а также зашифрованные PIN-блоки не сохраняются после авторизации: • входящие данные о транзакции; • все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); • файлы истории; • файлы трассировки; • несколько схем 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).
3.3 Следует маскировать основной номер держателя карты при его отображении (максимально возможное количество знаков для отображения – первые шесть и последние четыре), чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь основной номер держателя карты. ***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).*	**3.3.a** Изучить письменные политики и процедуры маскировки основного номера держателя карты при его отображении и проверить их на наличие следующих требований: • требование о наличии документированного списка должностей, для которых требуется доступ к полному основному номеру держателя карты, каждая из которых должна иметь обоснованную коммерческую необходимость такого доступа; • требование маскировать основной номер держателя карты при его отображении, чтобы только сотрудники, которым это нужно для выполнения своих функциональных обязанностей, могли видеть весь этот номер; • сотрудники, занимающие любые другие должности, не должны видеть полный основной номер держателя карты без явного разрешения. **3.3.b** Проверить системные конфигурации и убедиться, что полный основной номер держателя карты отображается только для пользователей/должностей с документированной коммерческой необходимостью и маскируется для остальных запросов.	Отображение полного номера PAN на экранах компьютеров, квитанциях платежных карт, факсах или в бумажных отчетах может привести к тому, что эти данные станут известны неавторизованным лицам и могут быть использованы в мошеннических целях. Отображение полного основного номера держателя карты только для тех лиц, которым нужно видеть полный номер для выполнения своих функциональных обязанностей, позволяет снизить риск несанкционированного доступа к данным этого номера. Это требование касается защиты основного номера держателя карты, *отображаемого* на экранах, бумажных квитанциях и т.д., и его следует отличать от требования 3.4, которое касается защиты полного номера держателя карты при его *хранении* в файлах, базах данных и т.д.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
	3.3.c Проверить правила отображения основного номера держателя карты и убедиться, что эти номера маскируются при отображении данных держателя карты (например, на бумаге или экране монитора), кроме случаев, когда для работы сотрудников необходимо видеть весь основной номер держателя карты.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.4 PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий). Для этого следует использовать любой из следующих методов: • функция стойкого однонаправленного хеширования (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	**3.4.a** Изучить документацию о системе, используемой для защиты основного номера держателя карты, в том числе информацию о ее производителе, типе системы, применяемых алгоритмах шифрования (если они используются), и убедиться, что основной номер держателя карты приводится к нечитаемому виду с помощью одного из следующих методов: • функция стойкого однонаправленного хеширования; • 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.	все номера PAN, которые хранятся в основных хранилищах (базах данных, неструктурированных файлах, таких как текстовые файлы, таблицы и т.д.), а также во вспомогательных хранилищах (резервных копиях, журналах регистрации событий, журналах исключений и устранения неисправностей и т.д.), должны быть защищены. 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). Желательно, но не обязательно добавлять дополнительное вводимое значение к данным держателя карты перед хешированием, чтобы снизить вероятность сравнения данных (и получения
	3.4.b Изучить несколько таблиц или файлов из нескольких хранилищ данных и убедиться, что PAN представлен в нечитаемом виде (т. е. не хранится в открытом виде).	
	3.4.c Изучить несколько съемных носителей (например, кассеты с резервными копиями данных) и убедиться, что PAN представлен в нечитаемом виде.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
алгоритмы совместно с процессами и процедурами управления ключами. ***Примечание.*** *При наличии доступа одновременно к маскированному и хешированному номерам карты для злоумышленника не составит большого труда восстановить данные исходного PAN. Если маскированное и хешированное значение одного и того же PAN содержатся внутри среды какой-либо структуры, необходимо ввести дополнительные средства контроля для недопущения корреляции между маскированным и хешированным значениями, так как при этом исходный PAN становится легковосстановимым.*	**3.4.d** Изучить несколько журналов регистрации событий и убедиться, что PAN из них удален или представлен в нечитаемом виде.	основного номера держателя карты) с таблицами предварительно подсчитанных значений хеша. 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. Назначение стойкого криптографического алгоритма (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 с высокой стойкостью ключей шифрования (а не собственных алгоритмов). Посредством сопоставления хешированных и укороченных версий номера PAN злоумышленник может без труда узнать оригинальный номер PAN. Механизмы контроля, которые используются для предотвращения сопоставления этих данных, помогают обеспечить нечитаемость оригинального номера PAN.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.4.1 Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или столбцов базы данных), то управление логическим доступом должно осуществляться отдельно и независимо от механизмов аутентификации и контроля доступа операционной системы (например, локальных баз данных учетных записей или общих учетных данных для входа в сеть). Ключи дешифрования не должны быть связаны с учетными записями пользователей.	**3.4.1.a** Если применяется шифрование на уровне диска, изучить конфигурацию и проследить за процессом аутентификации, чтобы убедиться, что логический доступ к файловой системе реализован при помощи механизма, независимого от собственных механизмов аутентификации и контроля доступа операционной системы (например, локальных баз данных учетных записей или общих учетных данных для входа в сеть). **3.4.1.b** Проследить за процессами и опросить персонал, чтобы убедиться, что криптографические ключи хранятся безопасно (например, на съемном носителе, который защищен соответствующими процедурами контроля доступа). **3.4.1.c** Изучить конфигурации и проследить за процессами, чтобы убедиться, что данные держателей карт на съемных носителях хранятся только в зашифрованном виде. ***Примечание.*** *Если шифрование диска не используется для шифрования съемных носителей, данные на съемных носителях должны быть представлены в нечитаемом виде путем использования других методов шифрования.*	Назначение данного требования состоит в акцентировании внимания на приемлемости использования шифрования на уровне диска для приведения данных держателей карт к нечитаемому виду. При шифровании на уровне диска шифруется весь жесткий диск/раздел компьютера, а информация автоматически расшифровывается при запросе авторизованным пользователем. Многие решения для шифрования дисков перехватывают операции чтения/записи операционной системы и выполняют соответствующие криптографические преобразования, не требуя каких-либо дополнительных действий со стороны пользователя, за исключением ввода пароля или кодовой фразы в начале сеанса. С учетом данных характеристик шифрования на уровне диска, чтобы соответствовать данному требованию, метод шифрования не должен: 1) использовать тот же аутентификатор, что и операционная система; или 2) использовать ключ дешифрования, связанный или взятый из локальных баз данных учетных записей или общих учетных данных для входа в сеть. Полное шифрование диска помогает защитить данные в случае физической утраты диска и, следовательно, может быть полезно для портативных устройств, содержащих данные держателей карт.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.5 Задокументировать и внедрить процедуры для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования следующим образом. ***Примечание.*** *Это требование применяется к ключам шифрования данных держателей карт, а также для шифрования ключей, которые используются для защиты ключей шифрования данных. Такие ключи должны обладать таким же уровнем защиты, как и ключи для шифрования данных.*	**3.5** Проверить политики и процедуры управления ключами на наличие процессов для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования, которые должны включать следующие минимальные требования: • доступ к ключам шифрования должен быть разрешен как можно меньшему количеству сотрудников, ответственных за их хранение и использование; • ключи для шифрования ключей должны обладать таким же уровнем защиты, как и ключи для шифрования данных, которые они защищают; • ключи для шифрования ключей хранятся отдельно от ключей для шифрования данных; • ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.	Ключи шифрования должны быть надежно защищены, поскольку лица, получившие к ним доступ, смогут расшифровать данные. Ключи для шифрования ключей должны обладать таким же уровнем защиты, как и ключи для шифрования данных, чтобы гарантировать надлежащую защиту ключей, которые используются для шифрования данных, и самих данных, которые шифруются с помощью этих ключей. Требование по защите ключей от раскрытия и неправильного использования применяется как к ключам для шифрования ключей, так и к ключам для шифрования данных. Поскольку один ключ для шифрования ключей может предоставить доступ ко многим ключам для шифрования данных, ключи для шифрования ключей должны быть надежно защищены.
3.5.1 Доступ к ключам шифрования должен быть разрешен наименьшему возможному количеству ответственных за их хранение и использование сотрудников.	**3.5.1** Изучить списки доступа и убедиться, что доступ к ключам предоставлен наименьшему возможному количеству ответственных за их хранение и использование сотрудников.	Необходимо максимально уменьшить количество лиц, имеющих доступ к ключам шифрования. Обычно это лица, отвечающие за хранение ключей. Это позволит снизить вероятность разглашения данных держателей карт неуполномоченным лицам.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.5.2 Всегда хранить секретные и частные ключи шифрования/дешифрования данных держателей карт в одной (или нескольких) из следующих форм: • защищенными ключом для шифрования ключей, который имеет такой же уровень защиты, как и ключ для шифрования данных, и хранится отдельно от этого ключа; • в безопасном устройстве для шифрования данных (например, хост-модуле безопасности или платежном терминале, одобренном PTS); • в форме как минимум двух компонентов полноразмерного ключа или общего ключа в соответствии с принятым в отрасли методом. ***Примечание.*** *Хранение публичных ключей в одной из этих форм не обязательно.*	**3.5.2.a** Проверить документированные процедуры на наличие требования о том, что ключи шифрования/дешифрования данных держателей карт должны всегда существовать в одной (или нескольких) из следующих форм: • защищенными ключом для шифрования ключей, который имеет такой же уровень защиты, как и ключ для шифрования данных, и хранится отдельно от этого ключа; • в безопасном устройстве для шифрования данных (например, хост-модуле безопасности или платежном терминале, одобренном PTS); • в форме компонентов ключа или общего ключа в соответствии с признанным в отрасли методом.	Ключи шифрования должны храниться безопасно для предотвращения несанкционированного или ненужного доступа, который может привести к разглашению данных держателей карт. Это требование не подразумевает, что ключи для шифрования должны быть зашифрованы, но они должны быть защищены от раскрытия и неправильного использования в соответствии с требованием 3.5. В случае использования ключей для шифрования ключей, их хранение отдельно от ключей для шифрования данных (в физически и (или) логически отдельных местах) снижает риск несанкционированного доступа к тем и другим ключам.
	3.5.2.b Изучить системные конфигурации и места хранения ключей, и убедиться в том, что ключи шифрования/дешифрования данных держателей карт всегда существуют в одной (или более) из следующих форм: • защищенными ключом для шифрования ключей; • в безопасном устройстве для шифрования данных (например, хост-модуле безопасности или платежном терминале, одобренном PTS); • в форме компонентов ключа или общего ключа в соответствии с признанным в отрасли методом.	
	3.5.2.c При использовании ключей для шифрования ключей следует изучить системные конфигурации и места хранения ключей, и убедиться в том, что: • ключи для шифрования ключей обладает таким же уровнем защиты, как и ключи для шифрования данных, которые они защищают; • ключи для шифрования ключей хранятся отдельно от ключей для шифрования данных.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.5.3 Ключи должны храниться в как можно меньшем количестве мест.	**3.5.3** Изучить места хранения ключей и проследить за процессами, чтобы убедиться, что они хранятся в как можно меньшем количестве мест.	Хранение ключей шифрования в как можно меньшем количестве мест помогает организации отслеживать и осуществлять мониторинг всех мест хранения ключей и снижает вероятность разглашения ключей неуполномоченным лицам.
3.6 Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных держателей карт, в том числе следующие. ***Примечание.*** *Существует множество различных источников, из которых можно почерпнуть информацию о стандартах в управлении ключами (например, стандарт Национального института стандартов и технологий США (NIST), с которым можно ознакомиться на сайте http://csrc.nist.gov).*	**3.6.a** ***Дополнительная процедура проведения проверки для поставщиков услуг:*** если поставщики услуг предоставляют клиентам ключи шифрования для передачи или хранения данных держателей карт, следует проверить документацию, предоставляемую клиентам, на наличие рекомендаций по условиям их безопасной передачи, хранения и обновления, в соответствии с требованиями 3.6.1–3.6.8, приведенными ниже. **3.6.b** Изучить процедуры и процессы управления ключами шифрования данных держателей карт и выполнить следующее.	Способ управления ключами шифрования представляет собой критичную часть непрерывного обеспечения безопасности посредством шифрования. 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 3.6.1 по 3.6.8. 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.
3.6.1 Генерация стойких криптографических ключей	**3.6.1.a** Убедиться, что процедуры управления ключами указывают, как следует генерировать стойкие ключи.	Средство шифрования должно генерировать стойкие ключи согласно определению для

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
	3.6.1.b Изучить метод генерации ключей и убедиться в генерации стойких ключей.	термина "стойкий криптографический алгоритм", приведенного в документе "Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения". Использование стойких ключей шифрования значительно повышает уровень безопасности зашифрованных данных держателей карт.
3.6.2 Безопасное распространение ключей	**3.6.2.a** Убедиться, что процедуры управления ключами указывают, как следует безопасно распространять ключи.	Средство шифрования должно обеспечивать безопасное распространение ключей (то есть ключи не должны распределяться в открытом виде), и только для ответственных за их хранение и использование сотрудников в соответствии с требованием 3.5.1.
	3.6.2.b Изучить метод распространения ключей и убедиться в том, что ключи распространяются безопасно.	
3.6.3 Безопасное хранение ключей	**3.6.3.a** Убедиться, что процедуры управления ключами указывают, как следует безопасно хранить ключи.	Средство шифрования должно обеспечивать безопасное хранение ключей (например, шифруя их при помощи ключа шифрования ключей). Хранение ключей без надлежащей защиты может привести к предоставлению доступа злоумышленникам, дешифрованию и разглашению данных держателей карт.
	3.6.3.b Изучить метод хранения ключей и убедиться в том, что ключи хранятся безопасно.	
3.6.4 Смена ключей шифрования, криптопериод которых истек (например, когда истек установленный срок и (или) когда данным ключом было зашифровано некоторое количество криптотекста), основана на передовых практических методах индустрии безопасности и руководствах (например, специальное издание 800-57 NIST) и должна производиться согласно предписаниям соответствующего производителя или владельца ключа.	**3.6.4.a** Убедиться, что процедуры управления ключами устанавливают криптопериод для каждого типа ключей, а также процесс их изменения по завершении установленного криптопериода (криптопериодов).	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.
	3.6.4.b Опросить сотрудников и убедиться, что ключи изменяют по завершении установленного криптопериода (криптопериодов).	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
3.6.5 Изъятие или смена ключей (например, архивация, уничтожение и (или) аннуляция) при нарушении целостности (например, увольнение сотрудника, обладающего информацией об открытом компоненте ключа), а также ключей, относительно которых существуют подозрения во взломе. ***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.*	**3.6.5.a** Изучить процедуры управления ключами и подтвердить следующие процессы: • изъятие либо замена ключей в случае нарушения целостности; • замена ключей шифрования, которые были или могли быть взломаны; • проверка того, что удаленные или замененные ключи не используются для шифрования. **3.6.5.b** Опросить сотрудников и убедиться в том, что внедрены следующие процессы: • изъятие либо, при необходимости, замена ключей в случае нарушения целостности, включая увольнение сотрудника, обладающего информацией о ключе; • замена ключей шифрования, которые были или могли быть взломаны; • проверка того, что удаленные или замененные ключи не используются для шифрования.	Ключи, которые больше не используются или в которых нет необходимости, а также ключи, относительно которых существуют подозрения во взломе, 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. Средство шифрования должно обеспечивать возможность смены ключей, которые необходимо заменить или относительно которых существуют подозрения во взломе.
3.6.6 Если процедуры управления ключами шифрования в открытом виде осуществляются вручную, данные процедуры должны координироваться с использованием принципа разделения знания и двойного контроля. ***Примечание.*** *Примеры процедур управления ключами вручную включают, в том числе: генерацию ключа, его передачу, загрузку, хранение*	**3.6.6.a** Проверить процедуры управления открытыми ключами вручную на наличие следующих процессов: • разделенное знание о ключах таким образом, когда двое или более людей владеют компонентами одного ключа, и каждый из них знает только свой компонент ключа; • двойной контроль ключей таким образом, чтобы для выполнения любых операций по управлению ключами требовалось как минимум два человека, и ни один из них не обладал доступом к учетным данным (например, паролям или ключам) другого.	Разделенное знание между несколькими лицами и двойной контроль за ключами используются для исключения возможности того, что один человек получит доступ к целому ключу. Такой метод контроля обычно применяется для систем шифрования с ручным вводом ключа шифрования или в случае, когда управление ключами не реализовано в продукте шифрования. Разделенное знание – это метод, при использовании которого двое или более

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
и уничтожение.	**3.6.6.b** Опросить сотрудников и (или) проследить за процессами, чтобы убедиться, что процедуры ручного управления ключами в открытом виде предусматривают следующее: • разделенное знание; • двойной контроль.	людей раздельно владеют компонентами одного ключа; каждый из этих людей знает только свой компонент ключа, а отдельные компоненты не дают знания всего ключа 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.
3.6.7 Защита от неавторизованной замены ключа.	**3.6.7.a** Убедиться, что процедуры управления ключами включают процессы для защиты от неавторизованной замены ключей.	Средство шифрования не должно допускать или принимать замену ключей, инициированную неавторизованными источниками или неожиданными процессами.
	3.6.7.b Опросить сотрудников и (или) проследить за процессами, чтобы убедиться в наличии защиты от неавторизованной замены ключей.	
3.6.8 Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с официальным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности.	**3.6.8.a** Убедиться, что процедуры управления ключами включают процессы признания (в письменном или электронном виде) сотрудниками, ответственными за хранение и использование ключей, того, что они понимают и принимают свои обязанности.	Этот процесс поможет гарантировать исполнение сотрудниками, ответственными за хранение и использование ключей, своей работы, а также понимание и согласие со своими обязанностями.
	3.6.8.b Изучить документацию или другие доказательства того, что сотрудники, ответственные за хранение и использование ключей, подтвердили (в электронном виде или письменно), что понимают и принимают свои обязанности.	
3.7 Убедиться, что политики безопасности и процедуры защиты данных держателей карт документированы, используются и известны всем заинтересованным лицам.	**3.7** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры защиты данных держателей карт: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и документированных процедурах работы для обеспечения безопасного хранения данных держателей карт на постоянной основе.

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

Критичную информацию следует передавать через общедоступные сети, где ее легко перехватить, изменить или перенаправить, только в зашифрованном виде. Неправильно сконфигурированные беспроводные сети и уязвимости, связанные с использованием устаревших механизмов шифрования, могут быть легкими целями для злоумышленника и способствовать получению несанкционированного доступа к среде данных держателей карт.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
4.1 Для защиты данных держателей карт во время их передачи через общедоступные сети следует использовать надежные криптографические алгоритмы и протоколы защиты (например, SSL/TLS, IPSEC, SSH и т.д.), соответствующие следующим требованиям: • прием только доверенных ключей и сертификатов; • используемый протокол поддерживает только безопасные версии и конфигурации; • стойкость шифрования соответствует используемой методологии шифрования. *Примеры общедоступных сетей включают, помимо прочего:* • *Интернет;* • *беспроводные технологии, включая протоколы 802.11 и Bluetooth;* • *технологии сотовой связи, например GSM, CDMA;* • *GPRS;*	**4.1.a** Выявить все места хранения данных держателей карт, в которых осуществляется прием или передача данных через общедоступные сети. Изучить документированные стандарты и сравнить их с системными конфигурациями для подтверждения того, что везде используются протоколы безопасности и стойкое шифрование.	Критичные данные должны шифроваться при передаче по сетям общего пользования, потому что злоумышленник может перехватить и (или) изменить их маршрут при передаче. Безопасная передача данных держателей карт требует использования доверенных ключей/сертификатов, безопасного протокола передачи и шифрования достаточной стойкости для шифрования данных держателей карт. Не следует принимать запросы на подключение от систем, не поддерживающих требуемую стойкость шифрования, т.к. это приведет к небезопасному подключению. Обратите внимание на то, что некоторые версии протоколов (например, SSL 2.0, SSH 1.0 и TLS 1.0) содержат известные уязвимости, которые могут быть использованы злоумышленником для получения контроля над системой. Независимо от того, какой протокол используется, убедитесь, что он настроен для использования только безопасных конфигураций и версий для предотвращения небезопасного подключения. Например, можно использовать TLS версии 1.1 или более поздней с сертификатом,
	4.1.b Проверить документированные политики и процедуры на наличие следующих процессов: • прием только доверенных ключей и (или) сертификатов; • поддержка используемым протоколом только безопасных версий и конфигураций (небезопасные версии или конфигурации не поддерживаются); • применение шифрования достаточной стойкости согласно используемой методологии шифрования.	
	4.1.c Выбрать и отследить несколько входящих и исходящих транзакций, чтобы проверить, что данные держателей карт передаются в зашифрованном виде с использованием стойкого алгоритма шифрования.	
	4.1.d Изучить ключи и сертификаты, и убедиться, что принимаются только доверенные ключи и сертификаты.	
	4.1.e Изучить ключи и сертификаты, и убедиться, что протокол использует только безопасные конфигурации и не поддерживает небезопасные версии или конфигурации.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
• *спутниковые средства связи.*	**4.1.f** Изучить системные конфигурации и убедиться, что для шифрования данных применяется шифрование достаточной стойкости согласно используемой методологии шифрования (учесть рекомендации производителя и наиболее прогрессивные методы).	полученным от известного источника по выдаче публичных сертификатов и поддержкой только стойкого шифрования. Проверка того, что сертификат является доверенным (например, срок действия его не истек, и он получен из доверенного источника), помогает обеспечить целостность безопасного подключения.
	4.1.g При использовании протоколов SSL/TLS следует изучить системные конфигурации и убедиться, что SSL/TLS включен при каждой передаче или получении данных держателей карт. Например, для браузерных версий следует убедиться, что: • в качестве протокола URL-адреса указан HTTPS; и • данные держателей карт запрашиваются только в том случае, если URL-адрес содержит префикс HTTPS.	Как правило, URL-адрес должен начинаться с префикса HTTPS, а в окне веб-браузера должен быть значок замка. Многие поставщики SSL-сертификатов также предоставляют хорошо заметную печать подтверждения проверки (иногда называемую "печать безопасности", "печать безопасного сайта" или "печать доверия"), по которой можно щелкнуть для просмотра информации о веб-сайте.
4.1.1 При использовании беспроводных сетей, передающих данные держателей карт либо подключенных к среде данных держателей карт, следует использовать передовые практические методы индустрии безопасности (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных. ***Примечание.*** *Использование протокола WEP в качестве протокола защиты запрещено.*	**4.1.1** Выявить все беспроводные сети, передающие данные держателей карт либо подключенные к информационной среде держателей карт. Изучить документированные стандарты и сравнить их с системными конфигурациями для подтверждения соответствия всех обнаруженных беспроводных сетей следующим требованиям: • применение отраслевых рекомендаций (например, IEEE 802.11i) для обеспечения стойкого шифрования при аутентификации и передаче данных; • протоколы со слабым шифрованием (например, WEP, SSL версии 2.0 или более ранней) не используются в качестве протокола безопасности 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 внутренним сетям и данным.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
4.2 Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты и т.д.).	**4.2.a** В случае использования пользовательских технологий передачи данных держателей карт следует проследить за процессом отправки основного номера держателя карты и изучить несколько исходящих соединений, чтобы проверить, что основной номер держателя карты передается в нечитаемом виде или защищен посредством стойких криптографических механизмов защиты при использовании пользовательских технологий передачи сообщений.	Сообщения, передаваемые по электронной почте, с помощью систем мгновенного обмена сообщениями или в чате, могут быть перехвачены в процессе доставки, как во внутренней, так и во внешней общедоступной сети. Не следует использовать эти средства передачи сообщений для отправки основного номера держателя карты, если они не обеспечивают стойкого шифрования.
	4.2.b Изучить задокументированные политики и проверить наличие политики, запрещающей отправку незашифрованного основного номера держателя карты при помощи пользовательских технологий передачи сообщений.	
4.3 Убедиться, что политики безопасности и процедуры шифрования передаваемых данных держателей карт документированы, используются и известны всем заинтересованным лицам.	**4.3** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры шифрования передаваемых данных держателей карт: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения безопасной передачи данных держателей карт на постоянной основе.

