Digital Compliance

PCI Security Standards Council

Стандарт Безопасности Данных
Индустрии Платежных Карт (PCI)

Требования и процедуры аудита безопасности

Версия 3.2

Апрель 2016

Информация о переводе

Данный документ не является официальным переводом стандарта PCI DSS версии 3.2.
Перевод выполнен компанией Digital Compliance.
Настоящий документ не заменяет и не дополняет требования английской версии Стандарта.
Оригинальная английская версия Стандарта должна считаться приоритетной.

Редакция 0.9

http://digitalcompliance.ru/

115280, Москва, ул. Ленинская Слобода, 26
197046, Санкт-Петербург, Петроградская наб., 16 А
+7 (812) 703-15-47, +7 (495) 223-07-86, info@digitalcompliance.ru

Изменения документа

Дата	Версия	Описание	Страницы
Октябрь 2008 г.	1.2	В документе "Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования PCI DSS и процедуры оценки 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".	
Апрель 2015 г.	3.1	Изменение по сравнению с версией PCI DSS v.3.0. Детали изменений см. "PCI DSS: обзор изменений PCI DSS в версии 3.1 по сравнению с версией 3.0".	
Апрель 2016 г.	3.2	Изменение по сравнению с версией PCI DSS v.3.1. Детали изменений см. "PCI DSS: обзор изменений PCI DSS в версии 3.2 по сравнению с версией 3.1".	

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. Стандарт PCI DSS также применим для ***всех*** других организаций, которые хранят, обрабатывают или передают данные держателей карт (ДДК) и (или) критичные аутентификационные данные (КАД). Ниже приведен общий обзор 12 требований стандарта PCI DSS.

Стандарт безопасности данных индустрии платежных карт (PCI DSS): общий обзор

Построить и поддерживать защищенные сети и системы	**1.** Установить и поддерживать конфигурацию межсетевых экранов для защиты ДДК **2.** Не использовать пароли и другие системные параметры, заданные производителем по умолчанию
Защита данных держателей карт	**3.** Защищать хранимые данные держателей карт **4.** Шифровать ДДК при передаче через сети общего пользования
Поддерживать программу управления уязвимостями	**5.** Защищать все системы от вредоносного ПО и регулярно обновлять антивирусные ПО или программы **6.** Разрабатывать и поддерживать безопасные системы и приложения
Внедрить строгих мер контроля доступа	**7.** Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью **8.** Идентифицировать и аутентифицировать доступ к системным компонентам **9.** Ограничить физический доступ к данным держателей карт
Регулярный мониторинг и тестирование сетей	**10.** Отслеживать и контролировать любой доступ к сетевым ресурсам и данным держателей карт **11.** Регулярно тестировать системы и процессы обеспечения безопасности.
Поддерживать политики информационной безопасности	**12.** Разработать и поддерживать политику информационной безопасности для всех работников

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 инструкции и лучшие практики для содействия организациям при подготовке, проведении и составлении отчетных

материалов по результатам проверки на соответствие требованиям стандарта PCI DSS. Требования стандарта PCI DSS и Проверочные процедуры описываются, начиная со стр. 15.

Стандарт PCI DSS содержит минимальный набор требований для защиты данных держателей карт, который может быть расширен дополнительными мерами и методами для дальнейшего снижения рисков, а также требованиями и распоряжениями местного, регионального и отраслевого законодательства. Кроме того, в соответствии с законодательством или нормативными требованиями может требоваться особая защита персональных данных, или других элементов данных (например, имени держателя карты). PCI DSS не заменяет собой местные или региональные законы, постановления правительства 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 помочь организациям в проведении оценки и подтверждении их соответствия PCI DSS, включая:

- Библиотеку документов, в том числе:
  - *PCI DSS: обзор изменений PCI DSS в версии 3.2 по сравнению с версией 3.1*
  - *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"
- Обучающие курсы и информационные вебинары по PCI
- Список сертифицированных аудиторов безопасности (QSA) и авторизованных поставщиков услуг сканирования (ASV)
- Список одобренных PTS устройств и платежных приложений, прошедших проверку на соответствие стандарту PA-DSS

Примечание. *«Вспомогательные документы» относятся к сопроводительным документам PCI DSS. В них приводятся дополнительные аспекты и рекомендации по выполнению требований PCI DSS, которые при этом не заменяют, не исключают и не расширяют ни PCI DSS, ни любое 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 организацийб вовлеченных в обработку платежных карт: ТСП, процессинговых центров, финансовых учреждений и поставщиков услуг, а также всех 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 (CDE), 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 карточных данных (ДДК и (или) КАД). Некоторые требования PCI DSS также могут быть применены к организациям, передавшим платежные операции или управление информационной средой держателей карт (CDE) третьим лицам1. Кроме того, организации, передавшие платежные операции или управление информационной средой держателей карт (CDE) третьим лицам, обязуются гарантировать, что защита карточных 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 отдельным программам международных платежных систем по обеспечению соответствия требованиям

		Элемент данных	Хранение разрешено	Хранение данных в нечитаемом виде согласно требованию 3.4
Данные платежных карт	**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 конкретными международными платежными системами, 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 запрещено хранить после авторизации (даже в зашифрованном виде)
[3] Полные данные дорожки магнитной полосы или ее эквивалент на чипе или другом носителе
[4] Трех- или четырехзначное проверочное значение, напечатанное на лицевой или обратной стороне платежной карты.
[5] Персональный идентификационный номер, который вводится держателем карты при выполнении операции с предоставлением карты, и (или) зашифрованный PIN-блок, присутствующий в сообщении о транзакции.

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 согласно «Руководству по внедрению PA-DSS» (представляется разработчиком платежного приложения).

Все приложения, хранящие, обрабатывающие или передающие данные держателя карты, входят в область оценки организации на соответствие стандарту PCI DSS, включая приложения, прошедшие проверку на соответствие стандарту PA-DSS. Оценка соответствия стандарту PCI DSS призвана подтвердить, что платежное приложение, соответствующее стандарту PA-DSS, должным образом настроено и безопасно внедрено в соответствии с требованиями PCI DSS. Если приложение подверглось какой-либо модификации, оно потребует более тщательного изучения в ходе оценки соответствия стандарту PCI DSS, так как приложение может более не соответствовать версии, проверенной на соответствие PA-DSS.

Требования стандарта PA-DSS основаны на Требованиях PCI DSS и процедурах оценки безопасности (определенных в данном документе). Стандарт PA-DSS более детально описывает требования к платежному приложению для упрощения достижения организациями соответствия стандарту PCI DSS. Поскольку угрозы безопасности постоянно развиваются, приложения, которые более не поддерживаются разработчиками (к примеру, определенные разработчиками как «end of life») могут не обеспечивать тот же уровень безопасности, как поддерживаемые приложения.

При внедрении в среду, соответствующую стандарту PCI DSS, безопасные платежные приложения позволят снизить вероятность нарушений безопасности, 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, а также мошеннических действий, возникающих в результате таких нарушений.

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 межсетевые экраны) или влияющие на безопасность информационной среды держателей карт (например, dns- или прокси-серверы);
- компоненты виртуализации, такие как виртуальные машины, виртуальные коммутаторы и маршрутизаторы, виртуальные приложения/рабочие столы и гипервизоры;
- сетевые компоненты, включая, помимо прочего, межсетевые экраны, 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 NTP (Network Time Protocol - протокол 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, доступные через Интернет);
- любой компьютер или устройство, расположенное в среде держателей карт или подключенное к ней.

Первым этапом выполнения оценки соответствия требованиям PCI DSS является 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. Все системы и места хранения должны рассматриваться как часть процесса определения области аудита, включая резервные площадки, системы аварийного восстановления, компоненты отказоустойчивых систем.

Для того чтобы проверить корректность области применения PCI DSS, следует выполнить следующие действия:

- оцениваемая организация выявляет 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 ДДК);

Любые обнаруженные данные держателей карт подлежат включению 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 безопасно удалить, переместить в установленную на данный момент среду держателей карт или изменить переопределить среду держателей карт так, чтобы она включала эти данные. Организация сохраняет документы, описывающие, как область применения PCI DSS была определена. Документы сохраняются для их проверки аудитором и (или) для использования в качестве справочного материала при определении области применения PCI DSS в будущем году.

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

Сегментация сети

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

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

В случае отсутствия адекватной сегментации (т.н. "плоская сеть") в область оценки соответствия 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 оценки соответствия PCI DSS, должны быть изолированы (сегментированы) от среды держателей карт (CDE) так, чтобы даже в случае взлома таких компонентов это не повлияло бы на безопасность среды держателей карт.

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

Документирование потоков ДДК в виде диаграммы потоков данных помогает более лучше понять 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 выполнена надлежащим образом и позволяет уменьшить область оценки. Корректно выполненная сегментация сети изолирует системы, которые хранят, обрабатывают или передают данные держателей карт, от остальных систем. Корректность каждой реализации сетевой сегментации зависит от многих факторов, таких как конфигурации сети, используемых технологий и иных реализуемых защитных мер.

Приложение D. "Сегментация и выборка подразделений организации и/или 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 (POS) 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)

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 среды 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 находятся в области ответственности клиентов поставщиков услуг и должны быть проверены в рамках оценки соответствия PCI DSS клиента. Например, хостинг-провайдер должен четко определить, какие IP-адреса просканированы в рамках ежеквартального сканирования на наличие уязвимостей, и за ежеквартальное сканирование каких адресов ответственны клиенты.

Поставщики услуг несут ответственность за подтверждение своего соответствия стандарту PCI DSS. Также платежные системы могут обязать поставщиков услуг продемонстрировать свое соответствие. Поставщикам услуг следует обращаться к представителям соответствующей платежной системы или эквайеру для определения соответствующего способа подтверждения соответствия.

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

1) **Ежегодная оценка:** Поставщики услуг могут самостоятельно пройти ежегодную оценку соответствия стандарту PCI DSS и представить доказательство соответствия своим клиентам, или

2) **Многократные оценки, оценки по требованию:** если поставщики услуг не проводят собственную оценку соответствия стандарту PCI DSS, они обязуются проходить проверки по запросу своих клиентов и/или участвовать в каждой оценке соответствия стандарту PCI DSS своих клиентов, предоставляя результаты каждой оценки соответствующему клиенту.

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 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, межсетевые экраны, 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 мер (например, процесса или технического средства) для предотвращения 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 применения PCI DSS (например, новое правило межсетевого экрана, разрешающее подключение между системой в информационной среде держателей карт и другой системой, может привести к включению других систем или сетей в область применения PCI DSS);
   - определение требований PCI DSS, применимых к системам и сетям, на которые распространяются изменения (например, если новая система входит в область применения 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 применения PCI DSS и внедрение необходимых механизмов обеспечения безопасности;
4. Внесение изменений в организационную структуру (например, слияние или приобретение компаний) должно привести к официальному пересмотру области применения PCI DSS и требований.

5. Необходимо проводить регулярную оценку и опросы 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 выборок системных компонентов) с целью подтверждения того, что требования PCI DSS выполняются (например, применены стандарты конфигурации, 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 записей выполнения процедур - например, журналов аудита, отчетов о результатах сканирования на наличие уязвимостей, журналов пересмотра правил межсетевого экрана и т.д. - и облегчения подготовки организации к следующей оценке на соответствие требованиям.

6. Проверка 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 операционной деятельности организации. 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. Для некоторых организаций данные рекомендации также являются требованиями для обеспечения действующего соответствия стандарту PCI DSS. Например, описанные выше принципы включены в некоторые требования PCI DSS. Определенные организации должны подтверждать выполнение этих принципов в рамках выполнения требований Приложения A3 «Дополнительные проверки для выделенных организаций (DESV)» стандарта PCI DSS.

Все организации должны рассмотреть внедрение данных рекомендаций в свою среду, даже если организации не требуется подтверждать их выполнение.

Для аудиторов: выборка подразделений организации и системных компонентов

Выборочная оценка позволяет аудиторам ускорить процесс оценки при наличии большого количества подразделений организации и (или) системных компонентов.

Хотя аудитору разрешается делать выборку подразделений организации 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 подразделений организации и системных компонентов для проверки. Размер выборки должен быть определен сначала для подразделений организации, а затем для системных компонентов внутри каждого из них. Выборка должна быть репрезентативной как для всех типов и местоположений подразделений организации, так и для типов системных компонентов внутри подразделений . Выборка должна быть достаточно обширной, чтобы аудитор мог удостовериться в выполнении всех требований.

Примеры подразделений организации включают, но не ограничиваются: офисами организации, магазинами, франчайзинговыми предприятиями, центрами обработки данных и другими объектами в разных местах расположения. В выборку должны входить системные компоненты из каждого выбранного подразделения организации. Например, для каждого выбранного подразделения организации необходимо включать различные типы операционных систем, функции и приложения, относящиеся к проверяемой области.

Так, аудитор может определить, что выборка внутри подразделения организации включает в себя сервера Sun, на которых функционирует вебсервер 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 СУБД MySQL. Если все приложения работают на базе одной операционной системы (например, Windows 7 или Solaris 10), в выборку должны входить множество различных приложений (например, серверы базы данных, веб-серверы, серверы передачи данных).

При выборе подразделений организации и системных компонентов для оценки аудитор должен учесть следующее:

- при наличии стандартизированных по PCI DSS процессов и механизмов безопасности, которые должны соблюдаться всеми подразделениями организации и (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 подразделения организации 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 безопасности и (или) операционного процесса (например, для разных типов подразделений организации/системных компонентов), выборка должна быть достаточно большой, чтобы включать подразделения организации/системные компоненты, привязанные к каждому процессу;
- в случае отсутствия стандартизированных процессов размер выборки должен быть достаточно большим, чтобы аудитор мог убедиться, что требования PCI DSS корректно реализованы в каждом подразделении организации и(или) для каждого системного компонента;

- 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.

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

Также см.: Приложение D: "Сегментация и выборка подразделений организации и (или) системных компонентов".

Компенсационные меры

Ежегодно аудитор должен документировать, пересматривать и проверять все компенсационные меры и включать их 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

Инструкции по заполнению и требования к содержанию Отчета о соответствии указаны в *Шаблоне отчета о соответствии стандарту PCI DSS.*

Шаблон отчета о соответствии стандарту PCI DSS следует использовать как шаблон для создания *Отчета о соответствии.* Проверяемая организация должна выполнять требования каждой платежной системы по предоставлению подтверждения статуса соответствия. Для получения информации об инструкциях и требованиях по предоставлению подтверждения статуса соответствия следует обращаться к представителям соответствующей платежной системы или эквайеру.

Процесс проведения оценки соответствия стандарту PCI DSS

Процесс оценки соответствия стандарту PCI DSS включает выполнение следующих этапов:

1. Подтвердить область оценки соответствия PCI DSS.
2. Провести оценку среды на соответствие PCI DSS, следуя проверочным процедурам для каждого требования.
3. Заполнить соответствующий отчет о проведении оценки (*Анкету самооценки (SAQ) или Отчет о соответствии (ROC)), указав все компенсационные меры согласно применимым рекомендациям и инструкциям PCI.*
4. Заполнить Свидетельство о Соответствии (Attestation of Compliance) в полном объеме для поставщиков услуг или ТСП, в зависимости от обстоятельств. Свидетельства о соответствии доступны на сайте PCI SSC.
5. Направить SAQ или ROC и Свидетельство 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).
6. При необходимости устранить нарушения в отношении требований, которые не выполнены и предоставить обновленный отчет.

Версии стандарта PCI DSS

На дату публикации данного документа версия стандарта PCI DSS v3.1 действительна до 31 октября 2016 г., после чего она считается неактуальной. Все оценки по стандарту PCI DSS после указанной даты должны быть выполнены согласно версии 3.2 PCI DSS или более поздней.

Приведенная ниже таблица резюмирует данные по версиям стандарта PCI DSS и датам их вступления в силу6.

Версия	Дата публикации	Дата изъятия
PCI DSS v3.2 (данный документ)	Апрель 2016 г.	Не определена
PCI DSS v3.1	Апрель 2015 г.	Октябрь 31, 2016 г.

[6] Данные раздела могут меняться, исходя из публикации новой версии стандарта PCI DSS

Подробные требования PCI DSS и процедуры оценки безопасности

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

- **Требования PCI DSS** - в данном столбце описываются требования стандарта безопасности данных; соответствие PCI DSS проверяется по этим требованиям.
- **Проверочные процедуры** - в данном столбце описываются действия, которые должен выполнить аудитор для проверки выполнения требований PCI DSS.
- **Пояснение** - в данном столбце описывается назначение или цель каждого требования PCI DSS. В данном столбце описываются только рекомендации, должны помочь понять назначение каждого требования. Информация в этом столбце не заменяет и не дополняет требования и проверочные процедуры PCI DSS.

Примечание. *Требования стандарта PCI DSS не считаются выполненными, если меры не были внедрены либо запланированы на будущее. После того как все невыполненные требования будут выполнены организацией, аудитор должен провести повторную проверку для подтверждения того, 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 (ROC) в документе* ”Шаблон отчета о соответствии PCI DSS” (PCI DSS ROC Reporting Template).
- *См. инструкции и рекомендации по заполнению анкет самооценки (SAQ) в документе* "Инструкции и рекомендации по заполнению анкет самооценки PCI DSS" (PCI DSS SAQ Instructions and Guidelines).
- *См. инструкции по подаче отчета о соответствии стандарту PCI DSS в* Свидетельствах о соответствии стандарту PCI DSS (PCI DSS Attestations of Compliance).

