Стандарт безопасности данных
индустрии платежных карт (PCI DSS)

Требования и процедуры оценки безопасности

Версия 3.2

Апрель 2016 г.

Изменения документа

Дата	Версия	Описание	Страницы
Октябрь 2008 г.	1.2	В документе "PCI DSS Requirements and Security Assessment Procedures" («Стандарт безопасности данных индустрии платежных карт. Требования и процедуры оценки безопасности») версии 1.2 устранена избыточность документов, а также в него внесены общие и частные изменения в сравнении с версией 1.1 под названием "PCI DSS Security Audit Procedures" («Процедуры оценки безопасности»). Для получения полной информации см. "PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2." (Обзор изменений PCI DSS в версии 1.2 в сравнении с версией 1.1)	
Июль 2009 г.	1.2.1	Добавлено предложение, которое было неправильно удалено при переработке версии PCI DSS 1.1 в версию 1.2.	5
		Исправлено “then” (затем) на “than” (чем) в описании проверочных процедур 6.3.7.a и 6.3.7.b.	32
		Удалено выделение серым цветом для столбцов “in place” (выполнено) и “not in place” (не выполнено) в описании проверочных процедур 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 по любым требованиям, имеющим статус «Выполнено благодаря использованию компенсационных мер».	64
Октябрь 2010 г.	2.0	Обновлены и внесены изменения из версии 1.2.1. См. *«PCI DSS: обзор изменений PCI DSS в версии 2.0 в сравнении с версией 1.2.1».*	
Ноябрь 2013 г.	3.0	Изменение в сравнении с версией 2.0. См. *«PCI DSS: обзор изменений PCI DSS в версии 3.0 в сравнении с версией 2.0».*	
Апрель 2015 г.	3.1	Изменение в сравнении с PCI DSS версии 3.0. См. *«PCI DSS: обзор изменений PCI DSS версии 3.1 в сравнении с версией 3.0».*	
Апрель 2016 г.	3.2	Изменение в сравнении с PCI DSS версии 3.1. См. «PCI DSS: обзор изменений PCI DSS версии 3.2 в сравнении с версией 3.1».	

Этот документ (далее «Официальный перевод на русский язык") является официальным переводом на русский язык документа, описанного как PCI DSS v3.2, доступного по адресу https://www.pcisecuritystandards.org/document_library, ©2006-2016 PCI Security Standards Council, LLC (далее «Совет»). Данный официальный перевод на русский язык представлен с согласия и при поддержке компании ABBIS (далее «Компания») исключительно в информационных целях в соответствии с соглашением между Советом и Компанией. Настоящим переводом не предоставляются какие-либо права на реализацию описанных в нем спецификаций; такие права могут быть получены только в результате принятия условий лицензионного соглашения, текст которого находится по адресу: https://www.pcisecuritystandards.org/document_library. Версия документа на английском языке размещена по адресу https://www.pcisecuritystandards.org/document_library и для всех целей считается окончательной версией данного документа. В случае каких-либо неоднозначностей или противоречий между настоящей версией и версией документа на английском языке англоязычный текст имеет преимущественную силу, и в этой связи не следует руководствоваться данной версией для какой бы то ни было цели. Ни Совет, ни Компания не несут никакой ответственности за любые ошибки или неясности, содержащиеся в данном документе.

Содержание

Введение и обзор стандарта PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан, чтобы повысить уровень безопасности данных о держателях карт (ДДК) и содействовать широкому внедрению унифицированных мер защиты данных по всему миру. Стандарт PCI DSS содержит базовые технические и операционные требования, которые разработаны для защиты данных платежных карт (ДПК). Данный стандарт применяется для всех организаций, вовлеченных в обработку платежных карт: ТСП, процессинговых центров, эквайреров, эмитентов и поставщиков услуг, а также всех прочих организаций, которые хранят, обрабатывают или передают 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 к системам и другие параметры безопасности по умолчанию, заданные производителем.
Защищать ДДК	**3.**	Защищать хранимые ДДК
	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
Внедрять строгие меры контроля доступа	**7.**	Ограничивать доступ к ДДК в соответствии со служебной необходимостью.
	8.	Идентифицировать и аутентифицировать доступ к системным компонентам
	9.	Ограничивать физический доступ к ДДК
Осуществлять регулярный мониторинг и тестирование сетей	**10.**	Отслеживать и вести мониторинг всего доступа к сетевым ресурсам и ДДК
	11.	Регулярно тестировать системы и процессы безопасности
Поддерживать политику информационной безопасности	**12.**	Поддерживать политику информационной безопасности для всех работников.

В данном документе, *«Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности»*, 12 требований стандарта и соответствующие им проверочные процедуры скомбинированы в единый инструмент оценки безопасности. Данный документ предназначен для использования в процессе оценки соответствия требованиям PCI DSS как части процедуры подтверждения соответствия организации. Приведенные ниже разделы содержат информацию о передовом опыте и

подробные и инструкции, чтобы способствовать организациям в подготовке и проведении оценки соответствия требованиям PCI DSS, а также в предоставлении отчета по результатам ее проведения. Требования стандарта PCI DSS и проверочные процедуры описываются, начиная со стр. 15.

Стандарт PCI DSS содержит минимальный набор требований для защиты ДПК, который может быть расширен дополнительными защитными мерами и методами для дальнейшего снижения рисков, а также местными, региональными и отраслевыми законами и нормативными актами. Кроме того, в соответствии с законодательством или нормативными требованиями может требоваться особая защита данных, идентифицирующих личность, или других элементов данных (например, имени держателя карты). PCI DSS не заменяет собой местные или региональные законы, постановления правительства или иные требования законодательства.

Источники информации о PCI DSS

На сайте Совета PCI SSC (PCI Security Standards Council) (www.pcisecuritystandards.org) имеется множество дополнительных источников информации, призванных способствовать организациям в оценке и подтверждении соответствия PCI DSS, включая:

- Библиотеку документов, в том числе:
  - *PCI DSS: обзор изменений PCI DSS в версии 3.0 в сравнении с версией 2.0 (PCI DSS – Summary of Changes from PCI DSS version 2.0 to 3.0)*
  - *Краткий справочник по PCI DSS (PCI DSS Quick Reference Guide)*
  - *Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS*
  - *Рекомендации и Вспомогательные документы (Information Supplements and Guidelines)*
  - *Приоритетный подход к PCI DSS (Prioritized Approach for PCI DSS)*
  - *Шаблон Отчета о соответствии и инструкции по его заполнению*
  - *Опросные листы для самооценки (ОЛС), рекомендации и инструкции по их заполнению*
  - *Свидетельства о соответствии (AOC)*
- Часто задаваемые вопросы
- Веб-сайт PCI for Small Merchants («PCI для ТСП малого бизнеса»)
- Обучающие курсы и информационные вебинары по PCI
- Список сертифицированных аудиторов безопасности 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 организаций, вовлеченных в обработку платежных карт: ТСП, процессинговых центров, эквайреров, эмитентов и поставщиков услуг, а также всех прочих организаций, которые хранят, обрабатывают или передают ДДК и (или) КАД.

ДДК и КАД определяются следующим образом:

Данные платежных карт	
В ДДК входят:	**В КАД входят:**
▪ номер карты (PAN); ▪ имя держателя карты; ▪ дата истечения срока действия карты; ▪ сервисный код.	▪ полные данные треков (данные магнитной полосы или ее эквивалента на чипе); ▪ CAV2/CVC2/CVV2/CID ▪ ПИН-коды и (или) ПИН-блоки

Номер карты является определяющим фактором для ДДК. Если имя держателя карты, сервисный код и (или) дата истечения срока действия карты хранятся, обрабатываются или передаются вместе с PAN или иным образом присутствуют в среде ДДК (CDE), то они должны быть защищены согласно применимым требованиям PCI DSS.

Требования PCI DSS применимы к организациям, в которых осуществляется хранение, обработка или передача данных платежных карт (ДДК и (или) КАД). Некоторые требования PCI DSS также могут быть применены к организациям, передавшим платежные операции или управление своей средой ДДК на аутсорсинг[1]. Кроме того, организации, передавшие свои платежные операции или свою среду ДДК на аутсорсинг, отвечают за то, чтобы защита данных платежных карт осуществлялась третьими лицами в соответствии с применимыми требованиями PCI DSS.

Таблица на следующей странице иллюстрирует наиболее часто используемые элементы ДДК и КАД. В ней показано, разрешено или запрещено хранение каждого из них. Кроме того, по каждому элементу показано, требуется ли его защищать. Данная таблица не является исчерпывающей, она демонстрирует различные типы требований, которые применяются к каждому элементу данных.

		Элемент данных	Хранение разрешено	Привести хранимые данные к нечитаемому виду согласно требованию 3.4
ДПК	ДДК	Номер карты (PAN)	Да	Да
		Имя держателя карты	Да	Нет
		Сервисный код	Да	Нет
		Дата истечения срока действия карты	Да	Нет
	КАД[2]	Полные данные треков[3]	Нет	Нельзя хранить согласно требованию 3.2
		CAV2/CVC2/CVV2/CID[4]	Нет	Нельзя хранить согласно требованию 3.2
		ПИН-код и (или) ПИН-блок[5]	Нет	Нельзя хранить согласно требованию 3.2

Требования 3.3 и 3.4 PCI DSS применяются только к PAN. Если PAN хранится вместе с другими элементами ДДК, то согласно требованию 3.4 PCI DSS приводить к нечитаемому виду необходимо только PAN.

После авторизации хранить КАД запрещено (даже в зашифрованном виде). Данное требование действует, даже если PAN отсутствует в среде. Организациям следует связаться со своими эквайерами или напрямую с конкретными международными платежными системами, чтобы узнать, разрешается ли хранить КАД до авторизации, в течение какого срока, а также узнать о соответствующих требованиях к использованию и защите данных.

3 Полные данные треков на магнитной полосе, эквивалентные данные на чипе или в ином месте

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 ПИН-блок, присутствующий в сообщении о транзакции

Связь между стандартами PCI DSS и PA-DSS

Применимость PCI DSS к приложениям, соответствующим стандарту PA-DSS

Использование приложения, которое соответствует стандарту безопасности данных платежных приложений (PA-DSS), само по себе не обеспечивает соответствие организации требованиям PCI DSS. Это связано с тем, что приложение должно быть внедрено в среду, соответствующую стандарту PCI DSS, и согласно «Руководству по внедрению в соответствии с PA-DSS» (предоставляется разработчиком платежного приложения).

Все приложения, которые хранят, обрабатывают или передают ДДК, входят в область оценки организации на соответствие стандарту PCI DSS, даже если они уже были проверены на соответствие PA-DSS. Оценка соответствия стандарту PCI DSS призвана подтвердить, что платежное приложение, соответствующее стандарту PA-DSS, должным образом сконфигурировано и безопасно внедрено в соответствии с требованиями PCI DSS. Если платежное приложение подверглось какой-либо модификации, во время оценки соответствия стандарту PCI DSS потребуется более тщательное изучение, так как приложение может более не соответствовать версии, проверенной на соответствие PA-DSS.

Требования стандарта PA-DSS основаны на *требованиях и процедурах оценки безопасности стандарта PCI DSS* (определенных в данном документе). Стандарт PA-DSS более подробно описывает требования к платежному приложению, необходимые, чтобы организациям было проще достичь соответствия стандарту PCI DSS. Поскольку угрозы безопасности постоянно развиваются, приложения, которые уже не поддерживаются разработчиком (например, в отношении которых разработчик объявил об окончании срока эксплуатации), могут не обеспечивать такой же уровень безопасности как поддерживаемые разработчиком версии.

Безопасные платежные приложения, внедряемые в среду, соответствующую стандарту PCI DSS снижают вероятность нарушений безопасности (а также мошеннических действий, возникающих в результате таких нарушений), ведущих к компрометации PAN, полных данных треков, проверочных кодов и значений (CAV2, CID, CVC2, CVV2), ПИН-кодов и ПИН-блоков.

Чтобы определить, применим ли стандарт PA-DSS к определенному платежному приложению, следует обратиться к документу «Руководство по программе PA-DSS», который доступен на сайте www.pcisecuritystandards.org.

Применимость стандарта PCI DSS к разработчикам платежных приложений

PCI DSS может применяться к разработчикам платежных приложений, если они хранят, обрабатывают или передают ДДК или имеют доступ к ДДК своих клиентов (например, в качестве поставщика услуг).

Область применимости требований стандарта PCI DSS

Требования PCI DSS применяются ко всем системным компонентам, которые входят в среду ДДК или подключены к ней. Среда ДДК – это совокупность людей, процессов и технологий, которые хранят, обрабатывают или передают ДДК или КАД. Термин «системные компоненты» включает в себя сетевые и вычислительные устройства, серверы и приложения. Примерами системных компонентов являются, среди прочего:

- системы, которые:
  - — предоставляют службы безопасности (например, серверы аутентификации),
  - — способствуют сегментации сети (например, внутренние межсетевые экраны),
  - — могут влиять на безопасность среды ДДК (например, серверы разрешения имен или веб-переадресации);
- компоненты виртуализации, например:
  - — виртуальные машины,
  - — виртуальные коммутаторы и (или) маршрутизаторы,
  - — виртуальные приложения и (или) компьютеры,
  - — гипервизоры;
- сетевые компоненты, в том числе:
  - — межсетевые экраны,
  - — коммутаторы,
  - — маршрутизаторы,
  - — беспроводные точки доступа,
  - — устройства сетевой безопасности,
  - — прочие устройства безопасности;
- типы серверов, в том числе:
  - — веб-серверы,
  - — серверы приложений,
  - — серверы баз данных,
  - — серверы аутентификации,
  - — почтовые серверы,

— прокси-серверы,

— серверы службы времени (NTP),

— DNS-серверы;

- приложения, включая все приобретенные или заказные приложения, в том числе внутренние и внешние (например, доступные через Интернет);
- любой другой компонент или устройство, расположенное внутри среды ДДК или подключенное к ней.

Первым этапом выполнения оценки соответствия требованиям PCI DSS является корректное определение области применимости. Как минимум один раз в год и перед каждой ежегодной оценкой соответствия оцениваемая организация должна подтвердить корректность определения области применимости PCI DSS с помощью идентификации всех мест хранения и потоков ДДК и определения всех систем, соединенных с ними, или которые в случае компрометации могут влиять на среду ДДК (например, серверы аутентификации), чтобы убедиться в том, что они включены в эту область. Все типы систем и мест хранения должны рассматриваться в процессе определения области применимости требований PCI DSS, включая системы резервного копирования, восстановления и обеспечения отказоустойчивости.

Для того чтобы подтвердить корректность и точность определения среды ДДК, следует выполнить следующие действия:

- оцениваемая организация выявляет и документирует присутствие всех ДДК в своей инфраструктуре для того, чтобы убедиться, что ДДК отсутствуют вне определенной на текущий момент среды ДДК;
- после того, как все места расположения ДДК выявлены и документированы, организация использует эту информацию для проверки того, что область оценки PCI DSS определена надлежащим образом (например, результаты могут быть представлены в виде схемы или перечня мест расположения ДДК);
- любые обнаруженные ДДК подлежат включению в область оценки PCI DSS и в среду ДДК; если обнаружены данные, еще не включенные в среду ДДК, такие данные следует безопасно удалить, перенести в определенную на данный момент среду ДДК или переопределить среду ДДК так, чтобы в нее вошли эти данные;
- организация сохраняет документы, описывающие, каким образом была определена область оценки PCI DSS. Документы сохраняются для их проверки аудитором и (или) для использования при следующем ежегодном подтверждении области оценки PCI DSS.

При каждой оценке соответствия PCI DSS аудитор должен проверить, что область оценки корректно определена и документирована.