Программа управления уязвимостями

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

Большинство видов вредоносного программного обеспечения проникают в сеть через электронную почту сотрудников, сеть Интернет, съемные носители или мобильные устройства в результате использования системных уязвимостей Антивирусное программное обеспечение должно быть установлено на всех подверженных воздействию вирусов системах, чтобы защитить их от вредоносного кода. Дополнительные решения для защиты от вредоносного ПО могут использоваться в качестве дополнения к антивирусному ПО; однако такие дополнительные решения не заменяют антивирусное ПО.

Требования PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
5.1 Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).	**5.1** Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, убедиться, что используется антивирусная защита (если подходящая антивирусная технология существует).	Существует большое количество атак, часто называемых "атаками нулевого дня" (такие атаки используют ранее неизвестные уязвимости) и использующих широко распространенные уязвимости, которые направлены против, казалось бы, полностью защищенных систем. Без наличия регулярно обновляемого антивирусного ПО сеть подвержена воздействию новых видов вредоносного ПО, которые могут нарушить ее работу или привести к разглашению данных.
5.1.1 Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	**5.1.1** Изучить документацию поставщика и конфигурации антивирусов, чтобы убедиться в том, что антивирусы способны: • обнаруживать все известные виды вредоносного программного обеспечения; • удалять все известные виды вредоносного программного обеспечения; • обеспечивать защиту от всех известных видов вредоносного программного обеспечения. *Примерами вредоносного ПО являются вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.*	Важно обеспечить защиту от **ВСЕХ** типов и форм вредоносных программ.

Требования PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
5.1.2 Проводить периодические проверки для выявления и оценки рисков заражения вредоносным ПО на системах, которые считаются не подверженными заражению вредоносным ПО, с целью подтверждения отсутствия необходимости в антивирусном ПО.	**5.1.2** Опросить сотрудников и убедиться, что проводятся периодические проверки для выявления и оценки рисков заражения вредоносным ПО на системах, которые считаются не подверженными заражению вредоносным ПО, с целью подтверждения отсутствия необходимости в антивирусном ПО.	Обычно мэйнфреймы, компьютеры среднего уровня (например, AS/400) и подобные системы не подвержены заражению вредоносным ПО. Однако, тенденции в области вредоносного ПО могут быстро измениться, поэтому организациям важно знать о новых видах вредоносного ПО, которые могут быть опасны для их систем (например, путем мониторинга сообщений о безопасности от поставщиков ПО и новостных групп антивирусов, чтобы узнать, угрожают ли их системам новые виды вредоносного ПО). Тенденции использования вредоносных программ должны быть включены в процесс выявления новых уязвимостей в системе безопасности. Методы оценки новых тенденций и устранения связанных с ними уязвимостей должны быть внедрены в стандарты конфигурирования и механизмы защиты
5.2 Убедится, что все антивирусные механизмы: • актуальны; • выполняют периодическое сканирование; • создают журналы регистрации событий, которые хранятся согласно требованию 10.7 стандарта PCI DSS.	**5.2.a** Изучить политики и процедуры, и убедиться, что они регламентируют регулярное обновление антивирусного ПО и антивирусных баз.	Даже лучшие антивирусы имеют ограниченную эффективность при отсутствии последних обновлений безопасности, антивирусных баз или механизмов защиты от вредоносного ПО. Журналы регистрации событий предоставляют возможность мониторинга активности вирусов и вредоносного ПО, и реагирования на эту активность. Поэтому важно настроить решения для защиты от вредоносного ПО таким образом, чтобы можно было генерировать записи в журнале регистрации событий и управлять этими записями в соответствии с требованием 10.
	5.2.b Изучить конфигурацию антивирусов, включая установочные образы и убедиться, что антивирусные механизмы: • настроены на выполнение автоматического обновления; • настроены на выполнение периодического сканирования.	
	5.2.c Изучить выборку системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО и, убедиться, что: • используется последняя версия антивирусной программы и баз вирусов; • выполняется периодическое сканирование.	

Требования PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
	5.2.d Изучить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов и убедиться, что: • включено создание журналов регистрации событий; • журналы хранятся согласно требованию 10.7 стандарта PCI DSS.	

Требования PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
5.3 Необходимо убедиться, что антивирусные программы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени. ***Примечание.*** *Антивирусы могут быть временно отключены только в случае оправданной технической необходимости, с разрешения руководства на индивидуальной основе. Если антивирусная защита должна быть отключена для определенной цели, необходимо получить официальное разрешение. Также может понадобиться принятие дополнительных мер безопасности на период времени, в течение которого антивирусная защита будет неактивна.*	**5.3.a** Изучить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов и убедиться, что антивирусное ПО работает в активном режиме. **5.3.b** Изучить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов и убедиться, что антивирусное ПО не может быть отключено или изменено пользователями. **5.3.c** Опросить ответственных сотрудников и понаблюдать за процессами, чтобы проверить, что антивирусные программы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени.	Антивирус, работающий постоянно и защищенный от изменений, обеспечит надежную защиту от вредоносного ПО. Использование механизма контроля на основе политик на всех системах для предотвращения изменения или отключения приложений для защиты от вредоносного ПО не позволит злоумышленнику воспользоваться уязвимостью в системе. Также может понадобиться принятие дополнительных мер безопасности на период времени, в течение которого антивирусная защита будет неактивна (например, отключение незащищенной системы от Интернета на время отключения антивирусной защиты и выполнения полного сканирования после его повторного включения).
5.4 Убедиться, что политики безопасности и процедуры защиты систем от вредоносного ПО документированы, используются и известны всем заинтересованным лицам.	**5.4** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры защиты систем от вредоносного ПО: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения защиты систем от вредоносного ПО на постоянной основе.

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости в безопасности для получения привилегированного доступа к системе. Большинство из таких уязвимостей закрывается путем установки обновлений безопасности, выпускаемых производителем, которые должны быть установлены организацией, управляющей системой. На все системы должны быть установлены все необходимые обновления программного обеспечения для защиты данных держателей карт от раскрытия путем использования уязвимостей внутренними и внешними злоумышленниками, а также вредоносным ПО.

Примечание. *Подходящими являются те обновления, которые протестированы на совместимость с текущей конфигурацией безопасности. В случае самостоятельной разработки приложений множества уязвимостей удастся избежать, используя стандартные процессы разработки систем и приемы безопасного программирования.*

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.1 Должен быть внедрен процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также ранжирования риска (например, "высокий", "средний" или "низкий") недавно обнаруженных уязвимостей. ***Примечание.*** *Ранжирование рисков должно быть основано на общепринятых отраслевых рекомендациях с учетом потенциального воздействия. Например, критерии ранжирования риска могут основываться на уровне риска по шкале CVSS, и (или) классификации поставщика, и (или) типе поражаемых систем.* *Методы оценки уязвимостей и определения уровня риска зависят от среды организации и ее стратегии по оценке рисков. Уровень риска должен быть присвоен как минимум всем уязвимостям с высоким уровнем риска для среды. Уязвимости считаются критическими, если они представляют неотвратимую угрозу для среды, влияют на работу важнейших систем и (или) могут привести к взлому, если не будут	**6.1.a** Проверить политики и процедуры на наличие следующих процессов: • выявление новых уязвимостей; • присвоение уровня риска уязвимостям, включая все уязвимости с высоким и критическим уровнем риска; • использование авторитетных внешних источников информации об уязвимостях. **6.1.b** Опросить ответственных сотрудников и понаблюдать за процессами для подтверждения того, что: • выявляются новые уязвимости; • уязвимостям присваивается уровень риска, включая все уязвимости с высоким и критическим уровнем риска; • процессы выявления новых уязвимостей системы безопасности включают в себя использование для этого внешних источников информации.	Цель данного требования состоит в том, что организации должны своевременно узнавать о новых уязвимостях, которые могут оказать влияние на их среду. Источники информации об уязвимостях должны быть достоверными (например, веб-сайты поставщиков, отраслевые новостные группы, почтовые рассылки или RSS-потоки). Как только организация выявляет уязвимость, которая может оказать негативное влияние на ее среду, необходимо оценить и ранжировать риск, который представляет эта уязвимость. Следовательно, организация должна иметь в наличии метод оценки уязвимостей и присвоения им уровня риска на постоянной основе. Для этого недостаточно провести сканирование авторизованным поставщиком услуг сканирования (ASV) или внутреннее сканирование на наличие уязвимостей; для этого необходим процесс активного мониторинга отраслевых источников информации об уязвимостях. Оценка уровня риска (например, "высокий", "средний" или "низкий") позволяет организациям быстрее выявлять, устанавливать приоритет и устранять проблемы с высоким приоритетом, а также минимизировать вероятность

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
устранены. Примерами критически важных систем могут служить системы безопасности, потребительские устройства и системы, базы данных и другие системы, осуществляющие хранение, обработку или передачу данных держателей карт.		использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для системы безопасности.
6.2 Все системные компоненты и программное обеспечение должны быть защищены от известных уязвимостей путем установки необходимых обновлений системы безопасности, выпущенных поставщиком. Критичные обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем. ***Примечание.*** *Критичные обновления системы безопасности должны выявляться согласно процессу ранжирования рисков (см. требование 6.1).*	**6.2.a** Проверить политики и процедуры установки обновлений системы безопасности на наличие следующих процессов: • установка необходимых критичных обновлений безопасности в течение месяца с момента выпуска поставщиком; • установка всех необходимых критичных обновлений безопасности в течение определенного срока с момента выпуска поставщиком (например, в течение трех месяцев). **6.2.b** Для нескольких системных компонентов и связанного с ними программного обеспечения проверить, установлены ли актуальные обновления безопасности на каждой из систем, для подтверждения следующего: • установка необходимых критичных обновлений безопасности производится в течение месяца с момента выпуска поставщиком; • установка всех необходимых критичных обновлений безопасности производится в течение определенного срока с момента выпуска поставщиком (например, в течение трех месяцев).	Существует большое количество атак, часто называемых "атаками нулевого дня" (такие атаки используют ранее неизвестные уязвимости) и использующих широко распространенные уязвимости, которые направлены против, казалось бы, полностью защищенных систем. Без своевременного внедрения актуальных обновлений безопасности на критических системах злоумышленник может использовать эти уязвимости для проведения атак на систему и нарушения ее работы или для получения доступа к критичной информации. Установка приоритетов обновлений для критичной инфраструктуры обеспечивает скорейшую защиту высокоприоритетных систем и устройств от уязвимостей после выхода обновления. Необходимо определить приоритеты установки обновлений таким образом, чтобы критичные обновления безопасности устанавливались на критичные или подверженные риску системы в течение 30 дней, а обновления с меньшим уровнем риска – в течение 2–3 месяцев. Данное требование распространяется на необходимые обновления для любого установленного ПО.
6.3 Разработать безопасные внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс) с соблюдением	**6.3.a** Изучить задокументированные процессы разработки программного обеспечения и убедиться, что они основаны на отраслевых стандартах и (или) известных рекомендациях.	Если не уделять должного внимания безопасности информации на этапах разработки программного обеспечения (определения требований, проектирования, анализа и

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
следующих требований: • согласно требованиям PCI DSS (например, в отношении безопасной аутентификации и ведения журнала); • процесс разработки программного обеспечения должен быть основан на отраслевых стандартах и (или) известных рекомендациях; • информационная безопасность должна учитываться в течение всего цикла разработки ПО. ***Примечание**. Требование относится к любому ПО собственной разработки и заказному ПО, разработанному третьим лицом.*	**6.3.b** Изучить документацию по разработке программного обеспечения и убедиться, что она принимает во внимание информационную безопасность в течение всего цикла разработки.	тестирования), в среду эксплуатации непреднамеренно или сознательно могут быть внесены уязвимости в системе безопасности. Понимание процессов обработки критичных данных приложений – в том числе во время хранения, передачи и пребывания в памяти – может упростить определение методов защиты данных.
	6.3.c Изучить документацию по разработке программного обеспечения и убедиться, что разработка программных приложений учитывает требования стандарта PCI DSS.	
	6.3.d Опросить разработчиков программного обеспечения для подтверждения того, что разработка ПО ведется по задокументированным процессам.	
6.3.1 Удалить все учетные записи разработчиков, тестовые и (или) пользовательские учетные записи приложения, имена пользователей и пароли перед передачей программного обеспечения заказчикам или переводом его в производственный режим.	**6.3.1** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться в том, что все тестовые и (или) пользовательские учетные записи приложения, имена пользователей и (или) пароли удаляются перед передачей программного обеспечения заказчикам или переводом его в производственный режим.	Учетные записи разработчиков, тестовые и (или) пользовательские учетные записи приложения, имена пользователей и пароли следует удалить из производственного кода до активации приложения или предоставления приложения заказчикам, поскольку эти элементы могут использоваться для получения информации о функционировании приложения. Обладая этой информацией, злоумышленники могут получить доступ к приложению и данным держателей карт.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.3.2 Проверить программный код приложений на наличие потенциальных уязвимостей (вручную или автоматически) перед передачей готовых приложений заказчикам или переводом их в производственный режим с соблюдением следующих минимальных требований: • изменения программного кода должны контролироваться 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; • все необходимые корректировки вносятся до выпуска программного обеспечения; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска программного обеспечения. *(Продолжение на следующей странице)*	**6.3.2.a** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что в отношении всех изменений программного кода пользовательского приложения должен быть выполнен контроль 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 6.5 PCI DSS); • все необходимые корректировки вносятся до выпуска программного обеспечения; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска программного обеспечения.	Уязвимости в пользовательском коде обычно используются злоумышленниками для получения доступа к сети и кражи данных держателей карт. Контроль кода должны выполнять опытные специалисты, знакомые с методиками контроля кода. Для обеспечения объективной и независимой оценки контроль кода должны выполнять лица, которые не являются создателями кода. Автоматизированные средства или процессы могут использоваться в сочетании с контролем кода вручную, но учтите, что при использовании автоматизированных средств контроля некоторые ошибки или уязвимости в коде бывает сложно или вообще невозможно обнаружить. Исправление ошибок в коде перед передачей программного обеспечения заказчикам или переводом его в производственный режим позволяет предотвратить потенциальное использование кода злоумышленниками. Исправить ошибки в коде после передачи программного обеспечения заказчикам или переводом его в производственный режим 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
Примечание. *Данное требование по осуществлению контроля кода (code reviews) применимо ко всему разрабатываемому программному коду (как внутренних, так и общедоступных приложений) как составная часть жизненного цикла разработки системы.* *Контроль кода может проводиться компетентным внутренним персоналом или третьими сторонами. В отношении веб-приложений, которые находятся в публичном доступе, также подлежат применению дополнительные меры по защите от появляющихся угроз и уязвимостей после внедрения, как определено в требовании 6.6 стандарта PCI DSS.*	**6.3.2.b** Выберите несколько недавних изменений приложений и проверьте, что в отношении программного кода выполняется контроль кода согласно требованию 6.3.2.a, представленному выше.	
6.4 Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов. Это могут быть следующие процедуры.	**6.4** Проверить политики и процедуры на предмет соответствия следующим требованиям: • среды разработки/тестирования и производственного функционирования должны быть отделены друг от друга, и при этом должны быть внедрены механизмы контроля доступа; • обязанности по разработке/тестированию и производственному функционированию программного обеспечения должны быть разделены; • производственные данные (действующие основные номера держателей карт) не должны использоваться для тестирования и разработки; • тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим; • процедуры контроля изменений, относящихся к обновлениям безопасности, и изменений в конфигурации должны быть документированы.	Без надлежащего контроля изменений программного обеспечения возможности защиты могут быть непреднамеренно или сознательно упущены или отключены, возможно появление ошибок обработки или внедрение вредоносного кода.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.4.1 Отделить среды разработки/тестирования и производственного функционирования программного обеспечения друг от друга и при этом внедрить механизмы разграничения доступа.	**6.4.1.a** Изучить документацию сети и конфигурации сетевых устройств и убедиться в том, что среды разработки/тестирования и производственного функционирования программного обеспечения отделены друг от друга.	Как правило, среда разработки и тестирования менее защищена, чем производственная среда. Без надлежащего разделения производственная среда и данные держателей карт могут подвергаться риску взлома вследствие менее строгой конфигурации защиты или возможных уязвимостей в среде тестирования или разработки.
	6.4.1.b Изучить настройки контроля доступа. Убедиться в том, что внедрены механизмы разграничения доступа к средам разработки/тестирования и производственного функционирования.	
6.4.2 Существует разделение обязанностей между сотрудниками, работающими в среде разработки/тестирования, и сотрудниками, работающими в среде эксплуатации.	**6.4.2** Понаблюдать за процессами и опросить персонал, ответственный за среды разработки/тестирования и производственного функционирования, чтобы убедиться в том, что обязанности по разработке/тестированию и производственному функционированию программного обеспечения разделены.	Уменьшение количества сотрудников с доступом к производственной среде и данным держателей карт гарантирует, что доступ предоставляется только тем сотрудникам, кому он в действительности нужен для выполнения должностных обязанностей. Цель данного требования состоит в отделении функции разработки и тестирования от функций производственного функционирования. Например, разработчик может использовать учетную запись с правами уровня администратора в среде разработки и иметь отдельную учетную запись с правами доступа на уровне пользователя в среде производственного функционирования.
6.4.3 Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.	**6.4.3.a** Изучить процессы проведения тестирования и опросить сотрудников, чтобы убедиться в наличии процедур контроля за тем, что производственные данные (действующие основные номера держателей карт) не используются для тестирования и разработки.	В средах разработки или тестирования обычно осуществляется менее жесткий контроль за обеспечением безопасности. Использование в такой среде производственных данных позволит злоумышленникам получить неавторизованный доступ к информации, используемой в производственной среде (например, к данным держателей карт).
	6.4.3.b Изучить выборку тестовых данных и убедиться в том, что производственные данные (действующие основные номера держателей карт) не используются для тестирования и разработки.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.4.4 Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.	**6.4.4.a** Понаблюдать за процессами проведения тестирования и опросить персонал, чтобы убедиться в том, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	Тестовые данные и учетные записи следует удалить из кода приложения перед переводом его в производственный режим, поскольку эти элементы могут использоваться для получения информации о функционировании приложения или системы. Обладая этой информацией, злоумышленники могут получить возможность доступа к системе и данным держателей карт.
	6.4.4.b Изучить выборку данных и учетных записей из недавно установленных или обновленных производственных систем и убедиться в том, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	
6.4.5 Процедуры контроля изменений перед внедрением обновлений безопасности и изменений в конфигурации ПО должны включать следующее.	**6.4.5.a** Проверить процедуры контроля изменений, относящихся к обновлениям безопасности, и изменений в конфигурации на наличие следующих процедур: • документирование влияния изменения на систему; • документированное утверждение изменений уполномоченными лицами; • тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы; • процедуры отмены изменения.	Без надлежащего контроля обновления ПО и обновления безопасности могут не оказать надлежащего воздействия.
	6.4.5.b Сделать выборку системных компонентов и опросить ответственных сотрудников для определения недавних изменений/обновлений безопасности. Отследить эти изменения с помощью соответствующей документации по контролю изменений. Для каждого изменения нужно выполнить следующие проверки.	
6.4.5.1 Документирование влияния изменений	**6.4.5.1** Убедиться, что влияние изменений задокументировано по каждому из выбранных изменений.	Последствия изменений должны документироваться, чтобы все вовлеченные стороны могли надлежащим образом запланировать все изменения в обработке данных.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.4.5.2 Согласование изменения с руководством.	**6.4.5.2** Убедиться, что изменение было согласовано уполномоченными лицами.	Утверждение руководством указывает на то, что изменение является легитимным, авторизованным и санкционированным организацией.
6.4.5.3 Тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы.	**6.4.5.3.a** Для каждого изменения проверить, что производственная функциональность была протестирована, чтобы убедиться, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы.	Следует выполнять тщательное тестирование для проверки того, что внедрение изменения не оказывает негативного влияния на уровень безопасности среды. Цель тестирования состоит в подтверждении работоспособности всех существующих механизмов защиты данных и того, что эти механизмы работают надлежащим образом после внедрения изменений в среду.
	6.4.5.3.b Для изменений программного кода убедиться, что все обновления протестированы на соответствие требованию 6.5 PCI DSS перед их запуском в производственный режим.	
6.4.5.4 Процедуры отмены изменения.	**6.4.5.4** Убедиться, что предусмотрена процедура отмены для каждого изменения.	Для каждого изменения должна существовать документированная процедура отмены, которая позволит вернуть систему в первоначальное состояние в случае сбоя или неблагоприятного воздействия изменения на приложение или систему.
6.5 Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом: • обучение разработчиков методикам безопасного программирования, включая информацию о том, как избежать распространенных программных уязвимостей и как определить способ хранения критичных данных в памяти; • разработка приложений в соответствии с основными принципами безопасного программирования.	**6.5.a** Изучить политики и процедуры разработки ПО и убедиться, что разработчики обязаны проходить обучение методикам безопасного программирования в соответствии с известными отраслевыми рекомендациями и руководствами.	Прикладной уровень подвержен высокому риску и может являться целью как внутренних, так и внешних угроз. Требования 6.5.1–6.5.10 представляют собой минимально необходимые меры безопасности, и организации должны внедрять те методики безопасного программирования, которые применимы к определенным технологиям в их среде. Разработчики приложений должны проходить надлежащее обучение определению и устранению проблем, связанных с этими и другими распространенными уязвимостями программного кода. Осведомленность персонала
	6.5.b Опросить несколько разработчиков программного обеспечения и убедиться, что они знакомы с техникой безопасного программирования.	
	6.5.c Изучить документацию об обучении и убедиться, что разработчики прошли обучение методикам безопасного программирования, в том числе тому, как избежать распространенных программных уязвимостей и как определить способ хранения критичных данных в памяти.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
Примечание. *Уязвимости, перечисленные в требованиях 6.5.1 – 6.5.10 соответствовали отраслевым рекомендациям на момент публикации данной версии стандарта PCI DSS. В случае обновления лучших мировых практик управления уязвимостями (таких как руководство OWASP,SANS CWE Top 25, CERT Secure Coding и т.д.) следует использовать их актуальную версию.*	**6.5.d.** Убедиться, что при разработке приложений уделяется внимание защите, по меньшей мере, от следующих уязвимостей.	о правилах безопасного программирования позволит свести к минимуму количество уязвимостей, связанных с низким качеством кода. Обучение разработчиков может осуществляться как самой организацией, так и третьими лицами и должно соответствовать используемой технологии. Признанные методики безопасного программирования меняются со временем, поэтому методики программирования и обучения разработчиков в организации также должны обновляться для соответствия новым угрозам (например, атакам memory scraping). Уязвимости, указанные в требованиях 6.5.1–6.5.10, представляют собой лишь минимальный список. Соответствие тенденциям в области уязвимостей и внедрение соответствующих мер безопасности в свои методики безопасного программирования является задачей организации.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
Примечание. *Требования 6.5.1–6.5.6, приведенные ниже, распространяются на все приложения (внешние или внутренние).*		
6.5.1 Инъекции, в особенности, SQL-инъекции. Также следует учесть инъекции OS Command, LDAP и Xpath.	**6.5.1** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению внедрения кода, в том числе: • 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 и изменить данные, что позволяет ему атаковать компоненты внутри сети через приложение, инициировать такие атаки, как переполнение буфера, получить доступ к конфиденциальной информации или информацию о функционировании серверного приложения. Необходимо проверять информацию перед отправкой в приложение (например, посредством проверки всех буквенных символов, сочетания буквенных и цифровых символов и т.д.)
6.5.2 Переполнение буфера	**6.5.2** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению переполнений буфера, в том числе: • 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.5.3 Небезопасное криптографическое хранилище.	**6.5.3** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению небезопасного шифрования, в том числе: • защита от криптографических ошибок; • использование стойких криптографических алгоритмов и ключей.	Приложения, которые не используют для хранения данных стойкие криптографические методы надлежащим образом, подвергаются повышенному риску взлома и утечки данных держателей карт и (или) учетных данных для проверки подлинности. Если злоумышленник сможет использовать уязвимости, связанные со слабыми криптографическими процессами, он получит доступ к зашифрованным данным.
6.5.4 Небезопасная передача данных	**6.5.4** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению небезопасных коммуникаций, обеспечивающие надлежащую аутентификацию и шифрование всех критичных коммуникаций.	Приложения, которые не шифруют надлежащим образом сетевой трафик с применением стойких криптографических методов, подвергаются повышенному риску взлома и утечки данных держателей карт. Если злоумышленник сможет использовать уязвимости, связанные со слабыми криптографическими процессами, он сможет получить контроль над приложением или даже доступ к зашифрованным данным в открытом виде.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.5.5 Некорректная обработка ошибок.	**6.5.5** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению некорректной обработки ошибок путем использования методик, исключающих утечку информации через сообщения об ошибках (например, отображая общие, а не конкретные сведения об ошибке).	Вследствие некорректной обработки ошибок в приложении может происходить непреднамеренная утечка информации о конфигурации и внутренних процессах функционирования или разглашение информации о правах доступа. Злоумышленники используют эти проблемы 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 сервера. Например, сообщение "введен неправильный пароль" говорит злоумышленнику о том, что использовалось верное имя пользователя и теперь необходимо сфокусировать свои усилия только на подборе пароля. Следует использовать сообщения об ошибках более общего характера, например: "данные не могут быть подтверждены".
6.5.6 Все уязвимости с высокой степенью риска, найденные в процессе обнаружения уязвимостей (в соответствии с требованием 6.1 стандарта PCI DSS).	**6.5.6** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению уязвимостей с высокой степенью риска, которые могут повлиять на работу приложения (в соответствии с требованием 6.1 стандарта PCI DSS).	Все уязвимости, которым была присвоена высокая степень риска (в соответствии с требованием стандарта 6.1) и которые могут повлиять на работу приложения, должны быть выявлены и устранены во время разработки приложения.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
Примечание. *Требования 6.5.7–6.5.10, приведенные ниже, распространяются на веб-приложения и интерфейсы приложений (внешние или внутренние):*		веб-приложениям, как внутренним, так и внешним (общедоступным), свойственны уникальные риски для безопасности в связи с их архитектурой, а также относительная простота и распространенность взлома.
6.5.7 Межсайтовый скриптинг (XSS)	**6.5.7** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению межсайтового скриптинга (XSS), в том числе: • 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 жертвы для захвата сеансов пользователя, изменения вида веб-сайтов, возможного внедрения червей и т.д.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.5.8 Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий и отсутствие ограничения прав доступа пользователя к функциям).	**6.5.8** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению ошибок в контроле доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий), в том числе: • 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. Необходимо обеспечить надлежащий контроль доступа на уровне представления и бизнес-логики для всех URL-адресов. Часто единственным способом защиты критичной функциональности является предотвращение отображения ссылок или URL-адресов несанкционированным пользователям. Злоумышленники могут использовать эти уязвимости для выполнения неавторизованных операций посредством прямого доступа к URL-адресам. Злоумышленник может просканировать структуру директорий веб-сайта (обход директорий), чтобы получить неавторизованный доступ к данным или информации о функционировании сайта. Если пользовательские интерфейсы не ограничивают доступ к запрещенным функциям, это может позволить злоумышленникам получить доступ к привилегированным учетным данным или данным держателей карт.доступ к прямым ссылкам на конфиденциальный ресурс должен быть разрешен только авторизованным пользователям. Ограничение доступа к ресурсам данных поможет предотвратить передачу данных держателей карт на неавторизованные ресурсы.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.5.9 Подделка межсайтовых запросов (CSRF).	**6.5.9** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению подделки межсайтовых запросов и обеспечению того, чтобы приложения не полагались 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).
6.5.10 Противодействие взлому механизмов аутентификации и управления сеансами ***Примечание.*** *До 30 июня 2015 года требование 6.5.10 носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**6.5.10** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по противодействию взлому механизмов аутентификации и управления сеансами, в том числе: • 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.6 Следует обеспечить защиту общедоступных веб-приложений от известных атак (а также регулярно учитывать новые угрозы и уязвимости) одним из следующих методов: • проверять приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности приложений не реже одного раза в год, а также после внесения изменений. ***Примечание.*** *Данная оценка отличается от сканирования на наличие уязвимостей в требовании 11.2.* • Перед общедоступным веб-приложением должно быть установлено техническое средство для постоянной проверки всего трафика (например, веб-брандмауэр) с целью обнаружения и предупреждения веб-атак.	**6.6** Для *общедоступных* веб-приложений *проверить* выполнение одного из следующих требований: • изучить документированные процессы и отчеты о результатах анализа защищенности приложений и опросить сотрудников, чтобы убедиться, что анализ (с использованием средств или методов ручного или автоматического анализа защищенности приложений) общедоступных веб-приложений проходит следующим образом: - не реже одного раза в год; - после любых изменений; - организацией, которая специализируется на безопасности приложений; - анализ включает как минимум проверку на наличие всех уязвимостей, приведенных в требовании 6.5; - все уязвимости устраняются; - безопасность приложения анализируется повторно после принятия корректирующих действий. • Изучить стандарты системной конфигурации и опросить ответственных сотрудников, чтобы убедиться, что перед общедоступным веб-приложением установлено автоматизированное техническое средство (например, веб-брандмауэр) для обнаружения и предупреждения веб-атак, отвечающее следующим требованиям: - расположение перед общедоступным веб-приложением для обнаружения и предупреждения веб-атак; - работа в активном режиме и постоянное обновление; - создание журналов регистрации событий; - настройка на блокирование веб-атак или создание предупреждений о них.	Общедоступные веб-приложения являются основной целью для злоумышленников и некорректно написанные веб-приложения могут упростить злоумышленникам получение доступа к критичным данным и системам. Целью требования проверки приложений или установки веб-брандмауэра является снижение количества взломов веб-приложений вследствие высокой уязвимости программного кода или ненадлежащего контроля приложений. • Средства и методы ручной или автоматизированной оценки защищенности приложений используются для анализа и (или) проверки приложений на наличие уязвимостей • Межсетевые экраны прикладного уровня используются для фильтрации и блокировки ненужного трафика на уровне приложений. При использовании совместно с межсетевым экраном сетевого уровня правильно сконфигурированный межсетевой экран прикладного уровня позволяет предотвратить атаки уровня приложений, если приложения настроены ненадлежащим образом или имеются уязвимости в коде. ***Примечание.*** *Организацией, которая специализируется на безопасности приложений, может быть сторонняя компания или внутренняя организация, сотрудники которой специализируются на безопасности приложений и независимы от группы разработчиков.*