Построить и поддерживать защищенные сети и системы

Требование 1. Установить и поддерживать конфигурацию межсетевых экранов для защиты данных держателей карт

Межсетевые экраны - это устройства, контролирующие сетевой трафик между внутренней локальной сетью организации и недоверенными внешними сетями, 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 сетевой 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 веб-браузеров, доступ сотрудников к электронной почте, выделенные подключения со сторонними организациями, подключения по беспроводным сетям или иными способами. 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 обеспечивать функциональные возможности межсетевого экрана, если они отвечают минимальным требованиям к межсетевым экранам, приведенным в Требовании 1. Системные компоненты, использующиеся для обеспечения функциональности межсетевого экранирования внутри среды данных держателей карт, должны быть включены в область оценки и быть проверены на соответствие Требованию 1.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1 Должны быть разработаны и внедрены стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя следующее:	**1.1** Изучить стандарты конфигурации межсетевых экранов 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 убедиться, что в организации обеспечена надежная первая линия защиты данных.
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 межсетевых экранов и маршрутизаторов	Документированный и внедренный процесс утверждения и тестирования всех подключений и изменений межсетевых экранов и маршрутизаторов поможет не допустить возникновения проблем безопасности, связанных с неправильной настройкой сети, маршрутизатора или межсетевого экрана. Без формального утверждения и тестирования
	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	

Требования PCI DSS	Проверочные процедуры	Пояснение
	тестирование.	изменений записи об изменениях могут не обновляться, что может привести к несоответствию между сетевой документацией и реальной конфигурацией.
	1.1.1.c Сделать выборку реальных изменений в конфигурации межсетевого экрана 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 держателей карт во всех системах и сетях	**1.1.3** Изучить схему потоков данных и опросить сотрудников, чтобы убедиться, что схема соответствует следующим требованиям: • отображает все потоки ДДК во всех системах и сетях; • поддерживается в актуальном состоянии и обновляется в случае внесения изменений в среду ДДК.	На схемах потоков данных держателей карт указано расположение всех данных держателей карт, которые хранятся, обрабатываются или передаются внутри сети. Схемы сети и схемы потоков данных держателей карт помогают организации получить представление об области среды данных и отслеживать ее путем 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 межсетевого экрана на наличие требований о необходимости межсетевого экранирования каждого Интернет-соединения, а также между демилитаризованной зоной (DMZ) и внутренней сетью.	Использование межсетевого экрана на каждом входящем и исходящем подключении, а также между демилитаризованной зоной 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 межсетевого экрана 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.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.5 Описание групп, ролей и обязанностей по управлению сетевыми компонентами	**1.1.5.a** Убедиться, что стандарты конфигурации межсетевых экранов 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.	**1.1.6.a** Убедиться, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат документированный перечень всех служб, протоколов и портов и обоснование коммерческой необходимости для каждого из них.	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, позволяет организациям обеспечить отключение или удаление всех остальных служб, протоколов и портов. Утверждать изменения должны сотрудники, независящие от сотрудников, занимающихся администрированием устройств. 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. Для ознакомления с сервисами, протоколами или портами, считающимися небезопасными, см. промышленные стандарты и руководства (например, NIST, ENISA, OWASP и пр.)
	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 межсетевых экранов и маршрутизаторов и убедиться, что механизмы защиты документированы и внедрены для каждой небезопасной службы, протокола и порта.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.7 Требование пересмотра наборов правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода	**1.1.7.a** Убедиться, что стандарты конфигурации межсетевых экранов 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, для которых существует документированное коммерческое обоснование. Организациям, которые вносят много изменений в наборы правил межсетевого экрана 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 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*	**1.2** Изучить конфигурацию межсетевых экранов 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. При несоблюдении данной меры организация будет подвержена риску несанкционированного доступа злоумышленников или вредоносного программного обеспечения к данным. Для того, чтобы межсетевой экран действительно выполнял свои функции, он должен быть соответствующим образом настроен для контроля и (или) ограничения входящего и исходящего трафика в сети организации.
1.2.1 Ограничить входящий и исходящий трафик только соединениями, необходимыми для информационной среды держателей карт, а весь остальной трафик должен быть запрещен.	**1.2.1.a** Проверить, стандарты конфигураций межсетевого экрана и маршрутизатора у убедиться, что в них указан входящий и исходящий трафик, необходимый для среды данных держателей карт. **1.2.1.b** Проверить конфигурации межсетевого экрана и маршрутизатора и убедиться, что разрешен только входящий и исходящий трафик, необходимый для среды данных держателей карт. **1.2.1.c** Проверить конфигурации межсетевого экрана и маршрутизатора и убедиться, что весь прочий входящий и исходящий трафик явно запрещен, например, путем явного запрета "deny all" или неявного запрета по умолчанию после разрешающих правил.	Проверка всех входящих и исходящих соединений позволяет проверять и ограничивать трафик, основываясь на адресе источника и/или адресе назначения, тем самым предотвращая нелегитимный доступ между защищенной и недоверенной средой. Это требование направлено на предотвращение доступа злоумышленников к сети организации через неавторизованные IP-адреса или использование 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

Требования PCI DSS	Проверочные процедуры	Пояснение
		трафик, кроме необходимого, помогает предотвратить возникновение неочевидных брешей в системе безопасности из-за несанкционированного и потенциально вредоносного входящего или исходящего трафика.
1.2.2 Обеспечить безопасность и своевременную синхронизацию 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 межсетевые экраны 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	**1.2.3.a** Изучить конфигурации межсетевых экранов и маршрутизаторов и убедиться, что межсетевые экраны установлены между каждой беспроводной сетью и средой держателей карт.	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 межсетевые экраны не запрещают доступ к среде данных держателей карт из беспроводной сети, злоумышленники, которые имеют несанкционированный доступ к беспроводной

Требования PCI DSS	Проверочные процедуры	Пояснение
информационной средой данных держателей карт в том случае, если такой трафик необходим в целях совершения операций.	**1.2.3.b** Убедиться, что межсетевые экраны настроены на блокирование любого трафика из беспроводной сети, либо на разрешение только авторизованного трафика между беспроводной сетью и средой держателей карт в том случае, если такой трафик необходим в бизнес-целях.	сети, могут без труда подключиться к среде данных держателей карт и получить доступ к карточным данным. Межсетевые экраны должны быть установлены между всеми беспроводными сетями и средой ДДК 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 Запретить прямой публичный доступ между сетью Интернет и любым системным компонентом в среде ДДК.	**1.3** Проверить конфигурацию межсетевых экранов и маршрутизаторов, включая, помимо прочего, маршрутизатор на границе с сетью Интернет, маршрутизатор и межсетевой экран 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.	Возможны случаи, когда по обоснованным причинам к системам в ДМЗ предоставляется доступ через недоверенные соединения (например, чтобы обеспечить публичный доступ к веб-серверу). Такие соединения никогда не должны предоставляться для систем, размещенных во внутренней сети. Назначение межсетевых экранов 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 Реализовать 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 межсетевых экранов 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). Такие функциональные возможности позволяют предотвратить доступ злоумышленников к внутренней сети организации из Интернета и использование

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.2 Ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.	**1.3.2** Убедиться, что входящие Интернет-соединения в конфигурации межсетевого экрана и маршрутизатора ограничены только IP-адресами, находящимися в демилитаризованной зоне (DMZ).	служб, протоколов или портов несанкционированным образом.
1.3.3 Внедрить меры антиспуфинга для выявления и блокирования доступа в сеть IP-адресов из непроверенных источников. (К примеру, блокировать трафик между источниками из Интернета и адресами внутренних источников)	**1.3.3** Убедиться, что в конфигурации межсетевых экранов и маршрутизаторов внедрены меры антиспуфинга, например, пакеты с внутренними адресами не могут попасть от источника из Интернет в демилитаризованную зону (DMZ).	Обычно, пакет содержит IP-адрес компьютера, который его отправил, чтобы остальные компьютеры сети знали, откуда пакет был отправлен. Злоумышленники будут часто стараться подменить (или сымитировать) отправляемый IP-адрес таким образом, чтобы система-получатель сочла, что пакет из доверенного источника. Фильтрация входящего трафика позволяет, помимо прочего, предотвратить подмену IP-адресов (имитацию для пакета адреса внутренней сети организации).
1.3.4 Запретить неавторизованный исходящий трафик из среды данных держателей карт в сеть Интернет.	**1.3.4** Изучить конфигурации межсетевых экранов 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, должен быть проверен на соответствие установленным правилам. Необходимо проверить соединения, чтобы ограничить трафик только авторизованными соединениями (например, посредством ограничения адресов (портов) источника или назначения и (или) блокирования содержимого).
1.3.5 Разрешать только «established» (установленные) соединения в сети.	**1.3.5** Изучить конфигурации межсетевых экранов и маршрутизаторов и убедиться, что межсетевые экраны разрешаются только установленные соединения во внутреннюю сеть и блокируют любые входящие соединения, которые не связаны с предварительно установленной сессией/сеансом.	Межсетевой экран, обслуживающий «состояние» (или статус) каждого соединения через межсетевой экран, знает, является ли очевидный ответ на предыдущее соединение действительным авторизованным ответом (поскольку он сохраняет статус каждого соединения) или это мошеннический трафик, который пытается обманом заставить межсетевой экран разрешить соединение.
1.3.6 Разместить системные компоненты (например, базы данных), в которых хранятся данные держателей карт, во внутреннем сегменте сети, отделенном от DMZ и	**1.3.6** Изучить конфигурации межсетевых экранов 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 ДДК размещены 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

Требования PCI DSS	Проверочные процедуры	Пояснение
иных недоверенных сетей.		демилитаризованной зоны и иных недоверенных сетей межсетевым экраном, не позволит неавторизованному сетевому трафику дойти до системного компонента. ***Примечание:*** *Это требование не распространяется на временное хранение данных держателей карт в энергозависимой памяти.*
1.3.7 Не раскрывать частные IP-адреса и данные о маршрутах третьим сторонам, не имеющим санкционированного доступа к такой информации. ***Примечание****: Методы сокрытия IP-адресации включают, но не ограничиваются:* • *Network Address Translation (NAT);* • *размещение серверов, содержащих данные держателей карт, за прокси-серверами и (или) межсетевыми экранами;* • *удаление или фильтрация объявлений маршрутов для частных сетей, требующих зарегистрированной адресации;* • *внутреннее использование адресного пространства RFC1918 вместо зарегистрированных адресов.*	**1.3.7.a** Изучить конфигурации межсетевых экранов и маршрутизаторов и убедиться, что применяются методы, обеспечивающие предотвращение раскрытия частных IP-адресов и данных о маршрутизации из внутренней сети в сеть Интернет	Запрет передачи внутренних или частных IP-адресов является действенным способом предотвращения получения злоумышленником информации об 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
	1.3.7.b Опросить сотрудников и изучить документацию, чтобы убедиться, что любое раскрытие частных IP-адресов и данных о маршрутизации является санкционированным.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.4 Установить персональные межсетевые экраны или аналогичный функционал на все мобильные компьютеры (включая принадлежащие компании и/или сотрудникам), которые при нахождении вне сети организации подключены к сети Интернет (например, ноутбуки используемые сотрудниками) и которые также используются для доступа к среде ДДК. В настройках межсетевых экранов (или аналогов) должны содержаться: • конкретные настройки конфигурации для персональных межсетевых экранов; • персональные межсетевые экраны (или аналогичный функционал) активно работают; • запрет изменения настроек пользователями мобильных компьютеров.	**1.4.a** Изучить политики и стандартные конфигурации и убедиться, что: • требуется установка персональных межсетевых экранов или эквивалентного функционала на все мобильные компьютеры (например, ноутбуки) (включая принадлежащие компании и/или сотрудникам), которые при нахождении вне сети организации подключены к сети Интернет (например, ноутбуки используемые сотрудниками) и которые также используются для доступа к среде ДДК ; • определены конкретные настройки конфигурации для персональных межсетевых экранов (или аналогичного функционала); • персональные межсетевые экраны (или аналогичный функционал) настроены на активную работу; • настройки персональных межсетевых экранов (или аналогичного функционала) не могут быть изменены пользователями мобильных компьютеров. **1.4.b** Провести выборочную проверку мобильных устройств и (или) устройств, принадлежащих сотрудникам, и убедиться, что: • персональные межсетевые экраны (или аналогичный функционал) установлены и настроены согласно конкретным конфигурационным настройкам организации; • персональные межсетевые экраны (или аналогичный функционал) запущены; • настройки персональных межсетевых экранов (или аналогичного функционала) не могут быть изменены пользователями мобильных компьютеров.	Мобильные устройства с прямым доступом в Интернет вне зоны действия защиты межсетевого экрана организации более уязвимы к Интернет-угрозам. Использование функционала межсетевого экрана (например, персонального межсетевого экрана или устройства) помогает защитить устройства от Интернет-атак , которые могут использовать мобильное устройство для получения доступа к системам и данным организации после повторного подключения устройства к сети. Конкретные настройки конфигурации для персональных межсетевых экранов определяются организацией. ***Примечание:*** *Это требование применяется к компьютерам, принадлежащим сотрудникам или организации. Системы, которыми невозможно управлять с помощью корпоративных политик, создают уязвимости периметра сети, которыми могут воспользоваться злоумышленники. Разрешение недоверенных подключений к среде ДДК организации может привести к предоставлению доступа хакерам и другим злоумышленникам.*
1.5 Гарантировать, что политики безопасности и рабочие процедуры управления межсетевыми экранами документированы, используются и известны всем заинтересованным лицам.	**1.5** Проверить документацию и опросить сотрудников для подтверждения того, что политики безопасности и рабочие процедуры управления межсетевыми экранами: • документированы; • используются; • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения постоянного контроля над межсетевыми экранами 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	Проверочные процедуры	Пояснение
2.1 Всегда изменять значения параметров, заданные производителями по умолчанию, и отключать или удалять учетные записи по умолчанию **перед** установкой систем в сети. Это требование применимо ко ВСЕМ паролям по умолчанию, включая, в том числе, пароли к операционным системам, программам защиты, приложениям и системным учетным записям, *POS-терминалам* (в точках продаж), платежным приложениям, к строкам 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 производителем по умолчанию, чтобы убедиться, что ВСЕ установленные производителем пароли (включая пароли к операционным системам, программам защиты, приложениям и системным учетным записям, POS-терминалам (в точках продаж) и строки доступа SNMP) были изменены (Используйте руководства производителей и Интернет-ресурсы, чтобы узнать аутентификационные данные, устанавливаемые производителем по умолчанию).	Злоумышленники (находящиеся внутри и вне организации) часто используют настройки, учетные записи и пароли, заданные производителями 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 Для выборки системных компонентов следует убедиться, что все ненужные учетные записи по умолчанию (включая учетные записи к операционным системам, программам защиты, приложениям, устройствам, POS-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 производителем (включая пароли по умолчанию к операционным системам, программам защиты, приложениям и системным учетным записям, POS-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, POS-терминалам, строки доступа SNMP и т.д.) удаляются или отключаются перед подключением систем к сети.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2 Разработать стандарты конфигурации для всех системных компонентов. Стандарты должны учитывать все известные уязвимости безопасности, а также положения общепринятых отраслевых стандартов безопасной настройки систем. Примеры источников общепринятых отраслевых стандартов по безопасной настройке систем 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 (NIST).	**2.2.a** Изучить стандарты конфигурации всех системных компонентов. Убедиться, что стандарты конфигурации согласуются с требованиями отраслевых стандартов безопасной настройки систем. .	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 производителей. Стандарты конфигурации должны быть актуальными, чтобы гарантировать, что недавно обнаруженные уязвимости устраняются до установки системы в сети.
	2.2.b Изучить политики и опросить сотрудников для подтверждения того, что стандарты конфигурации обновляются по мере обнаружения новых уязвимостей безопасности, как определено в требовании 6.1.	
	2.2.c Изучить политики и опросить сотрудников для подтверждения того, что стандарты конфигурации применяются при настройке новых систем, и что перед установкой системы в сети выполняется проверка, что стандарты конфигурации применены. .	
	2.2.d Проверить стандарты конфигурации на наличие следующих процедур для всех типов системных компонентов: • изменить все параметры по умолчанию, заданные производителем, и удалить ненужные учетные записи по умолчанию; • реализовать на каждом сервере только одну основную функцию для того, чтобы исключить совмещение на одном и том же сервере функций, требующих различных уровней безопасности; ; • включать только необходимые службы, протоколы, управляющие программы и т.д., требующиеся для функционирования системы; • настроить дополнительные параметры безопасности для любых необходимых служб, протоколов и управляющих программ, которые признаны небезопасными; • настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы; • удалить из системы весь неиспользуемый функционал: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2.1 Реализовать на каждом сервере только одну основную функцию во избежание совмещения на одном и том же сервере функций, требующих различных уровней защиты. (Например, веб-серверы, серверы СУБД и DNS-серверы следует размещать на разных серверах). ***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 Включать 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 любые 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 Обеспечить дополнительные механизмы защиты для всех необходимых служб, протоколов и управляющих программ, которые могут быть небезопасными.	**2.2.3.a** 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. Надлежащая защита всех небезопасных служб,

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *Для систем, использующих протокол SSL/раннюю версию TLS необходимо выполнить требования Приложения A2*	**2.2.3.b** В случае применения протокола SSL/ранней версии TLS выполнить тестовые процедуры, представленные в Приложении A2: ***Дополнительные требования PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS***.	протоколов и управляющих программ затруднит злоумышленникам использование распространенных уязвимостей через сеть. Информацию относительно надежного шифрования и безопасных протоколов см. в промышленных стандартах и рекомендациях (например, NIST SP 800-52 и SP 800-57, OWASP и пр.)
2.2.4 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. 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.
	2.2.4.b Изучить стандарты конфигурации 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.	
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.	Неиспользуемые функции могут предоставить злоумышленникам дополнительные возможности для получения доступа к системе. Удаление ненужного функционала позволит организации сконцентрироваться на защите только необходимых функций и снизить риск использования неизвестных функций злоумышленниками. Включение этого требования в стандарты и процессы безопасной настройки позволит устранить риски связанные с неиспользуемыми функциями (например, удаление/отключение FTP или веб-сервера, если сервер не будет выполнять свои функции) .
	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 шифровать канал с использованием стойких	**2.3** Сделать выборку системных компонентов и убедиться, что канал неконсольного административного доступа зашифрован выполняя следующее:	Если при неконсольном (в т.ч. удаленном) администрировании не используется безопасная аутентификация и шифрование канала, существует возможность перехвата злоумышленником
	2.3.a Наблюдать за входом администратора в каждую систему и	

Требования PCI DSS	Проверочные процедуры	Пояснение
криптографических алгоритмов. ***Примечание:*** *Для случаев использования SSL/ранней версии TLS должны выполняться требования, приведенные в Приложении A2.*	изучить системные конфигурации для того, чтобы подтвердить активизацию механизмов шифрования до запроса пароля администратора.	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. Под использованием «стойкой криптографии (стойких криптографических алгоритмов)» понимается использование признанных в отрасли протоколов с надлежащей стойкостью ключей и процессами управления ключами в рамках используемых технологий удаленного доступа.(см. определение термина "стойкая криптография" в документе *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения* и промышленных стандартах и рекомендациях, таких как NIST SP 800-52 и SP 800-57, OWASP и пр.*)*.
	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 Проследить за входом администратора в каждую систему на предмет того, что административный доступ к любому веб-интерфейсу управления проходит шифрование с использованием стойкой криптографии. .	
	2.3.d Ознакомиться с документацией производителя и опросить сотрудников чтобы убедиться, что используются надежные криптографические алгоритмы в соответствии с последними отраслевыми стандартами и (или) рекомендациями поставщиков.	
	2.3.e Если используется SSL **и (или)** ранние версии TLS**, выполнить тестовые процедуры из *Приложения A2: Дополнительные требования PCI DSS для Организаций, использующих SSL и (или) ранние версии TLS***	
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 Гарантировать, что политики безопасности, процедуры управления	**2.5** Проверить документацию и опросить работников на предмет того, что политики безопасности, операционные процедуры управления	Сотрудники должны быть ознакомлены и следовать политикам безопасности и повседневным

Требования PCI DSS	Проверочные процедуры	Пояснение
учетными данными поставщиков по умолчанию и другие параметры безопасности документированы, используются и известны всем заинтересованным лицам.	параметрами по умолчанию, заданными производителями, и другими параметрами безопасности: • документированы; • используются; • известны всем заинтересованным лицам.	операционным процедурам, чтобы гарантировать постоянный контроль над учетными данными поставщиков, настроенными по умолчанию, и другими параметрами безопасности и предотвратить использование небезопасных конфигураций.
2.6 Поставщики услуг хостинга с общей средой 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 хостинга с общей средой".*	**2.6** Выполните Проверочные процедуры **A.1.1-A.1.4,** описанные в *Приложении A: "Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой"* для оценки соответствия таких поставщиков требованиям PCI DSS, чтобы проверить, что данные поставщики защищают размещенные у них среду и данные организаций (торгово-сервисные предприятия и поставщики услуг).	Данное требование предназначено для хостинг-провайдеров, которые предоставляют общую среду размещения 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 сред других клиентов. Поэтому злоумышленник может, получив доступ к данным одного клиента, без труда получить доступ к данным всех остальных клиентов. См. подробные сведения о требованиях в *Приложении A.*

Защита данных держателей карт

Требование 3. Защищать хранимые данные держателей карт

Методы защиты данных, такие как шифрование, усечение, маскирование и хеширование, являются важнейшими компонентами защиты данных держателей карт. Если взломщик обойдет остальные защитные меры 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 усеченного PAN, если не требуется хранение полного PAN, и избежание пересылки PAN с использованием пользовательских технологий передачи сообщений, таких как электронная почта и системы мгновенного обмена сообщениями.

См. *Глоссарий PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения* для определения термина "стойкая криптография" и других терминов.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.1 Ограничить хранение данных только необходимым минимумом. Разработать 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; • специфические требования к хранению данных держателей карт; • ежеквартальный процесс обнаружения и безопасного	**3.1.a** Изучить политики, процедуры и процессы хранения и уничтожения данных и проверить их на наличие следующих минимальных требований: • количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований • 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; • наличие ежеквартального процесса обнаружения и безопасного удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	Формальная 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 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 относятся к соответствующей отрасли и применяются к тому типу данных, которые хранятся.
	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	

Требования PCI DSS	Проверочные процедуры	Пояснение
удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	держателей карт.	
	3.1.c Для нескольких системных компонентов, хранящих данные держателей карт, необходимо: • проверить файлы и системные записи и убедиться, что сроки хранения данных не превышают сроки, определенные политикой хранения данных; • проверить механизм удаления на предмет того, что данные удаляются безопасным образом .	Обнаружение и удаление хранящихся данных с истекшим сроком хранения позволяет предотвратить хранение данных, которые больше не требуются. 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. ***Важно! 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, следует сделать все данные невосстановимыми до завершения процесса авторизации. *Эмитенты и компании, обеспечивающие услуги эмиссии, могут хранить критичные*	**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. Эмитенты платежных карт или компании,
	3.2.b При проверке эмитентов и (или) компаний, предоставляющих услуги эмиссии и хранящие критичных аутентификационных данных, проверить центры обработки данных и системные конфигурации, чтобы убедиться, что критичные аутентификационные данные надежно защищены.	