Сегментация сети

Сегментация сети, т. е. отделение среды ДДК от остальной части сети организации в отдельный сегмент (изоляция) не является требованием PCI DSS. Однако сегментация настоятельно рекомендуется 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 (снижаемый за счет объединения ДДК в меньшем количестве мест расположения, находящихся под более надежным контролем).

Если надлежащая сегментация сети отсутствует (так называемая «плоская сеть»), в область оценки соответствия PCI DSS попадает вся сеть. Сегментация сети может быть выполнена с использованием множества физических или логических мер, например, надлежащим образом сконфигурированных межсетевых экранов внутри сети, маршрутизаторов со строгими списками контроля доступа или при помощи иных технологий, которые ограничивают доступ к определенному сегменту сети. Для того чтобы системный компонент был исключен из области оценки PCI DSS, его следует должным образом изолировать (сегментировать) от среды ДДК так, чтобы даже в случае компрометации такого системного компонента это не повлияло бы на безопасность среды ДДК.

Важным предварительным условием к сокращению области среды ДДК является четкое понимание потребностей и процессов организации, связанных с хранением, обработкой или передачей ДДК. Размещение ДДК в минимально возможном количестве мест расположения за счет удаления неиспользуемых данных и объединения нужных данных может потребовать реорганизации устоявшейся практики ведения деятельности.

Документирование потоков ДДК с помощью схемы потоков данных помогает полностью разобраться во всех потоках ДДК и подтверждает результативность любой сегментации при изолировании среды ДДК.

Если сегментация сети реализована и используется для уменьшения области оценки соответствия PCI DSS, аудитор должен убедиться в том, что сегментация выполнена надлежащим образом и позволяет уменьшить область оценки. В целом, надлежащая сегментация сети изолирует системы, которые хранят, обрабатывают или передают ДДК, от систем, которые этого не делают. Достаточность той или иной реализации сегментации сети, однако, очень зависит от множества факторов и обстоятельств, например, конфигурации данной сети, используемых технологий и иных реализуемых защитных мер.

В Приложении D: «Сегментация и выборка подразделений организации и (или) системных компонентов» содержится дополнительная информация о влиянии сегментации сети и выборки на определение области оценки соответствия PCI DSS.

Беспроводные сети

Если в организации используются беспроводные технологии для хранения, обработки или передачи ДДК (например, транзакции с использованием беспроводных POS-терминалов для ускорения обслуживания клиентов) или если беспроводная локальная сеть (WLAN) подключена к среде ДДК или является ее частью, то применению и выполнению подлежат требования и проверочные процедуры PCI DSS для беспроводных окружений (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 ТСП могут привлекать сторонние организации к обработке, хранению и передаче ДДК от их имени или к управлению компонентами, такими, как маршрутизаторы, межсетевые экраны, физическая безопасность и (или) серверы, что, однако, может оказывать воздействие на безопасность среды ДДК.

Стороны должны четко определить, какие услуги и системные компоненты входят в область оценки поставщика услуг на соответствие требованиям PCI DSS, какие требования покрываются поставщиком услуг, а какие находятся в области ответственности его клиентов и должны быть включены в рамки оценки их собственного соответствия PCI DSS. Например, поставщик услуг управляемого хостинга должен четко указать, какие IP-адреса просканированы в рамках его ежеквартального сканирования на наличие уязвимостей, и за какие IP-адреса отвечают клиенты и должны включать их в свои собственные ежеквартальные сканирования.

Поставщики услуг ответственны за подтверждение своего соответствия требованиям стандарта PCI DSS, и международные платежные системы могут потребовать от них такого подтверждения. Поставщики услуг должны связаться со своим эквайрером и (или) международной платежной системой для определения подходящего способа подтверждения соответствия.

Сторонние поставщики услуг могут подтвердить соответствие требованиям двумя способами:

1) ежегодная оценка: поставщики услуг могут проходить ежегодную оценку (ежегодные оценки) соответствия PCI DSS по своей инициативе и предоставить подтверждение соответствия своим клиентам, или
2) неоднократные оценки, оценки по запросу: если поставщики услуг не проходят оценку PCI DSS по своей инициативе, они могут проходить оценки по требованию своих клиентов и (или) быть проверены в рамках каждой оценки соответствия, которую проходят клиенты данного поставщика услуг, с предоставлением результатов оценки соответствующему клиенту (соответствующим клиентам).

Если сторонний поставщик услуг проходит оценку соответствия PCI DSS по своей инициативе, он должен представить своим клиентам достаточное подтверждение того, что его область применимости PCI DSS включает услуги, относящиеся к клиенту, и что выполнение соответствующих требований PCI DSS были проверено и подтверждено. Конкретный вид подтверждения, которое поставщик услуг должен предоставить своим клиентам, зависит от действующих соглашений и (или) договоров между этими сторонами. Например, Свидетельство о соответствии и (или) соответствующие разделы Отчета о соответствии поставщика услуг (отредактированного для защиты конфиденциальной информации) могут предоставить всю или некоторую информацию.

Дополнительно ТСП и поставщики услуг должны распоряжаться всеми связанными с ними сторонними поставщиками услуг, которые имеют доступ к ДДК, и отслеживать их статус соответствия PCI DSS. *Подробнее см. требование 12.8.*

Передовой опыт по внедрению стандарта PCI DSS в привычные бизнес-процессы

Для того чтобы обеспечить надлежащую реализацию защитных мер, стандарт PCI DSS должен быть внедрен в привычные бизнес-процессы в рамках общей стратегии безопасности организации. Это позволит организации постоянно следить за эффективностью защитных мер и поддерживать среду в соответствии с требованиями PCI DSS в период между оценками соответствия PCI DSS. Примеры внедрения PCI DSS в привычные бизнес-процессы включают, помимо прочего, следующие действия:

1. Вести мониторинг защитных мер (например, межсетевых экранов, систем обнаружения или предотвращения вторжений, систем мониторинга целостности файлов, антивирусного ПО, механизмов контроля доступа и т. д.), чтобы обеспечить их эффективную работу, соответствующую их назначению.
2. Своевременно обнаруживать сбои в работе защитных мер и реагировать на них. Включать следующие действия в процессы реагирования на сбои защитных мер:
   - восстановить защитную меру;
   - определить причину сбоя;
   - определить и решить любые проблемы с безопасностью, возникшие в период сбоя защитных мер;
   - реализовать меры по смягчению последствий, такие как процесс или технические меры, во избежание повторного возникновения причины сбоя;
   - возобновить мониторинг защитной меры, возможно, с временным усилением мониторинга, чтобы проверить, что мера работает эффективно.
3. Рассматривать изменения среды (например, добавление новых систем, внесение изменений в систему или конфигурацию сети) до внесения изменений и выполнить следующие действия:
   - определять потенциальное воздействие на область оценки PCI DSS (например, новое правило межсетевого экранирования, разрешающее подключение между системой в среде ДДК и другой системой, может привести к включению дополнительных систем или сетей в область применимости PCI DSS);
   - определять требования PCI DSS, применимые к системам и сетям, на которые распространяются изменения (например, если новая система входит в область применимости PCI DSS, ее необходимо настроить согласно стандартам конфигурации, включая мониторинг целостности файлов, антивирусное ПО, обновления, ведение журналов аудита и т. д., и включить в план ежеквартального сканирования на наличие уязвимостей);
   - обновлять область применимости PCI DSS и внедрять необходимые защитные меры.
4. Официально пересматривать влияние на область применимости требований PCI DSS после изменений в организационной структуре (например, слияния или приобретения компаний).
5. Проводить периодические проверки и опросы, чтобы подтвердить, что требования PCI DSS по-прежнему выполняются, а работники соблюдают процессы обеспечения безопасности. Такие периодические проверки должны распространяться на все

подразделения и места расположения, в том числе торговые точки, центры обработки данных и т. д. Они должны включать в себя проверку системных компонентов (или выборок системных компонентов) на предмет того, что требования PCI DSS по-прежнему выполняются (например, применяются стандарты конфигурации, используются последние обновления и антивирусное ПО, проводится мониторинг журналов аудита и т. д.). Частота проведения регулярных проверок должна определяться организацией в соответствии с размером и сложностью ее среды.

Они также могут использоваться, чтобы проверить, что ведутся надлежащие записи, например, журналы аудита, отчеты о результатах сканирования на наличие уязвимостей, журналы межсетевого экранирования и т. д., чтобы облегчить подготовку организации к следующей оценке соответствия требованиям.

6. Проверять аппаратные и программные технологии не реже одного раза в год, чтобы убедиться, что вендор продолжает их поддержку и что они соответствуют требованиям организации к безопасности, включая PCI DSS. Если будет установлено, что технологии более не поддерживаются вендором или не соответствуют требованиям организации к безопасности, организация должна подготовить план решения проблемы, при необходимости включающий замену технологий.

Кроме вышеуказанных мер организации также могут принять решение о разделении обязанностей по обеспечению безопасности так, чтобы функции по обеспечению безопасности и (или) проведению проверок были отделены от операционной деятельности. В средах, где один работник выполняет несколько обязанностей (например, администрирование и выполнение действий по обеспечению безопасности), обязанности могут быть распределены таким образом, чтобы ни один работник не обладал полным контролем над процессом без независимого надзора. Например, за настройку и за утверждение изменений могут отвечать разные лица.

Примечание: *для некоторых организаций информация об этом передовом опыте также является требованиями по непрерывному обеспечению соответствия PCI DSS. Например, эти принципы включены в некоторые требования PCI DSS, и дополнительная проверка организаций зоны повышенного риска (Приложение A3 PCI DSS) требует от организаций зоны повышенного риска проверки выполнения этих принципов.*

Все организации должны уделять внимание внедрению этого передового опыта в их среду, даже если организация не обязана проверять выполнение этих требований.

Для аудиторов: выборка подразделений организации и системных компонентов

Выборка позволяет аудиторам облегчить процесс оценки при наличии большого количества подразделений организации и (или) системных компонентов.

Хотя аудитору разрешается проводить выборку подразделений организации и системных компонентов в рамках проверки организации на соответствие требованиям PCI DSS, организациям запрещается применять требования PCI DSS только к части своей среды (например, требования о проведении ежеквартального сканирования на наличие уязвимостей распространяются на все системные компоненты). Аналогично, аудитору запрещается проверять соответствие только выборке требований PCI DSS.

После того, как аудитор изучил в целом область и сложность оцениваемой среды, он может самостоятельно сделать репрезентативную выборку подразделений организации и системных компонентов, чтобы оценить соответствие организации требованиям PCI DSS. Выборка должна быть определена сначала для подразделений организации, а затем для системных компонентов внутри каждого из них. Выборка должна быть репрезентативной как для всех типов и мест расположения подразделений организации, так и для типов системных компонентов внутри выбранных подразделений организации. Выборка должна быть достаточно обширной, чтобы аудитор мог удостовериться в надлежащей реализации защитных мер.

Примеры подразделений организации включают среди прочего: офисы организации, магазины, франчайзинговые предприятия, процессинговые центры, центры обработки данных и другие типы подразделений с разными местами расположения. В выборку должны включаться системные компоненты из каждого выбранного подразделения организации. Например, для каждого выбранного подразделения организации следует включать набор различных ОС, функций и приложений, относящихся к проверяемой области.

Например, аудитор может определить, что выборка внутри подразделения организации должна включать:

— серверы Sun, на которых функционирует Apache,

— Windows-серверы, на которых функционирует СУБД Oracle,

— мейнфреймы, на которых функционируют унаследованные платежные приложения,

— серверы передачи данных под управлением HP-UX,

— Linux-серверы с MySQL.

Если все приложения работают на базе одной версии ОС (например, Windows 7 или Solaris 10), в выборку все же необходимо включать набор различных приложений (например, серверы базы данных, веб-серверы, серверы передачи данных).

При самостоятельном составлении выборки подразделений организации и системных компонентов аудитор должен учесть следующее:

- выборка может быть меньше, если реализованы стандартизованные и централизованные защитные и операционные процессы и меры PCI DSS, которые обеспечивают единство подходов и которые должны соблюдаться всеми подразделениями организации или во всех системных компонентах; выборка должна быть достаточно большой, чтобы предоставить аудитору достаточную уверенность в том, что все подразделения организации и (или) системные компоненты сконфигурированы в соответствии со

стандартизованными процессами; аудитор должен убедиться в том, что стандартизованные и централизованные защитные меры реализованы и работают;

- при наличии более одного типа действующих стандартизованных операционных и (или) защитных процессов (например, для разных типов подразделений организации и (или) системных компонентов) выборка должна быть достаточно большой, чтобы включать в себя подразделения организации и (или) системные компоненты, привязанные к каждому типу процесса;
- если действующие стандартизованные процессы и меры по соблюдению требований PCI DSS отсутствуют, а управление каждым подразделением организации и (или) каждым системным компонентом осуществляется с использованием нестандартизованных процессов, то выборка должна быть больше для того, чтобы аудитор мог убедиться, что в каждом подразделении организации и в каждом системном компоненте требования PCI DSS выполняются надлежащим образом;
- 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 выбранного метода формирования выборки и ее размера;
- документировать и утвердить стандартизованные процессы и механизмы PCI DSS, используемые для определения размера выборки;
- объяснить, почему сделанная выборка адекватна и репрезентативна для общего количества элементов.

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

Аудиторы должны перепроверять обоснование выборки при каждой оценке. Если используется выборка, то для каждой оценки соответствия должны выбираться разные подразделения организации и системные компоненты.

Компенсационные меры

Аудитор должен ежегодно документировать все компенсационные меры, пересматривать их, утверждать и включать в Отчет о соответствии согласно *Приложению B: «Компенсационные меры»* и *Приложению C: «Компенсационные меры – Форма для заполнения».*

Для каждой отдельно взятой компенсационной меры в обязательном порядке должна быть заполнена форма «Компенсационные меры – Форма для заполнения» *(Приложение C)* . Кроме того, результаты применения компенсационных мер должны быть отражены в Отчете о соответствии в пункте соответствующего требования PCI DSS.

Подробнее о компенсационных мерах см. *в вышеупомянутых Приложениях B* и *C*.

Инструкции и содержание 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 должен использоваться для создания *Отчета о соответствии*. Проверяемая организация должна выполнять соответствующие требования каждой международной платежной системы по предоставлению подтверждения статуса соответствия. Для получения информации об инструкциях и требованиях по предоставлению подтверждения статуса соответствия следует обращаться к представителям каждой международной платежной системы или к эквайреру.

Процесс проведения оценки соответствия стандарту PCI DSS

Процесс проведения оценки соответствия стандарту PCI DSS включает выполнение следующих шагов:

1. Подтвердить область оценки соответствия PCI DSS.
2. Провести проверку среды на соответствие PCI DSS, следуя проверочным процедурам для каждого требования.
3. Заполнить соответствующий отчет о проведении оценки (например, *Опросный лист для самооценки* или Отчет о соответствии), включая документирование всех компенсационных мер, согласно применимым рекомендациям и инструкциям PCI.
4. Полностью заполнить Свидетельство о соответствии для поставщиков услуг или для ТСП, в зависимости от обстоятельств. Свидетельства о соответствии доступны на сайте Совета PCI SSC.
5. Предоставить Опросный лист для самооценки или Отчет о соответствии и Свидетельство о соответствии вместе со всей требуемой документацией – например, отчетом об ASV-сканировании – эквайреру (для ТСП), или международной платежной системе или другой заинтересованной организации (для поставщиков услуг).
6. При необходимости провести исправление по невыполненным требованиям и предоставить обновленный отчет.

Версии стандарта PCI DSS

По состоянию на дату публикации данного документа стандарт PCI DSS версии 3.1 действителен до 31 октября 2016 г., после чего он будет недействителен. Все процедуры подтверждения соответствия стандарту PCI DSS после указанной даты должны проводиться по стандарту PCI DSS версии 3.2 или более поздних версий.