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
6.7 Убедиться, что политики безопасности и процедуры разработки для обеспечения безопасности систем и приложений документированы, используются и известны всем заинтересованным лицам.	**6.7** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры разработки и обеспечения безопасности систем и приложений: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения безопасной разработки и защиты систем и приложений от уязвимостей на постоянной основе.

Внедрение строгих мер контроля доступа

Требование 7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью

Для гарантии того, что доступ к конфиденциальным данным есть только у авторизованного персонала, системы и приложения должны ограничивать доступ к данным в соответствии с принципом служебной необходимости.

Принцип служебной необходимости – права доступа предоставляются только к тем данным, которые необходимы для выполнения должностных или договорных обязанностей.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
7.1 Доступом к вычислительным ресурсам и данным держателей карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	**7.1** Изучить задокументированную политику контроля доступа и убедиться, что она отражает требования 7.1.1–7.1.4 следующим образом: • определение прав доступа и назначение привилегий для каждой должности; • доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей; • назначение прав доступа пользователям должно быть основано на классификации должностей и их должностных обязанностях; • документированное утверждение всех прав доступа полномочными сторонами (в письменной или электронной форме) с описанием конкретных утвержденных привилегий.	Чем больше людей имеют доступ к данным держателей карт, тем выше риск использования злоумышленниками пользовательских учетных записей. Предоставление доступа лишь тем сотрудникам, которым он необходим для выполнения должностных обязанностей, позволит организации предотвратить ненадлежащее обращение с данными держателей карт, связанное с отсутствием опыта или злым умыслом.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
7.1.1 Определение прав доступа для каждой должности, включая: • системные компоненты и ресурсы данных, доступ к которым необходим для каждой должности для выполнения должностных обязанностей; • необходимый уровень привилегий (например, пользователь, администратор и т.д.) для доступа к ресурсам.	**7.1.1** Сделать выборку должностей и убедиться, что права доступа для каждой должности определены и включают: • системные компоненты и ресурсы данных, доступ к которым необходим для каждой должности для выполнения должностных обязанностей; • список прав доступа, необходимых для каждой должности для выполнения должностных обязанностей.	Для предоставления доступа к данным держателей карт только тем лицам, которым он необходим, сначала нужно определить права доступа для каждой должности (например, системного администратора, сотрудника колл-центра, продавца), системы, устройства и данные, доступ к которым необходим для каждой должности, и уровень прав доступа, необходимых для каждой должности для эффективного выполнения должностных обязанностей. После определения должностей и необходимых прав доступа, лицам могут быть назначены соответствующие права доступа.
7.1.2 Предоставить пользователям с учетными записями с широкими полномочиями доступ только к тем полномочиям, которые необходимы им для выполнения своих должностных обязанностей.	**7.1.2.a** Опросить сотрудников, ответственных за назначение прав доступа, для подтверждения того, что доступ к учетным записям с широкими полномочиями: • предоставлен только сотрудникам, которым он необходим; • включает только те полномочия, которые необходимы сотрудникам для выполнения своих должностных обязанностей.	При назначении учетных записей с широкими полномочиями важно предоставлять лицам доступ только к тем полномочиям, которые необходимы для выполнения должностных обязанностей ("минимально необходимые полномочия"). Например, администратор баз данных или администратор резервного копирования не должны иметь те же полномочия, что и системный администратор. *(Продолжение на следующей странице)*
	7.1.2.b Сделать выборку учетных записей с широкими полномочиями и опросить руководство для подтверждения того, что назначенные полномочия: • необходимы для выполнения должностных обязанностей; • включают только те полномочия, которые необходимы сотрудникам для выполнения своих должностных обязанностей.	Назначение минимальных полномочий 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
7.1.3 Назначать права доступа пользователям на основании классификации должностей и их должностных обязанностей.	**7.1.3** Сделать выборку учетных записей и опросить руководство для подтверждения того, что полномочия назначены на основании классификации должностей и должностных обязанностей сотрудников.	После определения прав доступа для каждой должности (согласно требованию 7.1.1 стандарта PCI DSS) сотрудникам можно легко назначить права доступа на основании классификации должностей и их должностных обязанностей, используя для этого уже созданные должности.
7.1.4 Требовать документального утверждения прав доступа уполномоченными лицами с указанием необходимых полномочий.	**7.1.4** Сделать выборку учетных записей и сравнить их с документированным утверждением, чтобы убедиться, что: • имеется документированное утверждение назначенных полномочий; • права доступа утверждены уполномоченными лицами; • указанные полномочия соответствуют должности сотрудника.	Документированное утверждение (например, в письменном или электронном виде) гарантирует, что права доступа и полномочия известны и утверждены руководством, а доступ необходим для выполнения должностных обязанностей.
7.2 Следует установить систему контроля доступа к системным компонентам, основанную на принципе необходимых полномочий и применить принцип "запрещено все, что явно не разрешено" ("deny all"). Система контроля доступа должна включать следующее.	**7.2** Изучить настройки системы и документацию изготовителя, убедиться, что система контроля доступа включает в себя следующее.	Без механизма предоставления доступа по принципу служебной необходимости пользователь может получить доступ к данным держателей карт, не испытывая необходимости в этом для выполнения своих должностных обязанностей. Система контроля доступа автоматизирует процесс ограничения доступа и назначения полномочий. Кроме того, параметр по умолчанию "запрещено все, что явно не разрешено" ("deny all") гарантирует, что ни один сотрудник не получит прав доступа, до тех пор пока не будет создано правило, в соответствии с которым будут предоставлены эти права. ***Примечание.*** *Некоторые механизмы контроля доступа применяют правило "разрешить все" по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.*
7.2.1 Покрытие всех системных компонентов.	**7.2.1** Подтвердить, что система контроля доступа внедрена на всех системных компонентах	
7.2.2 Назначение полномочий пользователям должно быть основано на их должностных обязанностях.	**7.2.2** Назначение привилегий пользователям основано на их должностных обязанностях.	
7.2.3 По умолчанию должен быть запрещен любой доступ.	**7.2.3** Запрещение любого доступа по умолчанию.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
7.3 Убедиться, что политики безопасности и процедуры ограничения доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**7.3** Изучить документацию и опросить сотрудников, чтобы убедиться в том, что политики безопасности и процедуры по ограничению доступа к данным держателей карт: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения контроля доступа и предоставления доступа только к необходимым данным и минимально необходимым привилегиям на постоянной основе.

Требование 8. Определять и подтверждать доступ к системным компонентам

Назначение уникального идентификатора каждому лицу, имеющему доступ, обеспечивает однозначную ответственность этого лица за его действия. Это гарантирует, что действия, производимые с критичными данными и системами, производятся известными и авторизованными пользователями и могут быть отслежены.

Эффективность пароля во многом зависит от устройства и реализации системы аутентификации, в особенности от того, насколько часто может производиться попытка ввода пароля и какие меры безопасности предпринимаются для защиты паролей пользователей в точке ввода, в момент передачи и во время хранения.

Примечание. *Данные требования применимы ко всем учетным записям, включая учетные записи на терминалах оплаты, имеющие административные полномочия, и все учетные записи, использующиеся для просмотра или доступа к данным держателей карт или системам, содержащим данные держателей карт. Сюда относятся учетные записи поставщиков и других третьих лиц (например, для поддержки или техобслуживания).*

Однако требования 8.1.1, 8.2, 8.5, 8.2.3–8.2.5 и 8.1.6–8.1.8 не относятся к учетным записям пользователей платежных приложений в точках продаж, которые обладают единовременным доступом только к одному номеру карты для проведения одной транзакции (например, кассовые счета).

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.1 Определить и внедрить политики и процедуры управления идентификацией сотрудников (не клиентов) и администраторов на всех системных компонентах, регламентирующие следующие требования.	**8.1.a** Изучить процедуры и подтвердить, что они регламентируют процессы для выполнения каждого из нижеуказанных требований 8.1.1–8.1.8	Уникально идентифицируя каждого пользователя – вместо использования одного идентификатора для нескольких сотрудников – организация может поддерживать индивидуальную ответственность сотрудников за свои действия и эффективно отслеживать все действия, выполняемые каждым сотрудником. Это поможет ускорить разрешение и предотвращение происходящих инцидентов, связанных с информационной безопасностью.
	8.1.b Убедиться в том, что процедуры управления идентификацией пользователей соответствуют следующим требованиям.	
8.1.1 Каждому пользователю должен быть назначен уникальный идентификатор до предоставления ему доступа к системным компонентам или данным держателей карт.	**8.1.1** Опросить административный персонал и подтвердить, что каждому пользователю назначен уникальный идентификатор для доступа к системным компонентам или данным держателей карт.	
8.1.2 Контроль добавления, удаления и изменения идентификаторов пользователей, аутентификационных данных и иных объектов идентификации.	**8.1.2** Сделать выборку учетных записей с широкими полномочиями и общих учетных записей, изучить связанные с ними авторизационные мероприятия и проверить настройки системы, чтобы убедиться, что каждая учетная запись наделена только теми полномочиями, которые указаны в документированном утверждении.	Для обеспечения гарантии того, что получившие доступ к системам пользователи действительны и правомочны, любые добавления, удаления и изменения пользовательских идентификаторов и других учетных данных для проверки подлинности должны строго контролироваться.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.1.3 Немедленный отзыв доступа при увольнении пользователя.	**8.1.3.a** Сделать выборку уволенных за прошедшие шесть месяцев сотрудников и проанализировать списки доступа – как локального, так и удаленного, – чтобы убедиться в том, что их учетные записи заблокированы или удалены из списков доступа.	Если сотрудник уволился из компании и все еще имеет доступ к сети через свою учетную запись, существует риск несанкционированного или злонамеренного доступа к данным держателей карт через старую и (или) неиспользуемую учетную запись со стороны бывшего сотрудника или злоумышленника. Для предотвращения несанкционированного доступа пользовательские учетные данные и другие средства аутентификации должны быть отозваны немедленно (как можно скорее) после ухода сотрудника.
	8.1.3.b Убедиться, что все физические средства аутентификации (например, смарт-карты, токены и т.д.) были возвращены или деактивированы.	
8.1.4 Проводить удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней.	**8.1.4** Изучить учетные записи пользователей и убедиться в том, что неактивные более 90 дней учетные записи удаляются или блокируются.	Редко используемые учетные записи часто подвергаются атакам в связи с меньшей вероятностью того, что изменения (например, смена пароля) будут замечены. Следовательно, такие учетные записи легче взломать и использовать для доступа к данным держателей карт.
8.1.5 Управлять учетными записями, используемыми поставщиками для удаленного доступа, поддержки и обслуживания системных компонентов, следующим образом: • включать только на необходимый промежуток времени и отключать, когда они не используются; • проводить мониторинг во время их использования.	**8.1.5.a** Опросить сотрудников и изучить процессы управления учетными записями, используемыми поставщиками для доступа, поддержки и обслуживания системных компонентов, чтобы убедиться в том, что учетные записи, используемые поставщиками для удаленного доступа: • отключаются, когда они не используются; • включаются только когда они нужны поставщику и отключаются, когда они не используются.	Предоставление поставщикам круглосуточного доступа в сеть организации семь дней в неделю для поддержки систем увеличивает вероятность несанкционированного доступа, осуществляемого пользователями из среды поставщика или злоумышленником, который обнаружит и сможет использовать внешнюю, постоянно доступную для подключений точку входа в сеть. Включение доступа только на необходимый промежуток времени и отключение его, когда в нем нет необходимости, помогает предотвратить ненадлежащее использование таких подключений. Мониторинг доступа поставщиков позволяет убедиться в том, что поставщики получают доступ только к необходимым системам и только в соответствующий промежуток времени.
	8.1.5.b Опросить сотрудников и изучить процессы, чтобы убедиться, что во время выполнения работ учетные записи, используемые поставщиками дистанционно, контролируются.	
8.1.6 Блокировать учетные записи	**8.1.6.a** Сделать выборку системных компонентов,	Без реализованного механизма блокировки