Требования PCI DSS	Проверочные процедуры	Пояснение
аутентификационные данные, если: • *имеется производственная необходимость и* • *данные хранятся безопасно* К критичным аутентификационным данным относятся данные, перечисленные в требованиях 3.2.1 3.2.3.	**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** Для всех других организаций, если организация принимает КАД, проверить процедуры и изучить процесс безопасного удаления данных, и убедиться, что данные невосстановимы.	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 безопасно, в соответствии с требованиями стандарта PCI DSS и требованиями конкретной платежной системы. Для неэмитентов сохранение критичных аутентификационных данных после аутентификации запрещено.
3.2.1 Запрещается хранить полное содержимое любой дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, ее аналога 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;*	**3.2.1** Проверить источники данных в выборке 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 полные данные дорожки сохранены, злоумышленник, получивший доступ к этим данным, может использовать их для воспроизведения платежных карт и осуществления мошеннических транзакций.

Требования PCI DSS	Проверочные процедуры	Пояснение
• *номер платежной карты (PAN);* • *дата истечения срока действия карты;* • *сервисный код.* *Для минимизации рисков храните только указанные элементы данных, если в этом есть служебная необходимость*		
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), после авторизации.	**3.2.2** Проверить источники данных в выборке 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), 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 (т.н. «card-not-present») (например, при заказе товаров через Интернет, по почте или по телефону). В случае кражи этих данных, злоумышленник получит возможность совершения мошеннических операций через Интернет, по почте или телефону.
3.2.3 Запрещается хранить персонального идентификационный номер (PIN) или зашифрованный PIN-блок после авторизации.	**3.2.3** Проверить источники данных в выборке системных компонентов, включая, в том числе, перечисленные ниже, и убедиться, что персональные идентификационные номера (PIN) или 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 у злоумышленника появится возможность совершения мошеннических дебетовых операций с использованием PIN-кода (например, для получения наличных через банкомат).

Требования PCI DSS	Проверочные процедуры	Пояснение
3.3 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 полный PAN. ***Примечание:*** *Это требование не заменяет собой иные более строгие требования к отображению данных держателей карт (например, юридические требования или требования платежных систем к чекам POS-терминалов).*	**3.3.a** Изучить письменные политики и процедуры маскирования основного номера держателя карты при его отображении и убедиться, что: • список ролей, которым требуется доступ к полному PAN, документирован, и для каждой роли обоснована служебная необходимость такого доступа; • PAN должен маскироваться при отображении, так что полный PAN виден только тем сотрудникам, у которых на то есть служебная необходимость; • для всех остальных ролей, которым явным образом не разрешено видеть полный PAN, должен быть виден только маскированный PAN.	Отображение полного номера PAN на экранах компьютеров, чеках об оплатах по платежным картам, 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. Принцип маскировки должен всегда обеспечивать отображение только минимального количества цифр номера, требуемого для выполнения необходимой коммерческой функции. К примеру, если для выполнения какой-либо коммерческой функции достаточно только последних четырех цифр номера, замаскируйте основной номер держателя карты так, чтобы сотрудник, выполняющий эту операцию, видел только последние четыре цифры. Еще пример, если функция требует доступа к банковскому идентификационному номеру (БИК) для процесса маршрутизации, при выполнении нужной операции снимите маскировку только с номера БИК (обычно первые шесть цифр). 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.
	3.3.b Проверить системные конфигурации и убедиться, что PAN отображается только для пользователей/ролей с документированной коммерческой необходимостью и маскируется для остальных запросов.	
	3.3.c Проверить правила отображения PAN и убедиться, что PAN маскируются при отображении данных держателя карты (например, на бумаге или экране монитора), и только сотрудники с обоснованной коммерческой необходимостью могут видеть весь PAN.	

Требования PCI DSS	Проверочные процедуры	Пояснение
3.4 Привести PAN в нечитаемый вид во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий), используя 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 индексные маркеры и шифровальные блокноты (такие блокноты при хранении должны быть защищены) • стойкие криптографические 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-*	**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); • индексные маркеры и шифровальные блокноты, причем такие блокноты при хранении должны быть защищены; • стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами. **3.4.b** Изучить несколько таблиц или файлов из выборки хранилищ данных и убедиться, что PAN представлен в нечитаемом виде (т. е. не хранится в открытом виде). **3.4.c** Изучить выборку съемных носителей (например, кассеты с резервными копиями данных) и убедиться, что PAN представлен в нечитаемом виде. **3.4.d** Изучить выборку журналов регистрации событий, включая журналы регистрации платежных приложений, и убедиться, что PAN из них удален или представлен в нечитаемом виде. **3.4.e** При хранении в среде усеченных и хешированных данных одних и тех же PAN, изучить внедренные средства контроля и убедиться, что усеченные или хешированные PAN не имеют корреляции, которая позволила бы восстановить исходный номер.	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 однонаправленного хеширования на основе стойкой криптографии. Использование хеширования целесообразно тогда, когда нет необходимости в восстановлении основного номера держателя карты (так как однонаправленное хеширование является необратимым). Желательно, но не обязательно добавлять дополнительное вводимое значение к данным держателя карты перед хешированием, чтобы снизить вероятность сравнения данных (и получения 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

Требования PCI DSS	Проверочные процедуры	Пояснение
либо структуры, необходимо ввести дополнительные средства контроля для недопущения корреляции между маскированным и хешированным значениями, так как при этом исходный PAN становится легковосстановимым.		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.
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, не используются локальные базы данных учетных записей или основные учетные данные для входа в сеть). Ключи дешифрования не должны быть связаны с учетными записями пользователей. ***Примечание:*** *Требование дополнительно применяется ко всем другим требованиям относительно типов шифрования и управления ключами в стандарте PCI DSS.*	**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, не используются локальные базы данных учетных записей или основные учетные данные 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.*	Назначение данного требования состоит в определении условий к использованию 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 то же имя пользователя, которое используется для аутентификации в операционной системе, 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

Требования PCI DSS	Проверочные процедуры	Пояснение
		данные в случае физической утраты диска и, следовательно, может быть полезно для портативных устройств, содержащих данные держателей карт.
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 ДДК 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 ***Дополнительное требование только для поставщиков услуг***: Вести документированное описание шифровальной архитектуры, которая будет включать: • подробную информацию обо всех алгоритмах, протоколах, и ключах, использованных для защиты данных держателей карт, включая стойкость ключей и дату истечения срока действия; • описание применения ключа для каждого ключа; • описание любого модуля безопасности (HSM) и прочих	**3.5.1** Опросить ответственных сотрудников и изучить документацию для подтверждения того, что в наличии имеется документ, описывающий шифровальную архитектуру и включающий: • подробную информацию обо всех алгоритмах, протоколах, и ключах , использованных для защиты данных держателей карт, включая стойкость ключей и дату истечения срока действия; • описание применения ключа для каждого ключа; • описание любого модуля безопасности (HSM) и прочих средств шифрования (SCD), используемых для управления ключами защиты.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является поставщиком услуг.* Поддержание в актуальном состоянии документации, описывающей архитектуру используемого криптографического решения, дает организации возможность понять какие алгоритмы, протоколы и криптографические ключи, используются для защиты данных держателей карт так же, как и устройства, которые генерируют, используют и защищают ключи. Это позволяет организации быть в курсе новых угроз для используемой криптографической архитектуры, позволяя планировать обновления из-за меняющихся уровней стойкости различных алгоритмов/ключей.

Требования PCI DSS	Проверочные процедуры	Пояснение
средств шифрования (SCD), используемых для управления ключами ***Примечание:*** *Данное требование является лучшей практикой до 31 января 2018 г., после указанного срока оно приобретет статус требования.*		Ведение указанной документации, помимо прочего, позволяет организации выявить потерянные или отсутствующие ключи или устройства управления ключами, и обнаружить ранее не идентифицированные узлы/дополнения в архитектуре используемого криптографического решения .
3.5.2 Ограничить доступ к ключам шифрования. Разрешить доступ наименьшему возможному количеству ответственных за их хранение и использование сотрудникам.	**3.5.2** 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.
3.5.3 Хранить секретные и закрытые ключи шифрования/дешифрования данных держателей карт в одной (или нескольких) из следующих форм: • зашифрованны ключом для шифрования ключей, который имеет такой же уровень защиты, как и ключ для шифрования данных, и хранится отдельно от этого ключа; • в защищенном криптографическом устройстве (таком, как аппаратный модуль безопасности (HSM) или POI-терминал, утвержденный согласно требованиям PCI PTS) ; • в форме как минимум двух компонентов полноразмерного ключа или в форме разделяемого секрета в соответствии с принятым в отрасли методом.	**3.5.3.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: • зашифрованные ключом для шифрования ключей, который имеет такой же уровень защиты, как и ключ для шифрования данных, и хранится отдельно от этого ключа; • в защищенном криптографическом устройстве (таком, как аппаратный модуль безопасности (HSM) или POI- терминал, утвержденный согласно требованиям PCI PTS); • в форме как минимум двух компонентов полноразмерного ключа или в форме разделяемого секрета в соответствии с принятым в отрасли методом. **3.5.3.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: • зашифрованны ключом для шифрования ключей; • в защищенном криптографическом устройстве (таком, как аппаратный модуль безопасности (HSM) или POI- терминал, утвержденный согласно требованиям PCI PTS); • в форме компонентов ключа или в форме разделяемого секрета в	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.

Требования PCI DSS	Проверочные процедуры	Пояснение
	соответствии с принятым в отрасли методом.	
Примечание: *Хранение публичных ключей в одной из этих форм не требуется.*	**3.5.3.c** При использовании ключей для шифрования ключей следует изучить системные конфигурации и места хранения ключей, и убедиться в том, что: • ключи для шифрования ключей обладают таким же уровнем защиты, как и ключи для шифрования данных, которые они защищают; • ключи для шифрования ключей хранятся отдельно от ключей для шифрования данных.	
3.5.4 Хранить криптографические ключи в минимально возможном количестве мест.	**3.5.4** 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 посторонним лицам.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6 Полностью документировать и внедрить все процессы и процедуры управления ключами шифрования ДДК, в том числе следующие. ***Примечание:*** *Существует множество различных источников, из которых можно получить информацию о стандартах управления ключами (например, стандарт Национального института стандартов и технологий США (NIST), с которым можно ознакомиться на сайте http://csrc.nist.gov).*	**3.6.a** ***Дополнительная проверочная процедура 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. ***Примечание:*** *Процедура проверки 3.6 является дополнительной процедурой, которая применима только к поставщикам услуг.*
3.6.1 Генерировать стойкие криптографические ключи	**3.6.1.a** Убедиться, что процедуры управления ключами указывают, каким образом генерировать стойкие ключи. **3.6.1.b** Изучить метод генерации ключей и убедиться в генерации стойких ключей.	Средство шифрования должно генерировать стойкие ключи согласно определению для термина "Генерация криптографических ключей", приведенного в документе " Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS ". Использование стойких ключей шифрования значительно повышает уровень безопасности зашифрованных данных держателей карт.
3.6.2 Безопасно распространять ключи шифрования	**3.6.2.a** Убедиться, что процедуры управления ключами указывают, как безопасным образом распространять ключи. **3.6.2.b** Изучить метод распространения ключей и убедиться в том, что	Средство шифрования должно обеспечивать безопасное распространение ключей (то есть ключи не должны распределяться в открытом виде), и только среди ответственных за их хранение и

Требования PCI DSS	Проверочные процедуры	Пояснение
	ключи распространяются безопасно.	использование сотрудников в соответствии с требованием 3.5.1.
3.6.3 Безопасно хранить ключи шифрования	**3.6.3.a** Убедиться, что процедуры управления ключами указывают, как хранить ключи безопасным образом.	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 Заменять криптографические ключи с истекшим криптопериодом (например, когда истек установленный срок и (или) когда данным ключом было зашифровано некоторое количество данных), в соответствии с указаниями соответствующего вендора приложений или владельца ключа и на основании отраслевых рекомендаций и руководств (например, специальная публикация NIST 800-57).	**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).	Криптопериод — это период времени, в течение которого ключ шифрования можно использовать по его назначению. При определении криптопериода необходимо учитывать: стойкость используемого алгоритма, размер или длину ключа, риск компрометации ключа и критичность данных, зашифрованных с помощью ключа. Периодическая смена 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 заменяются по завершении установленного криптопериода (криптопериодов).	

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6.5 Заменять ключи или изымать их из обращения (например, архивировать, уничтожать и (или) отзывать) по мере необходимости, при нарушении целостности (например, увольнение сотрудника, обладающего информацией об открытой компоненте ключа), либо ключей, относительно которых существуют подозрения во взломе. ***Примечание:*** *Если существует необходимость сохранения изъятых из обращения или замененных ключей, они должны быть безопасно заархивированы (например, с использованием 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 скомпрометированны; • проверка того, что удаленные или замененные ключи не используются для операций 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 исключить 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 в компрометации.
	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 скомпрометированны; • проверка того, что удаленные или замененные ключи не используются для операций шифрования.	

Требования PCI DSS	Проверочные процедуры	Пояснение
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 и уничтожение.*	**3.6.6.a** Проверить процедуры управления открытыми ключами вручную на наличие следующих процессов: • разделенное знание ключей, где как минимум двое 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 аутентификационным данным (например, паролям или ключам) другого.	Разделенное знание 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 средствах шифрования, где управление ключами не реализовано. Разделенное знание - это метод, при использовании которого двое или более людей раздельно владеют компонентами одного ключа; каждый из этих людей знает только свой компонент ключа, а отдельные компоненты не дают знания всего ключа шифрования (компонентами ключа являются псевдослучайные последовательности результатом сложения которых по модулю 2 (функция xor) является исходный ключ шифрования. Компонентами ключа не могут являться части ключа, полученные посредством конкатенации ключа – прим.ред.). 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.
	3.6.6.b Опросить сотрудников и (или) проследить за процессами, чтобы убедиться, что процедуры ручного управления ключами в открытом виде предусматривают следующее: • разделенное знание; • двойной контроль.	
3.6.7 Исключить несанкционированную замену криптографического ключа .	**3.6.7.a** Убедиться, что процедуры управления ключами определяют 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.	

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6.8 Обеспечить формализованное подтверждение сотрудниками, ответственными за хранение и использование ключей, их согласия с ознакомлением и принятием таких обязанностей.	**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 и опросить сотрудников чтобы убедиться, что сотрудники, ответственные за хранение и использование ключей, подтвердили (в электронном виде или письменно), что понимают и принимают свои обязанности.	
3.7 Гарантировать, 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; • 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 протоколов шифрования и аутентификации, могут быть легкими целями для злоумышленника и способствовать получению несанкционированного доступа к среде данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
4.1 Использовать стойкую криптографию и безопасные протоколы чтобы защитить критичные ДДК при их передаче с учетом следующего: • принимаются только доверенные ключи и сертификаты; • используемый протокол поддерживает только безопасные версии и конфигурации; • стойкость шифрования соответствует используемой методологии шифрования. ***Примечание:*** *В случаях применения протокола SSL/ранней версии TLS необходимо выполнять требования, приведенные в Приложении A2.* *Примеры общедоступных сетей включают, помимо прочего:* • *Интернет;* • *беспроводные технологии, включая протоколы 802.11 и Bluetooth;* • *технологии сотовой связи, например GSM, CDMA;* • *GPRS ;* • *Спутниковые средства связи.*	**4.1.a** Выявить все места, где осуществляется прием или передача ДДК через открытые общедоступные сети. Проверить документированные стандарты и сравнить их с системными конфигурациями для подтверждения того, что везде используются протоколы безопасности и стойкое шифрование. **4.1.b** Проверить документированные политики и процедуры на наличие следующих процессов: • принимаются только доверенные ключи и сертификаты; • 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 выборку входящих и исходящих транзакций (например, путем изучения системных процессов или сетевого трафика), 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 (или) сертификаты.	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. Безопасная передача данных держателей карт требует использования проверенных ключей/сертификатов, безопасного протокола передачи и соответствующей стойкости шифрования для шифрования данных держателей карт. Запросы на соединения от систем, которые не поддерживают требуемую стойкость шифрования и могут привести к ненадежному соединению, не должны приниматься. Обратите внимание на то, что некоторые версии протоколов (например, SSL, SSH v1.0 и TLS v1.0) содержат известные уязвимости, которые могут быть использованы злоумышленником для получения контроля над уязвимой системой. Независимо от того, какой протокол используется, убедитесь, что он

Требования PCI DSS	Проверочные процедуры	Пояснение
	4.1.e Изучить ключи и сертификаты, и убедиться, что протокол использует только безопасные конфигурации и не поддерживает небезопасные версии и конфигурации.	настроен для использования только безопасных версий и конфигураций. Например, можно использоваться только доверенные сертификаты и поддерживать только стойкое шифрование (не поддерживая слабые, ненадежные протоколы или методы). Проверка того, что сертификат является доверенным (например, срок действия его не истек, и он получен из доверенного источника), помогает обеспечить целостность безопасного подключения. Как правило, URL-адрес должен начинаться с префикса HTTPS, а в окне веб-браузера должен быть значок замка. Многие поставщики TLS-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. Информацию по стойкому шифрованию и безопасным протоколам можно найти в промышленных стандартах и рекомендациях (например, NISP SP 800-52 и SP 800-57, OWASP и пр.)
	4.1.f Изучить системные конфигурации и убедиться, что для используемой методологии шифрования применяется шифрование достаточной стойкости (См. рекомендации производителя и (или) лучшие практики).	
	4.1.g При использовании протокола TLS следует изучить системные конфигурации и убедиться, что TLS включен при каждой передаче или получении данных держателей карт. Например, для браузерных версий следует убедиться, что: • в качестве протокола URL-адреса указан HTTPS; • данные держателей карт запрашиваются только в том случае, если URL-адрес содержит префикс HTTPS.	
	4.1.h При использовании протокола SSL/ранней версии TLS необходимо выполнить тестовые процедуры, описанные в *Приложении A2: Дополнительные требования PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS*	
4.1.1 Убедиться, что при использовании беспроводных сетей, передающих данные держателей карт либо подключенных к среде данных держателей карт, используются передовые практические методы индустрии безопасности, чтобы реализовать стойкое шифрование при аутентификации и передаче данных.	**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: • применяются отраслевые рекомендации для обеспечения стойкого шифрования при аутентификации и передаче данных; • протоколы со слабым шифрованием (например, WEP, SSL) 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	Проверочные процедуры	Пояснение
4.2 Запрещается пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (например, электронная почта, системы мгновенного обмена сообщениями, чаты и т.д.).	**4.2.a** В случае использования пользовательских технологий передачи ДДК 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 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. В дополнение, если организация запрашивает PAN посредством технологий обмена мгновенными сообщениями, организация должна обеспечить применение средства или метода защиты PAN с использованием стойкой криптографии или приводить PAN в нечитаемый формат до передачи.
	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 Гарантировать, 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; • 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, включая вирусы, черви, трояны, 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 вредоносного ПО системах, чтобы защитить системы от текущих и возможных угроз со стороны вредоносного ПО. 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	Проверочные процедуры	Пояснение
5.1 Развернуть антивирусное программное обеспечение на всех системах, подверженных воздействию вредоносного ПО (особенно на рабочих станциях и серверах).	**5.1** Для выборки системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО, убедиться, что используется антивирусная защита (при наличии применимой антивирусной технологии).	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. *Примерами вредоносного ПО являются вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.*	5.1.1 Изучить документацию поставщика и конфигурации антивирусов, чтобы убедиться в том, что антивирусные программы способны: • обнаруживать все известные виды вредоносного программного обеспечения; • удалять все известные виды вредоносного программного обеспечения; • обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	Важно обеспечить защиту от **ВСЕХ** типов и форм вредоносного ПО.
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

Требования PCI DSS	Проверочные процедуры	Пояснение
		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 конфигураций и механизмы защиты
5.2 Гарантировать, что все антивирусные механизмы: • поддерживаются в актуальном состоянии; • 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 поддержание антивирусного ПО и антивирусных баз в актуальном состоянии.	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 на генерирацию журналов регистрации событий 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.	
	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.	
5.3 Убедиться, что антивирусные механизмы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени.	**5.3.a** Изучить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов и убедиться, что антивирусное ПО работает в активном режиме.	Антивирус, работающий постоянно и защищенный от изменений, обеспечит надежную защиту от вредоносного ПО. Использование политик по предотвращению изменений или отключения антивирусной защиты на всех системах позволит предотвратить использование уязвимостей систем злоумышленником..