В следующей таблице представлена сводная информация о версиях стандарта PCI DSS и их сроках действия[6].

Версия	Дата публикации	Дата окончания действия
Стандарт PCI DSS версии 3.2 (настоящий документ)	апрель 2016 г.	будет определена позже
Стандарт PCI DSS версии 3.1	апрель 2015 г.	31 октября 2016 г.

Подробные требования и процедуры оценки безопасности стандарта PCI DSS

В приведенной ниже таблице требований и процедур оценки безопасности стандарта PCI DSS заголовки столбцов означают следующее:

- **Требования PCI DSS** – в данном столбце определены требования стандарта безопасности данных; соответствие PCI DSS проверяется по этим требованиям.
- **Проверочные процедуры** – в данном столбце указаны действия, которые должен выполнить аудитор для проверки выполнения требований PCI DSS и простановки отметки «Выполнено».
- **Пояснение** – в данном столбце описано назначение или цель с точки зрения безопасности, преследуемая каждым требованием PCI DSS. В данном столбце даются только пояснения, которые помогают 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 либо еще не внедрены, либо запланированы на будущее. После того как организацией будут обработаны все невыполненные требования или требования, выполнение которых планируется в будущем, аудитор должен провести повторную оценку на предмет того, что проблемы устранены и все требования выполнены.*

Для получения инструкций по документированию оценки соответствия PCI DSS см. документы (доступные на сайте Совета PCI SSC):

- *инструкции по заполнению Отчета о соответствии в* Шаблоне отчета о соответствии стандарту PCI DSS;
- *инструкции и рекомендации по заполнению Опросных листов для самооценки в документе* Инструкции и рекомендации по заполнению ОЛС PCI DSS;
- *инструкции по заполнению отчетов о подтверждении соответствия стандарту PCI DSS в* Свидетельствах о соответствии стандарту PCI DSS.

Построить и поддерживать защищенные сети и системы

Требование 1. Установить и поддерживать конфигурацию межсетевых экранов для защиты ДДК.

Межсетевые экраны – это устройства, которые контролируют сетевой трафик, разрешенный между локальными (внутренними) сетями организации и недоверенными (внешними) сетями, а также которые контролируют входящий и исходящий трафик в зонах повышенной критичности, находящихся внутри доверенных сетей организации. Среда ДДК является примером зоны повышенной критичности внутри доверенной локальной сети организации.

Межсетевой экран анализирует весь сетевой трафик и блокирует соединения, которые не удовлетворяют заданным критериям безопасности.

Все системы должны быть защищены от несанкционированного доступа из недоверенных сетей, будь то подключение систем электронной торговли к сети через Интернет, доступ работников к Интернету через браузеры, доступ работников к электронной почте, выделенные подключения со сторонними организациями, подключения по беспроводным сетям или иными способами. Зачастую кажущиеся малозначимыми каналы связи с недоверенными сетями могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – важнейшие механизмы обеспечения безопасности любой компьютерной сети.

Иные системные компоненты могут обеспечивать функциональные возможности межсетевого экрана, если эти компоненты отвечают минимальным требованиям к межсетевым экранам, приведенным в Требовании 1. Если иные системные компоненты обеспечивают функциональные возможности межсетевого экрана в составе среды ДДК, они должны быть включены в область оценки и проверены на соответствие Требованию 1.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1 Разработать и внедрить стандарты конфигурации межсетевых экранов и маршрутизаторов. Стандарты должны включать в себя:	**1.1** Проверить стандарты конфигурации межсетевых экранов и маршрутизаторов, а также иную указанную ниже документацию, на предмет полноты стандартов и их надлежащего внедрения следующим образом:	Межсетевые экраны и маршрутизаторы – это ключевые компоненты архитектуры, которая используется для контроля входа в сеть и выхода из нее. Эти устройства являются программным или аппаратным обеспечением, которое блокирует нежелательный доступ и управляет санкционированным доступом на входе в сеть и выходе из нее. Стандарты конфигурации и процедуры конфигурирования помогают обеспечить надежность первой линии обороны организации в защите ее данных.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.1Формализованный процесс утверждения и тестирования всех сетевых соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов.	**1.1.1.a**Проверить документированные процедуры на предмет того, что существует формализованный процесс тестирования и утверждения всех: • сетевых соединений; • 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 формализованного утверждения и тестирования изменений записи об изменениях могут не обновляться, что может привести к несоответствию между сетевой документацией и реальной конфигурацией.
	1.1.1.b Для выборки сетевых соединений опросить ответственных работников и проверить записи на предмет того, что сетевые соединения были протестированы и утверждены.	
	1.1.1.c Определить выборку реальных изменений, произведенных в конфигурациях межсетевого экрана и маршрутизатора, сравнить их с записями об изменениях и опросить ответственных работников на предмет того, что изменения были протестированы и утверждены.	
1.1.2 Актуальную схему сети, которая указывает все подключения между средой ДДК и другими сетями, включая все беспроводные сети	**1.1.2.a** Проверить схему (схемы) и конфигурации сети на предмет наличия актуальной схемы сети, а также того, что в схеме отмечены все подключения к ДДК и что она включает все беспроводные сети.	Схемы сети описывают конфигурацию сетей и определяют места расположения всех сетевых устройств. Без актуальных схем сети устройства могут быть пропущены, невольно к ним не будут применены защитные меры, которые были внедрены для выполнения требований стандарта PCI DSS, и таким образом, эти устройства будут уязвимы к компрометации.
	1.1.2.b Опросить ответственных работников на предмет того, что схема поддерживается в актуальном состоянии.	
1.1.3 Актуальную схему, отображающую все потоки ДДК по системам и сетям.	**1.1.3** Проверить схему потоков данных и опросить работников на предмет того, что схема: • отражает все потоки ДДК по системам и сетям; • поддерживается в актуальном состоянии и обновляется, если в среду вносятся изменения.	Схемы потоков ДДК определяют расположение всех ДДК, которые хранятся, обрабатываются или передаются внутри сети. Схемы сети и потоков ДДК, демонстрирующие как ДДК перемещаются по сетям и между отдельными системами и устройствами, помогают организации получить представление об области своей среды и отслеживать ее.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.4 Требования о необходимости межсетевого экранирования каждого Интернет-соединения и соединений между каждой демилитаризованной зоной и внутренней сетью.	**1.1.4.a** Проверить стандарты конфигурации межсетевого экрана на наличие требований о необходимости межсетевого экранирования каждого Интернет-соединения, а также соединений между каждой демилитаризованной зоной и внутренней сетью.	Использование межсетевого экрана на каждом входящем (и исходящем) Интернет-соединении, а также между каждой демилитаризованной зоной и внутренней сетью позволяет организации отслеживать доступ, контролировать его и свести к минимуму возможности злоумышленников на получение доступа к внутренней сети через незащищенное соединение.
	1.1.4.b Убедиться, что актуальная схема сети соответствует стандартам конфигурации межсетевых экранов.	
	1.1.4.c Проверить конфигурации сети на наличие межсетевого экрана на каждом Интернет-соединении и между каждой демилитаризованной зоной и внутренней сетью согласно документированным стандартам конфигурации и схемам сети.	
1.1.5 Описание групп, ролей и обязанностей по управлению сетевыми компонентами	**1.1.5.a** Убедиться, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат описание групп, ролей и обязанностей по управлению сетевыми компонентами.	Данное описание ролей и распределение обязанностей гарантирует, что работники знают, кто отвечает за безопасность всех компонентов сети, и что лица, назначенные для управления компонентами, знают о своих обязанностях. Без формализованного назначения ролей и обязанностей можно потерять контроль над устройствами.
	1.1.5.b Опросить работников, отвечающих за управление компонентами сети на предмет того, что роли и обязанности назначены в соответствии с документацией.	
1.1.6 Документирование служебного обоснования и утверждение для использования всех разрешенных служб, протоколов и портов, а также документация по реализованным средствам защиты тех протоколов, которые признаны небезопасными.	**1.1.6.a** Убедиться, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат документированный перечень всех служб, протоколов и портов, обоснование служебной необходимости и утверждение каждого из них.	Зачастую компрометация происходит из-за наличия неиспользуемых или небезопасных служб и портов, поскольку они часто содержат известные уязвимости, и многие организации не устанавливают обновления для уязвимостей служб, протоколов и портов, которые не используются этими организациями (даже при наличии таких 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. Утверждение должно предоставляться
	1.1.6.b Выявить разрешенные небезопасные службы, протоколы и порты и проверить документальное оформление средств защиты для каждой службы.	
	1.1.6.c Проверить конфигурацию межсетевых экранов и маршрутизаторов на предмет того, что документированные средства защиты внедрены для каждой небезопасной службы, протокола и порта.	

Требования PCI DSS	Проверочные процедуры	Пояснение
		работниками, независимыми от работников, которые осуществляют конфигурирование. Если небезопасные службы, протоколы или порты необходимы для осуществления деятельности, организация должна четко понимать и принимать риск, связанный с их использованием, обосновать необходимость их использования, а также документировать и внедрить средства защиты, которые позволят безопасно использовать эти протоколы. Если эти небезопасные службы, протоколы или порты не являются необходимыми для осуществления деятельности, их следует отключить или удалить. За пояснениями по службам, протоколам и портам, считающимися небезопасными, обращайтесь к отраслевым стандартам и руководствам (например, NIST, ENISA, OWASP и другие).
1.1.7Требование пересмотра набора 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 набора правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода. **1.1.7.b** Проверить документацию, относящуюся к пересмотру наборов правил, и опросить ответственных работников на предмет того, что наборы правил пересматриваются как минимум раз в полгода.	Пересмотр наборов правил дает организации возможность удаления всех ненужных, устаревших или некорректных правил как минимум раз в полгода и гарантирует, что все наборы правил разрешают доступ только авторизованным службам и портам, которые соответствуют документированному служебному обоснованию. Организациям, которые вносят много изменений в наборы правил межсетевых экранов и маршрутизаторов, рекомендуется проводить пересмотр чаще, чтобы гарантировать, что наборы правил по-прежнему соответствуют требованиям организации.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.2 Создать конфигурации межсетевых экранов и маршрутизаторов, которые ограничивают соединения между недоверенными сетями и любыми системными компонентами в среде ДДК. ***Примечание:*** *недоверенной является любая сеть, внешняя по отношению к сетям, принадлежащим проверяемой организации и (или) сеть, которая не находится ни под контролем, ни под управлением проверяемой организации.*	**1.2** Проверить конфигурацию межсетевых экранов и маршрутизаторов и выполнить следующие действия, чтобы убедиться, что соединения между недоверенными сетями и системными компонентами, находящимися в среде ДДК, ограничены:	Необходимо установить защиту сети между внутренней доверенной сетью и любой недоверенной внешней сетью и (или) сетью, которая не находится под контролем организации. Если данная мера будет реализована некорректно, организация будет уязвима к несанкционированному доступу со стороны злоумышленников или вредоносного ПО. Для того чтобы межсетевой экран действительно выполнял свои функции, его необходимо должным образом сконфигурировать так, чтобы он контролировал и (или) ограничивал входящий и исходящий трафик в сети организации.
1.2.1 Ограничить входящий и исходящий трафик только теми соединениями, которые необходимы для среды ДДК. Весь остальной трафик должен быть явным образом запрещен.	**1.2.1.a** Проверить стандарты конфигурации межсетевого экрана и маршрутизатора на предмет того, что они определяют входящий и исходящий трафик, необходимый для среды ДДК. **1.2.1.b** Проверить конфигурации межсетевого экрана и маршрутизатора на предмет того, что входящий и исходящий трафик ограничен только тем трафиком, который необходим для среды ДДК. **1.2.1.c** Проверить конфигурации межсетевого экрана и маршрутизатора на предмет того, что весь прочий входящий и исходящий трафик явным образом запрещен, например, путем явного запрета "deny all" или неявного запрета по умолчанию после разрешающих правил.	Изучение всех входящих и исходящих соединений позволяет проверять и ограничивать трафик по адресу источника и (или) адресу назначения, тем самым предотвращая нефильтрованный доступ между недоверенными и доверенными средами. Этопредотвращает доступ злоумышленников к сети организации с несанкционированных IP-адресов или с использованием служб, протоколов или портов несанкционированным способом (например, для отправки на недоверенный сервер данных, которые злоумышленники получили из сети организации). Установка запрета на весь входящий и исходящий трафик, кроме явно необходимого, помогает предотвратить возникновение непреднамеренных брешей, которые делают возможным несанкционированный и потенциально вредоносный входящий или исходящий трафик.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.2.2 Обеспечить безопасность и синхронизацию конфигурационных файлов маршрутизаторов.	**1.2.2.a** Проверить конфигурационные файлы маршрутизаторов на предмет того, что они защищены от несанкционированного доступа. **1.2.2.b** Проверить конфигурации маршрутизаторов на предмет того, что они синхронизированы, например, что рабочий (или активный) и стартовый (используемый при загрузке устройств) конфигурационные файлы совпадают.	В то время как рабочие (или активные) конфигурационные файлы включают текущие безопасные настройки, в файлы стартовой конфигурации (используемые маршрутизаторами при перезапуске или загрузке) необходимо внести те же самые безопасные настройки для их применения при каждом запуске. Поскольку они выполняются только время от времени, о стартовых конфигурационных файлах часто забывают и не обновляют их. Если маршрутизатор выполняет перезапуск и загружает стартовую конфигурацию без безопасных настроек, которые имелись в рабочем конфигурационном файле, это может привести к применению менее безопасных правил, и этим могут воспользоваться злоумышленники для проникновения в сеть.
1.2.3 Установить пограничные межсетевые экраны между каждой беспроводной сетью и средой ДДК и настроить их так, чтобы они блокировали любой трафик, либо разрешали только авторизованный трафик – если такой трафик необходим в служебных целях – между беспроводной сетью и средой ДДК.	**1.2.3.a** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что межсетевые экраны установлены на периметре между всеми беспроводными сетями и средой ДДК. **1.2.3.b** Убедиться, что межсетевые экраны настроены так, чтобы блокировать любой трафик, либо разрешать только авторизованный трафик – если такой трафик необходим в служебных целях – между беспроводной сетью и средой ДДК.	Санкционированное (или несанкционированное) внедрение и использование беспроводных технологий в сети часто приводит к тому, что злоумышленники получают доступ к сети и ДДК. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может просто и незаметно проникнуть в сеть. Если межсетевые экраны не ограничивают доступ из беспроводной сети к среде ДДК, злоумышленники, которые получили несанкционированный доступ к беспроводной сети, могут без труда подключиться к среде ДДК и скомпрометировать данные платежных карт. Межсетевые экраны должны быть установлены между всеми беспроводными сетями и средой ДДК независимо от назначения среды, к которой подключена беспроводная сеть. Это могут быть, среди прочего, корпоративные сети, розничные