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
после шести неудачных попыток входа подряд.	проверить настройки системной конфигурации и убедиться в том, что учетная запись пользователя блокируется после не более чем шести неудачных попыток входа. **8.1.6.b** ***Дополнительная процедура проведения проверки для поставщиков услуг*****:** Изучить внутренние процессы и клиентскую/пользовательскую документацию и понаблюдать за внедренными процессами, чтобы убедиться в том, что неклиентская учетная запись временно блокируется после не более чем шести неудачных попыток входа.	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 записи.
8.1.7 Установить период блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором.	**8.1.7** Сделать выборку системных компонентов, проверить настройки системной конфигурации и убедиться в том, что учетная запись пользователя блокируется не менее чем на 30 минут, либо до момента, пока администратор не снимет блокировку.	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 или специалист технической поддержки может установить, действительно ли ее запросил владелец учетной записи.
8.1.8 Блокировать сеанс работы пользователя через 15 минут простоя с требованием ввода пароля для разблокировки, повторной активации терминала или сеанса.	**8.1.8** Сделать выборку системных компонентов, проверить настройки системной конфигурации и убедиться в том, что сеанс работы пользователя или система блокируется не позднее чем через 15 минут простоя.	Когда пользователи отлучаются от работающих компьютеров, имеющих доступ к критичным компонентам сети или данным держателей карт, эти компьютеры могут использоваться кем-нибудь в их отсутствие, что приведет к несанкционированному доступу к учетной записи и (или) ненадлежащему ее использованию. Повторная проверка подлинности может быть применена на системном уровне для защиты всех сеансов, запущенных на компьютере или на уровне приложений.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.2 Помимо назначения уникального идентификатора, для обеспечения надлежащего управления аутентификацией сотрудников (не пользователей) и администраторов на уровне всех системных компонентов должен применяться хотя бы один из следующих методов аутентификации всех пользователей: • то, что вы знаете (например, пароль или парольная фраза); • то, что у вас есть (например, ключи или смарт-карты); • то, чем вы обладаете (например, биометрические параметры).	**8.2** Проверить, что для аутентификации пользователей применяются уникальный идентификатор и дополнительные механизмы аутентификации (например, пароль или парольная фраза) для доступа к информационной среде держателей карт.для этого: • изучить документацию, описывающую метод (методы) аутентификации; • для каждого типа метода аутентификации и каждого типа системного компонента проверить, что метод аутентификации работает в соответствии с документацией.	Данные методы аутентификации при использовании совместно с уникальными идентификаторами помогают защитить уникальные идентификаторы пользователей от взлома, поскольку злоумышленнику нужно знать и уникальный идентификатор, и пароль (или другой элемент аутентификации). Учтите, что цифровой сертификат является подходящим вариантом для аутентификации по типу "то, что у вас есть", если он уникальный. Поскольку одним из первых действий, которые злоумышленник предпринимает для получения доступа к системе, является использование простых или отсутствующих паролей, важно внедрить и использовать надежные процессы управления аутентификацией пользователей.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.2.1 Все учетные данные для проверки подлинности (например, пароли/парольные фразы) должны храниться и передаваться только в зашифрованном виде с использованием стойкого шифрования на всех компонентах системы.	**8.2.1.a** Изучить документацию поставщика и настройки системной конфигурации, чтобы убедиться, что пароли защищены стойким шифрованием во время передачи и хранения.	Многие сетевые устройства и приложения передают незашифрованные пароли по сети и (или) хранят пароли без применения шифрования. Злоумышленник может перехватить незашифрованные пароли при их передаче, используя анализатор пакетов, или получить прямой доступ к незашифрованным паролям в файлах, в которых они хранятся, и использовать эти данные для получения несанкционированного доступа.
	8.2.1.b Сделать выборку системных компонентов, изучить файлы паролей и убедиться в том, что пароли нечитаемы при хранении.	
	8.2.1.c Сделать выборку системных компонентов, изучить процессы передачи данных и убедиться в том, что пароли нечитаемы при передаче.	
	8.2.1.d ***Дополнительная процедура проведения тестирования для поставщиков услуг*:** изучить файлы паролей и убедиться в том, что клиентские пароли нечитаемы при хранении.	
	8.2.1.e ***Дополнительная процедура проведения проверки для поставщиков услуг:*** изучить процессы передачи данных и убедиться в том, что клиентские пароли нечитаемы при передаче.	
8.2.2 Перед изменением учетных данных для проверки подлинности (например, сбросом пароля, предоставлением новых токенов или генерацией новых ключей) необходимо установить личность пользователя.	**8.2.2** Изучить процедуры аутентификации и процедуры изменения учетных данных для проверки подлинности и убедиться в том, что при запросе сброса учетных данных для проверки подлинности по телефону, электронной почте, с использованием веб-приложения или иным удаленным способом, личность пользователя удостоверяется перед выполнением запроса.	Многие злоумышленники используют социальную инженерию – например, звонят в службу поддержки для изменения пароля и действуют как легитимный пользователь, чтобы затем получить возможность использовать идентификатор пользователя. Рекомендуется использовать секретный вопрос, ответ на который может дать только реальный пользователь, для помощи администраторам в идентификации пользователя перед сбросом или изменением учетных данных для проверки подлинности.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.2.3 Пароли/парольные фразы должны соответствовать следующим требованиям: • наличие в пароле не менее семи символов; • наличие в пароле и цифр, и букв; как вариант, пароли/парольные фразы должны иметь сложность и стойкость, сравнимые с указанными выше параметрами.	**8.2.3.a** Сделать выборку системных компонентов, проверить настройки системной конфигурации и убедиться в том, что пароли должны соответствовать следующим требованиям к сложности и стойкости: • наличие в пароле не менее семи символов; • наличие в пароле и цифр, и букв.	Надежные пароли/парольные фразы являются первой линией обороны в сети, поскольку злоумышленник обычно сначала пытается найти учетные записи с простыми или отсутствующими паролями. Злоумышленнику относительно просто найти слабозащищенные учетные записи и проникнуть в сеть под видом настоящего пользователя, если используются короткие или легкоугадываемые пароли. В соответствии с данным требованием пароли/парольные фразы должны насчитывать не менее семи символов и содержать и 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/парольных фраз разных форматов.
	8.2.3.b ***Дополнительная процедура проведения проверки для поставщиков услуг*:** изучить внутренние процессы и клиентскую/пользовательскую документацию и убедиться в том, что пароли сотрудников должны соответствовать следующим требованиям к сложности и стойкости: • наличие в пароле не менее семи символов; • наличие в пароле и цифр, и букв.	
8.2.4 Изменение паролей/парольных фраз пользователей не реже одного раза в 90 дней.	**8.2.4.a** Сделать выборку нескольких системных компонентов, проверить настройки системной конфигурации и убедиться в том, что пользователь должен менять пароль не реже одного раза в 90 дней.	Пароли/парольные фразы, не изменяемые в течение длительного времени, дают злоумышленникам больше возможностей для их взлома.
	8.2.4.b ***Дополнительная процедура проведения проверки для поставщиков услуг**: изучить внутренние* процессы и клиентскую/пользовательскую документацию и убедиться в том, что: • требуется периодическое изменение паролей сотрудников (не клиентов); и • сотрудники (не клиенты) получают инструкции о том, когда и при каких обстоятельствах пароль должен быть изменен.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.2.5 Запрет смены пароля/парольной фразы на какие-либо из четырех последних паролей/парольных фраз данного пользователя, использованных им ранее.	**8.2.5.a** Сделать выборку нескольких системных компонентов, проверить настройки системной конфигурации и убедиться в том, что новый пароль должен отличаться от четырех использованных ранее паролей.	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.
	8.2.5.b ***Дополнительная процедура проведения проверки для поставщиков услуг:*** изучить внутренние процессы и клиентскую/пользовательскую документацию и убедиться в том, что новый пароль сотрудника (не клиента) должен отличаться от четырех предыдущих паролей, которые он использовал ранее.	
8.2.6 Установка уникального первоначального пароля/парольной фразы для каждого пользователя и их немедленное изменение при первом входе пользователя в систему.	**8.2.6** Изучить парольные процедуры и убедиться в том, что для первого входа в систему новому пользователю устанавливается, а для существующих пользователей предустанавливается уникальный первоначальный пароль, который изменяется при первом входе в систему.	Если для каждого нового пользователя устанавливается один и тот же пароль, то внутренний пользователь, бывший сотрудник или злоумышленник могут знать или легко обнаружить этот пароль и использовать его для получения доступа к учетным записям.
8.3 Для средств удаленного доступа сотрудников (включая пользователей и администраторов) и любых третьих лиц (включая доступ поставщиков для поддержки или техобслуживания) во внутреннюю сеть из внешней сети должен быть реализован механизм двухфакторной аутентификации. ***Примечание.*** *Двухфакторная аутентификация требует, чтобы для аутентификации использовались два из трех методов аутентификации (описание методов аутентификации см. в Требовании 8.2). Использование одного метода дважды (например, использование двух различных паролей) не считается двухфакторной аутентификацией.* *К примерам технологий двухфакторной аутентификации*	**8.3.a** Изучить системные конфигурации серверов и систем удаленного доступа и убедиться, что двухфакторная аутентификация требуется для: • любого доступа сотрудников, осуществляемого удаленно; • любого доступа третьих лиц/поставщиков, осуществляемого удаленно (включая доступ к приложениям и системным компонентам в целях поддержки или техобслуживания).	Двухфакторная аутентификация требует двух форм аутентификации для доступа с более высоким уровнем риска, например доступа к сети извне Данное требование применяется ко всем сотрудникам (включая обычных пользователей, администраторов и поставщиков, осуществляющих поддержку или техобслуживание), которые имеют удаленный доступ к сети, если такой удаленный доступ может привести к доступу к информационной среде держателей карт. Если удаленный доступ осуществляется к сети, которая сегментирована таким образом, что удаленные пользователи не могут получить доступ к среде данных держателей карт, двухфакторная аутентификация для удаленного доступа к такой сети не является обязательной. Однако двухфакторная аутентификация требуется для удаленного доступа к сети, если пользователь получает доступ к среде данных
	8.3.b Проследить за тем, как сотрудники (например, пользователи или администраторы) осуществляют удаленный доступ к сети и убедиться, что используются как минимум два из трех методов аутентификации.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
относятся такие технологии, как RADIUS с токенами; TACACS с токенами и другие технологии, способствующие двухфакторной аутентификации.		держателей карт, и рекомендуется для любого удаленного доступа к сетям организации.
8.4 Задокументировать и проинформировать всех пользователей о процедурах и политиках аутентификации, включая: • рекомендации по выбору стойких учетных данных для аутентификации; • рекомендации по защите учетных данных для аутентификации; • указания не использовать ранее использованные пароли; • инструкции по смене пароля в случае подозрения на взлом.	**8.4.a** Изучить процедуры и опросить сотрудников для подтверждения того, что процедуры и политики аутентификации доведены до всех пользователей.	Информирование всех пользователей о процедурах в отношении паролей и аутентификации помогает пользователям понять эти процедуры и следовать этим политикам. Например, рекомендации по выбору стойких паролей могут включать советы по выбору трудноугадываемых паролей, которые не содержат словарных слов или информацию о пользователе (например, имя пользователя, имена членов семьи, дата рождения и т.д.). Рекомендации по защите учетных данных для проверки подлинности могут быть следующими: не записывать пароли и не сохранять их в незащищенных файлах (это помогает пользователям понять эти процедуры и следовать политике). А также предупреждать пользователей о злоумышленниках, которые могут попытаться использовать их пароли (например, звонящих сотруднику с просьбой дать его пароль для решения какой-либо проблемы). Рассылка пользователям рекомендации сменить пароли, если есть вероятность, что пароль больше не является надежным, может не позволить злоумышленникам использовать реальный пароль для получения несанкционированного доступа.
	8.4.b Изучить процедуры и политики аутентификации для пользователей и убедиться, что они включают: • рекомендации по выбору стойких учетных данных для аутентификации; • рекомендации по защите учетных данных для аутентификации; • указания не использовать ранее использованные пароли; • инструкции по смене пароля в случае подозрения на взлом.	
	8.4.c Опросить несколько пользователей, чтобы убедиться в том, что им известны положения политик и процедур аутентификации.	
8.5 Не использовать групповые, общие и стандартные учетные записи и пароли, а также прочие подобные методы аутентификации и убедиться в том, что: • стандартные учетные записи заблокированы или удалены;	**8.5.a** Сделать выборку системных компонентов, проверить списки учетных записей пользователей и убедиться в следующем: • стандартные учетные записи заблокированы или удалены; • общие учетные записи для функций администрирования и иных критичных функций не существуют;	При использовании несколькими пользователями одних и тех же учетных данных для аутентификации (например, учетной записи и пароля) становится невозможным проследить за доступом в систему и действиями того или иного пользователя. Это, в свою очередь, не позволит организации назначить

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
• общие учетные записи для системного администрирования и иных критичных функций не существуют; • общие и стандартные учетные записи не используются для администрирования каких-либо системных компонентов.	• общие и стандартные учетные записи не используются для администрирования каких-либо системных компонентов.	ответственность за действия, выполненные тем или иным пользователем, или фактически регистрировать события, связанные с этими действиями, поскольку эти действия могут быть совершены любым членом группы, которому известны учетные данные для аутентификации.
	8.5.b Изучить политику и процедуры аутентификации и убедиться, что они запрещают использование групповых и общих учетных записей, паролей и прочих подобных средств аутентификации.	
	8.5.c Опросить системных администраторов и убедиться в том, что пользователям не выдаются групповые и общие учетные записи и (или) пароли и прочие подобные средства аутентификации, даже если таковые запрашиваются.	
8.5.1 ***Дополнительное требование для поставщиков услуг:*** поставщики услуг, имеющие удаленный доступ к помещению клиента (например, для поддержки систем или серверов кассовых терминалов), обязаны использовать уникальные учетные данные для аутентификации (например, пароль/парольная фраза) для каждого клиента. ***Примечание.*** *Это требование не распространяется на хостинг-провайдеров, осуществляющих доступ к своей общей хостинговой среде, в которой размещены среды нескольких клиентов.* ***Примечание.*** *До 30 июня 2015 года требование 8.5.1 носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**8.5.1** ***Дополнительная процедура проведения тестирования для поставщиков услуг:*** изучить политики и процедуры аутентификации и опросить сотрудников для подтверждения того, что для каждого клиента используются свои учетные данные.	Чтобы предотвратить взлом учетных записей нескольких клиентов путем взлома единых учетных данных, поставщики, осуществляющие удаленный доступ к средам клиентов, должны использовать разные учетные данные для аутентификации каждого клиента. Такие технологии, как двухфакторная аутентификация, обеспечивающая уникальность учетных данных для каждого подключения (например, с помощью одноразового пароля), также могут отвечать данному требованию.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
8.6 В случае использования других механизмов аутентификации (например, физических или логических токенов безопасности, смарт-карт, сертификатов и т.д.), эти механизмы должны назначаться следующим образом: • механизмы аутентификации должны назначаться для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу; • необходимо использовать физические и (или) логические механизмы контроля, чтобы только авторизованный пользователь мог использовать такие механизмы для получения доступа.	**8.6.a** Изучить политики и процедуры аутентификации, чтобы убедиться, что процедуры использования механизмов аутентификации (например, физических токенов безопасности, смарт-карт и сертификатов) определены и включают следующие требования: • механизмы аутентификации должны назначаться для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу; • необходимо использовать физические и (или) логические механизмы контроля, чтобы только авторизованный пользователь мог использовать такие механизмы для получения доступа.	Если механизмы пользовательской аутентификации (например, физические токены безопасности, смарт-карты и сертификаты) могут использоваться несколькими учетными записями, то определить пользователя, использующего этот механизм аутентификации, будет невозможно. Наличие физических и (или) логических механизмов контроля (например, PIN-код, биометрические данные или пароль), уникальных для каждого пользователя, не позволит злоумышленникам получить доступ с помощью общего механизма аутентификации.
	8.6.b Опросить сотрудников службы безопасности и убедиться, что механизмы аутентификации назначаются для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу.	
	8.6.c Изучить настройки системной конфигурации и, при необходимости, физические механизмы контроля, чтобы убедиться, что только авторизованный пользователь может использовать такие механизмы для получения доступа.	
8.7 Любой доступ к базе данных держателей карт (включая доступ со стороны приложений, администраторов и любых других пользователей) должен быть ограничен следующим образом: • доступ, запросы и операции с базами данных должны осуществляться только программными методами; • разрешение запросов и прямого	**8.7.a** Проанализировать настройки баз данных и приложений, проверить, что пользователи проходят аутентификацию перед предоставлением доступа.	Если аутентификация пользователя для доступа к базам данных и приложениям не выполняется, увеличивается риск неавторизованного или злонамеренного доступа. Кроме того, события, связанные с таким доступом, не могут быть зарегистрированы, поскольку пользователь не аутентифицируется и, следовательно, неизвестен системе. Доступ к базам данных должен предоставляться только программными методами (например, с использованием хранимых процедур), а не посредством прямого доступа к базе данных конечными
	8.7.b Проанализировать настройки баз данных и приложений и убедиться, что пользовательские операции с данными (доступ, запрос, перемещение, копирование, удаление) осуществляются только программными методами (например, с использованием хранимых процедур).	
	8.7.c Убедиться, что настройки контроля доступа к базам данных и настройки приложений для доступа к базам	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
доступа к базам данных только для администраторов баз данных; • учетные записи приложений по управлению базами данных могут использоваться только приложениями (но не пользователями или иными процессами).	данных разрешают запросы и прямой доступ к базам данных только для администраторов баз данных. **8.7.d** Изучить настройки контроля доступа к базам данных, настройки и учетные записи приложений для доступа к базам данных и убедиться в том, что учетные записи приложений могут использоваться только приложениями (но не пользователями или иными процессами).	пользователями (за исключением администраторов баз данных, которым может потребоваться прямой доступ к базе данных для выполнения своих административных обязанностей).
8.8 Убедиться, что политики безопасности и процедуры идентификации и аутентификации документированы, используются и известны всем заинтересованным лицам.	**8.8** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры идентификации и аутентификации: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах управления идентификацией и аутентификацией на постоянной основе.