Требования PCI DSS	Проверочные процедуры	Пояснение
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.b** Изучить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов и убедиться, что антивирусное ПО не может быть отключено или изменено пользователями.	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 выполнение полного сканирования после его повторного включения).
	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.	
5.4 Гарантировать, 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; • известны всем заинтересованным лицам.	Сотрудники должны быть осведомлены и следовать политикам безопасности и процедурам работы для обеспечения защиты систем от вредоносного ПО на постоянной основе.

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости безопасности для получения привилегированного доступа к системам. Большинство из таких уязвимостей закрывается путем установки обновлений безопасности, выпускаемых производителем, которые должны быть установлены организациями, управляющими системами. 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 текущими конфигурациями безопасности. В случае самостоятельной разработки приложений множества уязвимостей удастся избежать, используя стандартные процессы разработки систем и приемы безопасного программирования.*

Требования PCI DSS	Проверочные процедуры	Пояснение
6.1 Создать 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.*	**6.1.a** Проверить политики и процедуры на наличие следующих процессов: • выявление новых уязвимостей; • присвоение уровня риска уязвимостям, в т. ч. идентифицировать все уязвимости с «высоким» и «критичным» уровнями; • использование авторитетных внешних источников информации об уязвимостях.	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

Требования PCI DSS	Проверочные процедуры	Пояснение
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 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.	**6.1.b** Опросить ответственных сотрудников и понаблюдать за процессами для подтверждения того, что: • выявляются новые уязвимости; • уязвимостям присваивается уровень риска, в т. ч. идентифицировать все уязвимости с «высоким» и «критичным» уровнями; • процессы выявления новых уязвимостей системы безопасности включают в себя использование для этого внешних источников информации.	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 использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для системы безопасности.
6.2 Гарантировать, что 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	**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 соответствующего 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

Требования PCI DSS	Проверочные процедуры	Пояснение
с момента их выпуска производителем. ***Примечание:*** *Критичные обновления системы безопасности должны выявляться согласно процессу ранжирования рисков (см. требование 6.1).*	**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 соответствующего срока с момента выпуска поставщиком (например, в течение трех месяцев).	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 применимые обновления для любого установленного ПО, включая платежные приложения (и те, что сертифицированы по стандарту PA-DSS и те, что нет).
6.3 Разработать безопасные внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс) с соблюдением следующих требований: • согласно требованиям PCI DSS (например, в отношении безопасной аутентификации и журналирования); • 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.a** Изучить задокументированные процессы разработки программного обеспечения и убедиться, что они основаны на отраслевых стандартах и (или) известных рекомендациях. **6.3.b** Изучить документацию по разработке программного обеспечения и убедиться, что она принимает во внимание информационную безопасность в течение всего цикла разработки. **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.	Если не уделять должного внимания безопасности на этапах разработки программного обеспечения (определения требований, проектирования, анализа и тестирования), в производственную среду непреднамеренно или сознательно могут быть внесены уязвимости. Понимание процессов обработки критичных данных приложений - в том числе во время хранения, передачи и пребывания в памяти - поможет упростить определение методов защиты данных.

Требования PCI DSS	Проверочные процедуры	Пояснение
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 удалять из производственного кода до перевода приложения в производственный режим или передачи 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	Проверочные процедуры	Пояснение
6.3.2 Контролировать 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	**6.3.2.a** Изучить задокументированные процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что в отношении всех изменений разрабатываемого программного кода 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 самописном коде обычно используются злоумышленниками для получения доступа к сети и кражи данных держателей карт. Контроль кода (code review) должны выполнять опытные специалисты, знакомые с методиками контроля кода. Для обеспечения объективной и независимой оценки контроль кода должны выполнять лица, которые не участвовали в написании проверяемого ими 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

Требования PCI DSS	Проверочные процедуры	Пояснение
принципами безопасного программирования; • все необходимые корректировки вносятся до выпуска программного обеспечения; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска программного обеспечения. ***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.	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.
6.4 Соблюдать процессы и процедуры управления изменениями системных компонентов. Эти процессы должны в себя включать следующее:	**6.4** Проверить политики и процедуры на предмет наличия в них следующих требований: • 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	Без надлежащего документирования и выполнения процесса контроля за изменениями, механизмы защиты могут быть непреднамеренно или сознательно не использоваться или быть отключены, возможно появление ошибок обработки или внедрение вредоносного кода.

Требования PCI DSS	Проверочные процедуры	Пояснение
	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; • документировать процедуры контроля изменений, относящиеся к внедрению обновлений безопасности и изменений ПО.	
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. **6.4.1.b** Изучить настройки контроля доступа. Убедиться в том, что внедрены механизмы разграничения доступа к средам разработки/тестирования и производственного функционирования.	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.
6.4.2 Разделить обязанности 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 персонал, ответственный за производственное функционирование, 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 производственных функций. 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 производственной среде.
6.4.3 Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.	**6.4.3a** 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

Требования PCI DSS	Проверочные процедуры	Пояснение
	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.	злоумышленникам получить неавторизованный доступ к информации, используемой в производственной среде (например, к данным держателей карт).
6.4.4 Удалить все тестовые данные и платежные счета должны из системы перед переводом ее в эксплуатацию/ 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 удалять из кода приложения перед переводом его в производственный режим (в эксплуатацию), 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 Включить в процедуры контроля изменений следующее:	**6.4.5.a** Проверить процедуры контроля изменений 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, влияние изменений системы - обновления ПО или аппаратного обеспечения и установки обновления систем безопасности - может быть не достаточно изучено, что может привести к непредусмотренным последствиям.
	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 изменения задокументировано по каждому из выбранных изменений.	Последствия изменений должны документироваться, чтобы все вовлеченные стороны могли надлежащим образом запланировать все изменения в обработке данных.
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.

Требования PCI DSS	Проверочные процедуры	Пояснение
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. **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.	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 и того, что эти механизмы работают надлежащим образом после внедрения изменений в среду.
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.
6.4.6 По завершении значимого изменения, во всех новых или измененных системах и сетях, должны быть реализованы все соответствующие требования стандарта PCI DSS и по необходимости обновлена документация. ***Примечание:*** *Данное требование является лучшей практикой до 31 января 2018 г., после указанного срока оно приобретет статус требования.*	**6.4.6** Для выборки значимых изменений, изучить записи об изменениях, опросить сотрудников и понаблюдать за измененными системами/сетями, чтобы убедиться, что все применимые требования стандарта PCI DSS были реализованы и документация обновлена как часть изменений.	Наличие процедур для анализа значимых изменений помогает гарантировать применение всех соответствующих стандарту PCI DSS мер защиты для любых систем или сетей, добавленных или измененных в рамках области проверяемой среды. Встраивание данной проверки в процедуры управления изменениями способствует поддержанию в актуальном состоянии перечня устройств и стандартов конфигураций, а также применения защитных мер там, где это требуется. Процедура управления изменениями должна включать свидетельства, подтверждающие реализацию **требований** PCI DSS **или их** итеративное выполнение. Примеры требований стандарта PCI DSS, на которые могут повлиять изменения, включают, но не ограничиваются: • сетевая схема обновлена и отражает изменения; • системы настроены согласно стандартам конфигурации , с изменением всех паролей по умолчанию и отключением ненужных сервисов;

Требования PCI DSS	Проверочные процедуры	Пояснение
		• Системы защищены необходимыми механизмами (например, мониторинг целостности файлов (FIM), антивирус, обновления безопасности, ведение журналов аудита); • Подтверждение того, что критичные аутентификационные данные (SAD) не хранятся и, что все хранилища данных держателей карт задокументированы и включены в политики и процедуры хранения данных; • новые системы включены в ежеквартальное сканирование на наличие уязвимостей.
6.5 Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом: • как минимум ежегодно обучать разработчиков актуальным методикам безопасного программирования, включая информацию о том, как избежать распространенных программных уязвимостей; • разрабатывать приложения в соответствии с основными принципами безопасного программирования. ***Примечание:*** *Уязвимости, перечисленные в требованиях 6.5.1 - 6.5.10 соответствовали отраслевым рекомендациям на момент публикации данной версии стандарта*	**6.5.a** Изучить политики и процедуры разработки ПО и убедиться, что разработчики обязаны как минимум ежегодно проходить обучение актуальным методикам безопасного программирования в соответствии с известными отраслевыми рекомендациями и руководствами.	Уровень приложений 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 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.
	6.5.b Изучить документацию об обучении и убедиться, что разработчики прошли ежегодное обучение актуальным методикам безопасного программирования, в том числе тому, как избежать распространенных программных уязвимостей и как определить способ хранения критичных данных в памяти.	

Требования PCI DSS	Проверочные процедуры	Пояснение
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.c** Убедиться, что при разработке приложений уделяется внимание защите, по меньшей мере, от следующих уязвимостей:	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.
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: • проверяется, что введенная пользователями информация не может изменить существующие команды и запросы; • используются параметризованные запросы.	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 информации 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:	Переполнение буфера происходит, когда приложение не имеет соответствующих ограничений при проверке буферного пространства. Это может привести к тому, что информация, содержащаяся в буфере,

Требования PCI DSS	Проверочные процедуры	Пояснение
	• проверяются границы буфера; • усекаются строки ввода.	вытесняется за пределы пространства буферной памяти в пространство исполняемой памяти. Когда это происходит, злоумышленник получает возможность внедрить в конец буфера 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.
6.5.3 Небезопасное криптографическое хранилище.	**6.5.3** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при программировании учитывается небезопасность криптографического хранилища следующим образом: • защита от криптографических уязвимостей; • используют стойкие криптографические алгоритмы и ключи.	Приложения, которые не используют для хранения данных стойкие криптографические функции надлежащим образом, подвергаются повышенному риску взлома и утечки данных держателей карт и (или) аутентификационных данных. Если злоумышленник сможет использовать уязвимости криптографических процессов, 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 стойкой криптографии, 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.
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

Требования PCI DSS	Проверочные процедуры	Пояснение
		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.
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 кражи сеансов пользователя, изменения вида веб-сайтов, возможного внедрения червей и т.д.
6.5.8 Ошибки в контроле доступа (например, небезопасные прямые	**6.5.8** Изучить политики и процедуры разработки ПО и опросить ответственных сотрудников, чтобы убедиться, что при	Проблемы, связанные с контролем доступа, возникают, когда разработчик предоставляет ссылку

Требования PCI DSS	Проверочные процедуры	Пояснение
ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий и отсутствие ограничения прав доступа пользователя к функциям).	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.	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.
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 аутентифицированный запрос в уязвимое веб-приложение, что позволяет злоумышленнику совершить любые действия, которые может совершить жертва (например, обновление сведений о счете,

Требования PCI DSS	Проверочные процедуры	Пояснение
		совершение покупок или даже вход в приложение).
6.5.10 Противодействие взлому механизмов аутентификации и управления сеансами	**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.
6.6 Постоянно управлять новыми угрозами и уязвимостями общедоступных веб- приложений и обеспечить этим приложениям защиту от известных атак одним из следующих методов: • проверять общедоступные веб-приложения на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности не реже одного раза в год, а также после внесения любых изменений. ***Примечание:*** *Данная оценка отличается от сканирования на наличие уязвимостей в требовании 11.2.* • Перед общедоступными веб-приложениями должно быть установлено техническое средство для постоянной проверки всего трафика (например, межсетевой экран уровня приложений) 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 настройки системной конфигурации и опросить ответственных сотрудников, чтобы убедиться, что перед общедоступным веб-приложением установлено автоматизированное техническое средство (например, межсетевой экран уровня приложений) для обнаружения и предупреждения веб-атак, отвечающее следующим требованиям: - расположение перед общедоступными веб- приложениями 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 межсетевого экрана прикладного уровня 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*

Требования PCI DSS	Проверочные процедуры	Пояснение
		группы разработчиков
6.7 Гарантировать, 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; • 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	Проверочные процедуры	Пояснение
7.1 Ограничить доступ к системным компонентам и ДДК только теми лицами, которым такой доступ требуется 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.
7.1.1 Определить права 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.

Требования PCI DSS	Проверочные процедуры	Пояснение
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 для выполнения должностных обязанностей.	При назначении учетных записей с широкими полномочиями важно предоставлять лицам только те права, 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.
	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 для выполнения 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.
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 роли (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 роли.
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 Установить систему (-ы) контроля доступа к системным компонентам, которая ограничивает доступ в соответствии со служебной необходимостью пользователя и которая настроена запрещать все, что	**7.2** Изучить настройки системы и документацию изготовителя, убедиться, что система (-ы) 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

Требования PCI DSS	Проверочные процедуры	Пояснение
явным образом не разрешено. Система (-ы) контроля доступа должна включать следующее:		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. Организация может иметь одну или более системы контроля доступа для управления доступом пользователей. ***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 (-ы) контроля доступа внедрена на всех системных компонентах	
7.2.2 Назначение полномочий пользователям должно быть основано на их должностных обязанностях.	**7.2.2** Подтвердить, что назначение привилегий пользователям основано на их должностных обязанностях.	
7.2.3 По умолчанию должен быть запрещен любой доступ.	**7.2.3** Подтвердить, что по умолчанию запрещен любой доступ.	
7.3 Гарантировать, 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; • 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 процессами, 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 ко всем учетным записям, которые используются 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). Данные требования не распространяются на учетные записи, используемые клиентами (например, держатели карт).*

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	Проверочные процедуры	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.a Убедиться в том, что процедуры управления идентификацией пользователей реализованы, выполнив следующее:	
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 утверждающем документе.	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	Проверочные процедуры	Пояснение
8.1.3 Немедленно отзывать доступ у каждого уволенного 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. **8.1.3.b** Убедиться, что все физические средства аутентификации (например, смарт-карты, токены и т.д.) были возвращены или деактивированы.	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.
8.1.4 Удалять/блокировать неактивные учетные записи 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 третьими лицами 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 третьими лицами 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. **8.1.5.b** Опросить сотрудников и изучить процессы, чтобы убедиться, что во время выполнения работ учетные записи, используемые поставщиками дистанционно, контролируются.	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.
8.1.6 Блокировать учетные записи после шести неудачных попыток входа	**8.1.6.a** Сделать выборку системных компонентов, проверить настройки системной конфигурации и убедиться в том, что учетная запись	Без реализованного механизма блокировки учетных записей злоумышленник может непрерывно пытаться

Требования PCI DSS	Проверочные процедуры	Пояснение
подряд.	пользователя блокируется после не более чем шести неудачных попыток входа. **8.1.6.b** ***Дополнительная проверочная процедура 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.	подобрать пароль или вручную, или с использованием автоматизированных средств (программ взлома паролей) до достижения успеха и получения доступа к пользовательской учетной записи. ***Примечание:*** *Тестовая процедура 8.1.6 является дополнительной и применима только к поставщикам услуг*
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.
8.2 Помимо назначения уникального идентификатора, для обеспечения надлежащего управления	**8.2** Проверить, что для аутентификации пользователей применяются уникальный идентификатор и дополнительные механизмы аутентификации (например, пароль или парольная фраза) для доступа	Данные методы аутентификации при использовании совместно с уникальными идентификаторами помогают защитить идентификаторы пользователей

Требования PCI DSS	Проверочные процедуры	Пояснение
аутентификацией сотрудников (не пользователей) и администраторов на уровне всех системных компонентов применять 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).	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.	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 уникален для каждого конкретного пользователя. 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.
8.2.1 Все учетные данные для проверки подлинности (например, пароли/парольные фразы) хранить и передавать 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. ***Примечание:*** *Тестовые процедуры 8.2.1.d и 8.2.1.e являются дополнительными и применимы только к поставщикам услуг.*
	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.	
	8.2.1d ***Дополнительная проверочная процедура для поставщиков услуг:*** изучить файлы паролей и убедиться в том, что клиентские пароли нечитаемы при хранении.	
	8.2.1e ***Дополнительная проверочная процедура для поставщиков услуг:*** изучить процессы передачи данных и убедиться в том, что клиентские пароли нечитаемы при передаче.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.2 Перед изменением учетных данных для проверки подлинности (например, сбросом пароля, предоставлением новых токенов или генерацией новых ключей) 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 и проверки подлинности пользователя перед сбросом или изменением учетных данных.
8.2.3 Обеспечить соответствие паролей/парольных фраз 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. **8.2.3.b** ***Дополнительная проверочная процедура 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.	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 альтернативные решения, но руководствуясь принципом "эквивалентной надежности". Информацию относительно вариантности и равнозначности надежности паролей (так же называемой «энтропией») для паролей/парольных фраз различного формата см. в промышленных стандартах (например, актуальной версии NIST SP 800-63-1). ***Примечание:*** *Тестовая процедура 8.2.3.b является дополнительной и применима только к поставщикам услуг.*

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.4 Изменять пароли/парольные фразы 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. ***Примечание:*** *Тестовая процедура 8.2.4.b является дополнительной и применима только к поставщикам услуг*
	8.2.4.b ***Дополнительная проверочная процедура для поставщиков услуг:*** *изучить внутренние* процессы и клиентскую/пользовательскую документацию и убедиться в том, что: • требуется периодическое изменение паролей сотрудников (не клиентов); • сотрудники (не клиенты) получают инструкции о том, когда и при каких обстоятельствах пароль должен быть изменен.	
8.2.5 Запретить пользователю смену 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. ***Примечание:*** *Тестовая процедура 8.2.5.b является дополнительной и применима только к поставщикам услуг*
	8.2.5.b ***Дополнительная проверочная процедура 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 Устанавливать уникальный первоначальный пароль/парольную фразу для каждого пользователя и их немедленная смена 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 Обезопасить любой индивидуальный неконсольный административный доступ и любой удаленный доступ в среду ДДК используя многофакторную аутентификацию. ***Примечание:*** *Многофакторная*		Многофакторная аутентификация требует, как минимум, двух отдельных форм аутентификации (как описано в Требовании 8.2) до получения доступа. Многофакторная аутентификация дает дополнительную гарантию, что пользователь, пытающийся получить доступ тот, за кого себя выдает. При многофакторной аутентификации злоумышленнику придется взломать, как минимум, два аутентификационных механизма, что повышает

Требования PCI DSS	Проверочные процедуры	Пояснение
аутентификация требует, чтобы для аутентификации использовались как минимум два из трех методов аутентификации (описание методов аутентификации см. в Требовании 8.2). Использование одного метода дважды (например, использование двух различных паролей) не считается многофакторной аутентификацией.		сложность взлома и, как следствие, снижает риски. Многофакторная аутентификация не требуется и на системном уровне и на уровне приложений. Многофакторная аутентификация может быть выполнена или при аутентификации в конкретную сеть, или же на системному компоненте. Примеры технологий многофакторной аутентификации включают, но не ограничиваются: удаленная аутентификация и сервис внешнего подключения (RADIUS) с токенами; Система управления доступом для контроллера доступа к терминалу (TACACS) с токенами; и прочие технологии, которые обеспечивают многофакторную аутентификацию.
8.3.1 Реализовать многофакторную аутентификацию для всех средств неконсольного доступа сотрудников с правами администратора в среду ДДК. ***Примечание:*** *Данное требование имеет рекомендательный характер до 31 января 2018 г., далее оно приобретет статус требования.*	**8.3.1.a** Изучить системные конфигурации серверов и/или систем удаленного доступа и убедиться, что многофакторная аутентификация требуется для любого административного неконсольного доступа к среде ДДК. **8.3.1.b** Пронаблюдать за получением администраторами доступа к среде ДДК и убедиться, что используются как минимум два из трех методов аутентификации.	Данное требование применяется ко всем сотрудникам с административным доступом к информационной среде держателей карт. Требование применимо только к сотрудникам с административным доступом и только для удаленного доступа к среде держателей карт; оно неприменимо к учетным записям приложений или системным учетным записям, осуществляющим автоматизированные функции. Если организация не использует сегментацию для отделения среды держателей карт от остальной сети, администратор может использовать многофакторную аутентификацию либо для входа в информационную среду держателей карт, либо для входа в систему. Если внутренняя сеть отделена от остальной (внешней) сети организации, администратору потребуется использовать многофакторную аутентификацию для доступа в среду держателей карт из внешней сети. Многофакторная аутентификация может быть внедрена на уровне сети или на уровне системы/приложения; не обязательно на обоих. Если администратор использует многофакторную аутентификацию для доступа в среду держателей карт, то ему необязательно использовать многофакторную аутентификацию для доступа в определенную систему или приложение внутри самой среды держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.3.2 Внедрить многофакторную аутентификацию для всех средств удаленного сетевого доступа (пользователей и администраторов, включая доступ любых третьих лиц для поддержки или техобслуживания), исходящего извне сети организации	**8.3.2.a** Изучить системные конфигурации серверов и систем удаленного доступа и убедиться, что многофакторная 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). **8.3.2.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.	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 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, многофакторная аутентификация для удаленного доступа к такой сети не является обязательной. Однако многофакторная аутентификация требуется для удаленного доступа к сети из которой можно получить доступ к среде ДДК и рекомендована для всего удаленного доступа в сеть 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. **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.	Информирование всех пользователей о политиках и 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). Информирование пользователей о необходимости сменить пароли, если есть вероятность, что пароль

Требования PCI DSS	Проверочные процедуры	Пояснение
		больше не является надежным, может предотвратить использование злоумышленниками реального пароля для получения несанкционированного доступа.
8.5 Не использовать групповые, общие и стандартные учетные записи и пароли, а также прочие методы аутентификации и убедиться в том, что: • • стандартные учетные записи заблокированы или удалены; • 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.	**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; • общие и стандартные учетные записи не используются для администрирования каких-либо системных компонентов.	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 устанавливать ответственность за действия конкретного пользователя, или фактически регистрировать события, связанные с этими действиями, поскольку эти действия могут быть совершены любым членом группы, которой 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.	
8.6 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	**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.	