Требования PCI DSS	Проверочные процедуры	Пояснение
		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, демилитаризованную зону сегмента с ДДК, маршрутизатор на периметре и внутренний сегмент сети с ДДК. Проделать следующие действия, чтобы убедиться, что прямой доступ отсутствует между сетью Интернет и системными компонентами внутреннего сегмента сети с ДДК:	Могут быть легитимные основания для разрешения недоверенных соединений с системными компонентами, расположенными в демилитаризованной зоне (DMZ) (например, чтобы разрешить публичный доступ к веб-серверу), однако, такие соединения не могут быть разрешены системным компонентам во внутренней сети. Назначение межсетевого экрана состоит в управлении и контроле всех соединений между общедоступными системами и внутренними системами, особенно теми, которые используются для хранения, обработки или передачи ДДК. Если разрешен прямой доступ между общедоступными системами и средой ДДК, реализуемая межсетевым экраном защита обходится, и системные компоненты, хранящие ДДК, могут стать уязвимыми к компрометации.
1.3.1 Реализовать демилитаризованную зону таким образом, чтобы ограничить входящий трафик только теми системными компонентам, которые обеспечивают работу разрешенных общедоступных служб, протоколов и портов.	**1.3.1**Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что демилитаризованная зона реализована таким образом, чтобы входящий трафик был ограничен только теми системными компонентами, которые обеспечивают работу разрешенных общедоступных служб, протоколов и портов.	Демилитаризованная зона – это часть сети, которая управляет соединениями между сетью Интернет (или другими недоверенными сетями) и службами, к которым у организации есть необходимость предоставить публичный доступ (такими как веб-сервер). Такие функциональные возможности предназначены для предотвращения доступа злоумышленников к внутренней сети организации из Интернета и использования служб, протоколов или портов несанкционированным образом.
1.3.2 Ограничить входящий интернет-трафик IP-адресами, находящимися в демилитаризованной зоне.	**1.3.2** Проверить конфигурации межсетевого экрана и маршрутизатора на предмет того, что входящий интернет-трафик ограничен IP-адресами, находящимися в демилитаризованной зоне.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.3 Реализовать меры, которые противодействуют подмене IP-адреса благодаря тому, что позволяют определить фальшивые исходные IP-адреса и блокируют им доступ в сеть (например, блокируют трафик из сети Интернет, в котором в качестве адреса источника указан внутренний адрес).	**1.3.3** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что в них реализованы меры, которые противодействуют подмене IP-адреса (например, пакеты с внутренними адресами не могут попасть в демилитаризованную зону из сети Интернет).	Обычно пакет содержит IP-адрес компьютера, который его отправил. Это позволяет другим компьютерам в сети узнать, откуда был отправлен пакет. Злоумышленники часто пытаются подменить (или имитировать) IP-адрес отправителя так, чтобы система-получатель сочла, что пакет пришел из доверенного источника. Фильтрация входящих пакетов позволяет, помимо прочего, предотвратить подмену IP-адресов (имитацию адреса внутренней сети организации для пакета).
1.3.4 Запретить несанкционированный исходящий трафик из среды ДДК в сеть Интернет.	**1.3.4** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что исходящий трафик из среды ДДК в сеть Интернет явно авторизован.	Весь трафик, исходящий из среды ДДК, должен быть проверен на предмет его соответствия установленным и утвержденным правилам. Соединения должны быть проверены на предмет того, что трафик ограничивается только разрешенными соединениями (например, через ограничение адресов (портов) источника или назначения и (или) блокировку содержимого).
1.3.5 Разрешено пропускать в сеть пакеты только для установленных (“established”) соединений.	**1.3.5** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что межсетевой экран разрешает прохождение пакетов во внутреннюю сеть только для установленных соединений и отклоняет любые входящие соединения, если они не относятся к предварительно установленной сессии.	Межсетевой экран, отслеживающий состояние каждого соединения, проходящего через него, знает, являются ли пакеты, которые выглядят как ответ на предыдущее соединение, действительным авторизованным ответом (поскольку он хранит информацию о состоянии каждого соединения) или же это попытка вредоносного трафика обойти межсетевой экран, чтобы он разрешил соединение.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.6 Размещать системные компоненты, в которых хранятся ДДК (например, базы данных), во внутреннем сегменте сети, отделенном от демилитаризованной зоны и иных недоверенных сетей.	**1.3.6** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что системные компоненты, в которых хранятся ДДК, располагаются во внутреннем сегменте сети, отделенном от демилитаризованной зоны (DMZ) и иных недоверенных сетей.	Если ДДК размещены в демилитаризованной зоне, внешнему злоумышленнику проще получить эту информацию, поскольку ему нужно будет преодолеть меньшее количество уровней защиты. Защита системных компонентов, которые хранят ДДК, во внутреннем сегменте сети, отделенном от демилитаризованной зоны и иных недоверенных сетей межсетевым экраном, может предотвратить попадание несанкционированного сетевого трафика в системный компонент. ***Примечание:*** *это требование не распространяется на временное хранение ДДК в энергозависимой памяти.*
1.3.7 Не раскрывать частные IP-адреса и информацию о маршрутизации сторонам, не имеющим санкционированного доступа к такой информации. ***Примечание:*** *методы сокрытия IP-адресации включают, среди прочего:* • *преобразование сетевых адресов (NAT);* • *размещение серверов, содержащих ДДК, за прокси-серверами и (или) межсетевыми экранами;* • *удаление или фильтрацию объявлений о маршрутах для частных сетей, использующих открытое адресное пространство для зарегистрированных сетей;* • *внутреннее использование адресного пространства согласно RFC1918 вместо адресного пространства для зарегистрированных сетей.*	**1.3.7.a** Проверить конфигурации межсетевых экранов и маршрутизаторов на предмет того, что внедрены методы, исключающие раскрытие частных IP-адресов и данных о маршрутизации из внутренней сети в сеть Интернет. **1.3.7.b** Опросить работников и проверить документацию на предмет того, что любое раскрытие частных IP-адресов и данных о маршрутизации является санкционированным.	Ограничение передачи внутренних или частных IP-адресов необходимо для того, чтобы злоумышленник не имел возможности изучить IP-адреса внутренней сети и использовать эту информацию для получения доступа к сети. Средства, используемые для соблюдения этого требования, могут зависеть от конкретной используемой сетевой технологии. Например, меры, принятые для выполнения данного требования, могут отличаться для сетей IPv4 и сетей IPv6.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.4 Установить программные персональные межсетевые экраны или иную реализацию аналогичной функциональности на все портативные вычислительные устройства (например, используемые работниками ноутбуки), которые при нахождении вне сети подключены к сети Интернет и которые также используются для доступа к среде ДДК. Требования к конфигурациям межсетевых экранов или их аналогов: • определены конкретные настройки конфигурации; • персональные межсетевые экраны (или их аналоги) запущены; • настройки персональных межсетевых экранов (или их аналогов) не поддаются изменениям со стороны пользователей портативных вычислительныхустройств.	**1.4.a** Проверить политики и стандарты конфигурации на предмет того, что: • программные персональные межсетевые экраны или их аналоги требуются на всех портативных вычислительных устройствах, в том числе принадлежащих организации и (или) работникам, которые при нахождении вне сети подключены к сети Интернет (например, используемые работниками ноутбуки) и которые также используются для доступа к среде ДДК. • определены конкретные настройки конфигурации для персональных межсетевых экранов (или их аналогов); • персональные межсетевые экраны (или их аналоги) настроены на то, чтобы быть запущенными; • настройки персональных межсетевых экранов (или их аналогов) не поддаются изменениям со стороны пользователей портативных вычислительных устройств.	Переносные вычислительные устройства, которым разрешено подключаться к сети Интернет из сети, являющейся внешней по отношению к межсетевому экрану организации, более уязвимы к Интернет-угрозам. Использование функциональности межсетевого экрана (например, программного или аппаратного персонального межсетевого экрана) помогает защитить устройства от Интернет-атак, которые могут использовать устройство для получения доступа к системам и данным организации после повторного подключения устройства к сети. Организация сама определяет конкретные настройки конфигурации для персональных межсетевых экранов. ***Примечание:*** *это требование применяется к портативным вычислительным устройствам, принадлежащим работникам или организации. Системы, которыми невозможно управлять с помощью корпоративных политик, представляют собой уязвимые места и дают злоумышленникам возможности, которыми те могут воспользоваться. Разрешая недоверенным системам подключаться к среде ДДК организации, можно предоставить доступ атакующим и прочим злоумышленникам.*
	1.4.b Проверить выборку принадлежащих организации и (или) работникам устройств на предмет того, что: • персональные межсетевые экраны (или их аналоги) установлены и сконфигурированы согласно конкретным конфигурационным настройкам организации; • персональные межсетевые экраны (или их аналоги) запущены; • настройки персональных межсетевых экранов (или их аналогов) не поддаются изменениям со стороны пользователей портативных вычислительных устройств.	
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 работников на предмет того, что политики безопасности и рабочие процедуры управления межсетевыми экранами: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и рабочие процедуры, чтобы обеспечить постоянное управление межсетевыми экранами и маршрутизаторами во избежание несанкционированного доступа к сети.

Требование 2. Не использовать пароли к системам и другие параметры безопасности по умолчанию, заданные производителем.

Злоумышленники (внешние и внутренние по отношению к организации) часто используют для компрометации систем пароли и иные параметры по умолчанию, заданные производителем. Эти пароли и параметры хорошо известны в сообществах хакеров, и их легко получить из открытых источников.

Требования PCI DSS	Проверочные процедуры	Пояснение
2.1 Всегда изменять параметры по умолчанию, заданные производителями, а также удалять или отключать неиспользуемые 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, защитному программному обеспечению, учетным записям приложений и системным учетным записям, *POS-терминалам* (*терминалы в точках продаж), платежным приложениям, а также 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 учетные записи и пароли по умолчанию, устанавливаемые производителем, чтобы проверить, что ВСЕ пароли по умолчанию (включая пароли к операционным системам, защитному программному обеспечению, учетным записям приложений и системным учетным записям, POS-терминалам, а также строки доступа SNMP) были изменены. (Используйте руководства от вендоров и Интернет-ресурсы, чтобы узнать учетные записи и пароли по умолчанию, устанавливаемые производителем).	Злоумышленники (внешние и внутренние по отношению к организации) часто используют настройки, учетные записи и пароли по умолчанию, заданные производителем, для компрометации операционных систем, приложений и устройств, на которых они установлены. Поскольку эти настройки по умолчанию хорошо известны и часто публикуются в хакерских сообществах, их изменение снизит уязвимость систем к атакам. Даже если не планируется использовать учетную запись по умолчанию, 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 Проверить выборку системных компонентов на предмет того, что все неиспользуемые учетные записи по умолчанию (включая учетные записи к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям, устройствам, а также строки доступа SNMP и т. д.) удалены или отключены.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	2.1.c Опросить работников и проверить сопроводительную документацию на предмет того, что: • все учетные данные по умолчанию, заданные производителем (включая пароли по умолчанию к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям и системным учетным записям, а также строки доступа SNMP и т. д.) изменяются перед установкой системы в сети; • неиспользуемые учетные записи, настроенные по умолчанию, (включая учетные записи к операционным системам, POS-терминалам, защитному программному обеспечению, приложениям и системным учетным записям, а также строки доступа SNMP и т. д.) удаляются или отключаются перед установкой системы в сети.	
2.1.1 Для беспроводных окружений, которые подключены к среде ДДК либо передают ДДК, необходимо изменить ВСЕ параметры по умолчанию, заданные производителем, включая, помимо прочего, ключи шифрования для доступа к беспроводной сети, пароли, строки доступа SNMP.	**2.1.1.a** Опросить ответственных работников и проверить сопроводительную документацию на предмет того, что: • установленные по умолчанию ключи шифрования были изменены при установке; • ключи шифрования заменяются каждый раз, когда любое лицо, знающее данные ключи, увольняется из организации либо переходит на другую должность.	Если беспроводные сети реализованы без использования достаточно безопасных конфигураций (включая изменение настроек по умолчанию), анализаторы беспроводных сетей могут прослушивать трафик, без труда извлекать пароли и данные, а также легко проникать в сеть и атаковать ее. Кроме того, протокол обмена ключами для ранних версий протокола шифрования 802.11x (Wired Equivalent Privacy, WEP) был взломан, и может сделать шифрование бесполезным. Микропрограммное обеспечение для устройств следует обновить для поддержки более защищенных протоколов.
	2.1.1.b Опросить работников и проверить политики и процедуры на предмет того, что: • при установке требуется изменение строк доступа SNMP по умолчанию; • при установке требуется изменение паролей и (или) парольных фраз по умолчанию к точкам доступа.	
	2.1.1.c Проверить документацию вендора и выполнить вход на беспроводные устройства при содействии системного администратора, чтобы подтвердить, что: • не используются строки доступа SNMP по умолчанию; • не используются пароли и (или) парольные фразы по умолчанию к точкам доступа.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	2.1.1.d Проверить документацию вендора и настройки беспроводной конфигурации на предмет того, что микропрограммное обеспечение беспроводных устройств обновлено для того, чтобы поддерживать стойкие алгоритмы шифрования для: • аутентификации в беспроводных сетях; • передачи данных по беспроводным сетям.	
	2.1.1.e Проверить документацию вендора и настройки беспроводной конфигурации на предмет того, что прочие настройки безопасности по умолчанию, заданные производителем в беспроводных устройствах, были изменены, если это применимо.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2 Разработать стандарты конфигурации для всех системных компонентов. Убедиться в том, что стандарты учитывают все известные уязвимости, а также согласуются с положениями отраслевых стандартов безопасной настройки систем. Например, к источникам общепринятых отраслевых стандартов по безопасной настройке систем относятся, среди прочих: • 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** Проверить стандарты конфигурации организации для всех типов системных компонентов на предмет того, что эти стандарты согласуются с требованиями отраслевых стандартов безопасной настройки систем. **2.2.b** Проверить политики и опросить работников на предмет того, что стандарты конфигурации обновляются по мере обнаружения новых уязвимостей в соответствии с требованием 6.1. **2.2.c** Проверить политики и опросить работников на предмет того, что стандарты конфигурации применяются при настройке новых систем, и что перед установкой системы в сети выполняется проверка, что стандарты конфигурации выполнены. **2.2.d** Проверить стандарты системной конфигурации на наличие следующих процедур для всех типов системных компонентов: • изменить все параметры по умолчанию, заданные производителем, и исключить неиспользуемые 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; • реализовать дополнительные защитные меры для любых необходимых служб, протоколов и управляющих программ, которые признаны небезопасными; • настроить параметры безопасности системы таким образом, чтобы исключить возможность ее некорректного использования; • удалить все неиспользуемые функциональные возможности, такие как, скрипты, драйверы, функции, подсистемы, файловые системы, а также неиспользуемые веб-серверы.	У многих операционных систем, баз данных и корпоративных приложений существуют известные уязвимости, а также известные способы настройки данных систем для устранения этих уязвимостей. Чтобы помочь лицам, которые не являются экспертами в области безопасности, некоторые организации, специализирующиеся в области информационной безопасности, предоставляют рекомендации по безопасной настройке систем и устранению уязвимостей. К примерам источников, где можно найти рекомендации по стандартам настройки, относятся среди прочих: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org, а также веб-сайты вендоров. Стандарты конфигурации должны быть актуальными, чтобы гарантировать, что недавно обнаруженные уязвимости устраняются до установки системы в сети.