Требование 9. Ограничить физический доступ к данным держателей карт

Любой физический доступ к данным или системам, содержащим данные держателей карт, предоставляет возможность получить контроль над устройствами и данными, а также украсть устройство или документ, и должен быть соответствующим образом ограничен. Согласно Требованию 9, к понятию "персонал" относятся постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на территории организации. Под термином "посетитель" следует понимать поставщиков, гостей сотрудников, обслуживающий персонал и иных лиц, кратковременно находящихся на территории организации, как правило, не более одного дня. Термин "носитель данных" включает в себя бумажные или электронные носители, которые содержат данные держателей карт.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.1 Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные держателей карт.	**9.1** Проверить наличие средств контроля физического доступа в каждый вычислительный центр, дата-центр и иные помещения, в которых располагаются системы, которые хранят, обрабатывают или передают данные держателей карт: • убедиться, что доступ контролируется при помощи устройств считывания бейджей или иных устройств, в том числе утвержденных бейджей и механических замков; • наблюдать за попыткой системного администратора выполнить консольный вход в случайно выбранные системы в среде данных держателей карт и убедиться в том, что он заблокирован, чтобы избежать несанкционированного доступа.	Без физических механизмов контроля доступа (например, бейджей и контроля за входом в помещения) посторонние могут без труда получить доступ к помещениям с целью кражи, отключения, порчи и уничтожения критичных систем и данных держателей карт. Блокировка экрана входа в консоль не позволит посторонним получить доступ к критичной информации, внести изменения в конфигурацию систем, внести уязвимости в сеть или уничтожить данные.
9.1.1 Следует использовать камеры видеонаблюдения или иные механизмы контроля доступа, чтобы следить за критичными	**9.1.1.a** Убедиться в том, что камеры видеонаблюдения и (или) иные механизмы контроля доступа применяются для мониторинга доступа к критичным помещениям/выхода из критичных помещений.	Эти средства контроля помогают выявить лиц, которые имеют физический доступ к критичным помещениям, а также установить, когда они вошли и вышли.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
помещениями. Данные, собранные механизмами контроля доступа, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством. ***Примечание.*** *Критичными являются помещения, относящиеся к любому центру обработки данных, серверной комнате или иному помещению, в котором расположены системы, хранящие, обрабатывающие или передающие данные держателей карт. Исключением являются места расположения кассовых терминалов с открытым доступом, такие как кассовые зоны торговых комплексов.*	**9.1.1.b** Убедиться, что камеры и (или) иные средства защищены от взлома или отключения.	Злоумышленники, желающие получить физический доступ к критичным помещениям, часто пытаются отключить или обойти механизмы слежения. Для защиты таких устройств от взлома можно разместить видеокамеры за пределами досягаемости и (или) установить наблюдение за попытками взлома. Механизмы контроля доступа также могут находиться под наблюдением или быть оснащены физическими средствами защиты от повреждения или отключения злоумышленниками. *(Продолжение на следующей странице)*
	9.1.1.c Убедиться в том, что данные с камер видеонаблюдения и (или) иных механизмов контроля доступа хранятся не менее трех месяцев.	Критичными являются такие помещения, как комнаты с серверами корпоративных баз данных, внутренние помещения, где хранятся данные держателей карт, и хранилища с большим объемом данных держателей карт. Каждая организация должна составить список критичных помещений и убедиться в наличии надлежащих механизмов физического наблюдения.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.1.2 Внедрить механизмы физического и (или) логического контроля для ограничения доступа к сетевым разъемам, расположенным в общедоступных местах. *Например, сетевые разъемы, расположенные в общедоступных местах и местах, доступных посетителям, можно включать только, если доступ к сети однозначно разрешен. Также можно внедрить процессы, исключающие наличие посетителей без сопровождения в помещениях с работающими сетевыми разъемами.*	**9.1.2** Опросить ответственных сотрудников и проверить помещения с общедоступными сетевыми разъемами, чтобы убедиться в наличии механизмов физического и (или) логического контроля для ограничения доступа к сетевым разъемам, расположенным в общедоступных местах.	Ограничение доступа к сетевым разъемам (или портам) поможет предотвратить подключение злоумышленника к сетевым разъемам и получение доступа к внутренним сетевым ресурсам. Независимо от типа используемых механизмов контроля (физических, логических или их комбинации) они должны обеспечивать достаточную защиту от несанкционированного доступа к сети со стороны лиц или устройств.
9.1.3 Доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи должен быть ограничен.	**9.1.3** Убедиться, что физический доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи должным образом ограничен.	Без защиты доступа к беспроводным компонентам и устройствам злоумышленники могут использовать неконтролируемые беспроводные устройства организации для получения доступа к сетевым ресурсам или даже подключать собственные устройства к беспроводной сети для получения несанкционированного доступа. Кроме того, благодаря защите сетевого и коммуникационного оборудования злоумышленники не смогут перехватить сетевой трафик или физически подключить свои собственные устройства к проводным сетевым ресурсам.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.2 Разработать процедуры, позволяющие легко различать персонал организации и посетителей и включающие: • идентификацию новых сотрудников или посетителей (например, путем выдачи бейджей); • внесение изменений в права доступа; • процедуры отзыва или отключения средств идентификации уволенного сотрудника или средств идентификации посетителей с истекшим сроком действия (например, бейджей).	**9.2.a** Проанализировать документированные процессы и убедиться в наличии процедур идентификации и различения сотрудников и посетителей. Проверить, что среди процедур есть следующие: • идентификация новых сотрудников или посетителей (например, путем выдачи бейджей); • изменения прав доступа; • отзыв средств идентификации уволенного сотрудника или средств идентификации посетителей с истекшим сроком действия (например, бейджей).	Выявление авторизованных посетителей помогает предотвратить предоставление доступа неавторизованным посетителям к местам хранения данных держателей карт.
	9.2.b Изучить процессы идентификации и различения сотрудников и посетителей и убедиться, что: • посетители четко идентифицированы; и • можно легко отличить сотрудников организации от посетителей.	
	9.2.c Убедиться, что доступом к системе идентификации (например, к системе выдачи бейджей) обладает только авторизованный персонал.	
	9.2.d Необходимо осмотреть использующиеся средства идентификации (например, бейджи) и убедиться, что посетители четко идентифицированы, и можно легко отличить сотрудников организации от посетителей.	
9.3 Контролировать физический доступ сотрудников к критичным помещениям следующим образом: • права доступа сотрудников должны быть утверждены на основании классификации должностей и их должностных обязанностей; • доступ должен быть отозван сразу после его прекращения и все механизмы физического доступа (например, ключи, карты доступа	**9.3.a** Сделать выборку сотрудников с физическим доступом к информационной среде держателей карт, опросить ответственных сотрудников и изучить списки контроля доступа, чтобы убедиться, что: • доступ к информационной среде держателей карт санкционирован; • доступ необходим для выполнения должностных обязанностей.	Контроль физического доступа к информационной среде держателей карт позволяет гарантировать, что доступ предоставляется только авторизованным сотрудникам, которым он необходим для выполнения должностных обязанностей. При увольнении сотрудника из организации необходимо немедленно (как можно скорее) вернуть или отключить все средства физического доступа, чтобы сотрудники не смогли получить физический доступ к среде
	9.3.b Проследить за входом сотрудников в информационную среду держателей карт и убедиться, что все сотрудники проходят авторизацию перед получением доступа.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
и т.д.) должны быть возвращены или отключены.	**9.3.c** Сделать выборку недавно уволенных сотрудников с физическим доступом и изучить списки контроля доступа, чтобы убедиться, что у них нет физического доступа к информационной среде держателей карт.	данных держателей карт после увольнения.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.4 Внедрить процедуры идентификации и авторизации посетителей. Процедуры должны быть следующими.	**9.4** Проверить наличие авторизации и механизмов контроля доступа посетителей.	Контроль над посетителями снижает риск получения доступа в помещения организации (и, потенциально, к данным держателей карт) посторонними и злоумышленниками. Контроль над посетителями осуществляется для того, чтобы они идентифицировались именно как посетители, а сотрудники могли отслеживать их перемещения и действия; и чтобы продолжительность их нахождения на территории организации была ограничена допустимым временем посещения. Возврат бейджей посетителей после истечения срока действия или завершения посещения не даст злоумышленникам воспользоваться ранее авторизованным пропуском для получения физического доступа в здание после завершения визита. Журнал регистрации посетителей является недорогим и несложным в поддержке средством идентификации физического доступа в здание или помещение и потенциального доступа к данным держателей карт.
9.4.1 Посетители должны проходить авторизацию перед входом в помещения, где обрабатываются или хранятся данные держателей карт, и находиться под наблюдением во время пребывания в них.	**9.4.1.a** Изучить процедуры и опросить сотрудников, чтобы убедиться, что посетители должны проходить авторизацию перед входом в помещения, где обрабатываются или хранятся данные держателей карт, и находиться под наблюдением во время пребывания в них.	
	9.4.1 Понаблюдать за использованием бейджей посетителей или других средств идентификации и убедиться в том, что бейдж не дает возможность получить доступ в помещения, где хранятся данные держателей карт, без сопровождения персонала организации.	
9.4.2 Идентифицировать посетителей и выдавать им бейдж или другое средство идентификации, имеющее ограничение срока действия и позволяющее отличить посетителя от сотрудника организации.	**9.4.2.a** Осмотреть бейджи персонала и посетителей и убедиться в использовании бейджей или других средств идентификации посетителей и в том, что посетителей легко отличить от сотрудников организации.	
	9.4.2.b Убедиться, что бейдж или другое средство идентификации посетителя имеет ограниченный срок действия.	
9.4.3 Требовать от посетителей возврата выданного бейджа или другого средства идентификации при выходе с объекта или при истечении срока его действия.	**9.4.3** Ознакомиться с процессом ухода посетителей с объекта, убедиться, что от посетителей требуется возврат бейджа или другого средства идентификации при уходе либо окончании срока действия.	
9.4.4 Ведется журнал регистрации посетителей как на входе в офисные помещения, так и на входе в вычислительные центры и центры	**9.4.4.a** Убедиться в том, что ведется журнал регистрации посетителей как на входе в офисные помещения, так и на входе в вычислительные центры и центры обработки данных, в которых хранятся или передаются данные держателей карт.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
обработки данных, в которых хранятся или передаются данные держателей карт. В журнале следует регистрировать имя посетителя, организацию, которую он представляет, а также сотрудника организации, разрешившего доступ посетителю. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством.	**9.4.4.b** Убедиться, что журнал содержит: • имя посетителя; • название фирмы, которую он представляет; и • имя сотрудника организации, разрешившего доступ посетителю.	
	9.4.4.c Убедиться в том, что журнал хранится не менее трех месяцев.	
9.5 Должна быть обеспечена физическая безопасность всех видов носителей.	**9.5** Проверить, что процедуры физической защиты данных держателей карт включают меры по защите всех видов носителей (включая, в том числе: компьютеры, съемные электронные носители, бумажные чеки, бумажные отчеты и факсы).	Механизмы обеспечения физической безопасности носителей предназначены для предотвращения несанкционированного доступа к данным держателей карт на носителях любого типа. Если данные держателей карт не защищены должным образом на съемных и портативных носителях, распечатаны или оставлены без присмотра у какого-либо сотрудника на столе, существует вероятность их просмотра, копирования или сканирования неавторизованными лицами.
9.5.1 Носители с резервными копиями данных следует хранить в безопасных местах (желательно вне объекта), таких как запасной центр обработки данных, или же воспользовавшись услугами организаций, обеспечивающих безопасное хранение. Безопасность мест хранения должна проверяться не реже одного раза в год.	**9.5.1.a** Проверить физическую безопасность места хранения носителей с резервными копиями данных и убедиться, что оно безопасно.	Резервные копии могут содержать данные держателей карт, и в случае их хранения в незащищенных помещениях есть риск их утери, кражи или копирования со злым умыслом.
	9.5.1.b Убедиться в том, что безопасность мест хранения резервных копий проверяется не реже одного раза в год.	Периодическая проверка хранилища позволяет организации вовремя устранять обнаруженные проблемы с безопасностью, сводя к минимуму потенциальный риск.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.6 Должен быть обеспечен строгий контроль за передачей всех видов носителей информации внутри организации и вне ее, в том числе следующее.	**9.6** Убедиться в наличии политики, регламентирующей порядок передачи всех видов носителей информации, а также распространение носителей информации среди отдельных лиц.	Процедуры и процессы помогают защитить данные держателей карт на носителях, которые передаются сотрудникам организации или сторонним пользователям. В отсутствие таких процедур существует риск потери или кражи данных либо их использования в мошеннических целях.
9.6.1 Классифицировать носители информации для определения уровня критичности хранимых данных.	**9.6.1** Убедиться в том, что носители информации классифицированы для определения уровня критичности хранимых данных.	Важно, чтобы носитель был промаркирован таким образом, чтобы его статус был очевиден. Носитель, который не маркирован как конфиденциальный, может быть не защищен должным образом, вследствие чего он может быть потерян или украден. ***Примечание.*** *Это не означает, что необходимо прикреплять к носителям маркировку "конфиденциально"; цель требования состоит в идентификации носителей, содержащих критичные данные, для их защиты.*
9.6.2 Пересылку носителей осуществлять только с доверенным курьером или иным способом, который может быть тщательно проконтролирован.	**9.6.2.a** Опросить сотрудников и изучить записи, чтобы убедиться в том, что вынос любого носителя за пределы предприятия должен быть зарегистрирован, а пересылка носителей осуществляется только с доверенным курьером или иным способом, который может быть тщательно проконтролирован и отслежен.	Носитель может быть утерян или украден при отправке с использованием неотслеживаемого метода, такого как обычная почта. Использование услуг курьерской службы для доставки всех носителей, которые содержат данные держателей карт, позволяет организации использовать систему отслеживания, чтобы вести учет местонахождения посылок.
	9.6.2.b Посмотреть недавние записи в журнале перемещения всех носителей за пределы охраняемой территории за несколько последних дней и убедиться, что сведения о перемещении носителей документируются.	
9.6.3 Убедиться, что любой вынос носителей за пределы охраняемой территории (включая передачу носителя частным лицам) утверждается руководством.	**9.6.3** Посмотреть недавние записи в журнале перемещения всех носителей за пределы охраняемой территории за несколько последних дней. Изучить журналы и опросить ответственных сотрудников, чтобы убедиться, что любой вынос носителей за пределы охраняемой территории (включая передачу носителя частным лицам) утверждается руководством.	Без утверждения руководством любого выноса носителей за пределы охраняемой территории невозможно обеспечить отслеживание и надлежащую защиту носителей, их местонахождение будет неизвестно, что приведет к потере или краже носителей.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.7 Должен быть обеспечен строгий контроль хранения носителей и управление доступом к ним.	**9.7** Изучить политику хранения носителей, убедиться в том, что она регламентирует регулярную инвентаризацию носителей.	Без использования методов инвентаризации и контроля за хранением факт кражи или утери носителя может оставаться незамеченным в течение неопределенного периода времени. Если инвентаризация носителей не выполняется, то факт кражи или утери носителя может оставаться незамеченным в течение длительного периода времени.
9.7.1 Должны поддерживаться в актуальном состоянии журналы инвентаризации всех носителей данных держателей карт; инвентаризация носителей должна проводиться не реже одного раза в год.	**9.7.1** Изучить журналы инвентаризации носителей и убедиться, что такие журналы ведутся, а инвентаризация носителей проводится не реже одного раза в год.	
9.8 Носители, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, должны быть уничтожены следующим образом.	**9.8** Изучить политику регулярного уничтожения носителей и убедиться в том, что она распространяется на все носители, и содержит следующие требования: • печатные копии документов должны измельчаться, сжигаться или преобразовываться в целлюлозную массу способом, исключающим их восстановление; • контейнеры для материалов, приготовленных для уничтожения, должны быть защищены; • уничтожение данных держателей карт на электронном носителе должно осуществляться с помощью программы безопасного удаления данных (в соответствии с отраслевыми стандартами безопасного удаления) или путем физического уничтожения носителя.	Если уничтожение информации, содержащейся на жестких дисках компьютеров, портативных накопителях, CD- и DVD-дисках или на бумаге, не выполняется надлежащим образом, злоумышленники могут извлечь эту информацию с утилизированных носителей и получить доступ к данным держателей карт. Например, злоумышленники могут использовать прием, известный под названием "dumpster diving" (исследование содержимого мусорных контейнеров), при котором они просматривают мусорные корзины и используют найденную информацию для проведения атак. Защита контейнеров для материалов, приготовленных для уничтожения, позволяет предотвратить перехват критичной информации при сборе материалов. Например, контейнеры с материалами, подлежащими измельчению, могут быть оборудованы замком для предотвращения доступа к их содержимому. Для безопасного уничтожения электронных носителей можно использовать такие методы, как безопасное стирание, размагничивание или физическое разрушение носителя (например, измельчение жесткого диска).
9.8.1 Измельчение, сжигание или преобразование бумажного носителя в целлюлозную массу, чтобы данные держателей карт не могли быть восстановлены. Контейнеры для материалов, приготовленных для уничтожения, должны быть защищены.	**9.8.1.a** Опросить сотрудников и изучить процедуры, чтобы убедиться, что печатные копии документов измельчаются, сжигаются или преобразуются в целлюлозную массу способом, исключающим их восстановление.	
	9.8.1.b Осмотреть контейнеры для материалов, приготовленных для уничтожения, и убедиться, что они надежно защищены.	
9.8.2 Уничтожение данных держателей карт на электронном носителе, исключающее возможность их восстановления.	**9.8.2** Убедиться в том, что уничтожение данных держателей карт на электронном носителе осуществляется с помощью программы безопасного удаления данных в соответствии с отраслевыми стандартами безопасного удаления или путем физического уничтожения носителя.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.9 Обеспечить защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой, от подделки и подмены. ***Примечание.*** *Данные требования распространяются на устройства считывания данных путем прямого физического взаимодействия с картой (при проведении карты через устройство или при вставке карты в устройство) в точке продаж. Данное требование не распространяется на компоненты ручного ввода ключа (например, компьютерные клавиатуры и клавиатуры кассового терминала).* ***Примечание.*** *До 30 июня 2015 года требование 9.9 носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**9.9** Проверить документированные политики и процедуры на наличие следующих требований: • ведение списка устройств; • периодическая проверка устройств на случай взлома или подмены; • сотрудники должны наблюдать за подозрительными лицами и сообщать о взломе или подмене устройств.	Злоумышленники часто пытаются украсть данные держателей карт путем кражи или подмены считывающих устройств и терминалов. Например, они пытаются украсть устройства, чтобы понять, как их взломать и часто пытаются заменить настоящие устройства на поддельные, присылающие им информацию о платежной карте при каждой вставке карты. Злоумышленники также пытаются установить снаружи устройств так называемые "скиммеры", предназначенные для перехвата данных о платежной карте еще перед ее вставкой в устройство (например, прикрепляя дополнительный кард-ридер сверху настоящего, чтобы данные о платежной карте считывались дважды – сначала поддельным, а затем настоящим компонентом устройства). Таким образом, "скиммеры" считывают информацию с платежной карты, не прерывая финансовую операцию. Данное требование является рекомендуемым, но не обязательным, для компонентов ручного ввода ключа (например, компьютерных клавиатур и клавиатур кассовых терминалов). Дополнительные рекомендации по предотвращению скимминга можно найти на сайте PCI SSC.
9.9.1 Составление и регулярное обновление списка устройств. Список должен включать следующую информацию: • марка и модель устройства; • местонахождение устройства (например, адрес объекта, в котором находится устройство); • серийный номер устройства или другой уникальный	**9.9.1.a** Убедиться, что список устройств включает следующую информацию: • марка и модель устройства; • местонахождение устройства (например, адрес объекта, в котором находится устройство); • серийный номер устройства или другой уникальный идентификатор. **9.9.1.b** Сделать выборку устройств из списка, проверить местонахождение устройств и убедиться, что список является точным и актуальным.	Составление и регулярное обновление списка устройств помогает организации отслеживать предполагаемое местонахождение устройства и быстро обнаружить пропажу. Составление списка устройств может выполняться автоматически (например, с помощью системы управления устройствами) или вручную (например, ведение электронных или бумажных записей). Сведения о местонахождении устройства в процессе перемещения могут включать имя сотрудника,

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
идентификатор.	**9.9.1.c** Опросить сотрудников и убедиться, что список обновляется при каждом добавлении, перемещении, списании устройств и т.д.	за которым это устройство закреплено.
9.9.2 Периодически проверять поверхность устройств для обнаружения признаков взлома (например, прикрепленных к устройствам "скиммеров") или подмены (например, путем проверки серийного номера или других характеристик устройств, чтобы убедиться, что устройство не было заменено на мошенническое). ***Примечание.*** *Признаком того, что устройство было взломано, может служить наличие подозрительных насадок или кабелей, подключенных к устройству, отсутствующие или измененные защитные наклейки (пломбы), поврежденный или перекрашенный корпус, изменение серийного номера или иных внешних обозначений.*	**9.9.2.a** Проверить документированные процедуры на наличие следующих процессов: • процедуры осмотра устройств; • частота осмотра. **9.9.2.b** Опросить ответственных сотрудников и понаблюдать за проведением осмотра для подтверждения того, что: • сотрудники ознакомлены с процедурами осмотра устройств; • все устройства периодически проверяются на наличие следов взлома или замены.	Регулярный осмотр устройств позволит организациям быстрее обнаружить взлом или подмену устройства и, следовательно, снизить потенциальный вред от поддельных устройств. Вид осмотра зависит от устройства (например, можно использовать фотографию изначально безопасного устройства для сравнения текущего вида устройства с оригинальным и обнаружения изменений). Также можно использовать защитный маркер (например, видимый в ультрафиолетовом излучении) для маркировки поверхностей и отверстий устройства, чтобы любой взлом или подмену можно было легко заметить. Злоумышленники часто заменяют внешний кожух устройства, чтобы скрыть следы взлома, и указанные выше методы помогут обнаружить такую замену. Поставщики устройств также часто предоставляют рекомендации по защите и инструкции, которые помогут определить, было ли устройство взломано. Частота осмотра зависит от таких факторов, как местонахождение устройства и наличие наблюдения за устройством. Например, устройства, оставленные сотрудниками организации без присмотра в общедоступном месте, требуют более частых осмотров, чем устройства, расположенные в безопасном месте и находящиеся под присмотром. Тип и частота осмотра определяется торговой точкой согласно процессу ежегодной оценки рисков.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
9.9.3 Обучать сотрудников распознаванию признаков взлома или подмены устройств. Обучение должно включать следующую информацию: • следует установить личность третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами; • не следует устанавливать, заменять или возвращать устройство поставщику без такой проверки; • следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство); • сотрудники должны сообщать о признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности).	**9.9.3.a** Изучить обучающие материалы для сотрудников в точках продаж и убедиться, что они включают следующую информацию: • следует установить личность третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами; • не следует устанавливать, заменять или возвращать устройства без проверки; • следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство); • сотрудники должны сообщать о признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности). **9.9.3.b** Опросить несколько сотрудников в местах установки кассовых терминалов и убедиться, что они прошли обучение и знают, что: • следует установить личность третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами; • не следует устанавливать, заменять или возвращать устройства без проверки; • следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство); • сотрудники должны сообщать о признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности).	Злоумышленники часто выдают себя за авторизованный обслуживающий персонал для получения доступа к устройствам кассовых терминалов. Следует проверять всех третьих лиц, запрашивающих доступ к устройствам перед предоставлением им доступа, например, посовещавшись с руководством или позвонив в компанию, обслуживающую кассовые терминалы (например, поставщику или эквайеру) для проверки. Злоумышленники часто пытаются обмануть сотрудников, одевшись соответствующим образом (например, носят с собой чемоданчик с инструментами и одеваются в служебную униформу) и также могут быть осведомлены о местонахождении устройств, поэтому важно, чтобы сотрудники всегда соблюдали установленные процедуры. Еще один излюбленный трюк злоумышленников – отправка почтой "новой" системы кассового терминала с указанием установить его вместо настоящего и "вернуть" настоящий терминал по указанному адресу. Злоумышленники даже могут оплатить почтовые расходы по возврату настоящего терминала, так как они очень хотят заполучить такого рода устройства. Перед установкой и (или) эксплуатацией устройства сотрудники должны всегда удостоверять у руководителя и поставщика, что оно настоящее и получено из доверенного источника.
9.10 Убедиться, что политики безопасности и процедуры ограничения физического доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**9.10** Изучить документацию и опросить сотрудников, чтобы убедиться в том, что политики безопасности и процедуры по ограничению физического доступа к данным держателей карт: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах по ограничению физического доступа к данным держателей карт и информационной среде держателей карт на постоянной основе.