Требования PCI DSS	Проверочные процедуры	Пояснение
использовать такие механизмы для получения доступа.	**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 Ограничить доступ к любой базе данных, содержащей ДДК (включая доступ со стороны приложений, администраторов и любых других пользователей) следующим образом: • доступ, запросы и операции с базами данных должны осуществляться только программными методами; • разрешение запросов и прямого 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).	**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 пользователями (за исключением администраторов баз данных, которым может потребоваться прямой доступ к базе данных для выполнения своих административных обязанностей).
	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 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).	
8.8 Гарантировать, 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; • 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 доступ к устройствам и данным, а также украсть системы или печатные материалы. Такой доступ 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	Проверочные процедуры	Пояснение
9.1 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 над 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 записи.
9.1.1 Использовать камеры видеонаблюдения или иные механизмы контроля доступа (или и то и другое), чтобы следить за критичными 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,*	**9.1.1.a** Убедиться в том, что камеры видеонаблюдения или иные механизмы контроля доступа (или и то и другое) применяются для мониторинга доступа к критичным помещениям/выхода из критичных помещений. **9.1.1.b** Убедиться, что камеры или иные средства защищены (или и то и другое) от взлома или отключения. **9.1.1.c** Убедиться в том, что данные с камер видеонаблюдения или иных механизмов контроля доступа (или и того и другого) хранятся не менее трех месяцев.	Эти средства контроля помогают выявить лиц, которые имеют физический доступ к критичным помещениям, а также установить, когда они вошли и вышли. 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. Критичными являются такие помещения, как комнаты с серверами корпоративных баз данных, внутренние

Требования PCI DSS	Проверочные процедуры	Пояснение
хранящие, обрабатывающие или передающие данные держателей карт. Исключением являются места расположения кассовых терминалов с открытым доступом, такие как кассовые зоны торговых комплексов.		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 физических механизмов наблюдения.
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 Ограничить доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи.	**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	Проверочные процедуры	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).	Идентифицируя авторизованных посетителей так, чтобы их можно было легко отличать от работников объекта, можно исключить предоставление доступа посторонним посетителям к местам хранения ДДК.
	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.	
9.3 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 и т.д.) должны быть возвращены или отключены.	**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 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 сотрудник не смог получить физический доступ к среде данных держателей карт после увольнения.
	9.3.b Проследить за входом сотрудников в информационную среду держателей карт и убедиться, что все сотрудники проходят авторизацию перед получением доступа.	
	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.	
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

Требования PCI DSS	Проверочные процедуры	Пояснение
9.4.1 Выдавать разрешение посетителям до входа в помещения, где обрабатываются или хранятся ДДК, и постоянно сопровождать посетителей во время пребывания в этих помещениях. .	**9.4.1.a** Изучить процедуры и опросить сотрудников, чтобы убедиться, что посетители получают разрешение до получения доступа в помещения, где обрабатываются или хранятся ДДК, и посетителей постоянно сопровождают во время пребывания в этих помещениях .	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.b 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 Вести 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.	
	9.4.4.b Убедиться, что журнал содержит: • имя посетителя; • название фирмы, которую он представляет; • имя сотрудника организации, разрешившего доступ посетителю.	
	9.4.4.c Убедиться в том, что журнал хранится не менее трех месяцев.	
9.5 Обеспечить физическую безопасность	**9.5** Проверить, что процедуры физической защиты данных держателей	Механизмы обеспечения физической безопасности

Требования PCI DSS	Проверочные процедуры	Пояснение
всех видов носителей.	карт включают меры по защите всех видов носителей (включая, в том числе: компьютеры, съемные электронные носители, бумажные чеки, бумажные отчеты и факсы).	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 несанкционированного просмотра, копирования или сканирования.
9.5.1 Хранить носители с резервными копиями данных следует в безопасных местах (желательно вне объекта), таких как альтернативное или резервное место, или же воспользоваться услугами организаций, обеспечивающих безопасное хранение. Проверять безопасность мест хранения не реже одного раза в год.	**9.5.1** Проверить физическую безопасность места хранения носителей с резервными копиями данных и убедиться, что оно безопасно и безопасность мест хранения резервных копий проверяется не реже одного раза в год.	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. Периодическая проверка хранилища позволяет организации вовремя устранять обнаруженные проблемы с безопасностью, сводя к минимуму потенциальный риск.
9.6 Обеспечить 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.*

Требования PCI DSS	Проверочные процедуры	Пояснение
9.6.2 Пересылать носители 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. **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.	Если носитель отправляется способом, не предусматривающим отслеживание (например, обычной почтой), то он может быть утерян или украден. Использование услуг курьерской службы для доставки всех носителей, которые содержат данные держателей карт, позволяет организации использовать систему отслеживания, чтобы вести учет местонахождения посылок.
9.6.3 Гарантировать, 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.
9.7 Обеспечить 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 Поддерживать 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 Уничтожать носители, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, следующим способом:	**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	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

Требования PCI DSS	Проверочные процедуры	Пояснение
	должно осуществляться с помощью программы безопасного удаления данных (в соответствии с отраслевыми стандартами безопасного удаления) или путем физического уничтожения носителя.	используют найденную информацию для проведения атак. Защита контейнеров для материалов, приготовленных для уничтожения, позволяет предотвратить получение критичной информации при сборе материалов. Например, контейнеры с материалами, подлежащие 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 Измельчать, сжигать или преобразовывать бумажные носители 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 Уничтожать данные 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.	
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).*	**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 каждый раз, когда вставляется карта. 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

Требования PCI DSS	Проверочные процедуры	Пояснение
		(например, компьютерных клавиатур и клавиатур кассовых терминалов). Дополнительные рекомендации по предотвращению скимминга можно найти на сайте PCI SSC.
9.9.1 Составлять и регулярно обновлять списки 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 идентификатор.	**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. **9.9.1.c** Опросить сотрудников и убедиться, что список обновляется при каждом добавлении, перемещении, списании устройств и т.д.	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, 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.	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,

Требования PCI DSS	Проверочные процедуры	Пояснение
		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 ТСП согласно процессу ежегодной оценки рисков.
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	**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).	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.

Требования PCI DSS	Проверочные процедуры	Пояснение
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).	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 Гарантировать, 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 компрометации 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	Проверочные процедуры	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 включить 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 скомпрометированны или неправильно использованы.
10.2.2 Все действия, совершенные с использованием привелегий суперпользователя или	**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

Требования PCI DSS	Проверочные процедуры	Пояснение
администратора;		не регистрировать события, организация не сможет отслеживать проблемы, связанные с ошибками администрирования или ненадлежащим использованием прав доступа.
10.2.3 Доступ ко всем 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	Проверочные процедуры	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 журналов протоколирования событий 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 легитимности таких изменений.
10.3 Записывать в журналах регистрации событий для каждого события каждого системного компонента, 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	Проверочные процедуры	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 Синхронизировать все системные часы и системное время на критичных системах и обеспечить выполнение следующих требований 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, точность и согласование времени на всех системах и время совершения каждого действия является критичным для установления способов компрометации системам.
10.4.1 На критичных системах установить 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.	
	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	

Требования PCI DSS	Проверочные процедуры	Пояснение
	(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 Защитить данные о времени.	**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 Получать настройки времени 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).	
10.5 Защитить журналы протоколирования событий 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 Ограничить доступ к просмотру	**10.5.1** Доступом к журналам протоколирования событий должны	Надежная защита журналов регистрации событий

Требования PCI DSS	Проверочные процедуры	Пояснение
журналов регистрации событий только теми работниками, которым такой доступ необходим в соответствии с их должностными обязанностями .	обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	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 Защитить журналы протоколирования событий 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 Оперативно сохранять резервные копии журналов протоколирования событий на централизованном сервере протоколирования или отдельном носителе, 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 Сохранять копии журналов протоколирования событий для технологий, к которым возможен доступ извне, на безопасный и централизованный внутренний сервер протоколирования или носитель.	**10.5.4** Журналы протоколирования событий доступных извне систем (беспроводных устройств, межсетевых экранов, 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.
10.5.5 Применять ПО для мониторинга контроля целостности файлов или обнаружения изменений в журналах регистрации событий, чтобы данные существующих журналов нельзя было изменить без создания уведомлений (однако добавление новых данных не должно вызывать тревожного сигнала).	**10.5.5** Изучить системные настройки, отслеживаемые файлы и результаты мониторинга и убедиться в использовании ПО для мониторинга контроля целостности файлов или обнаружения изменений в журналах регистрации событий.	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 Проверять журналы	**10.6** Выполнить следующее:	Большое количество компрометаций существует в

Требования PCI DSS	Проверочные процедуры	Пояснение
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.*		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.
10.6.1 Проверять 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, межсетевых экранов, систем обнаружения и предотвращения вторжений,серверов аутентификации, серверов	**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, межсетевых экранов, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.) **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;	Большое количество компрометаций происходит за несколько 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, межсетевых экранов, 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.

Требования PCI DSS	Проверочные процедуры	Пояснение
перенаправления электронной торговли и т.д.).	• журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, межсетевых экранов, 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 оценки рисков.	**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.	Следует периодически проверять журналы всех остальных системных компонентов для обнаружения признаков потенциальных проблем или попыток получить доступ к критичным системам через другие, менее критичные системы. Частота проведения проверки определяется организацией в рамках ежегодной оценки рисков.
	10.6.2.b Изучить документацию по оценке рисков и опросить сотрудников, чтобы убедиться, что проверка выполняется в соответствии с политиками и стратегией управления рисками, принятыми в организации.	
10.6.3 Изучать 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 Хранить журналы регистрации событий не менее одного года, и 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

Требования PCI DSS	Проверочные процедуры	Пояснение
		восстановления данных журнала, выполнения анализа и выявления систем или данных, подвергшихся влиянию нарушения.
10.8 ***Дополнительное требование только для поставщиков услуг***: Внедрить процедуру для своевременного выявления и регистрации всех отказов механизмов обеспечения безопасности, включая, но не ограничиваясь: • межсетевые экраны • системы обнаружения и предотвращения вторжений (IDS/IPS) • мониторинг целостности файлов (FIM) • антивирус • физический контроль доступа • логический контроль доступа • механизмы ведения журнала аудита • контроль сегментации (если применяется) ***Примечание:*** *Данное требование является лучшей практикой в срок до 31 января 2018 г., после указанного срока оно приобретет статус требования.*	**10.8.a** Изучить документированные политики и процедуры, чтобы убедиться в наличии определенных процедур своевременного выявления и регистрации всех отказов механизмов обеспечения безопасности, включая, но не ограничиваясь, отказы: • межсетевые экраны • системы обнаружения и предотвращения вторжений (IDS/IPS) • мониторинг целостности файлов (FIM) • антивирус • физический контроль доступа • логический контроль доступа • механизмы ведения журнала аудита • контроль сегментации (если применяется) **10.8.b** Изучить процедуры выявления и оповещения и опросить персонал, чтобы убедиться, что процедуры внедрены для всех механизмов обеспечения безопасности и, что отказ какого-либо механизма обеспечения безопасности приводит к генерации оповещений.	***Примечание:*** *Данное требование применимо только к поставщикам услуг.* Без формальных процедур выявления и оповещения при отказе механизма обеспечения безопасности, отказы могут оставаться не выявленными продолжительный период, тем самым, давая злоумышленникам достаточно времени для взлома системы и кражи критичных данных из среды данных держателей карт. Определенные типы отказов могут варьироваться в зависимости от функции устройства и используемой технологии. Типичные отказы включают остановку работы системы, реализующей функций безопасности, или ее некорректное функционирование: например, удаление межсетевым экраном всех его правил или его отключение.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.8.1 Дополнительное требование только для поставщиков услуг: Своевременно реагировать на любые отказы критичных механизмов обеспечения безопасности. Процедуры реагирования на отказы систем безопасности должны включать: • восстановление функций систем безопасности • идентификация и документирование длительности (даты и времени от начала до конца) отказа систем безопасности • идентификация и документирование причины (причин) отказа, включая основную причину, и документирование исправлений, требуемых для устранения	**10.8.1.a** Изучить документированные политики и процедуры и опросить персонал, чтобы убедиться, что процедуры для реагирования на отказы механизмов обеспечения безопасности определены и внедрены, и включают: • восстановление функций систем безопасности • идентификация и документирование длительности (даты и времени от начала до конца) отказа систем безопасности • идентификация и документирование причины (причин) отказа, включая основную причину, и документирование исправлений, требуемых для устранения основной причины • выявление и устранение любых проблем по безопасности, возникающих в процессе отказа • выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты • внедрение процедур регулирования для предотвращения повторного возникновения причины отказа • возобновление мониторинга механизмов обеспечения безопасности	***Примечание:*** *Данное требование применимо только к поставщикам услуг* Если на оповещение (сигнал) об отказе критичных механизмов обеспечения безопасности не следует быстрого и эффективного реагирования, злоумышленники могут использовать это время для внедрения вредоносного программного обеспечения, получить контроль над системой или украсть данные из среды организации. Документированные доказательства (к примеру, записи в рамках системы управления проблемами) должны подтвердить, что процессы и процедуры реагирования на отказ системы безопасности находятся в рабочем состоянии . В дополнение сотрудники должны знать свои зоны ответственности в случае отказа. Действия и реагирование на отказы должны быть отслежены и задокументированы.

Требования PCI DSS	Проверочные процедуры	Пояснение
основной причины • выявление и устранение любых проблем безопасности, возникающих в процессе отказа • выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты • внедрение процедур регулирования для предотвращения повторного возникновения причины отказа • возобновление мониторинга механизмов обеспечения безопасности ***Примечание:*** *Данное требование является лучшей практикой в срок до 31 января 2018 г., после указанного срока оно приобретет статус требования.*	**10.8.1.b** Изучить документацию, чтобы убедиться, что отказы механизмов обеспечения безопасности задокументированы и включают: • Идентификацию причины (причин) отказа, включая основную причину • Длительность (дату и время начала и конца) отказа механизма обеспечения безопасности • Детали исправлений, требуемых для устранения основной причины	
10.9 Гарантировать, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**10.9** 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; • 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 злоумышленниками и исследователями, а также появляются вместе с новым программным обеспечением. Системные компоненты, процессы и написанное на заказ программное обеспечение следует периодически тестировать, чтобы убедиться, что их защищенность поддерживается на должном уровне при меняющейся среде.

Требования PCI DSS	Проверочные процедуры	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.	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. Зная, какие беспроводные устройства авторизованны, администраторы могут быстро обнаружить неавторизованные беспроводные устройства и отреагировать на это, что позволит снизить уязвимость среды держателей карт к действиями злоумышленников. 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 обуславливает необходимость использования соответствующих инструментов и процессов для предотвращения установки в среде 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; • сканирование всех системных компонентов и объектов проводится, по крайней мере, ежеквартально.	
	11.1.d Если внедрен автоматизированный мониторинг (например, системы обнаружения вторжений (IDS) предотвращения вторжений (IPS) по беспроводным сетям, контроль сетевого доступа и т.п.), убедиться, что он генерирует уведомления персоналу организации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
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.	
11.2 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*	**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 с использованием автоматизированных средств. Эти средства проверяют внутренние и внешние сетевые устройства и серверы и предназначены для того, чтобы выявлять потенциальные уязвимости, 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);

Требования PCI DSS	Проверочные процедуры	Пояснение
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.		• внутреннее и внешнее сканирование после значительного 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.
11.2.1 Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей. Устранять уязвимости и проводить повторные сканирования, пока не будут устранены все уязвимости, представляющие высокий риск согласно рейтингу уязвимостей компании (согласно Требованию 6.1). Сканирование должны выполнять	**11.2.1.a** Изучить результаты внутренних сканирований на наличие уязвимостей и убедиться, что четыре последних сканирования производились ежеквартально в течение последних 12 месяцев. **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.	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

Требования PCI DSS	Проверочные процедуры	Пояснение
квалифицированные специалисты.	**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).	(например, администратор межсетевого экрана не должен быть ответственным за сканирование межсетевого экрана), либо организация может воспользоваться услугами другой организации, которая занимается сканированием на наличие уязвимостей.
11.2.2 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. ***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.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). Надежная программа сканирования обеспечивает выполнение своевременного сканирования и устранение уязвимостей.
	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).	
	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).	

Требования PCI DSS	Проверочные процедуры	Пояснение
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 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	**11.3** Изучить методологию проведения тестов на 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	Тест на проникновение выполняется для 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.

Требования PCI DSS	Проверочные процедуры	Пояснение
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.	мер, предпринятых для устранения уязвимостей.	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 оценки рисков организации*
11.3.1 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. **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).	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, что существующие механизмы продолжают быть эффективны после обновления или

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3.2 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.	модификации.
	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 Устранять эксплуатируемые уязвимости, обнаруженные во время теста на проникновение, и проводить повторное тестирование для проверки их устранения.	**11.3.3** Изучить результаты теста на проникновение и 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, проводить тестирование на проникновение 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.	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
	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.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	11.3.4.c Убедиться в том, что тест 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).	сетями.
11.3.4.1 ***Дополнительное требование только для поставщиков услуг***: В случае применения сегментации, подтвердить область применения стандарта PCI DSS выполнением тест на проникновение в отношении механизмов сегментации не реже одного раза в полгода и при любых изменениях механизмов/методов сегментации. ***Примечание:*** *Данное требование является лучшей практикой в срок до 31 января 2018 г., после указанного срока оно приобретет статус требования.*	**11.3.4.1.a** Изучить результаты позднего теста на проникновение и убедиться, что: • тесты на проникновение осуществляются для проверки механизмов сегментации, как минимум, каждые полгода и при любых изменениях механизмов/методов сегментации • тесты на проникновение охватывают все используемые механизмы/методы сегментации • тесты на проникновение подтверждают, что все механизмы/методы сегментации являются рабочими и эффективными, и изолируют все внешние системы от систем среды данных держателей карт. **11.3.4.1.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).	***Примечание:*** *Данное требование применимо только к поставщикам услуг* Для поставщиков услуг подтверждение области применения стандарта PCI DSS должно выполняться настолько часто, насколько это возможно для того, чтобы убедиться, что область применения стандарта PCI DSS остается актуальной и совпадает с изменяющимися бизнес-целями.
11.4 Использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Осуществлять мониторинг сетевого трафика по периметру среды данных держателей карт и в критичных	**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.	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

Требования PCI DSS	Проверочные процедуры	Пояснение
точках внутри среды данных держателей карт, и оповещать сотрудников о подозрительных действиях. Поддерживать системы обнаружения и предотвращения вторжений и их сигнатуры в актуальном состоянии.	**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.	другое вредоносное программное обеспечение и т.д.), отправляют предупреждения и (или) блокируют попытку проведения атаки. Не используя превентивные меры для обнаружения несанкционированной деятельности, можно не заметить атаки на компьютерные ресурсы (или их ненадлежащее использование) в момент выполнения. Необходимо вести мониторинг предупреждений, генерируемых данными средствами, для своевременного блокирования предпринятых вторжений.
	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.	
11.5 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 использовании механизма защиты от изменений 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, программ 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.	