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 баз данных и DNS-серверы следует размещать на разных серверах). ***Примечание:*** *при использовании технологии виртуализации, необходимо реализовывать только одну основную функцию для каждого виртуального системного компонента.*	**2.2.1.a** Сделать выборку системных компонентов и проверить системные конфигурации на предмет того, что выполняется правило «один сервер — одна основная функция». **2.2.1.b** Если используются технологии виртуализации, проверить системные конфигурации на предмет того, что на одном виртуальном системном компоненте или устройстве реализована только одна основная функция.	Если функции, для которых необходим разный уровень безопасности, расположены на одном сервере, уровень безопасности функций с более высокими требованиями к безопасности будет понижен ввиду наличия функций с более низким уровнем безопасности. Кроме того, функции с более низким уровнем безопасности могут содержать уязвимости для безопасности других функций того же сервера. Путем рассмотрения требований к безопасности разных функций сервера в стандартах конфигураций и относящихся к ним процессах, организации могут убедиться в отсутствии функций с разными уровнями 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 и проверить включенные службы, управляющие программы и протоколы на предмет того, что включены только необходимые службы или протоколы. **2.2.2.b** Выявить любые включенные небезопасные службы, управляющие программы и протоколы, и опросить работников на предмет того, что использование таких служб, управляющих программ и протоколов обосновано в документированных стандартах конфигурации.	Как сказано в требовании 1.1.6, существует много протоколов, которые могут быть необходимы для работы (или включены по умолчанию) и которые обычно используются злоумышленниками для компрометации сети. Включение этого требования в стандарты конфигурации и относящиеся к ним процессы организации гарантирует, что будут включены только необходимые службы и протоколы.
2.2.3 Внедрить дополнительные защитные меры для любых необходимых служб, протоколов и управляющих программ, которые признаны небезопасными. ***Примечание:*** *в случаях, когда*	**2.2.3.a** Проверить настройки конфигурации на предмет того, что защитные меры документированы и внедрены для всех небезопасных служб, управляющих программ и протоколов.	Включение защитных мер до развертывания новых серверов исключит установку серверов в среду с небезопасной конфигурацией. Надлежащая защита всех небезопасных служб, протоколов и управляющих программ с помощью соответствующих защитных мер

Требования PCI DSS	Проверочные процедуры	Пояснение
используется SSL и (или) ранние версии TLS, требования, описанные в Приложении A2, должны быть выполнены.	**2.2.3.b** Если используется SSL и (или) ранние версии TLS, выполнить проверочные процедуры, описанные в *Приложении A2: Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS.*	затруднит злоумышленникам использование распространенных уязвимостей через сеть. Для получения информации о стойкой криптографии и безопасных протоколах необходимо обратиться к отраслевым стандартам и передовому опыту (например, NIST SP 800-52 и SP 800-57, OWASP и т.д.).
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 безопасности на предмет того, что им известны настройки основных параметров безопасности системных компонентов.	Стандарты конфигурации и относящиеся к ним процессы должны явным образом учитывать настройки и параметры безопасности, которые несут в себе известные последствия для безопасности каждого типа используемой системы. Чтобы обеспечить безопасную настройку систем, работники, отвечающие за настройку и (или) администрирование систем, должны быть осведомлены о конкретных параметрах безопасности и настройках, применимых к системе.
	2.2.4.b Проверить стандарты конфигурации на предмет того, что они включают основные параметры безопасности.	
	2.2.4.c Сделать выборку системных компонентов и проверить основные параметры безопасности на предмет того, что они выставлены надлежащим образом и согласно стандартам конфигурации.	
2.2.5 Удалить все неиспользуемые функциональные возможности, например, скрипты, драйверы, функции, подсистемы, файловые системы, а также неиспользуемые веб-серверы.	**2.2.5.a** Сделать выборку системных компонентов и проверить конфигурации на предмет того, что неиспользуемые функциональные возможности (например, скрипты, драйверы, функции, подсистемы, файловые системы и т. д.) удалены.	Неиспользуемые функции могут предоставить злоумышленникам дополнительные возможности для получения доступа к системе. Благодаря удалению неиспользуемых функциональных возможностей, организация может сконцентрироваться на защите требуемых функций и снизить риск злоупотребления неизвестными функциями. Включение этого требования в стандарты и процессы безопасной настройки обрабатывает последствия для безопасности, связанные с неиспользуемыми функциями (например, удаление и (или) отключение FTP- или веб-сервера, если сервер не будет выполнять такие функции).
	2.2.5.b Проверить документацию и параметры безопасности на предмет того, что включенные функции документированы и поддерживают безопасную конфигурацию.	
	2.2.5.c Проверить документацию и параметры безопасности на предмет того, что в выборке системных компонентов присутствуют только документированные функциональные возможности.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.3 При использовании любого неконсольного административного доступа к системе всегда шифровать канал с использованием стойкой криптографии. ***Примечание:*** *в случаях, когда используется SSL и (или) ранние версии TLS, требования, описанные в Приложении A2, должны быть выполнены.*	**2.3** Сделать выборку системных компонентов и проверить, что канал неконсольного административного доступа зашифрован следующим образом:	Если при неконсольном (в т. ч. удаленном) администрировании не используются безопасная аутентификация и шифрование канала, существует возможность перехвата злоумышленником критичной информации (например, идентификаторов и паролей администратора). Злоумышленник может использовать эту информацию для получения доступа к сети, получения прав администратора и кражи данных. Незашифрованные протоколы (например, HTTP, Telnet и т. д.) передают трафик или аутентификационные данные в открытом виде, упрощая перехват этой информации злоумышленником. Для того чтобы криптография была признана стойкой, следует применять признанные в отрасли протоколы с надлежащей стойкостью ключей и процессы управления ключами, соответствующие типу используемой технологии. (См. определение термина «стойкая криптография» в документе *Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS*, а также отраслевые стандарты и передовой опыт, такие как NIST SP 800-52 и SP 800-57, OWASP и т.д.).
	2.3.a Проследить за входом администратора в каждую систему и проверить системные конфигурации на предмет того, что метод стойкого шифрования применяется до запроса пароля администратора.	
	2.3.b Проверить службы и файлы параметров на системах на предмет того, что Telnet и другие небезопасные протоколы удаленного доступа к системе недоступны 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 вендора и опросить работников на предмет того, что для используемых технологий используется стойкая криптография, и что она внедрена в соответствии с передовым опытом и (или) рекомендациями вендоров.	
	2.3.e Если используется SSL и (или) ранние версии TLS, выполнить проверочные процедуры, описанные в *Приложении A2: Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS.*	
2.4Вести учет системных компонентов, на которые распространяется действие стандарта PCI DSS.	**2.4.a** Проверить системный учет на предмет того, что поддерживается список программных и аппаратных компонентов, включающий описание функции и (или) применения для каждого из них.	Благодаря ведению текущего списка всех системных компонентов, организация может точно и эффективно определять область своей среды для внедрения защитных мер PCI DSS. Без такого учета некоторые системные компоненты могут быть забыты или случайно исключены из стандартов конфигурации организации.
	2.4.b Опросить работников на предмет того, что учетная документация поддерживается в актуальном состоянии.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.5 Гарантировать, что политики безопасности и операционные процедуры управления параметрами по умолчанию, заданными производителями, и другими параметрами безопасности документированы, используются и известны всем заинтересованным лицам.	**2.5** Проверить документацию и опросить работников на предмет того, что политики безопасности, операционные процедуры управления параметрами по умолчанию, заданными производителями, и другими параметрами безопасности: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны быть ознакомлены с политиками безопасности и повседневными операционными процедурами, а также соблюдать их, чтобы обеспечить постоянный контроль над параметрами по умолчанию, заданными производителями, и другими параметрами безопасности и исключить небезопасные конфигурации.
2.6 Поставщики услуг хостинга с общей средой должны защищать среды и ДДК каждой организации, размещенные на хостинге. Эти поставщики должны соответствовать особым требованиям, описанным в *Приложении A1: «Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой»*.	**2.6** Выполнить проверочные процедуры **A.1.1**–**A.1.4**, описанные в *Приложении A1: «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 (ТСП и поставщиков услуг).	Данное требование предназначено для поставщиков услуг хостинга, которые предоставляют общие среды размещения для нескольких клиентов на одном и том же сервере. Когда все данные находятся на одном и том же сервере и под управлением единой среды, отдельные клиенты обычно не имеют возможности управлять настройками этих совместно используемых серверов. Это позволяет клиентам добавлять небезопасные функции и скрипты, которые влияют на безопасность сред всех остальных клиентов, и таким образом, злоумышленник может, получив доступ к данным одного клиента, скомпрометировать данные всех остальных клиентов. См. подробные сведения о требованиях в *Приложении A1*.

Защищать ДДК

Требование 3. Защищать хранимые ДДК

Такие методы защиты, как шифрование, усечение, маскирование и хеширование являются важнейшими компонентами защиты ДДК. Если злоумышленник обходит иные защитные меры и получает доступ к зашифрованным данным без надлежащего криптографического ключа, то эти данные остаются для злоумышленника нечитаемыми и непригодными для использования. Иные эффективные методы защиты хранимых данных также следует рассматривать как потенциальные возможности снижения риска. Например, методы минимизации риска включают в себя отказ от хранения ДДК, кроме случаев крайней необходимости, усечение ДДК, если полный PAN не требуется, и отказ от передачи PAN в незащищенном виде с использованием технологий обмена сообщениями для конечных пользователей, таких как электронная почта и системы мгновенного обмена сообщениями.

См. *«Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS»* для определения термина «Стойкая криптография» и других терминов PCI DSS.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.1 Свести хранение ДДК к минимуму с помощью политик, процедур и процессов хранения и уничтожения данных, в которые включены, как минимум, следующие требования для всех хранилищ ДДК: • ограничение количества хранимых данных и сроки хранения до значений, необходимых для выполнения законодательных, нормативных и (или) служебных требований; • конкретные требования к хранению ДДК; • процессы безопасного удаления данных, когда в них уже нет	**3.1.a** Проверить политики, процедуры и процессы хранения и уничтожения данных на предмет наличия в них следующих требований для всех хранилищ ДДК: • ограничение количества хранимых данных и сроков хранения до значений, необходимых для выполнения законодательных, нормативных и (или) служебных требований; • конкретные требования к хранению ДДК (например, ДДК требуется хранить в течение срока X по причинам Y); • процессы безопасного удаления ДДК, если в их хранении больше нет необходимости в соответствии с законодательными, нормативными или служебными требованиями; • наличие ежеквартального процесса обнаружения и безопасного удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	Официальная политика хранения данных определяет, какие данные необходимо хранить и где находятся эти данные, чтобы их можно было безопасно уничтожить или удалить, когда они больше не требуются. После авторизации разрешается хранить только номер карты (PAN) (приведенный в нечитаемый вид), дату истечения срока действия, имя держателя карты и сервисный код. Знание мест хранения ДДК необходимо для их надлежащего хранения или удаления, когда они больше не требуются. Чтобы определить надлежащие требования к хранению, организации сначала следует выяснить свою

Требования PCI DSS	Проверочные процедуры	Пояснение
необходимости; • ежеквартальный процесс обнаружения и безопасного удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	**3.1.b** Опросить работников на предмет того, что: • все места хранения ДДК включены в процессы хранения и удаления данных; • реализован ежеквартальный процесс обнаружения и безопасного удаления ДДК, проводимый вручную или автоматически; • этот процесс реализуется для всех мест хранения ДДК.	служебную необходимость, а также любые законодательные или нормативные требования, которые применимы к ее отрасли и (или) к типу хранимых данных.
	3.1.c Для выборки системных компонентов, которые хранят ДДК: • проверить файлы и системные записи на предмет того, 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 можно автоматизировать (полностью или частично) или выполнять вручную. Например, можно запрограммировать процедуру обнаружения и удаления данных (автоматическую или ручную) и (или) проверять места хранения данных вручную. Внедрение методов безопасного удаления данных гарантирует, что данные, когда они больше не требуются, восстановить будет невозможно. ***Важно! Не хранить данные, если они не нужны!***
3.2 Запрещается хранить КАД после авторизации (даже в зашифрованном виде). Если КАД получены, следует сделать все данные невосстановимыми до завершения процесса авторизации. *Эмитенты и компании, которые поддерживают услуги эмиссии, могут хранить КАД, если:*	**3.2.a** Для эмитентов и (или) компаний, поддерживающих услуги эмиссии и хранящих КАД, проверить политики и опросить работников на предмет того, что у этих организаций есть документированное обоснование для хранения КАД.	КАД состоят из полных данных треков, кода или значения проверки подлинности карты и данных ПИН-кода. Хранить КАД после авторизации запрещается! Эти данные представляют большую ценность для злоумышленников, т.к. последние, используя такие данные, могут генерировать поддельные платежные карты и осуществлять мошеннические транзакции.
	3.2.b Для эмитентов и (или) компаний, поддерживающих услуги эмиссии и осуществляющих хранение КАД, проверить места хранения данных и системные конфигурации на предмет того, что КАД защищены.	

Требования PCI DSS	Проверочные процедуры	Пояснение
• имеется служебное обоснование, и • данные хранятся безопасно. К КАД относятся данные, перечисленные в требованиях 3.2.1 – 3.2.3.	**3.2.c** Для всех других организаций, если организация принимает КАД, проверить политики, процедуры и системные конфигурации на предмет того, что данные не сохраняются после авторизации.	Эмитенты платежных карт или компании, которые оказывают или поддерживают услуги эмиссии, часто создают и контролируют КАД в рамках процесса эмиссии. Компаниям, которые оказывают, содействуют или поддерживают услуги выпуска карт, разрешается хранить КАД ТОЛЬКО В ТОМ СЛУЧАЕ, если у них есть в этом обоснованная служебные необходимость. Следует отметить, что все требования стандарта PCI DSS распространяются на эмитентов, и единственное исключение для эмитентов и их процессинговых центров заключается в том, что они могут хранить КАД, если у них в этом есть обоснованная потребность. Под такой потребностью понимается не удобство, а необходимость для выполнения эмитентом своей функции. Любые такие данные должны храниться безопасно, в соответствии с требованиями стандарта PCI DSS и требованиями конкретной международной платежной системы.
	3.2.d Для всех других организаций, если организация принимает КАД, проверить процедуры и процессы безопасного удаления данных на предмет того, что данные восстановить невозможно.	Для неэмитентов хранение КАД после авторизации запрещено.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.2.1 Запрещается хранить полное содержимое любого трека (магнитной полосы на обратной стороне карты, эквивалентных данных на чипе или в ином месте) после авторизации. Эти данные также называются «полные данные треков», «трек», «трек 1», «трек 2» и «данные магнитной полосы». ***Примечание:*** *для повседневного ведения деятельности может быть необходимо хранение следующих элементов данных магнитной полосы:* • *имя держателя карты;* • *номер карты (PAN);* • *дата истечения срока действия карты;* • *сервисный код.* *Для минимизации рисков храните только те элементы данных, в хранении которых есть служебная необходимость.*	**3.2.1** Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что полные данные любого трека магнитной полосы, находящейся на обратной стороне карты (или ее аналога на чипе), не сохраняются после авторизации: • входящие данные о транзакции; • все журналы (например, журналы транзакций, хронологии, отладки, ошибок); • файлы хронологии; • файлы трассировки; • несколько схем баз данных; • содержимое баз данных.	Если сохранены полные данные треков, злоумышленники, получившие доступ к этим данным, могут использовать их для воспроизведения платежных карт и осуществления мошеннических транзакций.
3.2.2 Запрещается хранить код или значение проверки подлинности карты (трех- или четырехзначное число, напечатанное на лицевой или обратной стороне карты, используемые для подтверждения транзакций, выполняемых без предоставления платежной карты) после авторизации.	**3.2.2** Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что трех- или четырехзначный код или значение проверки подлинности карты, напечатанные на лицевой стороне карты или на месте для подписи (данные CVV2, CVC2, CID, CAV2), не сохраняются после авторизации: • входящие данные о транзакции; • все журналы (например, журналы транзакций, хронологии, отладки, ошибок); • файлы хронологии; • файлы трассировки; • несколько схем баз данных; • содержимое баз данных.	Код проверки подлинности карты предназначен для защиты операций без предоставления платежной карты (например, при оплате через Интернет, по почте или по телефону, т. е. в транзакциях, где не присутствуют ни карта, ни ее держатель). В случае кражи этих данных, злоумышленник получит возможность совершения мошеннических транзакций через Интернет, по почте или телефону.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.2.3 Запрещается хранить ПИН-код или зашифрованный ПИН-блок после авторизации.	**3.2.3** Проверить источники данных в выборке системных компонентов, включая перечисленные ниже, на предмет того, что ПИН-коды, а также зашифрованные ПИН-блоки не сохраняются после авторизации: • входящие данные о транзакции; • все журналы (например, журналы транзакций, хронологии, отладки, ошибок); • файлы хронологии; • файлы трассировки; • несколько схем баз данных; • содержимое баз данных.	Данные значения должны быть известны только держателю карты или банку-эмитенту карты. В случае кражи этих данных злоумышленник получит возможность совершения мошеннических дебетовых транзакций с использованием ПИН-кода (например, для получения наличных через банкомат).
3.3 Маскировать PAN при его отображении (максимально возможное количество отображаемых цифр – первые шесть и последние четыре), чтобы только работники с обоснованной служебной необходимостью могли видеть больше чем первые шесть и (или) последние четыре цифры PAN. ***Примечание:*** *это требование не заменяет собой существующие более строгие требования к отображению ДДК (например, требования законодательства или международных платежных систем к чекам POS-терминалов).*	**3.3.a** Проверить письменные политики и процедуры маскирования PAN при его отображении на предмет того, что: • список ролей, которым требуется доступ к больше чем первые шесть и (или) последние четыре цифры (в том числе полный PAN), документирован, и для каждой роли обоснована служебная необходимость такого доступа; • PAN должен маскироваться при отображении, так чтобольше чем первые шесть и (или) последние четыре цифры PAN видны только тем работникам, у которых на то есть служебная необходимость; • для всех ролей, которым явным образом не разрешено видеть полный PAN, должен быть виден только маскированный PAN. **3.3.b** Проверить системные конфигурации на предмет того, что полный PAN отображается только для пользователей и (или) ролей, у которых есть документированная служебная необходимость, и маскируется для всех остальных запросов.	Отображение полного PAN на экранах компьютеров, чеках об оплатах с использованием платежных карт, факсах или в бумажных отчетах может привести к тому, что эти данные станут известны посторонним лицам и могут быть использованы в мошеннических целях. Отображение полного PAN только тем лицам, у которых есть такая обоснованная служебная необходимость, минимизирует риски того, что посторонние лица получат доступ к данным PAN. Метод маскирования всегда должен обеспечивать отображение минимального количества цифр, которые необходимы для выполнения конкретной производственной функции. Например, если только последние четыре цифры нужны для выполнения производственной функции, PAN маскируется так, что работник, выполняющий данную