Регулярный мониторинг и тестирование сети

Требование 10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

Наличие механизмов ведения записей о событиях, а также возможность проследить действия пользователей, важны для обнаружения, предотвращения и минимизации последствий кражи данных. Необходимо наличие журналов во всех средах, что позволяет отслеживать действия, оповещения и анализировать нештатные ситуации. Определение причин инцидентов затруднено в отсутствие журналов записей о событиях в системе.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.1 Внедрить журнал регистрации событий, связывающий любой доступ к системным компонентам с конкретным пользователем.	**10.1** Путем наблюдения и опроса системного администратора убедиться, что: • включено и действует ведение журналов протоколирования событий системных компонентов; • доступ к системным компонентам соотносится с конкретными пользователями.	Важно иметь процесс или систему, которые связывают доступ пользователей с компонентами системы, к которым он осуществлен. Данная система будет генерировать журналы регистрации событий и позволит отслеживать подозрительную деятельность определенного пользователя.
10.2 Для каждого системного компонента должен быть включен механизм протоколирования следующих событий.	**10.2** Путем опроса ответственных сотрудников, изучения журналов протоколирования событий и настроек журналов протоколирования осуществить следующие проверки.	Генерация журналов регистрации событий подозрительной деятельности позволяет предупреждать системного администратора, отправлять данные другим устройствам мониторинга (например, системам обнаружения вторжений), а также отслеживать хронологию событий для расследования инцидентов безопасности; Регистрация следующих событий позволяет организации выявить и отследить потенциально вредоносную активность
10.2.1 Любой доступ пользователя к данным держателей карт	**10.2.1** Убедиться в том, что факты доступа пользователя к данным держателей карт регистрируются.	Злоумышленники могут получить информацию об учетной записи пользователя с доступом к системам в среде данных держателей карт 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.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.2.2 Любые действия, совершенные с использованием административных полномочий.	**10.2.2** Убедиться в том, что любые действия, совершенные с использованием административных полномочий, регистрируются.	Учетные записи с расширенными правами доступа, такими как “administrator” или “root”, могут влиять на безопасность или функционирование системы. Если не регистрировать события, организация не сможет отслеживать проблемы, связанные с ошибками администрирования или ненадлежащим использованием прав доступа.
10.2.3 Любой доступ к записям о событиях в системе	**10.2.3** Убедиться в том, что факты доступа к записям о событиях в системе регистрируются.	Злоумышленники часто пытаются изменить записи в журнале, чтобы скрыть свои действия. Регистрация событий доступа позволяет организации определять несоответствия или факт подмены записей в журнале. Доступ к журналам изменений, добавлений и удалений может помочь отследить несанкционированные действия сотрудников.
10.2.4 Неуспешные попытки логического доступа.	**10.2.4** 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.
10.2.5 Использование и изменение механизмов идентификации и аутентификации, включая, помимо прочего, создание новых учетных записей, расширение привилегий, а также все изменения, добавления, удаления учетных записей с правами суперпользователя ("root") или администратора	**10.2.5.a** Убедиться в том, что использование механизмов идентификации и аутентификации регистрируется.	Без знания того, кто входил в систему на момент возникновения инцидента, невозможно выявить учетные записи, которые могли быть использованы. Злоумышленники могут также предпринимать попытки обхода механизмов аутентификации.
	10.2.5.b Убедиться в том, что любое расширение полномочий регистрируется.	
	10.2.5.c Убедиться в том, что любые изменения, добавления или удаления учетных записей с правами суперпользователя или администратора регистрируются.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.2.6 Инициализация, остановка или приостановка ведения журналов протоколирования событий	**10.2.6** Убедиться в том, что следующие события регистрируются: • инициализация журналов протоколирования событий; • остановка или приостановка ведения журналов протоколирования событий.	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.
10.2.7 Создание и удаление объектов системного уровня.	**10.2.7** Убедиться в том, что регистрируются факты создания и удаления объектов системного уровня.	Вредоносное программное обеспечение часто создает или заменяет объекты системного уровня на целевой системе, чтобы получить контроль над определенной функцией или операцией в этой системе. Регистрация создания или замены объектов системного уровня, таких как таблицы баз данных или запрограммированные процедуры, упростит процесс установления правомочности таких изменений.
10.3 Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры.	**10.3** Посредством опроса и изучения журналов протоколирования событий выполнить следующие действия для каждого протоколируемого события (из требования 10.2):	записывая указанные элементы для контролируемых событий, перечисленных в требовании 10.2, можно быстро идентифицировать потенциальную компрометацию и иметь достаточно сведений о том, кто, что, когда, где и как сделал.
10.3.1 Идентификатор пользователя.	**10.3.1** Убедиться в том, что идентификатор пользователя включен в записи журнала.	
10.3.2 Тип события.	**10.3.2** Убедиться в том, что тип события включен в записи журнала.	
10.3.3 Дата и время	**10.3.3** Убедиться в том, что дата и время включены в записи журнала.	
10.3.4 Успешным или неуспешным было событие.	**10.3.4** Убедиться в том, что в журнале указано, успешным или неуспешным было событие.	
10.3.5 Источник события.	**10.3.5** Убедиться в том, что источник события включен в записи журнала.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.3.6 Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.	**10.3.6** Убедиться в том, что идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие, включены в записи журнала.	
10.4 Все системные часы и системное время на критичных системах должны быть синхронизированы, Необходимо убедиться в исполнении данного требования для получения, распространения и хранения данных о времени. ***Примечание.*** *Примером технологии синхронизации времени является Протокол синхронизации времени (Network Time Protocol).*	**10.4** Изучить конфигурационные стандарты и процессы и убедиться, что для синхронизации часов используется технология синхронизации времени, удовлетворяющая требованиям 6.1 и 6.2 стандарта PCI DSS.	Технология синхронизация времени используется для синхронизации часов на нескольких системах. Если часы синхронизированы некорректно, бывает сложно или даже невозможно сравнить файлы журналов из различных систем и установить точную последовательность событий (что имеет большое значение при расследовании каких-либо нарушений). Для групп, расследующих инциденты, время совершения каждого действия является критичным для определения способов получения доступа к системам.
10.4.1 На критичных системах установлено точное и согласованное время.	**10.4.1.a** Изучить процесс получения, распространения и хранения точного времени в организации, и убедиться, что: • только назначенные центральные серверы времени получают информацию о времени из внешних источников, а данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC); • точное время на назначенных центральных серверах времени, если их несколько, совпадает; • системы получают информацию о времени от назначенных центральных серверов времени.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
	10.4.1.b Сделать выборку системных компонентов и изучить системные параметры времени, чтобы убедиться, что: • только назначенные центральные серверы времени получают информацию о времени из внешних источников, а данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC); • точное время на назначенных центральных серверах времени, если их несколько, совпадает; • системы получают время от назначенных центральных серверов времени.	
10.4.2 Данные о времени защищены.	**10.4.2.a** Изучить конфигурации систем и настройки синхронизации времени и убедиться, что доступ к данным о времени разрешен только персоналу, имеющему служебную необходимость.	
	10.4.2.b Изучить конфигурацию систем, настройки, журналы и процессы синхронизации времени и убедиться, что любые изменения в настройках времени на критичных системах отслеживаются, контролируются и регистрируются.	
10.4.3 Получение настроек времени происходит из признанных индустрией безопасности источников.	**10.4.3** Изучить конфигурацию систем и убедиться, что серверы времени принимают обновления времени от специализированных, общепринятых отраслевых внешних источников (чтобы предотвратить смену времени злоумышленником). Данные обновления могут быть дополнительно зашифрованы симметричным ключом и списками контроля доступа, определяющими IP-адреса машин, которым разрешено получать обновления времени (чтобы предупредить неавторизованное использование внутренних серверов времени).	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.5 Журналы протоколирования событий должны быть защищены от изменений.	**10.5** Опросить системных администраторов и изучить системные конфигурации и права доступа, чтобы убедиться в том, что журналы протоколирования событий защищены от изменений.	Обычно злоумышленники, проникшие в сеть, пытаются внести изменения в журналы регистрации событий для того, чтобы скрыть свои действия. При недостаточной защите журналов гарантировать их полноту, точность и целостность будет невозможно, и они будут бесполезны в качестве средства расследования после компрометации.
10.5.1 Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	**10.5.1** Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	Надежная защита журналов регистрации событий подразумевает строгий контроль доступа (ограничение доступа к журналам по принципу служебной необходимости) и использование физического или сетевого разделения, чтобы затруднить поиск и модификацию журналов. Оперативное сохранение резервных копий журналов протоколирования событий на централизованный сервер протоколирования или носитель, где их изменение затруднено, позволяет защитить журналы даже в случае взлома системы.
10.5.2 Журналы протоколирования событий должны быть защищены от неавторизованного изменения.	**10.5.2** Актуальные журналы протоколирования событий должны быть защищены от неавторизованного изменения при помощи механизмов контроля доступа, физического разделения и (или) разделения на уровне сетей.	
10.5.3 Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено.	**10.5.3** Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования или отдельный носитель, где их изменение затруднено.	
10.5.4 Копии журналов протоколирования событий для технологий, к которым возможен доступ извне, должны сохраняться на безопасный и централизованный внутренний сервер протоколирования или носитель.	**10.5.4** Журналы протоколирования событий доступных извне систем (беспроводных устройств, брандмауэров, DNS, почтовых систем) должны сохраняться на безопасный и централизованный внутренний сервер протоколирования или носитель.	При записи журналов протоколирования событий с публично доступных компонентов, таких как беспроводные сети, межсетевые экраны, DNS и почтовые серверы, риск потери или изменения этих записей снижается, поскольку они надежнее защищены во внутренней сети. Журналы могут сохраняться напрямую или загружаться и копироваться с внешних систем на безопасную внутреннюю систему или носитель.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.5.5 Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала).	**10.5.5** Изучить системные настройки, отслеживаемые файлы и результаты мониторинга и убедиться в наличии ПО для мониторинга целостности файлов или защиты журналов протоколирования событий от несанкционированных изменений.	Системы мониторинга целостности файлов или системы защиты от несанкционированных изменений выполняют проверку на внесение изменений в критичные файлы и генерируют предупреждения при обнаружении изменений. В целях мониторинга целостности файлов система выполняет мониторинг файлов, которые обычно не меняются, но изменение которых может свидетельствовать о компрометации.
10.6 Изучать журналы протоколирования событий и события безопасности всех системных компонентов с целью обнаружения аномалий или подозрительной активности. ***Примечание.*** *Для обеспечения соответствия данному требованию могут использоваться средства сбора и анализа журналов протоколирования событий, а также средства оповещения.*	**10.6** Выполнить следующее.	Большое количество компрометаций существует в течение нескольких дней или даже месяцев до обнаружения. Ежедневная проверка журналов регистрации событий позволяет минимизировать время обнаружения и снизить риск компрометации. Регулярная проверка журналов вручную или автоматически позволяет обнаружить и предотвратить несанкционированный доступ к среде данных держателей карт. Проверку журналов не обязательно выполнять вручную. Использование средств сбора и анализа журналов событий, а также средств оповещения поможет облегчить проверку благодаря идентификации событий, которые требуют проверки.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
10.6.1 Проверяйте не реже одного раза в день: • все события безопасности; • журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и (или) критичных аутентификационных данных, или влияющих на их безопасность; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, брандмауэров, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.).	**10.6.1.a** Проверить политики и процедуры на наличие процедур проведения следующих проверок вручную или автоматически не реже одного раза в день: • все события безопасности; • журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и (или) критичных аутентификационных данных, или влияющих на их безопасность; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции защиты (например, брандмауэров, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.)	Большое количество компрометаций существует в течение нескольких дней или даже месяцев до обнаружения. Ежедневная проверка журналов регистрации событий позволяет минимизировать время обнаружения и снизить риск компрометации. Ежедневная проверка событий безопасности (например, уведомлений или предупреждений о подозрительной или аномальной активности), журналов критичных системных компонентов и журналов систем, выполняющих функции защиты (например, брандмауэров, систем обнаружения и предотвращения вторжений, систем мониторинга целостности файлов) необходимо для обнаружения потенциальных проблем. Учтите, что значение термина "событие безопасности" зависит от организации и может включать ограничения по типу технологий, местонахождении и функции устройства. Организациям также рекомендуется определить так называемый "нормальный" трафик в целях идентификации аномального поведения.
	10.6.1.b Понаблюдать за процессами и опросить сотрудников для подтверждения того, что не реже раза в день проверяются: • все события безопасности; • журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и (или) критичных аутентификационных данных, или влияющих на их безопасность; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, брандмауэров, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.).	
10.6.2 Периодически изучать журналы других системных компонентов на основании политик и стратегии управления рисками, определяемой в рамках ежегодной	**10.6.2.a** Проверить политики и процедуры безопасности на наличие процедур проведения периодической проверки журналов всех остальных системных компонентов (вручную или автоматически) на основании политик и стратегии управления рисками.	Также следует периодически проверять журналы всех остальных системных компонентов для обнаружения признаков потенциальных проблем или попыток получить доступ к критичным системам через другие,

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
оценки рисков.	**10.6.2** Изучить документацию по оценке рисков и опросить сотрудников, чтобы убедиться, что проверка выполняется в соответствии с политиками и стратегией управления рисками, принятыми в организации.	менее критичные системы. Частота проведения проверки определяется организацией в рамках ежегодной оценки рисков.
10.6.3 Изучить исключения и аномалии, обнаруженные во время проверки.	**10.6.3.a** Проверить политики безопасности и процедуры на наличие процедур изучения исключений и аномалий, обнаруженных во время проверки.	Если исключения и аномалии, обнаруженные во время проверки журналов, не будут изучены, организация может не узнать о несанкционированной и потенциально вредоносной активности внутри своей сети.
	10.6.3.b Понаблюдать за процессами и опросить сотрудников для подтверждения того, что проводится изучение исключений и аномалий.	
10.7 Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев (например, они могут находиться в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии).	**10.7.a** Проверить политики и процедуры и убедиться, что они включают: • политики хранения журналов регистрации событий; • процедуры хранения журналов регистрации событий в течение не менее одного года, в том числе в оперативном доступе не менее трех месяцев.	Хранение журналов по крайней мере в течение года связано с тем фактом, что на обнаружение компрометации требуется время, а журналы отражают достаточную хронологию событий при расследовании инцидентов и дают возможность более точного определения продолжительности существования потенциальной компрометации и систем, подверженных ее воздействию. Располагая журналами за три месяца, организация может быстро выявить нарушения и снизить их влияние. Хранение журналов на неподключенных к сети системах может затруднить получение к ним оперативного доступа и привести к увеличению времени, необходимого для восстановления данных журнала, выполнения анализа и выявления систем или данных, подвергшихся влиянию нарушения.
	10.7.b Опросить сотрудников и изучить журналы регистрации событий, чтобы убедиться, что они доступны по крайней мере в течение одного года.	
	10.7.c Опросить сотрудников и понаблюдать за процессами, чтобы убедиться, что журналы регистрации событий могут быть незамедлительно восстановлены для проведения анализа.	
10.8 Убедиться, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**10.8** Изучить документацию и опросить сотрудников, чтобы убедиться в том, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о политиках безопасности и повседневных процедурах мониторинга любого доступа к сетевым ресурсам и данным держателей карт на постоянной основе, и соблюдать их.

Требование 11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

Уязвимости непрерывно обнаруживаются взломщиками и исследователями, а также появляются вместе с новым программным обеспечением. Следует периодически, а также при внесении изменений проверять системные компоненты, процессы и программное обеспечение, чтобы убедиться, что их защищенность поддерживается на должном уровне.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
11.1 Внедрить процессы для проведения ежеквартальной проверки наличия беспроводных точек доступа (802.11) и для обнаружения авторизованных и неавторизованных беспроводных точек доступа. ***Примечание.*** *Методы, которые могут применяться, включают, но не ограничиваются: сканирование беспроводной сети, физическое/логическое обследование системных компонентов и инфраструктуры, контроль сетевого доступа (NAC) или беспроводные IDS/IPS.* *Какие бы методы ни использовались, они должны быть достаточно эффективными для обнаружения авторизованных и неавторизованных устройств.*	**11.1.a** Проверить политики и процедуры на наличие ежеквартальных процессов для обнаружения авторизованных и неавторизованных беспроводных точек доступа. **11.1.b** Убедиться, что методика пригодна для обнаружения и идентификации несанкционированных беспроводных точек доступа, включающих в себя, как минимум, следующее: • беспроводные адаптеры, вставленные в системные компоненты; • портативные или мобильные устройства, подключенные к системным компонентам для создания беспроводной точки доступа (например, через USB и т.п.); • беспроводные устройства, подключенные к сетевому порту или сетевому устройству. **11.1.c** Изучить результаты недавних сканирований беспроводных сетей и убедиться, что: • авторизованные и неавторизованные беспроводные точки доступа были обнаружены; и • сканирование всех системных компонентов и объектов проводится, по крайней мере, ежеквартально. **11.1.d** Если внедрен автоматизированный мониторинг (например, системы обнаружения вторжений (IDS)/системы предотвращения вторжений (IPS) по беспроводным сетям, контроль сетевого доступа и т.п.), убедиться, что он генерирует уведомления персоналу организации.	Злоумышленники часто используют беспроводные технологии и (или) уязвимости в них для получения доступа к сети и данным держателей карт. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может без труда и незаметно проникнуть в сеть. Неавторизованные беспроводные устройства могут быть скрыты или подключены к компьютеру, другому компоненту системы или непосредственно к сетевому порту или сетевому устройству, такому как маршрутизатор или коммутатор. Любое такое устройство может выполнять роль неавторизованной точки доступа в среду. Знание авторизованных беспроводных устройств может помочь администраторам быстро обнаружить неавторизованные беспроводные устройства и отреагировать на это, что позволит снизить уязвимость информационной среды держателей карт перед злоумышленниками. Вследствие того, что беспроводную точку доступа подключить к сети не составляет большого труда, а также вследствие сложности определения присутствия такой точки и выявления риска, связанного с неавторизованными беспроводными устройствами, эти процессы следует выполнять даже при наличии политики, запрещающей использование беспроводных технологий. Размер и сложность определенной среды

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
		обуславливает необходимость использования соответствующих инструментов и процессов для предотвращения установки в среде неавторизованных беспроводных точек доступа. *(Продолжение на следующей странице)*
11.1.1 Вести список авторизованных беспроводных точек доступа с указанием их необходимости для ведения дел.	**11.1.1** Изучить документацию и убедиться, что ведется список авторизованных беспроводных точек доступа с указанием необходимости каждой точки для ведения дел.	***Например:*** *В случае одного автономного розничного киоска в торговом центре, где все коммуникационные компоненты содержатся в устойчивом от взлома корпусе, выполнение подробного физического осмотра киоска может быть достаточно для того, чтобы быть уверенным в том, что к киоску не подключены беспроводные точки доступа. Однако в среде с несколькими узлами (например, в большом розничном магазине, колл-центре, серверной комнате или центре обработки данных) проведение подробного физического осмотра затруднительно. В этом случае для выполнения требования можно использовать несколько методов, например физический осмотр системы и анализ беспроводной связи.*
11.1.2 Внедрить процедуры реагирования на обнаружение неавторизованных беспроводных точек доступа.	**11.1.2.a** Изучить политику реагирования на инциденты (требование 12.10) и убедиться, что в ней указаны обязательные действия при обнаружении неавторизованной беспроводной точки доступа.	
	11.1.2.b Опросить ответственных сотрудников и (или) изучить результаты недавних сканирований и меры, предпринятые в связи с ними, и убедиться, что при обнаружении неавторизованных беспроводных точек доступа предпринимаются соответствующие меры.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
11.2 Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов). ***Примечание.*** *При проведении ежеквартального сканирования можно объединить несколько отчетов о результатах сканирования для подтверждения того, что все системы были просканированы, а все найденные уязвимости – устранены. Может потребоваться дополнительная документация для подтверждения того, что неустраненные уязвимости находятся в процессе устранения.* *Для первоначального соответствия стандарту PCI DSS успешное прохождение четырех ежеквартальных сканирований необязательно, если аудитор убедился в следующем: 1) последнее сканирование было пройдено успешно, 2) документированные политики и процедуры регламентируют необходимость ежеквартального сканирования, 3) обнаруженные уязвимости были устранены и это подтверждено повторным сканированием (сканированиями). Для всех последующих лет после первоначального подтверждения соответствия стандарту PCI DSS успешное прохождение всех четырех ежеквартальных сканирований обязательно.*	**11.2** Изучить отчеты о результатах сканирования и сопутствующую документацию и убедиться, что внешнее и внутреннее сканирование сети на наличие уязвимостей проводится следующим образом:	сканирование на наличие уязвимостей выполняется автоматизированными средствами в отношении внутренних и внешних сетевых устройств и серверов для обнаружения потенциальных уязвимостей, которые могут быть обнаружены и использованы злоумышленниками. Существует три типа сканирований на наличие уязвимостей, требуемых стандартом PCI DSS: • ежеквартальное внутреннее сканирование на наличие уязвимостей, проводимое квалифицированными специалистами (статус авторизованного поставщика услуг сканирования (ASV) по требованиям стандарта PCI SSC необязателен); • ежеквартальное внешнее сканирование на наличие уязвимостей, которое должны выполнять специалисты компании, имеющей статус авторизованного поставщика услуг сканирования (ASV); • внутреннее и внешнее сканирование после крупного изменения в сети. После обнаружения уязвимостей организации устраняют их и проводят повторное сканирование до устранения всех уязвимостей. Своевременное выявление и устранение уязвимостей снижает вероятность использования злоумышленником уязвимости и получения доступа к компонентам системы или данным держателей карт.

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
11.2.1 Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей и, при необходимости, повторные сканирования, пока не будут устранены все уязвимости, представляющие высокий риск (согласно определению в требовании 6.1). Сканирование должны выполнять квалифицированные специалисты.	**11.2.1.a** Изучить результаты внутренних сканирований на наличие уязвимостей и убедиться, что четыре последних сканирования производились ежеквартально в течение последних 12 месяцев.	Установленный процесс выявления уязвимостей во внутренних системах требует ежеквартального сканирования уязвимостей. Уязвимости, которые представляют большой риск для среды (например, те, которые имеют статус "высокий" согласно требованию 6.1), должны быть устранены в первую очередь. Внутреннее сканирование на наличие уязвимостей должны выполнять квалифицированные специалисты, которые являются независимыми относительно сканируемого компонента системы (например, администратор брандмауэра не должен быть ответственным за сканирование брандмауэра), либо организация может воспользоваться услугами другой организации, которая занимается сканированием на наличие уязвимостей.
	11.2.1.b Изучить отчеты о результатах сканирований и убедиться, что процесс сканирования предусматривает повторные сканирования до тех пор, пока все уязвимости высокого уровня, определенные в требовании 6.1 стандарта PCI DSS, не будут устранены.	
	11.2.1.c Опросить сотрудников и убедиться, что сканирование проводилось квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.2.2 Следует проводить ежеквартальное внешнее сканирование на наличие уязвимостей посредством авторизованного поставщика услуг сканирования (ASV), сертифицированного Советом по стандартам безопасности индустрии платежных карт (PCI SSC). Проводить повторные сканирования до достижения удовлетворительного результата.	**11.2.2.a** Изучить результаты четырех последних внешних сканирований на наличие уязвимостей и убедиться, что четыре последних внешних ежеквартальных сканирования проводились в течение последних 12 месяцев.	Поскольку внешние сети подвержены более высокому риску компрометации, ежеквартальное сканирование на наличие уязвимостей в таких сетях должны выполнять специалисты уполномоченной компании, имеющей статус PCI SSC Approved Scanning Vendor (ASV).
	11.2.2.b Изучить результаты каждого ежеквартального сканирования и убедиться, что они отвечают критериям успешности сканирования в "Руководстве по программе ASV" (например, отсутствуют уязвимости с оценкой 4.0 или выше по шкале CVSS и нет узлов, сканирование которых было автоматически прервано).	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
Примечание. *Ежеквартальное внешнее сканирование на наличие уязвимостей должно выполняться сторонней организацией (ASV), сертифицированной Советом PCI SSC.* *См. "Руководство по программе ASV", опубликованное на веб-сайте Совета по стандартам безопасности индустрии платежных карт (PCI SSC), для получения информации об обязанностях клиентов по проведению сканирования, подготовке к сканированию и т.д.*	**11.2.2.c** Изучить отчеты о результатах сканирования и убедиться, что сканирование производилось организацией, имеющей статус авторизованного поставщика услуг сканирования (ASV) Совета по стандартам безопасности индустрии платежных карт (PCI SSC).	
11.2.3 Проводить внутреннее и внешнее сканирования и, при необходимости, повторное сканирование после любого значительного изменения в сети. Сканирование должны выполнять квалифицированные специалисты.	**11.2.3.a** Изучить и сопоставить документацию по контролю изменений в сети и отчеты о результатах сканирования и убедиться, что выполнятся сканирование системных компонентов, подверженных значительным изменениям.	Определение значительного изменения сильно зависит от конфигурации среды. Если обновление или модификация могут обеспечить доступ к данным держателей карт или повлиять на безопасность среды данных держателей карт, то оно считается значительным. Сканирование среды после любых значительных изменений гарантирует, что изменения внедрены надлежащим образом, и безопасность среды не нарушена в результате этих изменений. Необходимо просканировать все системные компоненты, затронутые изменением.
	11.2.3.b Изучить отчеты о сканировании и убедиться, что процедура сканирования предусматривает повторные сканирования до тех пор, пока: • для внешнего сканирования – не будут устранены уязвимости со степенью критичности 4.0 или выше согласно CVSS; • для внутреннего сканирования – не будут устранены уязвимости с высокой степенью риска, согласно определению в требовании 6.1 стандарта PCI DSS.	
	11.2.3.c Проверить, что сканирование проводилось квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или ASV не требуется).	
11.3 Внедрить методологию проведения	**11.3** Изучить методологию проведения тестов на	Тест на проникновение выполняется для