Требования PCI DSS	Проверочные процедуры	Пояснение
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.	
11.6 Гарантировать, 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; • 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 характер 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	Проверочные процедуры	Пояснение
12.1 Разработать, опубликовать, поддерживать и распространять политику информационной 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 Пересматривать политику безопасности по меньшей мере, ежегодно и обновлять 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 изменения среды (например, покупки, слияния, перемещения и т.д.); • выявляет критические активы, угрозы и уязвимости; • завершается официальной оценкой рисков. *Примеры методик оценки рисков включают в том числе: OCTAVE, ISO 27005 и NIST SP 800-30.*	**12.2.a** Убедиться, что ежегодный документированный процесс оценки рисков документирует: • выявляет критические активы, угрозы и уязвимости; • завершается официальной оценкой рисков.	Оценка рисков позволяет выявить угрозы и связанные с ними уязвимости, которые могут негативно отразиться на ведении дел. Примерами различных видов риска, которые следует брать во внимание, являются кибрпреступления, веб-атаки, вредоносное ПО для POS-терминалов. Ресурсы можно эффективно распределить для 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	**12.3** Изучить правила эксплуатации критичных технологий и опросить	Политики использования могут либо запрещать

Требования PCI DSS	Проверочные процедуры	Пояснение
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.* Гарантировать, что правила эксплуатации критичных технологий предусматривают:	ответственных сотрудников, чтобы убедиться, что следующие политики внедрены и выполняются:	использование определенных устройств, либо содержать инструкции для сотрудников по их 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 Явное одобрение 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.
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 критичных устройств; • список 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.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3.4 Способ точно и быстро устанавливать владельца, контактных данных и назначения устройства (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 способы использования технологий.	**12.3.5** Убедиться, что правила эксплуатации регламентируют допустимые способы использования технологий.	Определяя допустимые сценарии использования и размещение устройств и технологий, утвержденных руководством, 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.
12.3.6 Допустимые точки размещения технологий в сети.	**12.3.6** Убедиться, что правила эксплуатации регламентируют допустимые точки размещения устройств в сети.	
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	**12.3.9** Убедиться, что правила эксплуатации регламентируют включение	

Требования PCI DSS	Проверочные процедуры	Пояснение
удаленного доступа для производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	механизмов для доступа производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	
12.3.10 Запрет копирования, перемещения и хранения ДДК на локальных жестких дисках и съемных электронных носителях работникам, имеющим доступ к ДДК через технологии удаленного доступа, если они явно не уполномочены для выполнения этих действий в рамках определенной служебной необходимости . 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.	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.
	12.3.10.b Для авторизованных сотрудников убедиться, что правила эксплуатации предписывают обеспечение защиты данных держателей карт в соответствии с требованиями стандарта PCI DSS.	
12.4 Гарантировать, что политика и процедуры обеспечения безопасности однозначно определяют обязанности по информационной безопасности для всего персонала организации,.	**12.4.a** Убедиться, что политики информационной безопасности явно определяют обязанности по обеспечению защиты для всех сотрудников.	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.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.4.1 ***Дополнительное требование только для поставщиков услуг***: Высшему руководству установить ответственность по защите данных держателей карт и программы соответствия стандарту PCI DSS, которая должна включать: • полную подотчетность за обеспечение соответствия стандарту PCI DSS; • определение устава программы соответствия стандарту PCI DSS и отчетности перед высшим руководством. ***Примечание:*** *Данное требование является лучшей практикой в срок до 31 января 2018 г., после указанного срока оно приобретет статус требования.*	**12.4.1.a** Изучить документацию, чтобы убедиться, что высшее руководство установило полную подотчетность за обеспечение соответствия организации стандарту PCI DSS.	***Примечание:*** *Данное требование применимо только к поставщикам услуг* Назначение высшим руководством ответственности за соответствие стандарту PCI DSS обеспечивает руководящему уровню прозрачность программы соответствия стандарту PCI DSS и дает возможность задавать соответствующие вопросы для определения эффективности программы и ее влияния на стратегические приоритеты. Полная ответственность за программу соответствия стандарту PCI DSS может быть возложена на определенных сотрудников и/или структурные подразделения внутри организации. Высшее руководство может вовлечь позиции С-уровня, совет директоров, или аналогичные должности. Специальные должности будут зависеть от конкретной организационной структуры. Уровень детализации отчетов, предоставляемой высшему руководству должен соответствовать конкретной организации и целевой аудитории.
	12.4.1.b Изучить устав компании в отношении стандарта PCI DSS, чтобы убедиться, что он излагает условия, на основании которых организована программа соответствия стандарту PCI DSS и ее подотчетность высшему руководству.	
12.5 Определенному сотруднику или группе сотрудников назначить 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 соответствующей политики. Без такой ответственности недочеты в процессах могут открыть доступ к критичным ресурсам или данным держателей карт. Организации также должны учитывать планы перехода и/или преемственности для ключевого персонала, чтобы избежать возможных пробелов при делегировании обязанностей за обеспечение защиты. Это может привести к тому, что обязанности не будут вовремя назначены и, следовательно, не будут выполняться.
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.	
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	**12.5.3** Убедиться, что ответственные за создание, документирование и	

Требования PCI DSS	Проверочные процедуры	Пояснение
распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.	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 Внедрить официальную программу 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 Проводить обучение персонала организации при приеме на работу, а также не реже одного раза в год. ***Примечание:*** *Методики обучения могут варьироваться в зависимости от обязанностей персонала и уровня доступа к ДДК.*	**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 информационной 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.	
	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 Требовать, чтобы персонал организации не реже одного раза в год подтверждал свое знание и понимание политик 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 Тщательно проверять кандидатов	**12.7** Убедиться в том, что при приеме на работу новых сотрудников,	Тщательное изучение биографии сотрудников, которые

Требования PCI DSS	Проверочные процедуры	Пояснение
(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.*	которым будет предоставляться доступ к данным держателей карт или информационной среде держателей карт, осуществляются кадровые проверки (с учетом особенностей местного законодательства).	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:	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. Некоторые примеры различных типов поставщиков услуг включают хранилища резервных копий на магнитной ленте, поставщики управляемых услуг, такие как компании веб-хостинга или поставщик услуг защиты, организации, которые получают данные с целью моделирования мошеннических операций и пр.
12.8.1 Составление и регулярное обновление перечня поставщиков услуг, с описанием поставляемых услуг.	**12.8.1** Убедиться в том, что перечень поставщиков услуг составлен и поддерживается в актуальном состоянии и содержит описание поставляемых услуг.	Перечень поставщиков услуг помогает оценить потенциальные риски, существующие за пределами организации.

Требования PCI DSS	Проверочные процедуры	Пояснение
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. Объем, за который поставщик несет ответственность в отношении безопасности данных держателей карт, зависит от конкретных услуг, которые он оказывает и договоренностей поставщика услуг с проверяемой организацией. 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 услуги.
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.	Данный процесс гарантирует, что возможность привлечения поставщика услуг тщательно изучается внутри организации и включает в себя 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.
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,
12.8.5 Хранить информацию о том, за	**12.8.5** Убедиться, что организация хранит информацию о том, за какие	

Требования PCI DSS	Проверочные процедуры	Пояснение
какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	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.
12.9 Дополнительное требование для поставщиков услуг: Поставщикам услуг давать 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: 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 проверочная процедура 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 PC1 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.	***Примечание:*** *Данное требование применимо к поставщикам услуг* 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 в рамках стандарта 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 Внедрить план реагирования на инциденты. Организация должна быть готова немедленно отреагировать на	**12.10** Ознакомиться с планом и процедурами реагирования на инциденты и убедиться, что организация готова немедленно	При отсутствии детального плана реагирования на инциденты безопасности, его распределения, чтения и понимания ответственными сторонами,

Требования PCI DSS	Проверочные процедуры	Пояснение
нарушение в работе системы.	отреагировать на взлом системы следующим образом:	замешательство и отсутствие унифицированного подхода к реагированию могут увеличить время вынужденного простоя для бизнеса, привести к появлению в средствах массовой информации нежелательной информации, а также к возникновению дополнительных юридических обязательств.
12.10.1 Разработать план реагирования на инциденты, применяемый в случае взлома системы. План должен, как минимум, 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	

Требования PCI DSS	Проверочные процедуры	Пояснение
	процедуры были выполнены.	
12.10.2 Анализировать и тестировать план не реже одного раза в год, включая все элементы, приведенные в Требовании 12.10.1.	**12.10.2** Опросить сотрудников и проверить документацию тестирования, чтобы убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год, включая все элементы, приведенные в Требовании 12.10.1.	Без надлежащего тестирования можно пропустить ключевые пункты, что может увеличить зону влияния инцидента.
12.10.3 Назначить соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7.	**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 подготовленной 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 помешать расследованию, проводимому после обнаружения инцидента.
12.10.4 Обеспечить надлежащее обучение сотрудников, ответственных за реагирование на нарушения безопасности.	**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, межсетевые экраны, 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 предназначены для того, чтобы отслеживать 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 Разработать 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.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.11 Дополнительное требование (только для поставщиков услуг): Выполнять проверки как минимум ежеквартально, чтобы убедиться в том, что сотрудники соблюдают политики безопасности и установленные регламенты. Проверкам должны подвергаться следующие процессы: • журнал ежедневного учета • параметры межсетевого экрана • применение стандартов конфигурации к новым системам • реагирование на оповещения системы безопасности • процессы управления изменениями ***Примечание:*** *данное требование является отраслевой рекомендацией до 31 января 2018 года, после чего его соблюдение станет обязательным.*	12.11.a Изучить политики и процедуры, чтобы убедиться в том, что сотрудники соблюдают политики безопасности и установленные регламенты, а следующие процессы подвергаются проверкам: • журнал ежедневного учета • параметры межсетевого экрана • применение стандартов конфигурации к новым системам • реагирование на оповещения системы безопасности • процессы управления изменениями 12.11.b Опросить ответственных сотрудников и изучить записи о проверках, чтобы убедиться в том, что проверки проводятся как минимум ежеквартально.	Регулярное подтверждение следования политикам и процедурам безопасности дает уверенность в том, необходимые меры безопасности применяются и работают как следует. Цель этих проверок не в повторном выполнении других требований PCI DSS, а в подтверждении того, что процедуры выполняются как ожидается.
12.11.1 Дополнительное требование (только для поставщиков услуг): Вести документацию о ежеквартальных проверках, включая: • Документирование результатов проверок • Изучение и утверждение результатов сотрудниками, ответственными за соблюдение требований PCI DSS. ***Примечание:*** *данное требование является отраслевой рекомендацией до 31 января 2018 года, после чего его соблюдение станет обязательным.*	12.11.1 Изучить документацию о ежеквартальных проверках, чтобы убедиться, что она включает: • Документирование результатов проверок • Изучение и утверждение результатов сотрудниками, ответственными за соблюдение требований PCI DSS.	***Примечание:*** *Это требование применяется то когда организация проверяется как поставщик услуг.* Цель этих независимых проверок состоит в подтверждении того, что деятельность по защите выполняется на регулярной основе. Эти проверки могут помочь подтвердить, что необходимые свидетельства их выполнения поддерживатся в актуальном состоянии (например, журналы событий, отчеты о сканировании на уязвимости, пересмотры правил межсетевых экранов, и т.д.) для помощи организации в подготовке к последующей оценке по PCI DSS.

Приложение A. Дополнительные требования PCI DSS

Приложение содержит дополнительные требования PCI DSS для разного типа организаций. Разделы приложения включают:

- Приложение A1: Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой
- Приложение A2: Дополнительные требования PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS
- Приложение A3: Дополнительные проверки для выделенных организаций

Пояснения и применимость приведены в каждом разделе.

Приложение A.1: Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой

Согласно требованиям 12.8 и 12.9 все поставщики услуг, имеющие доступ к данным держателей карт (включая поставщиков услуг хостинга с общей средой) должны выполнять требования PCI DSS. В дополнение к этому, требование 2.6 говорит о том, что поставщики услуг хостинга с общей средой 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 PCI DSS	Проверочные процедуры	Пояснение
A.1 Защитить данные каждого клиента (например, торговой точки или др.) согласно требованиям с A.1.1 по A.1.4: Поставщик услуг хостинга должен выполнять все эти и остальные чоответстсующие требования PCI DSS. ***Примечание:*** *Даже если поставщик услуг хостинга 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 поставщик услуг хостинга 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 хостинга с общей средой, которые желают предоставлять своим клиентам (торгово-сервисному предприятию или поставщику услуг) среду размещения данных, которая соответствует требованиям стандарта PCI DSS.
A.1.1 Ограничить доступ приложений каждого клиента только к своей среде данных держателей карт.	**A.1.1** Если поставщик услуг хостинга позволяет клиентам запускать приложения (например, скрипты), следует убедиться, что эти приложения выполняются под уникальной пользовательской учетной записью организации. Например: • ни одна организация в системе не может использовать совместно используемую учетную запись пользователя веб-сервера; • все CGI-скрипты, используемые клиентом, должны быть созданы и выполняться под уникальной пользовательской учетной записью организации.	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 привилегированного пользователя.
A.1.2 Ограничить доступ и	**A.1.2.a** Убедиться, что ни один из клиентов не обладает правами	Чтобы гарантировать, что доступ и полномочия

Требования PCI DSS	Проверочные процедуры	Пояснение
привилегии клиента только ее собственной средой данных держателей карт.	администратора/суперпользователя.	предоставляются так, что каждые ТСП или поставщик услуг имеют доступ только к собственной среде, необходимо принять во внимание, следующее: 1. полномочия пользовательской учетной записи ТСП или поставщика услуг; 2. разрешения на чтение, запись и исполнение файлов; 3. разрешения на запись в системные исполняемые файлы; 4. разрешения на доступ к файлам журналов ТСП или поставщика услуг; меры 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 пользователей организации нет доступа с правом записи к совместно используемым системным двоичным файлам.	
	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.	
A.1.3 Обеспечить включение протоколирования действий и событий для каждого клиента и соответствует требованию 10 стандарта PCI DSS.	**A.1.3** Убедиться, что поставщик услуг хостинга с общей средой обеспечивает ведение журналов регистрации событий для каждого ТСП и поставщика услуг следующим образом: • включено протоколирование для всех типичных используемых на сервере приложений сторонних производителей; • протоколирование включено по умолчанию; • журналы доступны для просмотра администратору и клиенту, для которого выполняется протоколирование; • месторасположения журналов доведены до сведения владеющей организации.	Журналы должны быть доступны в общей среде размещения данных так, чтобы ТСП и поставщики услуг имели доступ и могли просматривать журналы регистрации событий, относящиеся только к собственной информационной среде ДДК.
A.1.4 Реализовать процессы, позволяющие провести	**A.1.4** Убедиться в наличии у поставщика услуг хостинга политик, которые требуют своевременно проводить расследование с	Хостинг-провайдеры должны иметь процессы для быстрого реагирования в случае компрометации,

Требования PCI DSS	Проверочные процедуры	Пояснение
своевременное расследование с использованием компьютерной экспертизы в случае компрометации любых ТСП или поставщика услуг, размещенных на хостинге.	использованием компьютерной экспертизы соответствующих серверов в случае компрометации.	если требуется расследование инцидентов, вплоть до такого уровня детализации, чтобы можно было получить подробные сведения о конкретном ТСП или поставщике услуг.

Приложение A.2: Дополнительные требования PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS

Организации, использующие протокол SSL и раннюю версию TLS должны как можно скорее рассмотреть переход к надежному криптографическому протоколу. Кроме того, протокол SSL и ранняя версия TLS не должны внедряться в среды, где эти протоколы отсутствуют. На момент публикации стандарта, известные уязвимости сложно использовать в платежных средах POS POI. Тем не менее, в любой момент могут возникнуть новые уязвимости, и от организации зависит, защищена ли она от современных уязвимостей и может ли определить насколько она подвержена или не подвержена воздействию известных эксплойтов.

Непосредственно затронутые требования стандарта PCI DSS:

Требование 2.2.3 Необходимо обеспечить дополнительные механизмы защиты для всех необходимых служб, протоколов и управляющих программ, которые могут быть небезопасными.

Требование 2.3 При использовании неконсольного административного доступа к системе следует всегда шифровать канал с использованием стойких криптографических алгоритмов.

Требование 4.1 Для защиты данных держателей карт во время их передачи через общедоступные сети следует использовать надежные криптографические алгоритмы и шифрование

Для выполнения этих требований протокол SSL и ранняя версия TLS не должны быть использованы в качестве механизма обеспечения безопасности. Для помощи организациям, которые работают над переходом с протокола SSL и ранней версии TLS на более безопасные, включены следующие положения:

- Новые системы не должны использовать протоколы SSL и раннюю версию TLS в качестве механизмов обеспечения безопасности.
- Все поставщики услуг должны обеспечить безопасное предоставление услуг в срок до 30 июня 2016 года.
- После 30 июня 2018 года все организации должны отказаться от использования протокола SSL и ранней версии TLS в качестве механизмов обеспечения безопасности и использовать только защищенные версии протокола (допущения для определенных терминалов POS POI приведены в последнем пункте ниже).
- До 30 июня 2018 года для существующих систем, использующих протокол SSL и/или раннюю версию TLS, должен быть разработан и утвержден План снижения риска и миграции.
- Терминалы POS POI (и оконечные точки терминации SSL/TLS, к которым они подключены), которые могут быть верифицированы как устойчивые по отношению к любым известным эксплойтам для протокола SSL и ранней версии TLS, могут продолжать использовать эти протоколы, как механизмы обеспечения безопасности и после 30 июня 2018 года.