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.3.c Проверить варианты отображения PAN (например, на экране, на бумажных квитанциях) на предмет того, что эти номера маскируются при отображении ДДК и чтобольше чем первые шесть и (или) последние четыре цифры PAN видны только лицам, у которых есть обоснованная служебная необходимость.	функцию, может видеть только последние четыре цифры. Другой пример: если производственная необходимость требует доступ к банковскому идентификационному номеру (BIN) для маршрутизации, отображаются только цифры BIN (обычно это первые шесть цифр) в течение выполнения этой производственной функции. Это требование касается защиты PAN, ***отображаемого*** на экранах, бумажных квитанциях, распечатках и т. д., и его следует отличать от требования 3.4, которое касается защиты PAN при его ***хранении*** в файлах, базах данных и т. д.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.4 Привести PAN к нечитаемому виду во всех местах их хранения (включая журналы, резервные копии, съемные цифровые носители), используя для этого любой из следующих методов: • однонаправленное хеширование на основе стойкой криптографии (хеш-код должен быть сформирован из целого PAN); • усечение (хеш-код не может использоваться для замены усеченного сегмента PAN); • индексные маркеры и шифровальные блокноты (такие блокноты при хранении должны быть защищены); • стойкая криптография с сопутствующими процессами и процедурами управления ключами. ***Примечание:*** *при наличии доступа к PAN одновременно в усеченном и хешированном виде злоумышленнику будет несложно восстановить исходный PAN. Если в среде организации содержится PAN одновременно в усеченном и хешированном виде, должны быть введены дополнительные защитные меры, чтобы исключить возможность корреляции PAN в усеченном и хешированном виде и возможность восстановления исходного PAN.*	**3.4.a** Проверить документацию о системе, используемой для защиты PAN, в том числе информацию о ее вендоре, типе системы и (или) процесса, алгоритмах шифрования (при использовании таковых) на предмет того, что PAN приводится к нечитаемому виду с использованием одного из следующих методов: • однонаправленного хеширования на основе стойкой криптографии; • усечения; • индексных маркеров и шифровальных блокнотов, причем такие блокноты при хранении должны быть защищены; • стойкой криптографии с сопутствующими процессами и процедурами управления ключами. **3.4.b** Проверить несколько таблиц или файлов из выборки хранилищ данных на предмет того, что PAN приведены к нечитаемому виду (т. е. не хранятся как незашифрованный текст). **3.4.c** Проверить выборку съемных носителей (например, магнитные ленты с резервными копиями данных) на предмет того, что PAN на данных носителях приведены к нечитаемому виду. **3.4.d** Проверить выборку журналов аудита, включая журналы платежных приложений, на предмет того, что PAN приведены в них к нечитаемому виду или отсутствуют в журналах.	Защитить все 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 отладки и т. д.). Для приведения ДДК к нечитаемому виду можно использовать функции однонаправленного хеширования на основе стойкой криптографии. Их использование целесообразно тогда, когда нет необходимости в восстановлении исходного номера (так как однонаправленное хеширование является необратимым). Желательно (но на данный момент не является требованием) добавлять дополнительное входное значение к ДДК перед хешированием, чтобы у злоумышленника было меньше возможностей для сравнения данных (и получения PAN) с таблицами предварительно подсчитанных значений хеша. Цель усечения заключается в том, чтобы окончательно удалять часть PAN, так что только часть PAN(как правило, не больше шести первых и четырех последних цифр) хранится. Индексный маркер – это криптографический маркер, который заменяет PAN, основанный на определенном индексе значений, не поддающихся вычислению. Одноразовый блокнот – это система, в которой секретный ключ, сгенерированный случайным образом, используется только один раз для шифрования сообщения, которое затем

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.4.e Если в среде организации содержится PAN одновременно в усеченном и хешированном виде, проверить применяемые меры контроля на предмет того, что хешированная и усеченная версии PAN не могут быть скоррелированы для восстановления PAN в исходном виде.	расшифровывается с помощью соответствующего одноразового блокнота и ключа. Цель стойкой криптографии (см. определение в документе *Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS*) заключается в том, что шифрование должно быть основано на использовании протестированных и общепринятых отраслевых алгоритмов с высокой надежностью криптографических ключей (а не проприетарных или «самописных» алгоритмов). Сопоставляя хешированные и усеченные версии PAN, злоумышленник может без труда вычислить исходный PAN. Меры, которые используются, чтобы предотвратить сопоставление этих данных, помогают обеспечить нечитаемость исходного PAN.
3.4.1 Если используется шифрование диска (вместо шифрования на уровне файлов или шифрования базы данных на уровне столбцов), то управление логическим доступом должно осуществляться отдельно и независимо от нативных механизмов аутентификации и контроля доступа операционной системы (например, путем отказа от использования локальных баз данных учетных записей пользователей или основных учетных данных для входа в сеть). Ключи расшифрования не	**3.4.1.a** Если применяется шифрование диска, проверить конфигурацию и проследить за процессом аутентификации на предмет того, что логический доступ к зашифрованной файловой системе реализован при помощи механизма, независимого от нативных механизмов аутентификации операционной системы (например, путем отказа от использования локальных баз данных учетных записей или основных учетных данных для входа в сеть). **3.4.1.b** Проследить за процессами и опросить работников на предмет того, что криптографические ключи хранятся безопасно (например, на съемном носителе, который достаточно защищен надежными механизмами контроля доступа).	Цель этого требования состоит в том, чтобы определить условия, при которых можно использовать шифрование на уровне диска для приведения ДДК к нечитаемому виду. При шифровании диска в компьютере шифруется весь жесткий диск или раздел, а информация автоматически расшифровывается, когда ее запрашивает авторизованный пользователь. 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

Требования PCI DSS	Проверочные процедуры	Пояснение
должны быть связаны с учетными записями пользователей. ***Примечание:*** *это требование применяется в дополнение ко всем остальным требованиям PCI DSS по шифрованию и управлению ключами.*	**3.4.1.c** Проверить конфигурации и проследить за процессами на предмет того, что ДДК на съемных носителях хранятся только в зашифрованном виде. ***Примечание:*** *если шифрование диска не используется для шифрования съемных носителей, данные на таких съемных носителях должны быть приведены к нечитаемому виду с использованием какого-либо другого метода.*	предоставления пароля или парольной фразы при запуске системы или в начале сеанса. С учетом этих особенностей шифрования на уровне диска, для того, чтобы соответствовать данному требованию, метод шифрования не должен: 1) использовать тот же аутентификатор пользователя, что и операционная система; или 2) использовать ключ расшифрования, связанный или взятый из локальных баз данных учетных записей или основных учетных данных для входа в сеть. Полное шифрование диска помогает защитить данные в случае физической утраты диска и, следовательно, может быть целесообразно для портативных устройств, содержащих ДДК.
3.5 Документировать и внедрить процедуры защиты ключей, используемых для защиты хранимых ДДК от раскрытия или злоупотребления, следующим образом. ***Примечание:*** *это требование применяется к ключам шифрования хранимых ДДК, а также к ключам шифрования ключей, используемым для защиты ключей шифрования данных. Такие ключи должны обладать, как минимум, такой же надежностью, как и ключи шифрования данных.*	**3.5** Проверить политики и процедуры управления ключами на предмет того, что определены процессы для защиты ключей шифрования ДДК от раскрытия или злоупотребления, и в этих процессах предусмотрено, как минимум, следующее: • доступ к ключам шифрования ограничен минимально необходимым количеством хранителей ключа; • ключи шифрования ключей должны обладать такой же криптографической стойкостью, как и ключи шифрования данных, которые они защищают; • ключи шифрования ключей хранятся отдельно от ключей шифрования данных; • ключи хранятся безопасно в минимально возможном количестве мест и форм хранения.	Криптографические ключи должны быть надежно защищены, поскольку лица, получившие к ним доступ, смогут расшифровать данные. Ключи шифрования ключей, при использовании таковых, должны обладать, как минимум, такой же криптографической стойкостью, что и ключи шифрования данных. Это необходимо, чтобы обеспечить надлежащую защиту ключей шифрования данных, и самих данных, которые шифруются с использованием этих ключей. Требование по защите ключей от раскрытия и злоупотребления распространяется как на ключи шифрования ключей, так и на ключи шифрования данных. Поскольку один ключ шифрования ключей может предоставить доступ ко многим ключам шифрования данных, ключи шифрования ключей требуют надежных защитных мер.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5.1 ***Дополнительное требование только для поставщиков услуг***: вести документальное описание криптографической архитектуры, включающей: • детальную информацию о всех алгоритмах, протоколах и ключах, которые используются для защиты ДДК, в том числе стойкость ключа и дата окончания действия ключа; • описание назначения каждого из ключей; • учет любых HSM и SCD, которые используются для управления ключами. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**3.5.1** Опросить ответственных работников и проверить документацию на предмет того, что документ существует и описывает криптографическую архитектуру, включая: • детальную информацию о всех алгоритмах, протоколах и ключах, которые используются для защиты ДДК, в том числе стойкость ключа и дата окончания действия ключа; • описание назначения каждого из ключей; • учет любых HSM и SCD, которые используются для управления ключами.	***Примечание:*** *это требование применяется, только когда организация определена как поставщик услуг.* Ведение актуальной документации, описывающей криптографическую архитектуру, позволяет организации понимать, какие алгоритмы, протоколы и криптографические ключи используются для защиты ДДК, а также какие устройста генерируют, используют и защищают ключи. Это позволяет организации не отставать от меняющихся угроз для ее архитектуры и планировать обновления для обеспечения защиты с помощью изменения различных алгоритмов и (или) стойкости ключей. Ведение такой документации также позволяет организации выявлять потеренные ключи или устройства по управлению ключами и несанкционированные добавления в ее криптографическую архитектуру.
3.5.2 Ограничить доступ к криптографическим ключам минимально необходимым числом хранителей ключа.	**3.5.2** Проверить списки доступа пользователей на предмет того, что доступ к ключам ограничен минимально необходимым числом хранителей ключа.	Следует сократить до минимума количество лиц, имеющих доступ к криптографическим ключам (тем самым сокращая возможности раскрытия ДДК посторонним лицам). Обычно такими лицами являются работники, назначенные хранителями ключей.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5.3 Всегда хранить секретные и закрытые ключи шифрования и (или) расшифрования ДДК в одной (или более) форм из следующего перечня: • защищенные ключом шифрования ключей, который имеет такую же криптографическую стойкость, как и ключ шифрования данных, и хранится отдельно от ключа шифрования данных; • в защищенном криптографическом устройстве (таком как аппаратный модуль безопасности (HSM) или POI-терминал, утвержденный согласно требованиям PCI PTS); • в форме как минимум двух компонентов ключа полной длины или в форме разделяемого секрета в соответствии с принятым в отрасли методом. ***Примечание:*** *хранение публичных ключей в одной из этих форм не требуется.*	**3.5.3.a** Проверить документированные процедуры на предмет того, что криптографические ключи шифрования и (или) расшифрования ДДК должны существовать только в одной (или более) форм из следующего перечня: • защищенные ключом шифрования ключей, который имеет такую же криптографическую стойкость, как и ключ шифрования данных, и хранится отдельно от ключа шифрования данных; • 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 соответствии с принятым в отрасли методом.	Криптографические ключи должны храниться безопасно для предотвращения несанкционированного или ненужного доступа, который может привести к раскрытию ДДК. Это требование не подразумевает, что ключи шифрования ключей должны быть зашифрованы, но они должны быть защищены от раскрытия и злоупотребления в соответствии с требованием 3.5. Если используются ключи шифрования ключей, их хранение в местах, физически и (или) логически отделенных от ключей шифрования данных, снижает риск несанкционированного доступа к тем и другим ключам.
	3.5.3.b Проверить системные конфигурации и места хранения ключей на предмет того, что криптографические ключи шифрования ДДК всегда существуют в одной (или более) форм из следующего перечня: • защищенные ключом 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 соответствии с принятым в отрасли методом.	
	3.5.3.c Если используются ключи шифрования ключей, проверить системные конфигурации и места хранения ключей на предмет того, что: • ключи шифрования ключей обладают такой же криптографической стойкостью, что и ключи шифрования данных, которые они защищают; • ключи шифрования ключей хранятся отдельно от ключей шифрования данных.	