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
тестирования на проникновение, которая: • основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115); • охватывает весь периметр информационной среды держателей карт и критичные системы; • включает тестирование как снаружи сети, так и внутри сети; • включает тестирование на наличие механизмов сегментации и уменьшения охвата; • требует, чтобы тесты на проникновение на уровне приложения включали, как минимум, проверку на наличие уязвимостей, приведенных в требовании 6.5; • требует, чтобы тесты на проникновение на уровне сети охватывали не только операционные системы, но и другие компоненты, поддерживающие взаимодействие на сетевом уровне; • включает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев; • регламентирует хранение результатов тестов на проникновение и мер, предпринятых для устранения уязвимостей. ***Примечание.*** *До 30 июня 2015 года это обновленное требование 11.3 носит рекомендательный характер, а после этой даты становится обязательным требованием. Требования стандарта*	проникновение и опросить ответственных сотрудников, чтобы убедиться, что методология: • основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115); • охватывает весь периметр информационной среды держателей карт и критичные системы; • включает тестирование как снаружи сети, так и внутри сети; • включает тестирование на наличие механизмов сегментации и уменьшения охвата; • требует, чтобы тесты на проникновение на уровне приложения включали, как минимум, проверку на наличие уязвимостей, приведенных в требовании 6.5; • требует, чтобы тесты на проникновение на уровне сети охватывали не только операционные системы, но и другие компоненты, поддерживающие взаимодействие на сетевом уровне; • включает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев; • регламентирует хранение результатов тестов на проникновение и мер, предпринятых для устранения уязвимостей.	моделирования атаки с целью выявления того, насколько глубоко в среду может проникнуть злоумышленник. Это позволяет оценить степень риска и разработать стратегию защиты от атак. Отличие теста на проникновение от сканирования на наличие уязвимостей заключается в том, что тест на проникновение является активным процессом, который может включать использование обнаруженных уязвимостей. Сканирование на наличие уязвимостей – это один из первых шагов, который выполняет специалист по тестированию на проникновение для определения стратегии тестирования, но этот шаг не единственный. Даже если сканирование на наличие уязвимостей не обнаруживает известных уязвимостей, специалист, проводящий тестирование на проникновение, получает достаточно информации о системе, чтобы выявить потенциальные проблемы. Тесты на проникновение обычно выполняются вручную. Хотя можно использовать автоматизированные средства, тестировщик должен знать систему для проникновения в среду. Часто тестировщик использует несколько уязвимостей вместе, чтобы обойти несколько уровней защиты. Например, если тестировщик находит способ получить доступ к серверу приложений, он использует взломанный сервер для проведения атаки на ресурсы, доступ к которым имеет сервер. Таким образом, тестировщик имитирует методы, которыми пользуются злоумышленники, для выявления проблемных областей в среде. *Процедуры тестирования на проникновение различаются в зависимости от организации, а тип, глубина и сложность тестирования будут зависеть от конкретной среды и*

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
PCI DSS версии 2.0 к тестированию на возможность проникновения необходимо соблюдать до внедрения стандарта версии 3.0.		*оценки рисков организации.*
11.3.1 Следует проводить *внешний* тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера).	**11.3.1.a** Изучить объем работы и результаты последнего внешнего теста на проникновение и убедиться в том, что тест на проникновение осуществляется: • в соответствии с определенной методологией; • не реже одного раза в год; • после любых значительных изменений в среде.	Проведение тестов на проникновение на регулярной основе и после значительных изменений в среде – это мера проактивной защиты, позволяющая уменьшить вероятность доступа злоумышленников к информационной среде держателей карт. Определение значительного обновления или модификации сильно зависит от конфигурации среды. Если обновление или модификация могут обеспечить доступ к данным держателей карт или повлиять на безопасность среды данных держателей карт, то оно считается значительным. Проведение тестов на проникновение после обновления или модификации сети гарантирует эффективную работу существующих механизмов контроля после обновления или модификации.
	11.3.1.b Убедиться в том, что тест на проникновение был проведен квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости, если это возможно (при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.3.2 Следует проводить *внутренний* тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера).	**11.3.2.a** Изучить объем работы и результаты последнего внутреннего теста на проникновение и убедиться в том, что тест на проникновение проводится не реже одного раза в год и после всех значительных изменений в среде. • в соответствии с определенной методологией; • не реже одного раза в год; • после любых значительных изменений в среде.	
	11.3.2.b Убедиться в том, что тест на проникновение был проведен квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедиться в их организационной независимости, если это возможно (при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.3.3 Необходимо исправлять	**11.3.3** Изучить результаты теста на проникновение и	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
опасные уязвимости, обнаруженные во время тестирования на возможность проникновения и проводить повторное тестирование для проверки исправлений.	убедиться в том, что выявленные уязвимости были устранены и это подтверждено повторным тестом.	
11.3.4 В случае использования сегментации для изолирования информационной среды держателей карт от других сетей необходимо проводить тестирование на возможность проникновения не реже одного раза в год и после любого изменения механизмов/методов сегментации для проверки функционирования и эффективности методов сегментации и изолирования всех непроверенных систем от проверенных.	**11.3.4.a** Изучить механизмы сегментации и методологию тестирования на проникновение, чтобы убедиться, что процедуры тестирования на проникновение включают тестирование всех методов сегментации для проверки их функционирования и эффективности, и изолирования всех непроверенных систем от проверенных. **11.3.4.b** Изучить результаты последнего теста на проникновение и убедиться в том, что тест на проникновение для проверки механизмов сегментации осуществляется: • не реже одного раза в год и после любого изменения механизмов/методов сегментации; • распространяется на все используемые механизмы/методы сегментации; • включает проверку их функционирования и эффективности, и изолирование всех непроверенных систем от проверенных.	Тест на проникновение – это важный инструмент для проверки эффективности методов сегментации, используемых для изолирования информационной среды держателей карт от других сетей. Тест на проникновение необходимо сконцентрировать на механизмах сегментации, используемых как извне сети организации, так и изнутри сети, но вне информационной среды держателей карт для подтверждения невозможности получения доступа к информационной среде держателей карт в обход механизмов сегментации. Например, проверить и (или) просканировать сеть на наличие открытых портов для подтверждения невозможности соединения между проверенными и непроверенными сетями.
11.4 Следует использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Следует осуществлять мониторинг сетевого трафика по периметру среды данных держателей карт и в критичных точках внутри среды данных держателей карт, и оповещать сотрудников о подозрительных действиях. Системы обнаружения и предотвращения вторжений и их сигнатуры должны поддерживаться в	**11.4.a** Изучить системные конфигурации и схемы сети и убедиться в том, что методы мониторинга всего трафика (например, системы обнаружения и (или) предотвращения вторжений) используются: • по периметру среды данных держателей карт; • в критичных точках внутри среды данных держателей карт. **11.4.b** Изучить системные конфигурации и опросить ответственных сотрудников для подтверждения того, что средства обнаружения и (или) предотвращения вторжений оповещают сотрудников о подозрительных действиях.	Методы обнаружения и (или) предотвращения вторжений (например, система обнаружения вторжений (IDS)/система предотвращения вторжений (IPS)) сравнивают поступающий в сеть трафик с известными сигнатурами и (или) поведением (инструментарий злоумышленников, троянское и другое вредоносное программное обеспечение и т.д.), отправляют предупреждения и (или) блокируют попытку проведения атаки. Без проактивного подхода к обнаружению несанкционированной деятельности атаки на компьютерные ресурсы (или их ненадлежащее использование) могут

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
актуальном состоянии.	**11.4.c** Изучить конфигурации систем обнаружения вторжений (IDS)/предотвращения вторжений (IPS) и документацию поставщиков, чтобы убедиться в том, что средства обнаружения и (или) предотвращения вторжений настроены, поддерживаются и обновляются в соответствии с рекомендациями поставщика для обеспечения оптимальной защиты.	быть не замечены в момент выполнения. Необходимо вести мониторинг предупреждений, генерируемых данными средствами, для блокирования предпринятых вторжений.
11.5 Следует внедрить механизм защиты от изменений (например, мониторинг целостности файлов) для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных; сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю. ***Примечание.*** *Критичные файлы – это файлы, которые изменяются нечасто, но изменение которых может служить признаком взлома или попытки взлома системы. Средства защиты от изменений обычно содержат предустановленный перечень критичных файлов в используемой операционной системе. Другие критичные файлы, такие как файлы для клиентских приложений, должны быть определены самой организацией (т. е. торгово-сервисным предприятием или поставщиком услуг).*	**11.5.a** Убедиться в наличии механизма защиты от изменений в среде данных держателей карт путем изучения системных настроек и отслеживаемых файлов, а также проверки результатов мониторинга. Примеры файлов, подлежащих мониторингу: ▪ системные исполняемые файлы; ▪ прикладные исполняемые файлы; ▪ конфигурационные файлы и файлы параметров; ▪ централизованно хранимые файлы, файлы прошлых периодов или архивные файлы, файлы данных аудита и журналов протоколирования событий. ▪ дополнительные критичные файлы, определяемые организацией (например, путем оценки рисков или другими способами).	Средства защиты от изменений, например, инструменты для мониторинга целостности файлов выполняют проверку на внесение изменений в критичные файлы и генерируют предупреждения при обнаружении изменений. Если защита от изменений внедрена ненадлежащим образом, а ее отчеты не проверяются, то злоумышленник может изменить содержимое конфигурационных файлов, программы операционной системы или исполняемые файлы приложений. Незамеченные несанкционированные изменения могут снизить эффективность работы механизмов контроля и привести к краже данных держателей карт без заметного влияния на процессы обработки.
	11.5.b Убедиться, что механизм используется для оповещения сотрудников организации о несанкционированных изменениях критичных файлов, а сопоставительный анализ конфиденциальных файлов проводится не реже одного раза в неделю.	
11.5.1 Внедрить процесс реагирования на любое срабатывание механизма защиты от изменений.	**11.5.1** Опросить сотрудников и убедиться, что все предупреждения изучаются и устраняются.	

ТРЕБОВАНИЯ PCI DSS	ПРОЦЕДУРЫ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ	ПОЯСНЕНИЕ
11.6 Убедиться, что политики безопасности и процедуры мониторинга и проверки безопасности документированы, используются и известны всем заинтересованным лицам.	**11.6** Ознакомиться с документацией и опросить сотрудников для подтверждения того, что политики безопасности и процедуры мониторинга и проверки безопасности: • документированы; • используются; и • известны всем заинтересованным лицам.	Сотрудники должны быть постоянно осведомлены о политиках безопасности и процедурах мониторинга и проверки безопасности, и следовать им.

Поддержание политики информационной безопасности

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

Строгая политика безопасности задает атмосферу безопасности для всей организации и информирует персонал организации о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите. В контексте данного требования термином "персонал" обозначаются постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте организации или так или иначе имеющие доступ к среде данных держателей карт.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.1 Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности.	**12.1** Изучить политику информационной безопасности и убедиться в том, что она опубликована и распространена среди всех пользователей (включая поставщиков, подрядчиков и бизнес-партнеров).	Политика информационной безопасности компании помогает разработать стратегический план по реализации мер защиты наиболее ценных ресурсов. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите.
12.1.1 Политика безопасности должна пересматриваться по меньшей мере ежегодно и обновляться в случае изменения среды организации.	**12.1.1** Убедиться в том, что политика безопасности пересматривается по меньшей мере ежегодно и обновляется в случае изменения бизнес-целей или рисков среды организации.	Угрозы для безопасности и методы защиты быстро развиваются. Без обновления политики безопасности с учетом этих изменений не будут приняты актуальные меры защиты против новых угроз.
12.2 Внедрить процесс оценки рисков, который: • осуществляется не реже, чем раз в год и после значительного	**12.2.a** Убедиться, что ежегодный документированный процесс оценки рисков выявляет критические активы, угрозы и уязвимости, и завершается официальной оценкой рисков.	Оценка рисков позволяет выявить угрозы и связанные с ними уязвимости, которые могут негативно отразиться на ведении дел. Ресурсы можно эффективно распределить для

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
изменения среды (например, покупки, слияния, перемещения и т.д.); • выявляет критические активы, угрозы и уязвимости; и • завершается официальной оценкой рисков. *Примеры методик оценки рисков включают в том числе: OCTAVE, ISO 27005 и NIST SP 800-30.*	**12.2.b** Изучить документацию по оценке рисков и убедиться, что оценка рисков проводится по крайней мере раз в год и после значительных изменений в среде.	внедрения механизмов контроля, которые помогут снизить вероятность воздействия угроз. Проведение оценки рисков по крайней мере раз в год и после значительных изменений позволяет организации учитывать структурные изменения и реагировать на новые угрозы, тенденции и технологии.
12.3 Разработать правила эксплуатации критичных технологий и определить надлежащее применение для этих технологий. ***Примечание.*** *К критичным технологиям относятся в том числе: технологии удаленного доступа, беспроводные технологии, использование ноутбуков, планшетов, съемных носителей информации, электронной почты и Интернета.* Изучить правила эксплуатации критичных технологий и осуществить следующие проверки.	**12.3** Изучить правила эксплуатации критичных технологий и опросить ответственных сотрудников, чтобы убедиться, что следующие политики внедрены и выполняются:	Политики использования могут либо запрещать использование определенных устройств, либо содержать инструкции для сотрудников по надлежащему использованию и внедрению. Если политики использования отсутствуют, есть вероятность нарушения сотрудниками политик компании, в результате чего злоумышленники могут получить доступ к критичным системам и данным держателей карт.
12.3.1 Процедуру явного одобрения уполномоченными лицами.	**12.3.1** Убедиться в том, что правила эксплуатации включают процессы явного утверждения используемых технологий уполномоченными лицами.	Без утверждения у руководства необходимости внедрения этих технологий сотрудники могут непреднамеренно внедрить решение в соответствии с потребностями бизнеса, при этом создав брешь в системе безопасности и подвергнув критичные системы и данные риску потери или кражи злоумышленниками.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.3.2 Аутентификацию перед использованием устройства.	**12.3.2** Убедиться в том, что правила эксплуатации включают процессы аутентификации по имени и паролю, либо иному средству аутентификации (например, токену) перед использованием любых технологий.	Если технология реализована без надлежащей аутентификации (идентификаторы пользователей и пароли, электронные ключи, VPN и т.д.), злоумышленник может воспользоваться этой незащищенной технологией для получения доступа к критичным системам и данным держателей карт.
12.3.3 Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.	**12.3.3** Убедиться в том, что политики эксплуатации включают список всех используемых устройств и сотрудников, имеющих доступ к таким устройствам.	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве "черного хода". Сотрудники также могут обойти защиту и установить свои устройства. Тщательная инвентаризация и маркировка устройств позволит быстро идентифицировать несанкционированно установленные устройства.
12.3.4 Способ точного и оперативного определения владельца, контактных данных и назначения (например, маркировка, кодирование и (или) инвентаризация устройств).	**12.3.4** Убедиться в том, что правила эксплуатации регламентируют способ точного и оперативного определения владельца, контактных данных и назначения (например, маркировка, кодирование и (или) инвентаризация устройств).	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве "черного хода". Сотрудники также могут обойти защиту и установить свои устройства. Тщательная инвентаризация и маркировка устройств позволит быстро идентифицировать несанкционированно установленные устройства. Рекомендуется разработать официальную процедуру именования устройств и вести учет всех устройств с помощью механизмов инвентаризации. Можно применять логическую маркировку с использованием такой информации, как коды, которые помогают соотнести устройство с владельцем, контактной информацией и назначением.
12.3.5 Допустимые варианты использования технологий.	**12.3.5** Убедиться, что правила эксплуатации регламентируют допустимые варианты использования технологий.	Определяя допустимые сценарии использования и размещение устройств и технологий, утвержденных руководством,

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.3.6 Допустимые точки размещения технологий в сети.	**12.3.6** Убедиться, что правила эксплуатации регламентируют допустимые точки размещения устройств в сети.	компания может улучшить управление и контроль над появлением брешей в конфигурациях и операционных механизмах, чтобы исключить возможность появления "черных ходов", которыми могут воспользоваться злоумышленники для получения доступа к критичным системам и данным держателей карт.
12.3.7 Перечень одобренных компанией продуктов.	**12.3.7** Убедиться, что правила эксплуатации включают перечень одобренных компанией продуктов.	
12.3.8 Автоматическое отключение сессий удаленного доступа после определенного периода простоя.	**12.3.8.a** Убедиться, что правила эксплуатации регламентируют автоматическое отключение сеансов удаленного доступа после определенного периода простоя.	Технологии удаленного доступа часто могут играть роль "черных ходов", которые злоумышленники используют для доступа к критичным ресурсам и данным держателей карт. Отключение технологий удаленного доступа, когда они не используются (например, тех, что используются для поддержки систем поставщиками кассовых терминалов, другими поставщиками или партнерами по бизнесу), позволит ограничить доступ к сети и минимизировать риски для безопасности сетей.
	12.3.8.b Изучить конфигурации технологий удаленного доступа и убедиться, что сеансы удаленного доступа автоматически отключаются после определенного периода простоя.	
12.3.9 Включение механизмов удаленного доступа для производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	**12.3.9** Убедиться, что правила эксплуатации регламентируют включение механизмов для доступа производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.3.10 Персоналу, имеющему удаленный доступ к данным держателей карт, запрещается копировать, перемещать и хранить данные держателей карт на локальных жестких дисках и съемных электронных носителях, если это не обусловлено служебной необходимостью. При наличии подтвержденной служебной необходимости политики эксплуатации должны регламентировать защиту данных в соответствии со всеми действующими требованиями стандарта PCI DSS.	**12.3.10.a** Убедиться, что правила эксплуатации запрещают копирование, перемещение и хранение данных держателей карт на локальных дисках и иных съемных электронных носителях при удаленном доступе к данным. **12.3.10.b** Для авторизованных сотрудников убедиться, что правила эксплуатации предписывают обеспечение защиты данных держателей карт в соответствии с требованиями стандарта PCI DSS.	Для обеспечения осведомленности персонала о запрете хранения и копирования данных держателей карт на свои персональные компьютеры или другие носители информации политика компании должна явно запрещать действия такого рода, за исключением сотрудников, которым на выполнение такого действия дано специальное разрешение. Хранение или копирование данных держателей карт на локальный жесткий диск или другой носитель должно осуществляться в соответствии со всеми действующими требованиями стандарта PCI DSS.
12.4 Политика и процедуры обеспечения безопасности должны однозначно определять обязанности всего персонала организации, относящиеся к информационной безопасности.	**12.4.a** Убедиться, что политики информационной безопасности явно определяют обязанности по обеспечению защиты для всех сотрудников. **12.4.b** Опросить несколько ответственных сотрудников и убедиться в том, что они понимают содержание политики безопасности.	Без явно определенных ролей и обязанностей по обеспечению информационной безопасности взаимодействие между сотрудниками будет неэффективным, что может привести к небезопасному внедрению технологий или использованию устаревших или незащищенных технологий.
12.5 Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью.	**12.5** Изучить политики и процедуры информационной безопасности и убедиться, что: • присутствует официальное делегирование ответственности за обеспечение защиты руководителю службы безопасности (Chief Security Officer) или другому члену руководства, компетентному в вопросах обеспечения информационной безопасности; • следующие обязанности в отношении обеспечения информационной безопасности назначены явно и официально.	Каждое лицо или группа лиц, которые отвечают за управление информационной безопасностью, должны понимать свои обязанности и связанные с ними задачи, которые доводятся до их сведения посредством определенной политики. Без такой ответственности уязвимости в процессах могут открыть доступ к критичным ресурсам или данным держателей карт.
12.5.1 Разработка, документирование и распространение политики и процедур обеспечения безопасности.	**12.5.1** Убедиться, что ответственные за создание, документирование и доведение до сотрудников политик и процедур защиты назначены официально.	

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.5.2 Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных.	**12.5.2** Убедиться в том, что определена ответственность за мониторинг, анализ и доведение до сведения соответствующего персонала (специалистов по информационной безопасности и представителей бизнес-подразделений) информации о событиях, имеющих отношение к информационной безопасности.	
12.5.3 Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.	**12.5.3** Убедиться, что ответственные за создание, документирование и доведение до сотрудников политик и процедур реагирования на инциденты и сообщения о них назначены официально.	
12.5.4 Администрирование учетных записей пользователей, включая их добавление, удаление и изменение.	**12.5.4** Убедиться в том, что официально назначена ответственность за администрирование (добавление, удаление и изменение) учетных записей пользователей и управление аутентификацией.	
12.5.5 Мониторинг и контроль любого доступа к данным.	**12.5.5** Убедиться в том, что определена ответственность за мониторинг и контроль доступа к данным.	
12.6 Должна быть внедрена официальная программа повышения осведомленности персонала по вопросам безопасности с целью донести до них важность обеспечения безопасности данных держателей карт.	**12.6.a** Изучить программу повышения осведомленности персонала по вопросам безопасности и убедиться, что она разъясняет важность обеспечения безопасности данных держателей карт.	Если сотрудники не осведомлены о своих обязанностях по обеспечению информационной безопасности, реализованные меры и процессы защиты могут потерять свою эффективность вследствие непреднамеренных ошибок или умышленных действий таких сотрудников.
	12.6.b Изучить процедуры программы повышения осведомленности персонала по вопросам безопасности и выполнить следующие проверки.	
12.6.1 Обучение персонала организации должно проводиться при приеме на работу, а также не реже одного раза в год. ***Примечание.*** *Методики обучения могут варьироваться в зависимости от обязанностей персонала и уровня*	**12.6.1.a** Убедиться в том, что в программе повышения осведомленности персонала используются различные методы доведения информации до персонала (например, плакаты, письма, заметки, системы Интернет-обучения, специальные кампании).	Если программа повышения осведомленности персонала по вопросам безопасности не будет включать в себя периодические напоминания, сотрудники могут забыть или пренебречь основными процессами и процедурами обеспечения безопасности, что приведет к уязвимости критичных ресурсов и данных держателей карт.
	12.6.1.b Убедиться в том, что персонал организации проходит обучение вопросам безопасности при приеме на работу, а также не реже одного раза в год.	