Данное Приложение применимо к организациям, использующим протокол SSL/раннюю версию TLS в качестве механизмов обеспечения безопасности для защиты среды ДДК и/или данных держателей карт (например, протоколы SSL и ранняя версия TLS, которые ранее отвечали требованиям 2.2.3, 2.3 или 4.1 стандарта PCI DSS). Дальнейшие руководства по использованию протокола SSL/ранней версии TLS см. в *PCI SSC Information Supplement Migrating from SSL and Early TLS.*

Требования PCI DSS	Проверочные процедуры	Пояснение

Требования PCI DSS	Проверочные процедуры	Пояснение
A2.1 В случае применения терминалов POS POI (и точек терминации SSL/TLS, к которым они подключены) использующих SSL и (или) раннюю версию TLS организация должна: • Подтвердить, что устройства не подвержены никаким известным атакам на SSL/ранние версии TLS. ***Или*** • Иметь официальный План снижения риска и миграции	**A2.1** Для терминалов POS POI (и точек терминации SSL/TLS, к которым они подключены), использующих протокол SSL и/или раннюю версию TLS: • Подтвердить, что организация имеет документацию (к примеру, документацию от поставщика, данные о конфигурации системы/сети и пр.), подтверждающую, что устройства не подвержены никаким известным атакам на протокол SSL и/или раннюю версию TLS *Или* • Выполнить пункт A2.2, приведенный ниже.	POI могут продолжать использовать протоколы SSL/раннюю версию TLS, если можно удостовериться, что POI устойчив по отношению к любым известным эксплойтам. Тем не менее, протокол SSL является устаревшей технологией и в будущем может быть подвержен дополнительным уязвимостям; потому настоятельно рекомендуется перевести среду POI на надежный протокол в кратчайшие сроки. Если протокол SSL/ранняя версия TLS не требуются для среды, то использование и откат до этих версий необходимо прекратить. Если среда POS POI уязвима к любым известным эксплойтам, то необходимо срочно начинать планирование перехода на более безопасные технологии. ***Примечание:*** *Допущения для POS POI, которые, на текущий момент, устойчивы к известным эксплойтам основывается на действующих, известных рисках. При появлении новых эксплойтов, к которым среды POI уязвимы, среды POI придется обновить.*
A2.2 Для организаций с установленными у них решениями (иные, чем указаны в пункте A2.1), которые используют протокол SSL и/или раннюю версию TLS документировать План снижения риска и миграции.	**A2.2** Изучить документированный План снижения риска и миграции, чтобы убедиться, что он включает: • Описание использования, включая то, какие данные передаются, типы и количество систем, что использующих и/или поддерживающих протокол SSL и раннюю версию TLS, тип среды; • Результаты оценки рисков и используемые средства снижения рисков; • Описание процедур мониторинга новых уязвимостей, связанных с протоколом SSL/ранней версии TLS; • Описание процессов управления изменениями, обеспечивающих контроль за отсутствием SSL и ранних версий TLS в новых рабочих средах; • Обзор плана действий по переходу, включая установленные сроки завершения перехода, не позднее 30 июня, 2018 года.	План перехода и снижения риска – это документ, подготовленный организацией, который детально описывает планы организации по переходу на безопасный протокол, а также описывает действующие меры, используемые для снижения рисков, связанных с протоколом SSL/ранней версией TLS, до того момента, как переход будет завершен. Дальнейшие руководства по использованию протокола SSL/ранней версии TLS см. в документе *PCI SSC – Информационное приложение - Миграция с протокола SSL/и ранней версии TLS (PCI SSC Information Supplement Migrating from SSL and Early TLS)*.

Требования PCI DSS	Проверочные процедуры	Пояснение
A2.3 ***Дополнительное требование для поставщиков услуг*****:** Все поставщики услуг обязаны предоставить безопасные услуги к 30 июня 2016 года. ***Примечание:*** *До 30 июня 2016 года поставщик услуг обязан либо включить возможность использования безопасного протокола в свои услуги, либо иметь документированный план снижения риска и перехода на новый протокол (как в A2.2), который включает целевую дату предоставления возможности использования безопасного протокола не позднее 30 июня 2016 года. По истечении данного срока все поставщики услуг обязаны предоставить возможность использования безопасного протокола.*	**A2.3** Изучить системные конфигурации и сопутствующую документацию, чтобы убедиться, что поставщик услуг предоставляет безопасный протокол для своего сервиса.	Дальнейшие пояснения относительно «Поставщиков услуг» см. в *Глоссарии PCI DSS и PA-DSS: основные определения, аббревиатуры и сокращения*

Приложение A3: Дополнительные проверки для выделенных организаций

Данное приложение применимо только к организациям, выделенным платежной системой (-ами) или эквайером, как требующим дополнительной проверки по действующим требованиям стандарта PCI DSS. Примеры организаций, к которым **может быть** применено данное Приложение, включают:

- Те, что хранят, обрабатывают и/или передают большие объемы данных держателей карт;
- Те, что предоставляют точки сбора данных держателей карт; или
- Те, что пострадали от значительных или многократных компрометаций данных держателей карт.

Этапы дополнительной проверки нацелены на обеспечение больших гарантий того, что защитные меры согласно стандарту PCI DSS поддерживаются в должном состоянии и на постоянной основе путем проверки традиционных бизнес-процессов, и расширенных проверок, и анализа областей оценки.

Этапы дополнительной проверки в данном документе разделены на следующие области контроля:

A3.1 Внедрить программу соответствия стандарту PCI DSS.
A3.2 Задокументировать и подтвердить область применения PCI DSS.
A3.3 Подтвердить, что стандарт PCI DSS включен в традиционные бизнес-процессы.
A3.4 Контроль и управление логическим доступом в среду данных держателей карт.
A3.5 Выявлять и реагировать на подозрительные события.

Примечание: *Некоторые требования имеют определенные временные рамки (к примеру, выполнять не реже одного раза в квартал или каждые полгода), в пределах которых должны выполняться определенные процедуры. При первой проверке согласно данному документу, не требуется, чтобы процедура была реализована в каждый такой указанный временной период в течение предыдущего года, если аудитор сможет подтвердить, что:*
1) Процедура была выполнена в соответствии с применимым требованием в пределах недавнего времени (т.е. самого ближайшего прошлого квартала или полугодия) и
2) Организация задокументировала политики и процедуры для продолжения реализации деятельности в установленные сроки.
В последующие годы после первого аудита, процедура должна быть выполнена в каждый установленный срок, под требования которого она подпадает (к примеру, ежеквартальная процедура должна быть выполнена в каждый из четырех кварталов предыдущего года).

Примечание*: организация должна проходить проверку согласно данному Приложению,* ***ТОЛЬКО если было получено такое указание от эквайера или платежной системы****.*

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.1 Внедрить программу соответствия стандарту PCI DSS		
A3.1.1 Высшему руководству установить ответственность за защиту данных держателей карт и программу соответствия стандарту PCI DSS, которая будет включать: • полную подотчетность для обеспечения соответствия стандарту PCI DSS; • определение устава программы соответствия стандарту PCI DSS; • не реже одного раза в год предоставлять отчет высшему руководству и совету директоров относительно вопросов и инициатив по программе соответствия стандарту PCI DSS, включая процедуры исправлений недочетов. ***Ссылка на PCI DSS**: Требование 12*	**A3.1.1.a** Изучить документацию, чтобы убедиться, что высшее руководство установило полную подотчетность за обеспечение соответствия организации стандарту PCI DSS. **A3.1.1.b** Изучить устав программы соответствия стандарту PCI DSS, чтобы убедиться, что он излагает условия, на основании которых организована программа соответствия стандарту PCI DSS. **A3.1.1.c** Изучить протоколы совещаний и/или презентаций высшего руководства и совета директоров, чтобы убедиться, что инициативы по программе соответствия стандарту PCI DSS и процедурам исправлений недочетов доводятся до их сведения, как минимум, раз в год.	Назначение высшим руководством ответственности за соответствие стандарту PCI DSS обеспечивает руководящему уровню прозрачность программы соответствия стандарту PCI DSS и дает возможность задавать соответствующие вопросы для определения эффективности программы и ее влияние на стратегические приоритеты. Полная ответственность за программу соответствия стандарту PCI DSS может быть возложена на отдельных сотрудников и/или структурное подразделение внутри организации.
A3.1.2 Формальная программа соответствия стандарту PCI DSS должна включать: • определение процедур для поддержания и мониторинга полного соответствия стандарту PCI DSS, включая традиционные бизнес-процессы; • ежегодное проведение оценки соответствия стандарту PCI DSS; • процедуры непрерывной	**A3.1.2.a** Изучить политики и процедуры информационной безопасности, чтобы убедиться, что процедуры конкретно определены для следующего: • поддержание и мониторинг полного соответствия стандарту PCI DSS, включая традиционные бизнес-процессы; • ежегодное проведение оценки на соответствие стандарту PCI DSS; • процедуры непрерывной оценки требований стандарта PCI DSS; • анализ последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения.	Формальная программа соответствия позволяет организации отслеживать степень исправности ее механизмов и мер защиты, предупреждать случаи отказа механизмов, и эффективно обмениваться данными о действиях и статусе соответствия по всей организации. Программа соответствия стандарту PCI DSS может быть отдельной программой или частью программы соответствия и/или управления; должна включать четко определенную методологию, которая демонстрировала бы последовательную и эффективную оценку.

Требования PCI DSS	Проверочные процедуры	Пояснение
оценки требований стандарта PCI DSS (к примеру, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием).		
A3.1.3 Четко определить задачи и области ответственности в отношение соответствия стандарту PCI DSS, и формально возложить ответственность на одного или более сотрудников, и включать, как минимум, следующее: • управление процедурами PCI DSS относительно традиционных бизнес-процессов; • управление ежегодными оценками соответствия стандарту PCI DSS; • управление непрерывной оценкой требований стандарта PCI DSS (к примеру, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием); • управление анализом последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения. ***Ссылка на PCI DSS**: Требование 12*	**A3.1.3.a** Изучить политики и процедуры информационной безопасности и опросить сотрудников, чтобы убедиться, что задачи и области ответственности четко определены и обязанности распределены так, чтобы включали, как минимум, следующее: • управление процедурами PCI DSS относительно традиционных бизнес-процессов; • управление ежегодными оценками соответствие стандарту PCI DSS; • управление непрерывной оценкой требований стандарта PCI DSS (к примеру, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием); • управление анализом последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения. **A3.1.3.b** Опросить ответственных сотрудников и убедиться, что они осведомлены и выполняют возложенные на них обязанности по соблюдению соответствия стандарту PCI DSS	Формальное определение конкретных ролей и ответственности за соблюдение соответствия стандарту PCI DSS помогает обеспечить подотчетность и мониторинг текущей деятельности, ведущейся в отношении соблюдения соответствия стандарту PCI DSS. Данные роли могут быть назначены на одного сотрудника или на нескольких по разным направлениям. Роли должны назначаться сотрудникам, имеющим полномочия принимать решения и на ком лежит ответственность за определенную функцию. Обязанности должны быть формально определены и ответственные должны суметь продемонстрировать понимание своей зоны ответственности и подотчетности.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.1.4 Обеспечить обучение персонала по действующему стандарту PCI DSS и/или по вопросам информационной безопасности, как минимум, раз в год, для персонала, несущего ответственность за соответствие стандарту PCI DSS (указанных в пункте A3.1.3) ***Ссылка на PCI DSS**: Требование 12*	**A3.1.4.a** Изучить политики и процедуры информационной безопасности, чтобы убедиться, что обучение по стандарту PCI DSS и/или вопросам информационной безопасности требуются не реже одного раза в год для каждой функциональной роли, в обязанности которой входит соответствие стандарту PCI DSS.	Сотрудники, в обязанности которого входит соответствие стандарту PCI DSS, нуждаются в специальных знаниях, превышающих те, что обычно предоставляются на общих тренингах по безопасности. Сотрудники, в обязанности которого входит соответствие стандарту PCI DSS, должны проходить специальные тренинги, которые, в дополнение к общим знаниям по информационной безопасности, фокусируются на специальных вопросах, навыках, процедурах или методиках безопасности, которые должны соблюдаться указанными сотрудниками, для должного исполнения своих обязанностей. Тренинги могут проводиться третьей стороной – к примеру, SANS или PCI SSC (Ознакомление с PCI, PCIP, и ISA), платежными системами и эквайрерами – или же могут быть внутренними. Обучающие материалы должны разрабатываться для каждой роли и быть актуальными, содержать информацию обо всех последних угрозах безопасности и/или версии PCI DSS. Дополнительные пояснения по разработке обучающих материалов для конкретных ролей см. Информационное дополнение от PCI SSC – *Лучшие практики по внедрению программы повышения осведомленности в области безопасности*
	A3.1.4.b Опросить персонал и изучить сертификаты о прохождении курсов или прочие записи, чтобы убедиться, что персонал, в обязанности которого входит соответствие стандарту PCI DSS проходит обучение по стандарту PCI DSS и/или вопросам информационной безопасности не реже одного раза в год.	
A3.2 Задокументировать и подтвердить область применения PCI DSS		

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.1 Документировать и подтверждать правильность области применения PCI DSS не реже раза в квартал и при значительных изменениях в среде. Минимум, который должен входить в ежеквартальную проверку области применения стандарта: • определение всех сетей и системных компонентов, входящих в область применения стандарта; • определение всех сетей, не входящих в область применения стандарта, и подтверждение того, что они не входят в области действия, включая описание используемых механизмов сегментации; • идентификация всех подключенных организаций (например, сторонние организации, имеющие доступ к среде держателей карт). ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS*	**A3.2.1.a** Изучить документированные результаты проверки области применения стандарта и опросить сотрудников, чтобы убедиться, что проверка выполняется: • не реже одного раза в квартал; • рри значительных изменениях в среде ДДК. **A3.2.1.b** Изучить документированные результаты ежеквартальной проверки области действия стандарта, чтобы убедиться, что : • определены все сети и системные компоненты, входящие в область применения стандарта; • определены все сети, не входящие в область применения стандарта, и подтверждено то, что они не входят в область действия; • дано описание используемых механизмов сегментации; • идентифицированы все подключенные организации (например, сторонние организации, имеющие доступ к среде держателей карт).	Подтверждение области применения PCI DSS должно выполняться так часто, как это возможно, чтобы обеспечить актуальность области применения PCI DSS с учетом меняющихся бизнес-целей.
A3.2.2 Определять влияние всех изменений в системах или сетях, включая введение новых систем и новых сетевых соединений, на область применения PCI DSS. Процедуры должны включать: • выполнение формальной проверки влияния PCI DSS; • определение требований PCI	**A3.2.2** Изучить документацию по изменениям и опросить сотрудников, чтобы убедиться, что по каждому изменению в системе: • была выполнена формальная проверка влияния PCI DSS; • определены требования PCI DSS, применимые к системе или сети ; • обновлена область применения PCI DSS в соответствии с изменением; • подпись ответственного сотрудника (как описано в пункте A3.1.3) была получена и задокументирована.	Изменения в системах или сетях могут иметь значительное влияние на область применения PCI DSS. К примеру, изменения правил межсетевого экрана может привести к включению в область применения стандарта всех сегментов сети, или в среду ДДК могут быть добавлены новые системы, которые потребуют соответствующей защиты. Процедуры определения влияния изменений в системах или сетях на область применения PCI DSS,

Требования PCI DSS	Проверочные процедуры	Пояснение
DSS, применимых к системе или сети • Соответствующее обновление области применения PCI DSS; • документально подтвержденные подписью ответственного сотрудника результаты проверки влияния (как указано в пункте A3.1.3). ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS, Требования 1-12*		могут выполняться как часть отдельной программы соответствия стандарту PCI DSS или же быть частью общей программы соответствия и/или управления.
A3.2.2.1 По завершению изменения проверять все соответствующие требования стандарта PCI DSS по всем новым или измененным системам и сетям, и обновлять документацию соответствующим образом. Примеры требований PCI DSS, которые должны быть подтверждены, включают, но не ограничиваются: • сетевая схема обновлена и отражает изменения; • системы настроены согласно стандартам конфигурации, с изменением всех паролей по умолчанию и отключением ненужных сервисов; • системы защищены необходимыми механизмами (например, мониторинг целостности файлов (FIM), антивирус, обновления безопасности, ведение журналов аудита);	**A3.2.2.1** В качестве примера изменений систем и сетей изучить записи об изменениях, опросить сотрудников и пронаблюдать подвергшиеся изменениям системы/сети, чтобы убедиться, что применимые требования PCI DSS были внедрены и документация обновлена как часть изменений.	Наличие процедур для анализа значимых изменений помогает гарантировать применение всех соответствующих стандарту PCI DSS мер защиты для любых систем или сетей, добавленных или измененных в рамках области проверяемой среды. Встраивание данной проверки в процедуры управления изменениями способствует поддержанию в актуальном состоянии перечня устройств и стандартов конфигураций, а также применения защитных мер там, где это требуется. Процедура управления изменениями должна включать свидетельства, подтверждающие реализацию требований PCI DSS или их итеративное выполнение.

Требования PCI DSS	Проверочные процедуры	Пояснение
• подтверждение того, что критичные аутентификационные данные (SAD) не хранятся и, что все хранилища данных держателей карт задокументированы и включены в политики и процедуры хранения данных; • новые системы включены в ежеквартальное сканирование на наличие уязвимостей . ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS, Требования 1-12*		
A3.2.3 При изменении в организационной структуре (к примеру, слияние или приобретение компаний, смена или переназначение сотрудников, несущих ответственность за защитные меры) обеспечить формальную (внутреннюю) проверку влияния на область применения PCI DSS и применимость защитных мер. ***Ссылка на PCI DSS:*** *Требование 12*	**A3.2.3** Изучить политики и процедуры, чтобы убедиться, что изменение организационной структуры ведет к формальной (внутренней) проверке влияния на область применения PCI DSS и применимости защитных мер.	Структура и система управления организации определяют требования и протокол для эффективной и безопасной деятельности. Изменения этой структуры может оказать негативное влияние на существующие механизмы и инфраструктуру вследствие перераспределения или удаления ресурсов, которые поддерживали защитные меры PCI DSS, или же обретения новых обязанностей, для которых не применяются защитные меры. Потому важно пересматривать области применения и защитные меры PCI DSS при выполнении изменений, чтобы обеспечить реализацию защитных мер и их использование.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.4 При использовании сегментации, подтверждать область применения PCI DSS выполнением теста на проникновение, направленным на механизмы сегментации не реже, чем раз в полгода и при внесении любых изменений в методы/механизмы сегментации. ***Ссылка на PCI DSS:*** *Требование 11*	**A3.2.4** Изучить результаты последнего теста на проникновение, чтобы убедиться, что: • тест на проникновение выполняется с целью проверки механизмов сегментации не реже, чем раз в полгода и при внесении любых изменений в методы/механизмы сегментации; • тест на проникновение покрывает все используемые методы/механизмы сегментации; • Тест на проникновение подтверждает, что методы/механизмы сегментации действуют и эффективны, и отделяют все системы вне области применения стандарта от систем в среде данных держателей карт.	В случае использования сегментации для отделения сетей входящих в область применения стандарта от сетей вне этой области, данные механизмы сегментации должны быть проверены посредством теста на проникновение с целью подтвердить, что они работают надлежащим образом и эффективны. Техники проведения теста на проникновение должны следовать существующей методологии, как описано в Требовании 11 стандарта PCI DSS. Дополнительную информацию по эффективному проведению теста на проникновение можно найти в Информационном Дополнении от PCI SSC - *Руководство по Тестированию на проникновение (Penetration Testing Guidance)*.
A3.2.5 Внедрить методологию обнаружения данных для подтверждения области применения PCI DSS и определения всех источников и местоположения PAN, представленных в открытом виде, не реже раза в квартал и при значительных изменениях в среде ДДК или процессах. Методология обнаружения данных должна учитывать возможности того, что PAN, представленные в открытом виде, могут храниться в системах и сетях за пределами ранее определенной среды ДДК. ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS,*	**A3.2.5.a** Изучить документированную методологию обнаружения данных, чтобы убедиться в следующем: • Методология обнаружения данных включает процедуры для обнаружения всех источников и местоположения PAN, представленных в открытом виде; • Методология обнаружения учитывает возможности того, что PAN, представленные в открытом виде, могут храниться в системах и сетях за пределами ранее определенной среды ДДК. **A3.2.5.b** Изучить последние результаты проведенных работ по обнаружению данных и опросить ответственных сотрудников, чтобы убедиться, что обнаружение данных выполняется не реже раза в квартал и при значительных изменениях в среде ДДК или процессах.	Стандарт PCI DSS требует, чтобы проверяемые организации, как часть комплекса оценки, идентифицировали и документировали наличие всех PAN, представленных в открытом виде, в своей среде. Внедрение методологии обнаружения данных, которая определяет все источники и местоположение PAN и позволяет обнаруживать PAN за пределами ранее определенной среды ДДК, или же в неожиданных местах внутри определенной среды ДДК (например, журналах регистрации ошибок или файл дампа памяти) помогает убедиться, что неизвестные ранее местоположения PAN с нешифрованным текстом выявлены и должным образом защищены. Процесс обнаружения данных может быть выполнен с помощью разнообразных методов, включающих, но не ограничивающихся: (1) коммерческие программы обнаружения данных; (2) программа обнаружения данных, разработанная самой организацией; (3) ручной поиск. Вне зависимости от того, какой метод используется, целью работы является выявление всех источников и местоположений PAN (не только в рамках среды держателей карт).