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5.4 Хранить криптографические ключи в минимально возможном количестве мест расположения.	**3.5.4** Проверить места хранения ключей и проследить за процессами на предмет того, что ключи хранятся в минимально возможном количестве мест расположения.	Хранение криптографических ключей шифрования в минимально возможном количестве мест расположения помогает организации отслеживать и осуществлять мониторинг всех мест хранения ключей и снижает вероятность раскрытия ключей посторонним лицам.
3.6 Полностью документировать и внедрить все процессы и процедуры управления криптографическими ключами шифрования ДДК, в том числе: ***Примечание:*** *существует множество различных источников, из которых можно получить информацию о стандартах управления ключами (например, сайт института NIST - http://csrc.nist.gov).*	**3.6.a** ***Дополнительная проверочная процедура для поставщиков услуг:*** если поставщик услуг предоставляет клиентам ключи шифрования для передачи или хранения ДДК, проверить документацию, которую поставщик услуг предоставляет клиентам, на наличие в ней рекомендаций о том, как безопасно передавать, хранить и обновлять ключи клиентов, в соответствии с требованиями 3.6.1–3.6.8, приведенными ниже. **3.6.b** Проверить процедуры и процессы управления ключами шифрования ДДК и выполнить следующее:	Способ управления криптографическими ключами представляет собой критичную часть непрерывного обеспечения безопасности средства шифрования. В основе правильно организованного процесса управления ключами, вне зависимости от того, выполняется ли он вручную или автоматически в составе продукта шифрования, лежат отраслевые стандарты, и такой процесс учитывает все основные требования с 3.6.1 по 3.6.8. Предоставление потребителям рекомендаций по безопасной передаче, хранению и обновлению криптографических ключей помогает предотвратить неправильное управление ключами или их раскрытие посторонним организациям. Данное требование применяется к ключам шифрования хранимых ДДК, и любым соответствующим ключам шифрования ключей. ***Примечание:*** *проверочная процедура 3.6.a является дополнительной процедурой, применяемой только для организаций, которые определены как поставщики услуг.*
3.6.1 Генерировать криптографически стойкие ключи	**3.6.1.a** Убедиться, что процедуры управления ключами указывают, каким образом следует генерировать стойкие ключи.	Средство шифрования должно генерировать стойкие ключи согласно определению для термина «генерация криптографических

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.6.1.b Пронаблюдать процедуры генерации ключей на предмет того, что генерируются стойкие ключи.	ключей», приведенному в документе «Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS». Использование стойких криптографических ключей значительно повышает уровень безопасности зашифрованных ДДК.
3.6.2 Распространять криптографические ключи безопасным образом	**3.6.2.a** Убедиться, что процедуры управления ключами указывают, как безопасным образом распространять ключи.	Средство шифрования должно обеспечивать безопасный способ распространения ключей (то есть ключи не должны распределяться в незашифрованном виде), и только среди хранителей ключа, указанных в требовании 3.5.1.
	3.6.2.b Проверить метод распространения ключей на предмет того, что они распространяются безопасным образом.	
3.6.3 Защита хранения криптографических ключей	**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 с использованием ключа шифрования ключей). Хранение ключей без надлежащей защиты может дать злоумышленникам доступ, который приведет к расшифрованию и раскрытию ДДК.
	3.6.3.b Проверить метод хранения ключей на предмет того, что ключи хранятся в безопасности.	
3.6.4 Заменять криптографические ключи с истекшим криптопериодом (например, по прошествии определенного срока действия и (или) получении с помощью данного ключа определенного объема шифротекста) в соответствии с указаниями соответствующего вендора приложений или владельца ключа и на основании отраслевых рекомендаций и руководств (например, специальной публикации NIST 800-57).	**3.6.4.a** Убедиться, что процедуры управления ключами устанавливают криптопериод для каждого типа используемых ключей, а также определяют процесс их замены по завершении установленного криптопериода (криптопериодов).	Отрезок времени, в течение которого определенный криптографический ключ может использоваться по определенному для него назначению. Определяя криптопериод, следует учитывать, среди прочего: надежность используемого алгоритма, размер или длину ключа, риск компрометации ключа и критичность шифруемых данных. Когда криптопериод ключей шифрования подходит к концу, их следует периодически менять, чтобы минимизировать риск того, что злоумышленник получит ключи шифрования и сможет использовать их для расшифрования данных.
	3.6.4.b Опросить работников на предмет того, 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, если ослаблена целостность ключа (например, уволился работник, знающий компонент ключа в незашифрованном виде) либо есть подозрения, что ключи скомпрометированы. ***Примечание:*** *если существует необходимость сохранения изъятых из обращения или замененных ключей, следует заархивировать их безопасным образом (например, с использованием ключа шифрования ключей). Использовать помещенные в архив криптографические ключи только для расшифрования и (или) верификации.*	**3.6.5.a** Проверить процедуры управления ключами на предмет того, что они определяют следующие процессы: • изъятие либо замена ключей в случае ослабления целостности; • замена ключей, которые были или могли быть скомпрометированы; • исключение возможности того, что сохраненные, но изъятые из обращения или замененные ключи не используются для операций шифрования. **3.6.5.b** Опросить работников на предмет того, что внедрены следующие процессы: • изъятие либо, при необходимости, замена ключей в случае ослабления целостности, в т. ч. вследствие увольнения работника, обладающего информацией о ключе; • замена ключей шифрования, которые были или могли быть скомпрометированы; • исключение возможности того, что сохраненные, но изъятые из обращения или замененные ключи используются для операций шифрования.	Чтобы исключить возможность дальнейшего использования ключей, следует изымать из обращения и (или) уничтожать те из них, которые больше не используются или не требуются, а также те, которые (возможно) были скомпрометированы. Если требуется их хранение (например, для поддержки архивированных зашифрованных данных), ключи следует надежно защитить. Средство шифрования должно обеспечивать и поддерживать процесс замены ключей, по которым подошел срок замены или которые (возможно) были скомпрометированы.
3.6.6 Если применяются ручные процедуры управления незашифрованными криптографическими ключами, данные процедуры должны координироваться с использованием принципа разделения знания и двойного контроля. ***Примечание:*** *примеры ручных процедур управления ключами включают, как минимум, генерацию ключа, его передачу, загрузку,*	**3.6.6.a** Проверить ручные процедуры управления незашифрованными ключами на предмет того, что они определяют использование следующих процессов: • разделенное знание ключей, где как минимум двое людей владеют компонентами одного ключа, и каждый из них знает только свой компонент ключа; И • 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, чтобы исключить возможность доступа одного человека к целому ключу. Такая мера применима для операций управления ключами, выполняемых вручную, 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

Требования PCI DSS	Проверочные процедуры	Пояснение
хранение и уничтожение.	**3.6.6.b** Опросить работников и (или) проследить за процессами на предмет того, что в процедурах ручного управления незашифрованными ключами используется следующее: • разделенное знание; И • двойной контроль.	компоненты не дают никакой информации об исходном криптографическом ключе. Двойной контроль требует наличия двух или более людей для выполнения определенной функции, при этом ни один из них не имеет доступа к аутентификационным данным другого или возможности их использовать.
3.6.7 Исключить несанкционированную замену криптографического ключа.	**3.6.7.a** Убедиться, что процедуры управления ключами определяют процессы, исключающие несанкционированную замену ключей.	Средство шифрования не должно допускать или принимать замену ключей, инициированную неавторизованными источниками или непредусмотренными процессами.
	3.6.7.b Опросить работников и (или) проследить за процессами на предмет того, что несанкционированная замена ключей исключена.	
3.6.8 Обеспечить формализованное подтверждение хранителями ключа того, что они понимают и принимают свои должностные обязанности по хранению и использованию ключей.	**3.6.8.a** Проверить процедуры управления ключами на предмет того, что они определяют процессы, в рамках которых хранители ключа подтверждают (в письменном или электронном виде), что они понимают и принимают свои должностные обязанности по хранению и использованию ключей.	Этот процесс поможет работникам, выступающим в роли хранителей ключей, вступить в эту роль, а также понять и принять соответствующие обязанности.
	3.6.8.b Проверить документацию или иные доказательства того, что хранители ключа подтвердили (в письменном или электронном виде), что понимают и принимают свои обязанности.	
3.7 Гарантировать, что политики безопасности и операционные процедуры защиты хранимых ДДК документированы, используются и известны всем заинтересованным лицам.	**3.7** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры защиты хранимых ДДК: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и документированные операционные процедуры для управления безопасным хранением ДДК на постоянной основе.

Требование 4. Шифровать ДДК при передаче через сети общего пользования.

Критичная информация должна быть зашифрована при передаче через сети, к которым злоумышленники могут легко получить доступ. Неправильно сконфигурированные беспроводные сети и уязвимости устаревших протоколов шифрования и аутентификации остаются целями для злоумышленников, которые используют данные уязвимости, чтобы получить привилегированный доступ к среде ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
4.1 Использовать стойкую криптографию и безопасные протоколы, чтобы защитить критичные ДДК при их передаче через открытые общедоступные сети с учетом следующего: • принимаются только доверенные ключи и сертификаты; • используемый протокол поддерживает только безопасные версии и конфигурации; • стойкость шифрования соответствует используемой методологии шифрования. ***Примечание:*** *там, где используется SSL и (или) ранние версии TLS, требования, описанные в Приложении A2, должны быть выполнены.* *Примеры открытых общедоступных сетей включают, как минимум:* • *сеть Интернет;* • *беспроводные технологии, включая протоколы 802.11 и Bluetooth;* • *технологии сотовой 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 на предмет того, что во всех местах используются протоколы безопасности и стойкая криптография.	Критичная информация должна шифроваться при передаче по сетям общего пользования, потому что злоумышленник без труда может перехватить и (или) изменить их маршрут при передаче. Безопасная передача ДДК требует использования доверенных ключей и (или) сертификатов, безопасного протокола передачи и шифрования надлежащей стойкости для шифрования ДДК. Не следует принимать запросы на подключение от систем, не поддерживающих требуемую стойкость шифрования, т. к. это приведет к небезопасному подключению. Следует отметить, что некоторые версии протоколов (например, SSL, SSH 1.0 и ранние версии TLS) содержат известные уязвимости, которые могут быть использованы злоумышленником для получения контроля над подверженной этим уязвимостям системой. Независимо от того, какой протокол используется, следует убедиться, что он настроен на то, чтобы использовать только безопасные конфигурации и версии для предотвращения небезопасного подключения. Например, использовать только доверенные сертификаты и поддерживать только стойкое шифрование (не поддерживать нестойкие, небезопасные протоколы или методы).
	4.1.b Проверить документированные политики и процедуры на предмет того, что: • принимаются только доверенные ключи и (или) сертификаты; • используемым протоколом поддерживаются только безопасные версии и конфигураций (небезопасные версии или конфигурации не поддерживаются); • применяется шифрование надлежащей стойкости согласно используемой методологии шифрования.	
	4.1.c Сделать выборку входящих и исходящих отправок по мере их выполнения (например, отслеживая системные процессы или сетевой трафик) и проверить их на предмет того, что все ДДК передаются в зашифрованном виде с использованием стойкой криптографии.	
	4.1.d Проверить ключи и сертификаты на предмет того, что принимаются только доверенные ключи и (или) сертификаты.	
	4.1.e Проверить системные конфигурации на предмет того, что протокол реализован таким образом, чтобы использовать только безопасные конфигурации и что он не поддерживает небезопасные версии или конфигурации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
например GSM, CDMA; • *GPRS;* • *спутниковые средства связи.*	**4.1.f** Проверить системные конфигурации на предмет того, что в используемой методологии шифрования применяется шифрование надлежащей стойкости. (См. рекомендации вендора и (или) информацию о передовом опыте).	Проверка того, что сертификат является доверенным (например, срок действия его не истек, и он получен из доверенного источника), помогает обеспечить целостность безопасного подключения.
	4.1.g Если реализован протокол TLS, проверить системные конфигурации на предмет того, что TLS включен при каждой передаче или получении ДДК. Например, если протокол реализован на базе браузера: • в качестве протокола URL-адреса указан HTTPS; и • ДДК запрашиваются только в том случае, если URL-адрес содержит префикс HTTPS.	Как правило, URL-адрес должен начинаться с префикса HTTPS, и (или) в окне веб-браузера должен отображаться 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. Для получения информации о стойкой криптографии и безопасных протоколах необходимо обратиться к отраслевым стандартам и передовому опыту (например, NIST SP 800-52 и SP 800-57, OWASP и т.д.).
	4.1.h Если используются ранние версии TLS, выполнить проверочные процедуры, описанные в *Приложении A2: Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS.*	
4.1.1 Убедиться, что при использовании беспроводных сетей, передающих ДДК либо подключенных к среде ДДК, применяется передовой отраслевой опыт, чтобы реализовать стойкое шифрование при аутентификации и передаче данных.	**4.1.1** Выявить все беспроводные сети, передающие ДДК либо подключенные к среде ДДК. Проверить документированные стандарты и сравнить их с системными конфигурациями на предмет того, что во всех беспроводных сетях: • применяется передовой отраслевой опыт, чтобы реализовать стойкое шифрование при аутентификации и передаче данных; • не используется слабое шифрование (например, WEP, SSL) в качестве защитной меры для аутентификации или передачи данных.	Злоумышленники используют свободно распространяемые и широкодоступные средства для прослушивания беспроводного трафика. Использование стойкой криптографии может ограничить раскрытие критичной информации, передаваемой по беспроводным сетям. Чтобы предотвратить доступ злоумышленников к беспроводным сетям или использование беспроводных сетей для получения доступа к другим внутренним сетям или данным, требуется стойкая криптография для аутентификации и передачи ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
4.2 Запрещается пересылать незащищенные PAN с использованием технологий обмена сообщениями для конечных пользователей (например, электронная почта, системы мгновенного обмена сообщениями, SMS, чат и т. д.).	**4.2.a** Если для передачи ДДК используются технологии обмена сообщениями для конечных пользователей, то просмотреть процессы отправки PAN и проверить выборку передач исходящих данных по мере их выполнения на предмет того, что PAN приводится к нечитаемому виду или защищается с применением стойкой криптографии каждый раз при отправке с использованием технологий обмена сообщениями для конечных пользователей.	Сообщения, передаваемые по электронной почте, с помощью систем мгновенного обмена сообщениями, в чате, или SMS могут быть перехвачены в процессе доставки, как во внутренней, так и во внешней общедоступной сетях. Не используйте эти средства передачи сообщений для отправки PAN, если они не обеспечивают стойкого шифрования. Кроме того, если организация запрашивает PAN через технологии обмена сообщениями для конечных пользователей, она должна обеспечить средство или метод защиты таких PAN с помощью стойкой криптографии или приведения PAN к нечитаемому виду перед передачей.
	4.2.b Проверить письменные политики на предмет того, что в них запрещается отправлять незащищенные PAN с использованием технологий обмена сообщениями для конечных пользователей.	
4.3 Гарантировать, что политики безопасности и операционные процедуры шифрования передаваемых ДДК документированы, используются и известны всем заинтересованным лицам.	**4.3** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры шифрования передаваемых ДДК: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры для непрерывного управления безопасной передачей ДДК.

Поддерживать программу управления уязвимостями.

Требование 5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусные ПО или программы.

Вредоносное ПО, включая вирусы, червей и трояны, проникает в сеть во время выполнения многих разрешенных бизнесом действий, включая использование работниками электронной почты, сети Интернет, мобильных компьютеров, а также запоминающих устройств, что приводит к эксплуатации уязвимостей системы. Антивирусное ПО должно использоваться на всех системах, обычно подверженных воздействию вредоносного ПО, 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 снимают требование об обязательном наличии антивирусного ПО.

Требования PCI DSS	Проверочные процедуры	Пояснение
5.1 Развернуть антивирусное ПО на всех системах, обычно подверженных воздействию вредоносного ПО (особенно на персональных компьютерах и серверах).	**5.1** Проверить, что антивирусное ПО развернуто в выборке системных компонентов, включая все типы ОС, обычно подверженных воздействию вредоносного ПО, при наличии применимой антивирусной технологии.	Против, казалось бы, защищенных систем идет постоянный поток атак, в которых используются широкодоступные эксплойты и которые часто называются «атаками нулевого дня» (такие атаки используют ранее неизвестные уязвимости). Без регулярно обновляемого антивирусного ПО, новые формы вредоносного ПО могут атаковать системы, нарушать работу сети, приводить к компрометации данных.
5.1.1 Убедиться, что антивирусное ПО способно обнаруживать и устранять все известные типы вредоносного ПО, а также обеспечивать защиту от них.	**5.1.1** Проверить документацию вендора и конфигурации антивирусов на предмет того, что антивирусные программы: • обнаруживают все известные типы вредоносного ПО; • удаляют все известные типы вредоносного ПО; • защищают от всех известных типов вредоносного ПО. *Примерами типов вредоносного ПО являются вирусы, черви, трояны, шпионское и рекламное ПО, руткиты.*	Важно обеспечить защиту от **ВСЕХ** типов и форм вредоносного ПО.