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
доступа к данным держателей карт.	**12.6.1.c** Опросить несколько сотрудников и убедиться, что они прошли обучение вопросам безопасности и понимают важность обеспечения безопасности данных держателей карт.	
12.6.2 Персонал организации должен не реже одного раза в год подтверждать свое знание и понимание политики и процедур обеспечения информационной безопасности организации.	**12.6.2** Убедиться, что программа повышения осведомленности сотрудников по вопросам безопасности содержит требование о ежегодном подтверждении сотрудниками (в печатной или в электронной форме) прочтения и понимания корпоративной политики в отношении информационной безопасности.	Наличие подписи сотрудника (от руки или в электронном виде) гарантирует, что он действительно прочитал и понял все принципы и процедуры обеспечения безопасности, а также то, что он обязуется действовать в соответствии с этими документами.
12.7 Следует тщательно проверять кандидатов (будущий персонал) при приеме на работу для минимизации риска внутренних атак. (Примером кадровых проверок является изучение послужного списка, записей правоохранительных органов, кредитной истории, проверки рекомендаций). ***Примечание.*** *Для кандидатов на определенные должности, такие как, например, кассир в магазине, которые имеют доступ только к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.*	**12.7** Убедиться в том, что при приеме на работу новых сотрудников, которым будет предоставляться доступ к данным держателей карт или информационной среде держателей карт, осуществляются кадровые проверки (с учетом особенностей местного законодательства).	Тщательное изучение биографии сотрудников, которые имеют доступ к данным держателей карт, уменьшает риск несанкционированного использования основных номеров и других данных держателей карт сотрудниками с сомнительным или криминальным прошлым.
12.8 Внедрить и поддерживать следующие политики и процедуры взаимодействия с поставщиками услуг, которые имеют доступ к данным держателей карт или могут повлиять на безопасность данных держателей карт.	**12.8** Путем наблюдения, изучения политик, процедур и сопутствующей документации убедиться в наличии следующих процессов взаимодействия с поставщиками услуг, которые имеют доступ к данным держателей карт или могут повлиять на безопасность данных держателей карт (например, хранилища резервных копий на магнитной ленте, поставщики управляемых услуг, такие как компании веб-хостинга или поставщик услуг защиты).	Если торгово-сервисное предприятие или поставщик услуг передают данные держателей карт другому поставщику услуг, то необходимо выполнить определенные требования, чтобы обеспечить защиту таких данных со стороны поставщика услуг.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.8.1 Составление и регулярное обновление перечня поставщиков услуг.	**12.8.1** Убедиться в том, что перечень поставщиков услуг составлен и поддерживается в актуальном состоянии.	Перечень поставщиков услуг помогает оценить потенциальные риски, существующие за пределами организации.
12.8.2 Составление письменного соглашения, включающего положение о том, что поставщики услуг ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, или на безопасность которых они могут повлиять. ***Примечание.*** *Точная формулировка положения зависит от договора между двумя сторонами, сведений о предоставляемой услуге и обязанностей каждой из сторон. Формулировка положения не обязательно должна соответствовать формулировке, указанной в данном требовании.*	**12.8.2** Изучить письменные соглашения и убедиться, что они содержат положение о том, что поставщики услуг ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, или на безопасность которых они могут повлиять.	Поставщики услуг должны поддерживать надлежащий уровень безопасности данных держателей карт, которые они получают от своих клиентов. В сочетании с требованием 12.9 данное требование о составлении письменного соглашения между организацией и поставщиком услуг нацелено на обеспечение понимания сторонами своих обязанностей по стандарту PCI DSS. Например, соглашение может включать соответствующие требования PCI DSS, которые необходимо соблюдать при предоставлении услуг.
12.8.3 Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним.	**12.8.3** Убедиться, что политики и процедуры документированы, соблюдаются и включают необходимость выполнения проверок до взаимодействия с поставщиками услуг.	В организации должен использоваться процесс проверки поставщика услуг, включая анализ рисков, до установления деловых отношений с этим поставщиком. Конкретные процессы и цели проверки зависит от организации. Примерами факторов, учитываемых при проверке, могут служить отчетность поставщика, процедуры уведомления об уязвимостях и реагирования на инциденты, сведения о разделении обязанностей между сторонами, подтверждение поставщиком соответствия требованиям PCI DSS и доказательства этого и т.д.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.8.4 Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS по меньшей мере один раз в год.	**12.8.4** Убедиться, что в организации имеется программа проверки статуса соответствия поставщиков услуг требованиям PCI DSS, по меньшей мере один раз в год.	Когда вы знаете статус соответствия своих поставщиков услуг требованиям стандарта PCI DSS, вы можете быть уверены в том, что они соответствуют тем же требованиям, что и ваша организация. Если поставщик предоставляет широкий спектр услуг, данное требование применяется только к услугам, которые предоставляются клиенту, и только такие услуги клиент должен включать в область оценки на соответствие стандарту PCI DSS. Конкретная информация, которая должна храниться организацией, зависит от действующих соглашений с поставщиками, вида услуг и т.д. Цель данного требования – обеспечить понимание организацией требований PCI DSS, которые согласились выполнять поставщики.
12.8.5 Хранить информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	**12.8.5** Убедиться, что организация хранит информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.9 ***Дополнительное требование для поставщиков услуг*:** поставщики услуг дают клиентам письменное согласие с тем, что они ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, или на безопасность которых они могут повлиять. ***Примечание.*** *До 30 июня 2015 года данное требование носит рекомендательный характер, а после этой даты становится обязательным требованием.* ***Примечание.*** *Точная формулировка положения зависит от договора между двумя сторонами, сведений о предоставляемой услуге и обязанностей каждой из сторон. Формулировка положения не обязательно должна соответствовать формулировке, указанной в данном требовании.*	**12.9** ***Дополнительная процедура проведения проверки для поставщиков услуг:*** изучить политики и процедуры поставщиков услуг, а также шаблоны письменного соглашения и убедиться, что поставщики услуг дают клиентам письменное обязательство того, что они будут соблюдать все соответствующие требования PCI DSS к поставщикам, которые обрабатывают, имеют доступ, хранят или передают данные держателей карт или критичные аутентификационные данные, или управляют информационной средой держателей карт от имени клиента.	Данное требование распространяется только на поставщиков услуг. В сочетании с требованием 12.8.2 данное требование нацелено на обеспечение понимания поставщиком услуг и его клиентами своих обязанностей по стандарту PCI DSS. Поставщики услуг должны поддерживать надлежащий уровень безопасности данных держателей карт, которые они получают от своих клиентов. Форма письменного обязательства поставщика услуг должна быть согласована между ним и его клиентами.
12.10 Должен быть внедрен план реагирования на инциденты. Организация должна быть готова немедленно отреагировать на нарушение в работе системы.	**12.10** Ознакомиться с планом и процедурами реагирования на инциденты и убедиться, что организация готова немедленно отреагировать на взлом системы следующим образом:	При отсутствии детального плана реагирования на инциденты безопасности, его распределения, чтения и понимания ответственными сторонами, замешательство и отсутствие унифицированного подхода к реагированию могут увеличить время вынужденного бездействия для бизнеса, привести к появлению в средствах массовой информации нежелательной информации, а также к возникновению дополнительной юридической ответственности.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.10.1 Следует разработать план реагирования на инциденты, применяемый в случае взлома системы. План должен содержать: • описание ролей, обязанностей и схем оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем; • описание процедур реагирования на определенные инциденты; • описание процедур восстановления и обеспечения непрерывности бизнеса; • описание процессов резервного копирования данных; • анализ требований законодательства об оповещении о фактах компрометации; • описание всех критичных системных компонентов; • процедуры реагирования на инциденты международных платежных систем или ссылки на них.	**12.10.1.a** Убедиться, что план реагирования на инциденты включает в себя: • описание ролей, обязанностей персонала и схем оповещения в случае взлома, включая, как минимум, оповещение международных платежных систем; • описание процедур реагирования на определенные инциденты; • описание процедур восстановления и обеспечения непрерывности бизнеса; • описание процессов резервного копирования данных; • анализ требований законодательства об оповещении о фактах взлома (например, Закона Калифорнии №1386, который регламентирует уведомление пострадавших клиентов в случае взлома или подозрения на взлом любого предприятия, в базе данных которого есть жители Калифорнии); • охват всех критичных системных компонентов; • процедуры реагирования на инциденты международных платежных систем или ссылки на них.	План реагирования на инциденты должен быть подробным и содержать все ключевые элементы, которые позволят компании эффективно реагировать на обнаруженные инциденты, подвергающие риску данные держателей карт.
	12.10.1.b Опросить сотрудников, проверить документацию по нескольким ранее зарегистрированным инцидентам или оповещениям безопасности и убедиться, что документированный план реагирования на инцидент и процедуры были выполнены.	
12.10.2 План следует тестировать не реже одного раза в год.	**12.10.2** Убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год.	Без надлежащего тестирования можно пропустить ключевые пункты, что может ограничить область действия плана во время инцидента.

Требования PCI DSS	Процедуры проведения тестирования	Пояснение
12.10.3 Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги круглосуточно и ежедневно.	**12.10.3** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедиться в наличии сотрудников, ответственных за круглосуточное и ежедневное реагирование на инциденты, мониторинг свидетельств любой несанкционированной деятельности, обнаружение несанкционированных беспроводных точек доступа, критичных предупреждений систем обнаружения вторжений (IDS) и (или) сообщений о несанкционированных изменениях в критичных системных файлах или файлах данных.	Без наличия обученной и легкодоступной группы реагирования на инциденты сети может быть нанесен серьезный ущерб, а критичные данные и системы могут быть повреждены вследствие ненадлежащего обращения с целевыми системами. Это может препятствовать успешному процессу расследования, проводимому после обнаружения инцидента.
12.10.4 Сотрудники, ответственные за реагирование на нарушения безопасности, должны быть обучены соответствующим образом.	**12.10.4** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедиться в том, что сотрудники, ответственные за реагирование на нарушения безопасности, проходят периодическое обучение.	
12.10.5 План должен включать в себя процедуры реагирования на предупреждения систем мониторинга безопасности, включая, без ограничения, системы обнаружения и предупреждения вторжений, брандмауэры, а также системы мониторинга целостности файлов.	**12.10.5** Путем наблюдения и изучения процессов убедиться в том, что план реагирования на инциденты включает в себя процедуры реагирования на предупреждения систем мониторинга безопасности, в том числе обнаружение неавторизованных беспроводных точек доступа.	Данные системы мониторинга ориентированы на потенциальный риск в отношении данных и необходимы для быстрого реагирования в целях предотвращения инцидентов. Такие системы должны быть включены в процессы реагирования на инциденты.
12.10.6 Должен быть разработан процесс изменения и улучшения плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	**12.10.6** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедиться в том, что налажен процесс изменения и улучшения плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	Внесение "полученных уроков" в план реагирования на инциденты после возникновения инцидента помогает поддерживать актуальность плана и быстро реагировать на новые угрозы и тенденции в области безопасности.

Приложение A. Дополнительные требования PCI DSS для поставщиков услуг хостинга

Требование A.1. Поставщики услуг хостинга должны защищать среду данных платежных карт

Согласно требованиям 12.8 и 12.9 все поставщики услуг, имеющие доступ к данным держателей карт (включая поставщиков услуг общего хостинга) должны выполнять требования PCI DSS. В дополнение к этому, требование 2.6 говорит о том, что поставщики услуг общего хостинга должны обеспечивать безопасность сред и данных каждого клиента. Таким образом, поставщики услуг с общей средой (хостинг-провайдеры) должны дополнительно выполнять требования, перечисленные в этом приложении.

Требования	Процедуры проведения тестирования	Пояснение
A.1 Обеспечить защиту данных каждого клиента (например, торговой точки или др.) согласно требованиям с A.1.1 по A.1.4: хостинг-провайдер должен удовлетворять всем этим требованиям, помимо требований PCI DSS. ***Примечание.*** *Даже если хостинг-провайдер соответствует требованиям PCI DSS, это не значит, что каждая организация, которая пользуется его услугами, соответствует этим требованиям. Каждая организация должна соответствовать требованиям стандарта PCI DSS и подтверждать свое соответствие применимым для нее способом.*	**A.1** Чтобы убедиться, что хостинг-провайдер обеспечивает должный уровень защиты своих клиентов, выберите несколько серверов (под управлением Windows и Unix/Linux) в репрезентативной выборке торгово-сервисных организаций и поставщиков услуг и проведите проверки, перечисленные в пунктах с A.1.1 по A.1.4.	*Приложение A* к тексту стандарта PCI DSS предназначено для поставщиков услуг общего хостинга, которые желают предоставлять своим клиентам (торгово-сервисному предприятию или поставщику услуг) среду размещения данных, которая соответствует требованиям стандарта PCI DSS.

Требования	Процедуры проведения тестирования	Пояснение
A.1.1 Ограничить доступ приложений каждого клиента только к своей среде данных держателей карт.	**A.1.1** Если хостинг-провайдер позволяет клиентам запускать приложения (например, скрипты), следует убедиться, что эти приложения запущены под уникальным идентификатором. Например: • ни одно приложение и ни один пользователь не может использовать имя пользователя, от которого работает разделяемый веб-сервер; • все CGI-скрипты, используемые клиентом, должны быть созданы и запущены от имени идентификатора клиента.	Если торгово-сервисному предприятию или поставщику услуг разрешается выполнять свои собственные приложения на совместно используемом сервере, то они должны выполняться под учетной записью этого торгово-сервисного предприятия или поставщика услуг, а не под учетной записью пользователя с широкими полномочиями.
A.1.2 Ограничить доступ клиента только к своей среде данных держателей карт.	**A.1.2.a** Убедиться, что ни один из клиентов не обладает правами администратора/суперпользователя.	Чтобы гарантировать, что доступ и полномочия предоставляются так, что каждая торговая точка или поставщик услуг имеют доступ только к собственной среде, необходимо принять во внимание следующее: 1. полномочия торговой точки или поставщика услуг; 2. разрешения на чтение, запись и запуск файлов; 3. разрешения на запись в системные исполняемые файлы; 4. разрешения журналам торговой точки или поставщика услуг; 5. механизмы защиты системных ресурсов от монополизации.
	A.1.2.b Убедиться, что каждый клиент имеет права чтения, записи и выполнения только своих утилит и данных. Для ограничения могут применяться права доступа к файловой системе, списки контроля доступа, средства chroot, jailshell и т.п. **Обратите внимание!** Файлы клиента не должны быть доступны группе пользователей.	
	A.1.2.c Убедиться, что у клиента отсутствует право записи в разделяемые системные библиотеки и исполняемые файлы.	
	A.1.2.d Убедиться, что просмотр журналов протоколирования доступен только владельцу.	
	A.1.2.e Чтобы избежать ситуации, когда один клиент монопольно использует все ресурсы сервера для эксплуатации уязвимостей (таких как ошибки, конфликты и условия перезапуска, результатом которых может стать переполнение буфера), следует убедиться, что для каждого клиента установлены лимиты на использование следующих системных ресурсов: • дисковое пространство; • канал; • память; • ЦП.	

Требования	Процедуры проведения тестирования	Пояснение
A.1.3 Убедиться, что протоколирование действий и событий включено для каждого клиента и соответствует требованию 10 стандарта PCI DSS.	**A.1.3** Убедиться, что протоколирование событий удовлетворяет следующим критериям: • протоколирование настроено для всех типичных используемых на сервере приложений сторонних производителей; • протоколирование включено по умолчанию; • журналы доступны для просмотра администратору и клиенту, для которого выполняется протоколирование; • журналы расположены в каталогах, доступных клиенту.	Журналы должны быть доступны в общей среде размещения данных держателей карт так, чтобы торговые точки и поставщики услуг имели доступ и могли просматривать журналы регистрации событий, относящиеся только к собственной информационной среде держателей карт.
A.1.4 Убедиться в наличии процессов, позволяющих провести расследование инцидентов по каждому клиенту.	**A.1.4** Убедиться в наличии у хостинг-провайдера политик, описывающих правила проведения расследования в случае компрометации данных клиентов.	Хостинг-провайдеры должны иметь процессы для быстрого реагирования в случае компрометации, если требуется расследование инцидентов, вплоть до определенного уровня детализации для того, чтобы были доступны подробные сведения о торгово-сервисном предприятии или поставщике услуг.

Приложение B. Компенсационные меры

Компенсационные меры могут использоваться для требований PCI DSS в том случае, если проверяемая организация не может выполнить требование по обоснованным техническим или задокументированным бизнес-ограничениям, однако успешно снизила риск, связанный с требованием, путем реализации другой компенсирующей меры.

Компенсационные меры должны удовлетворять следующим требованиям.

1. Преследовать ту же цель, что и изначальное требование PCI DSS.
2. Обеспечивать ту же степень защищенности, что и изначальное требование PCI DSS, чтобы снизить риск так же эффективно, как и изначальное требование. (См. документ *"PCI DSS: Понимание назначения требований"* для определения цели каждого требования PCI DSS).
3. Обеспечивать определенную избыточность сверх требуемого. (Недостаточно просто удовлетворять всем остальным требованиям PCI DSS – это не является компенсирующей мерой).

   При анализе избыточности следует руководствоваться следующими моментами.

Примечание. *Пункты с а) по в), приведенные ниже, являются лишь примерами. Все компенсационные меры должны быть проверены и утверждены аудитором. Эффективность компенсационных мер – довольно специфичный момент, зависящий от многих факторов. Следует помнить, что одна и та же мера не может быть одинаково эффективна в разных системах.*

   a) Существующее требование PCI DSS НЕ МОЖЕТ рассматриваться как компенсационная мера, если она уже описана в отчете. Например, пароли на административный удаленный доступ должны передаваться в зашифрованном виде для защиты от перехвата. Организация не может использовать другие меры относительно паролей PCI DSS, такие как блокировка нарушителя, сложные пароли и т.д. для компенсации отсутствия зашифрованных паролей, поскольку эти меры не способствуют снижению риска перехвата паролей. Кроме того, другие меры уже являются требованиями PCI DSS для объекта, подлежащего проверке (пароли).

   b) Существующее требование PCI DSS МОЖЕТ рассматриваться как компенсационная мера, если оно снижает существующий риск. Например, двухфакторная аутентификация, являющаяся требованием при удаленном доступе. Она также может использоваться *и внутри сети* для защиты административного доступа, если шифрование аутентификационных данных невозможно. Двухфакторная аутентификация может быть приемлемой компенсирующей мерой при следующих условиях: 1) если она соответствует цели изначального требования и обеспечивает защиту от перехвата паролей администраторов и 2) если она настроена надлежащим образом и выполняется в защищенной среде.

   c) Существующие требования PCI DSS могут использоваться совместно с другими мерами как компенсационные. Например, если организация не может реализовать хранение данных держателей карт в нечитаемом виде в соответствии с требованием 3.4 (например, путем шифрования), компенсационной мерой может считаться использование устройства или комбинации устройств, приложений и мер, направленных на: 1) сегментацию сети; 2) фильтрацию по IP- или MAC-адресам и 3) использование двухфакторной аутентификации во внутренней сети.

4. Быть соизмеримыми с дополнительным риском, вызванным невозможностью выполнить требование PCI DSS.

Руководствуясь вышеперечисленными пунктами, аудитор должен проверить каждую компенсационную меру, чтобы убедиться, что она адекватно соотносится с риском, который призван уменьшить исходное требование PCI DSS. Следует также иметь установленные процедуры и использовать определенные меры по соответствию требованиям, чтобы гарантировать, что компенсационные меры остаются эффективными после выполнения оценки.

Приложение C. Компенсационные меры – Форма для заполнения

Пользуйтесь этой таблицей для описания компенсационной меры для каждого требования PCI DSS. Обратите внимание, что компенсационные меры должны быть отражены в отчете о соответствии в соответствующем разделе требования PCI DSS.

Примечание. *Только организации, выполнившие оценку рисков, могут пользоваться компенсационными мерами для достижения статуса соответствия.*

Номер и определение требования:

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	
2. Цель	Определите цель исходного требования и компенсирующей меры.	
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением исходного требования.	
4. Определение компенсационных мер	Опишите компенсационную меру и то, как она соответствует требованию, создает дополнительные риски (если создает).	
5. Проверка компенсационных мер	Опишите, как компенсационные меры были проверены и протестированы.	
6. Соблюдение	Опишите, как контролируется процесс соблюдения компенсационной меры.	

Перечень компенсационных мер – Пример заполнения

Пользуйтесь этой таблицей для описания компенсационных мер для требований, имеющих статус "Выполнено" благодаря использованию компенсационных мер.

Номер требования: *8.1.1. – Все ли пользователи имеют уникальный идентификатор для получения доступа к системным компонентам или данным держателей карт?*

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	*Компания XYZ использует Unix-сервера без LDAP-авторизации. Таким образом, на каждый из них требуется заходить под учетной записью суперпользователя ("root"). Организация не может управлять входом "root" и следить за использованием этой учетной записи каждым пользователем.*
2. Цель	Определите цель исходного требования и компенсирующей меры.	*Использование уникального идентификатора преследует две цели. Во-первых, с точки зрения безопасности недопустимо использовать общие учетные записи. Во-вторых, в таком случае невозможно определить, какой администратор ответственен за определенные действия.*
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением исходного требования.	*Дополнительный риск связан с тем, что не всем пользователям назначен уникальный идентификатор и их действия не могут быть отслежены.*
4. Определение компенсационных мер	Опишите компенсационную меру и то, как она соответствует требованию, создает дополнительные риски (если создает).	*Пользователям компании XYZ предписано использовать команду SU (substitute user – замена пользователя) для получения доступа к серверам со своих компьютеров. Это позволяет пользователю получить доступ к учетной записи с правами суперпользователя ("root"). При этом все действия, связанные с запуском этой команды, записываются в отдельный файл журнала. Таким образом, действия каждого пользователя можно отслеживать через учетную запись SU, не разглашая пароль учетной записи с правами суперпользователя ("root").*
5. Проверка компенсационных мер	Опишите, как компенсационные меры были проверены и протестированы.	*Компания XYZ продемонстрировала аудиторам, что команда SU выполняется и что действия тех пользователей, которые используют эту команду, записываются с целью определения того, что пользователь выполняет действия с правами суперпользователя ("root").*

6. Соблюдение	Опишите, как контролируется процесс соблюдения компенсационной меры.	*В компании XYZ задокументированы процессы и процедуры, которые обеспечивают неизменность конфигурации SU и невозможность выполнять команды пользователя "root" без отслеживания и протоколирования.*

Приложение D. Сегментация и выборка бизнес-объектов и системных компонентов