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.5.1 Обеспечить эффективность методов, используемых для обнаружения данных – т.е. методы должны быть в состоянии выявить PAN в открытом виде во всех типах системных компонентов (например, в каждой операционной системе или платформе) и используемых файловых форматах. Эффективность методов обнаружения данных должна подтверждаться не реже одного раза в год. ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS*	**A3.2.5.1.a** Опросить сотрудников и изучить документацию, чтобы убедиться, что: • В организации внедрена и используется процедура тестирования эффективности методов обнаружения данных; • Процедура включает подтверждение того, что методы в состоянии выявить PAN в открытом виде во всех типах системных компонентов и используемых файловых форматах. **A3.2.5.1.b** Изучить результаты недавних проверок на эффективность, чтобы убедиться, что эффективность методов, применяемых для обнаружения данных подтверждается не реже одного раза в год.	Процедура проверки эффективности методов обнаружения данных, обеспечивает завершенность и точность выявления данных держателей карт. Для полноты проверки в процедуру обнаружения данных должны, как минимум, быть включены выборки системных компонентов, как из систем в области оценки, так и вне ее. Полноту можно проверить, поместив тестовые PAN в выборку используемых системных компонентов и файлов, и далее подтвердив, что метод обнаружения данных обнаружил тестовые PAN.
A3.2.5.2 Внедрить процедуры реагирования на события обнаружения PAN в открытом виде вне среды данных держателей карт. Процедуры должны включать: • процедуры, определяющие порядок действий при выявлении PAN в открытом виде вне среды данных держателей карт, включая их извлечение, безопасное удаление и/или перенос в среду ДДК; • процедуры для определения того, как данные оказались вне среды держателей карт;	**A3.2.5.2.a** Изучить документированные процедуры реагирования, чтобы убедиться, что процедуры реагирования на события обнаружения PAN в открытом виде вне среды данных держателей карт определены и включают: • процедуры, определяющие порядок действий при выявлении PAN в открытом виде вне среды данных держателей карт, включая их извлечение, безопасное удаление и/или перенос в среду ДДК; • процедуры для определения того, как данные оказались вне среды держателей карт; • процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые привели к тому, что данные оказались вне среды ДДК ; • процедуры по определению источника данных; • процедуры для определения того, не хранятся ли данные дорожек вместе с PAN.	Наличие документированных процедур реагирования, которым необходимо следовать в случае выявлении PAN в открытом виде вне среды данных держателей карт, помогает определить нужные действия по устранению и предупреждению будущих утечек. К примеру, если PAN обнаружен вне среды данных держателей карт, необходимо выполнить анализ на: (1) определение того, был ли номер сохранен отдельно или же совместно с другими данными (или это была часть полной дорожки); (2) определение источника данных и (3) определение проблем в существующих мерах защиты, которые стали причиной нахождения данных вне среды данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
• процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые привели к тому, что данные оказались вне среды ДДК; • процедуры по определению источника данных; • процедуры для определения того, не хранятся ли данные дорожек вместе с PAN.	**A3.2.5.2.b** Опросить сотрудников и изучить документацию по процедурам реагирования, чтобы убедиться, что мероприятия по устранению последствий при выявлении PAN вне среды данных держателей карт выполняются.	
A3.2.6 Внедрить механизмы обнаружения и предотвращения утечки PAN в открытом виде из среды данных держателей карт через неавторизованные каналы, средства или механизмы, включая генерацию журналов событий и предупреждений. ***Ссылка на PCI DSS:*** *область действия стандарта PCI DSS*	**A3.2.6.a** Изучить документацию и пронаблюдать внедренные механизмы, чтобы убедиться, что механизмы: • внедрены и активно работают; • настроены на обнаружение и предотвращение утечки PAN в открытом виде из среды данных держателей карт через неавторизованные каналы, средства или механизмы; • генерируют журналы событий и предупреждения относительно утечки PAN из среды данных держателей карт через неавторизованный канал, средство или механизм. **A3.2.6.b** Изучить журналы аудита и предупреждения и опросить ответственных сотрудников, чтобы убедиться, что предупреждения анализируются.	Механизмами для обнаружения и предотвращения неавторизованной потери PAN в открытом виде могут быть соответствующие инструменты (такие как решения по Защите от потери данных (DLP)) и/или ручные процессы или механизмы. Механизмы должны обеспечивать обнаружение PAN в открытом виде в следующих местах, но не ограничиваясь: электронные письма, загрузки на съемные носители и вывод на принтер. Использование данных механизмов позволяет организации выявлять и предотвращать ситуации, которые могут привести к потери данных.
A3.2.6.1 Внедрить процедуры реагирования, которые будут выполняться при выявлении попытки удалить PAN в открытом виде из среды ДДК через неавторизованный канал, средство или механизм. Процедуры реагирования должны включать: • процедуры своевременного расследования предупреждений	**A3.2.6.1.a** Изучить документацию по процедурам реагирования, чтобы убедиться, что процедуры реагирования на попытки удалить PAN в открытом виде из среды данных держателей карт через неавторизованный канал, средство или механизм включают: • процедуры своевременного расследования предупреждений ответственными сотрудниками; • процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые потребуются для предотвращения потери данных.	Попытки удалить PAN в открытом виде из среды данных держателей карт через неавторизованный канал, средство или механизм могут указывать на кражу данных или на действия авторизованного сотрудника, который не знает или просто не следует должным методам. Своевременное расследование подобных случаев может выявить те зоны, где требуется исправление и дает ценную информацию, которая помогает понять, откуда исходит угроза.

Требования PCI DSS	Проверочные процедуры	Пояснение
ответственными сотрудниками; • процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые потребуются для предотвращения потери данных.	**A3.2.6.1.b** Опросить сотрудников и изучить записи о предпринятых действиях при выявлении утечки PAN в открытом виде из среды данных держателей карт через неавторизованный канал, средство или механизм и убедиться, что меры по устранению были предприняты.	
A3.3 Подтвердить, что стандарт PCI DSS включен в традиционные бизнес-процессы		
A3.3.1 Внедрить процесс для незамедлительного выявления и предупреждения отказов критических механизмов обеспечения безопасности. Примеры критических механизмов защиты включают, но не ограничиваются: • межсетевые экраны • системы обнаружения и предотвращения вторжений (IDS/IPS) • мониторинг целостности файлов (FIM) • антивирус • средства физического контроля доступа • средства логического контроля доступа • механизмы ведения журнала событий и аудита • средства сегментации (если используются) ***Ссылка на PCI DSS:*** *Требование 1 - 12*	**A3.3.1.a** Изучить документированные политики и процедуры, чтобы убедиться в наличии процедур своевременного выявления и регистрации всех отказов механизмов защиты. **A3.3.1.b** Изучить процедуры выявления и оповещения и опросить персонал, чтобы убедиться, что процедуры применены ко всем механизмам защиты и, что отказ какого-либо механизма защиты приводит к отправке оповещения.	Без формальных процедур выявления и оповещения при отказе механизма защиты, отказы могут оставаться невыявленными продолжительный период, тем самым, давая злоумышленникам достаточно времени для взлома системы и кражи критичных данных из среды данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3.1.1 Своевременно реагировать на любые отказы критичных механизмов защиты. Процедуры реагирования на отказы систем безопасности должны включать: • восстановление функций защиты; • идентификация и документирование длительности (даты и времени от начала до конца) отказа систем безопасности; • идентификация и документирование причины (причин) отказа, включая основную причину, и документирование исправлений, требуемых для устранения основной причины; • выявление и устранение любых	**A3.3.1.1.a** Изучить документированные политики и процедуры и опросить персонал, чтобы убедиться, что процедуры для реагирования на отказы механизмов обеспечения безопасности определены и внедрены, и включают: • восстановление функций защиты; • идентификация и документирование длительности (даты и времени от начала до конца) отказа систем безопасности; • идентификация и документирование причины (причин) отказа, включая основную причину, и документирование исправлений, требуемых для устранения основной причины; • выявление и устранение любых проблем по безопасности, возникающих в процессе отказа; • выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа системы безопасности; • внедрение мер для предотвращения повторного возникновения причины отказа; • возобновление мониторинга механизмов обеспечения безопасности.	Документированные доказательства (к примеру, записи в рамках системы управления проблемами) должны подтвердить, что процессы и процедуры находятся в рабочем состоянии для реагирования на отказ системы безопасности. В дополнение сотрудники должны знать свои зоны ответственности в случае отказа. Действия и реагирование на отказы должны быть отслежены и задокументированы.

Требования PCI DSS	Проверочные процедуры	Пояснение
проблем по безопасности, возникающих в процессе отказа; • выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа системы безопасности; • внедрение мер для предотвращения повторного возникновения причины отказа; • возобновление мониторинга механизмов обеспечения безопасности. ***Ссылка на PCI DSS:*** *Требование 1 - 12*	**A3.3.1.1.b** Изучить документацию, чтобы убедиться, что отказы механизмов обеспечения безопасности задокументированы и включают: • идентификацию причины (причин) отказа, включая основную причину; • длительность (дату и время начала и конца) отказа механизма обеспечения безопасности; • детали исправлений, требуемых для устранения основной причины.	
A3.3.2 Оценивать аппаратные и программные технологии не реже одного раза в год для подтверждения продолжения их соответствия требованиям PCI DSS (например, оценка технологий, которые более не поддерживаются поставщиком и/или не отвечают требованиям безопасности организации). Процесс оценки включает план по выведению из эксплуатации технологий, которые уже не отвечают требованиям PCI DSS, и включая замену технологии, если применимо. ***Ссылка на PCI DSS:*** *Требования 2,6*	**A3.3.2.a** Изучить документированные политики и процедуры и опросить персонал, чтобы убедиться, что процедуры оценки аппаратных и программных технологий для подтверждения продолжения их соответствия требованиям PCI DSS определены и внедрены. **A3.3.2.b** Изучить результаты последних оценок, чтобы убедиться, что оценки выполняются не реже одного раза в год. **A3.3.2.c** Подтвердить, что относительно любых технологий, признанных уже не отвечающими требованиям PCI DSS, имеется в наличии план по выведению из эксплуатации этих технологий.	Аппаратные и программные технологии постоянно развиваются и организации должны быть в курсе изменений в технологиях, которые они используют, так же как и развивающихся угроз для этих технологий. Организации так же должны быть в курсе сделанных производителем изменений в их продукте или в схеме поддержки, чтобы понимать насколько эти изменения могут повлиять на применение организацией технологии. Регулярные оценки технологий, которые оказывают влияние на механизмы безопасности PCI DSS, могут помочь в приобретении, использовании и стратегиях развёртывания, и обеспечить эффективность механизмов, которые зависят от этих технологий.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3.3 Выполнять проверки, как минимум, раз в квартал, чтобы подтвердить, что традиционные бизнес-процессы соблюдаются. Проверки должны выполняться сотрудниками, назначенными на программу соответствия стандарту PCI DSS (как указано в A3.1.3) и включать следующее: • подтверждение, что реализуются все традиционные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1); • подтверждение, что персонал следует политикам безопасности и операционным процедурам (к примеру, ежедневный анализ журналов событий, пересмотр правил межсетевого экранирования, разработка стандартов конфигураций для новых систем и пр.); • документирование того, как были выполнены оценки, включая то, как было подтверждено наличие всех традиционных бизнес-процессов; • собрание всех документальных свидетельств, которые требуются для ежегодного аудита PCI DSS; • оценка и визирование результатов сотрудниками, ответственными за программу соответствия стандарту PCI DSS (**как указано в A3.1.3**); • сохранение записей и документации, которые охватывают все традиционные	**A3.3.3.a** Изучить политики и процедуры, чтобы убедиться, что определены процедуры оценки и подтверждения традиционных бизнес-процессов. Проверить, что процедуры: • подтверждают, что реализуются все традиционные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1); • подтверждают, что персонал следует политикам безопасности и операционным процедурам (к примеру, ежедневный анализ журналов событий, пересмотр правил межсетевого экранирования, разработка стандартов конфигураций для новых систем и пр); • документируют то, как были выполнены оценки, включая то, как было подтверждено наличие всех традиционных бизнес-процессов; • собирают все документальные свидетельства, которые требуется для ежегодного аудита PCI DSS; • оценивают и визируют результаты сотрудниками, ответственными за программу соответствия стандарту PCI DSS (**как указано в A3.1.3**); • сохраняют записи и документацию, которые охватывают все традиционные бизнес-процессы в течение, как минимум, 12 месяцев. **A3.3.3.b** Опросить персонал и изучить записи оценок, чтобы убедиться, что: • оценки выполнены сотрудниками, назначенными на программу соответствия стандарту PCI DSS; • оценки выполняются не реже одного раза в квартал.	Внедрение механизмов безопасности стандарта PCI DSS в традиционные бизнес-процессы является эффективным методом, гарантирующим, что безопасность является частью обычной коммерческой деятельности на постоянной основе. Потому важно, чтобы выполнялись независимые проверки для подтверждения того, что механизмы традиционных бизнес-процессов активны и работают надлежащим образом. Целью этих независимых проверок является оценка свидетельств, подтверждающих, что традиционные бизнес-процессы выполняются. Данные проверки могут также быть использованы для подтверждения того, что ведутся соответствующие записи (к примеру, журналы проверки, отчеты сканирования уязвимостей, и пр.), которые могут помочь в подготовке организации к следующей проверке на соответствие стандарту PCI DSS.

Требования PCI DSS	Проверочные процедуры	Пояснение
бизнес-процессы в течение, как минимум, 12 месяцев. ***Ссылка на PCI DSS:*** *Требования 1 - 12*		
A3.4 Контроль и управление логическим доступом в среду данных держателей карт		
A3.4.1 Проверять учетные записи пользователей и привилегии доступа к системным компонентам области оценки не реже одного раза в полгода, чтобы убедиться, что пользовательские аккаунты и доступ остается соответствующим должностным обязанностям и авторизованным. ***Ссылка на PCI DSS:*** *Требование 7*	**A3.4.1** Опросить ответственных сотрудников и изучить сопутствующую документацию, чтобы убедиться, что • учетные записи пользователей и привилегии доступа к системным компонентам области оценки оцениваются не реже одного раза в полгода; • оценки подтверждают, что доступ остается соответствующим должностным обязанностям и весь доступ авторизован.	Потребности в доступе со временем меняются, вместе с изменением должностных функций сотрудников или их уходом из компании, а также с изменением сферы деятельности. Руководство должно регулярно проверять, переоценивать и, по необходимости, обновлять доступ пользователей, чтобы отражать изменения персонала, включая третьи лица, и должностные обязанности пользователей.
A3.5 Выявлять и реагировать на подозрительные события		
A3.5.1 Внедрить методологию своевременного обнаружения шаблонов атак и нежелательного поведения в системах (к примеру, использование скоординированных ручных проверок и/или централизованных или автоматических средств корреляции событий), которая должна включать, как минимум, следующее: • идентификацию аномалий или подозрительной активности, при их возникновении; • гарантию своевременного оповещения ответственных сотрудников при выявлении	**A3.5.1.a** Изучить документацию и опросить сотрудников, чтобы убедиться, что методология своевременного обнаружения шаблонов атак и нежелательного поведения в системах определена, внедрена и включает следующее: • идентификацию аномалий или подозрительной активности, при их возникновении; • гарантию своевременного оповещения ответственных сотрудников при выявлении подозрительной активности или аномалий • реагирование на уведомления в соответствии с задокументированными процедурами реагирования.	Возможность выявлять шаблоны атак и нежелательное поведение в системах является критичной с точки зрения предотвращения, выявления или минимизации последствий компрометации данных. Наличие журналов регистрации во всех средах делает возможным полное отслеживание, реагирование и анализ, в случае нарушений. Определить причины компрометации очень сложно, если не невозможно, без процесса анализа сообщений и уведомлений критичных системных компонентов и систем, выполняющих защитные функции (таких как межсетевые экраны, IDS/IPS, мониторинг целостности файлов (FIM)). Таким образом, журналы регистрации со всех критичных системных

Требования PCI DSS	Проверочные процедуры	Пояснение
подозрительной активности или аномалий; • реагирование на уведомления в соответствии с задокументированными процедурами реагирования. ***Ссылка на PCI DSS:*** *Требования 10,12*	**A3.5.1.b** Изучить процедуры реагирования на инциденты и опросить ответственных сотрудников, чтобы убедиться, что: • дежурные сотрудники своевременно получают уведомления; • реагирование на уведомления проходит согласно установленной процедуре.	компонентов и систем, выполняющим защитные функции, должны собираться, коррелироваться и поддерживаться. Этот процесс может включать использование программных продуктов и методологии обслуживания с целью выполнения анализа событий в реальном времени, оповещения и отчетности (например, SIEM (Security information and event management), мониторинг целостности файлов (FIM) или обнаружение изменений).

Приложение B: Компенсационные меры

Компенсационные меры могут использоваться для большинства требований PCI DSS в том случае, если организация не может выполнить требование по обоснованным техническим или задокументированным бизнес-ограничениям, но достаточно снизила риск, связанный с требованием, путем реализации иных компенсационных мер.

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 по сравнению с другими требованиями PCI DSS. (Недостаточно просто удовлетворять всем остальным требованиям PCI DSS - это не является компенсационной мерой).

   При анализе избыточности следует руководствоваться учитывать следующее:

Примечание: *Пункты с a) по c), приведенные ниже, являются лишь примерами. Все компенсационные меры должны быть проверены и утверждены аудитором, который проводит проверку на соответствие PCI DSS. Эффективность компенсационной меры зависит от среды, в которой она внедрена, контекста защитных мер и конфигурации компенсационной меры. Следует помнить, что одна и та же мера не может быть одинаково эффективна в разных средах.*

   a) Существующие требования PCI DSS НЕЛЬЗЯ рассматривать как компенсационные меры, если такие требования применимы в отношении проверяемых объектов. Например, чтобы снизить риск перехвата административных паролей в незашифрованном виде, пароли для неконсольного административного доступа должны передаваться в зашифрованном виде. Организации нельзя использовать другие требования к паролям PCI DSS, такие как блокировка нарушителя, сложные пароли и т. д., чтобы компенсировать отсутствие шифрования паролей, поскольку эти меры не снижают риск перехвата незашифрованных паролей. Кроме того, другие меры уже являются требованиями PCI DSS для объекта, подлежащего проверке (пароли).

   b) Существующие требования PCI DSS МОЖНО рассматривать как компенсационные меры, если они снижают существующий риск. Например, двухфакторная аутентификация является требованием PCI DSS для удаленного доступа. Она также может использоваться *и внутри сети* для защиты административного доступа, если шифрование аутентификационных данных невозможно. Двухфакторная аутентификация может быть приемлемой компенсационной мерой при следующих условиях: 1) если она соответствует цели изначального требования и обеспечивает защиту от перехвата паролей администраторов в открытом виде и 2) если она настроена надлежащим образом в защищенной среде.

   c) Существующие требования PCI DSS в сочетании с другими защитными мерами могут использоваться как компенсационные меры. 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 набора 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.

Аудитор должен тщательно оценивать компенсационные меры каждый раз, когда он выполняет ежегодную оценку соответствия организации требованиям PCI DSS. Вовремя такой проверки, аудитор должен подтвердить, что каждая компенсационная мера адекватно учитывает п. 1–4 выше и риск, для нейтрализации которого предназначено исходное требование PCI DSS. Чтобы сохранить соответствие стандарту, следует внедрить процессы и защитные меры, которые обеспечат работу компенсационных мер после выполнения оценки.

Приложение C: Компенсационные меры - Форма для заполнения

Используйте эту таблицу 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, которые выполнили анализ рисков и имеют обоснованные технические или документированные служебные ограничения, могут рассматривать использование компенсационных мер для обеспечения соответствия.*

Номер и определение требования:

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	
2. Цель	Определите цель исходного требования; указать цель, которая достигнута с помощью компенсационной меры.	
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением исходного требования.	
4. Определение компенсационных мер	Опишите компенсационную меру и объясните, как с их помощью достигаются цели исходного требования и снижается дополнительный риск (при его наличии).	
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; указать цель, которая достигнута с помощью компенсационной 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 объясните, как с их помощью достигаются цели исходного требования и снижается дополнительный риск (при его наличии). .	*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 подразделений организации и/или системных компонентов