Требования PCI DSS	Проверочные процедуры	Пояснение
5.1.2 Проводить периодические проверки в системах, которые обычно считаются не подверженными заражению вредоносным ПО, выявляя и оценивая угрозы заражения новыми формами вредоносного ПО, для того, чтобы проверять, что эти системы по-прежнему не требуют антивирусного ПО.	**5.1.2** Опросить работников на предмет того, что для выявления угроз заражения новыми формами вредоносного ПО ведется мониторинг и проверки систем, которые считаются не подверженными заражению вредоносным ПО, для того, чтобы подтвердить, что этим системам по-прежнему не требуется антивирусное ПО.	Как правило, мейнфреймы, компьютеры среднего уровня (например, AS/400) и подобные системы в данное время не подвержены заражению вредоносным ПО или не являются его мишенью. Однако тенденции в области вредоносного ПО могут быстро меняться, а значит, организациям важно знать о новых видах вредоносного ПО, которые могут быть опасны для их систем (например, отслеживая сообщения о безопасности от вендоров ПО и новостных групп антивирусов, чтобы узнать, угрожают ли их системам новые виды и формы вредоносного ПО). В процесс выявления новых уязвимостей в системе безопасности следует включить тенденции в области вредоносного ПО. Порядок реагирования на новые тенденции организации следует по необходимости включить в стандарты конфигурации и защитные меры.
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** Проверить политики и процедуры на предмет того, что они предписывают поддерживать антивирусные ПО и базы в актуальном состоянии.	Даже у лучших антивирусов снижается эффективность, если за ними не следить и не поддерживать в актуальном состоянии с помощью последних обновлений безопасности, антивирусных баз или защитных мер от вредоносного ПО. Журналы регистрации событий предоставляют возможность мониторинга активности вирусов и вредоносного ПО, и реагирования на эту активность. Поэтому следует настроить средства защиты от вредоносного ПО на генерацию журналов регистрации событий и управлять этими журналами в соответствии с требованием 10.
	5.2.b Проверить конфигурацию антивирусов, включая установочные образы, на предмет того, что антивирусные механизмы: • настроены на автоматическое обновление; • настроены на периодическое сканирование.	
	5.2.c Проверить выборку системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО, на предмет того, что: • антивирусное ПО и базы актуальны; • выполняется периодическое сканирование.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	5.2.b Проверить конфигурацию антивирусов, включая установочные образы и выборку системных компонентов, на предмет того, что: • включено создание журналов регистрации событий; • журналы хранятся согласно требованию 10.7 стандарта PCI DSS.	

Требования PCI DSS	Проверочные процедуры	Пояснение
5.3 Убедиться, что антивирусные механизмы постоянно запущены, и пользователи не могут их ни отключить, ни изменить без явного разрешения, которое выдается руководством на каждый конкретный случай и на ограниченный период времени. ***Примечание:*** *антивирусные средства могут быть временно отключены только в случае обоснованной технической необходимости, с разрешения руководства в каждом конкретном случае. Если антивирусную защиту нужно отключить для определенной цели, необходимо получить официальное разрешение. Также могут понадобиться дополнительные защитные меры на время, в течение которого антивирусная защита будет неактивна.*	**5.3.a** Проверить конфигурацию антивирусов, включая установочные образы ПО и выборку системных компонентов, на предмет того, что антивирусное ПО постоянно запущено. **5.3.b** Проверить конфигурацию антивирусов, включая установочные образы ПО и выборку системных компонентов, на предмет того, что антивирусное ПО не может быть отключено или изменено пользователями. **5.3.c** Опросить ответственных работников и проследить за процессами на предмет того, что антивирусное ПО не может быть отключено или изменено пользователями без явного разрешения руководства в каждом конкретном случае и на ограниченный период времени.	Антивирус, работающий постоянно и защищенный от изменений, обеспечит надежную защиту от вредоносного ПО. Использовать защитные меры на основе политик на всех системах, чтобы исключить возможность изменения или отключения защитных мер антивирусного ПО. Это позволит не допустить, чтобы злоумышленник мог воспользоваться уязвимостями систем. Также могут потребоваться дополнительные меры безопасности на период времени, в течение которого антивирусная защита будет отключена (например, отключение незащищенной системы от сети Интернет пока отключена антивирусная защита и запуск полного сканирования после его повторного включения).
5.4 Гарантировать, что политики безопасности и операционные процедуры защиты систем от вредоносного ПО документированы, используются и известны всем заинтересованным лицам.	**5.4** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры защиты систем от вредоносного ПО: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры для постоянной защиты систем от вредоносного ПО.

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости безопасности для получения привилегированного доступа к системам. Многие такие уязвимости устраняются с помощью обновлений безопасности, которые предоставляются вендором и которые должны устанавливаться организациями, управляющими системами. На все системы должны быть установлены все надлежащие обновления ПО, чтобы защититься от эксплуатации уязвимостей и от компрометации ДДК злоумышленниками и вредоносным ПО.

Примечание: *надлежащими являются те обновления, которые были оценены и протестированы в достаточной мере на предмет того, что они совместимы с существующими конфигурациями безопасности. В приложениях собственной разработки многих уязвимостей можно избежать, если использовать стандартные процессы разработки систем и приемы безопасного программирования.*

Требования PCI DSS	Проверочные процедуры	Пояснение
6.1 Наладить процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также процесс оценки критичности (например, «высокая», «средняя» или «низкая») для недавно обнаруженных уязвимостей. ***Примечание:*** *оценка критичности уязвимости должна быть основана на отраслевых рекомендациях и учитывать потенциальное воздействие. Например, критерии критичности уязвимости могут учитывать систему оценки CVSS base, классификацию вендора и (или) тип систем, подверженных воздействию.* *Методы оценки критичности уязвимостей и ранжирования рисков зависят от среды организации и ее стратегии по оценке рисков. При оценке критичности уязвимостей необходимо, как минимум, идентифицировать все уязвимости, уровень критичности которых для среды считается высоким. Помимо оценки критичности уязвимостей, они могут быть сочтены критическими, если представляют неотвратимую угрозу для среды,*	**6.1.a** Проверить политики и процедуры на предмет того, что в процессах требуется: • идентифицировать новые уязвимости; • оценивать критичность уязвимостей, в т. ч. идентифицировать все уязвимости с «высоким» и «критичным» уровнями; • использовать авторитетные внешние источники информации об уязвимостях. **6.1.b** Опросить ответственных работников и проследить за процессами на предмет того, что: • новые уязвимости выявляются; • уязвимости оцениваются по ранжированию рисков, при этом идентифицируются все «высокие» риски и «критичные» уязвимости; • процессы выявления новых уязвимостей безопасности включают в себя использование для этого авторитетных внешних источников информации об уязвимостях.	Цель данного требования состоит в том, чтобы организации были постоянно в курсе новых уязвимостей, которые могут воздействовать на ее среду. Источники информации об уязвимостях должны быть достоверными. Зачастую к таковым относятся веб-сайты вендоров, отраслевые новостные группы, почтовые рассылки или RSS-ленты. Как только организация выявляет уязвимость, которая может оказать негативное влияние на среду организации, необходимо оценить критичность уязвимости. Следовательно, в организации должен быть метод оценки уязвимостей и уровня их критичности на постоянной основе. Для этого недостаточно провести сканирование авторизованным поставщиком услуг сканирования (ASV) или внутреннее сканирование на наличие уязвимостей; для этого необходим процесс активного мониторинга отраслевых источников информации об уязвимостях. Ранжируя риски (например, «высокий», «средний» или «низкий» уровни), организация может быстрее идентифицировать наиболее высокие риски, устанавливать им приоритет и управлять ими, а также минимизировать

Требования PCI DSS	Проверочные процедуры	Пояснение
воздействуют на критичные системы и (или) могут привести к компрометации, если не будут нейтрализованы. К критичным системам могут, например, относиться системы безопасности, общедоступные устройства и системы, базы данных и другие системы, осуществляющие хранение, обработку или передачу ДДК.		вероятность использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для организации.
6.2 Гарантировать, что все системные компоненты и ПО защищены от известных уязвимостей путем установки применимых обновлений безопасности, которые выпускает производитель. Устанавливать критичные обновления безопасности в течение одного месяца с момента их выпуска. ***Примечание:*** *критичные обновления безопасности должны выявляться в соответствии с процессом ранжирования рисков (см. требование 6.1).*	**6.2.a** Проверить политики и процедуры, относящиеся к установке обновлений безопасности, на наличие процессов, которые требуют: • устанавливать применимые критичные обновления безопасности, которые выпускает производитель, в течение месяца после их выхода; • устанавливать все применимые обновления безопасности, которые выпускает производитель, в течение соответствующего срока с момента их выхода (например, в течение трех месяцев).	Против, казалось бы, защищенных систем идет постоянный поток атак, в которых используются широкодоступные эксплойты и которые часто называются «атаками нулевого дня» (такие атаки используют ранее неизвестные уязвимости). Если самые последние обновления не внедряются на критичных системах как можно быстрее, злоумышленник может использовать эти уязвимости, чтобы атаковать систему, нарушить ее работу или получить доступ к критичным данным. Установка приоритета для обновлений критичной инфраструктуры максимально быстро обеспечивает защиту систем и устройств с высоким приоритетом от уязвимостей после выхода обновления. Рекомендуется определить приоритеты установки обновлений таким образом, чтобы 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 всего установленного ПО, включая платежные приложения, как прошедшие проверку на соответствие стандарту PA-DSS, так и не проходившие данной проверки.
	6.2.b Сравнить перечень обновлений безопасности, которые установлены на каждой системе из выборки системных компонентов и связанного с ними ПО, с перечнем последних обновлений безопасности, которые выпускает производитель, на предмет того, что: • применимые критичные обновления безопасности, которые выпускает производитель, устанавливаются в течение месяца с момента выпуска; • все применимые обновления безопасности, которые выпускает производитель, устанавливаются в течение надлежащего срока с момента выпуска (например, в течение трех месяцев).	

Требования PCI DSS	Проверочные процедуры	Пояснение
6.3 Разрабатывать внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс) безопасно, с соблюдением следующих требований: • согласно требованиям PCI DSS (например, по безопасной аутентификации и ведению журналов регистрации событий); • на основе отраслевых стандартов и (или) рекомендаций; • с учетом информационной безопасности в течение всего цикла разработки ПО. ***Примечание**: настоящее требование относится к любому ПО собственной разработки и заказному ПО, разработанному третьим лицом.*	**6.3.a** Проверить документированные процессы разработки ПО на предмет того, что они основаны на передовом отраслевом опыте и (или) стандартах.	Если не учитывать информационную безопасность на этапах разработки ПО (определения требований, проектирования, анализа и тестирования), в производственную среду непреднамеренно или сознательно могут быть внесены уязвимости. Понимая, как критичные данные обрабатываются приложением – в том числе во время хранения, передачи и нахождения в памяти, возможно, будет проще определять места, где требуется защита данных.
	6.3.b Проверить документированные процессы разработки ПО на предмет того, что в них учитывается информационная безопасность в течение всего цикла разработки.	
	6.3.c Проверить документированные процессы разработки ПО на предмет того, что приложения разрабатываются в соответствии с PCI DSS.	
	6.3.d Опросить разработчиков ПО на предмет того, что реализованы документированные процессы разработки ПО.	
6.3.1 Удалять все учетные записи разработчиков, тестовые учетные записи и (или) учетные записи заказного приложения, идентификаторы пользователей и пароли перед передачей ПО заказчикам или переводом его в производственный режим.	**6.3.1** Проверить документированные процедуры разработки ПО и опросить ответственных работников на предмет того, что все допроизводственные учетные записи и (или) учетные записи заказного приложения, идентификаторы пользователей и (или) пароли удаляются перед передачей ПО заказчикам или переводом его в производственный режим.	Следует удалять учетные записи разработчиков, тестовые учетные записи и (или) учетные записи заказного приложения, имена пользователей и пароли из производственного кода до перевода приложения в производственный режим или предоставления приложения заказчикам, поскольку эти элементы могут использоваться для получения информации о функционировании приложения. Обладание этой информацией может помочь злоумышленникам скомпрометировать приложение и связанные с ним ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.3.2 Контролировать разрабатываемый код на наличие потенциальных уязвимостей (вручную или автоматически) перед передачей готовых приложений заказчикам или переводом их в производственный режим с соблюдением как минимум следующих требований: • контролировать изменения программного кода лицами, которые не являются авторами этого кода, и лицами, которые знают методики контроля кода и методы безопасного программирования; • контролируя программный код, убедиться, что он разработан в соответствии с рекомендациями безопасного программирования; • вносить все необходимые корректировки до выпуска ПО; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска ПО. *(Продолжение на следующей странице)*	**6.3.2.a** Проверить документированные процедуры разработки ПО и опросить ответственных работников на предмет того, что все изменения разрабатываемого программного кода обязательно контролируются (вручную или автоматически) с учетом следующих требований: • контролировать изменения программного кода лицами, которые не являются авторами этого кода, и лицами, которые знают методики контроля кода и методы безопасного программирования; • контролируя программный код, убедиться, что он разработан в соответствии с рекомендациями безопасного программирования (см. Требование 6.5 PCI DSS); • вносить все необходимые корректировки до выпуска ПО; • результаты контроля кода рассматриваются и утверждаются руководством до выпуска ПО.	Уязвимости в разрабатываемом коде обычно используются злоумышленниками для получения доступа к сети и компрометации ДДК. Контроль кода должны выполнять опытные специалисты, знакомые с методиками такого контроля. Чтобы обеспечить объективный и независимый контроль кода, такой контроль должны выполнять лица, отличные от разработчика кода. Автоматизированные средства или процессы могут заменять ручной контроль кода, однако следует учитывать, что автоматизированным средством контроля кода сложно или вообще невозможно обнаружить некоторые ошибки программирования. Благодаря исправлению ошибок программирования до того, как код разворачивается в производственной среде или передается заказчикам, код не создает потенциально используемые уязвимости в средах. Гораздо сложнее и дороже исправлять ошибки в коде после развертывания приложения или его запуска в производственных средах. Формализованный контроль кода и его утверждение руководством до выпуска ПО позволяет гарантировать, что код одобрен и разработан в соответствии с политиками и процедурами.

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *данное требование к контролю кода применимо ко всему разрабатываемому коду (как внутренних приложений, так и приложений, доступных из Интернета) как составная часть цикла разработки системы.* *Контроль программного кода может проводиться компетентными внутренними работниками или третьими лицами. Общедоступные веб-приложения также подлежат применению дополнительных мер по защите от текущих угроз и уязвимостей после внедрения, согласно требованию 6.6 стандарта PCI DSS.*	**6.3.2.b** Сделать выборку недавних изменений разрабатываемого приложения и проверить ее на предмет того, что его код контролируется согласно требованию 6.3.2.a, приведенному выше.	
6.4 Соблюдать процессы и процедуры контроля изменений по всем изменениям системных компонентов. Эти процессы должны включать в себя следующее:	**6.4** Проверить политики и процедуры на предмет наличия в них следующих требований: • отделить среды разработки и (или) тестирования от производственных сред; отделение реализовать с использованием мер контроля доступа; • разделить обязанности между работниками, относящимися к средам разработки и (или) тестирования и к производственным средам; • не использовать производственные данные (действующие PAN) для тестирования или разработки; • удалять тестовые данные и учетные записи из системы перед переводом ее в производственный режим; • документировать процедуры контроля изменений, относящиеся к внедрению обновлений безопасности и изменений ПО.	Если контроль изменений не документируется и не выполняется надлежащим образом, средства защиты могут быть непреднамеренно или сознательно упущены или отключены, могут возникать ошибки обработки или может быть внедрен вредоносный код.
6.4.1 Отделить среды разработки и (или) тестирования от производственных сред; отделение реализовать с использованием мер контроля доступа.	**6.4.1.a** Проверить документацию сети и конфигурации сетевых устройств на предмет того, что среды разработки и (или) тестирования отделены от производственных сред.	В связи с постоянными изменениями сред разработки и тестирования, они, как правило, менее защищены, чем производственная среда. Без надлежащего разделения производственная

Требования PCI DSS	Проверочные процедуры	Пояснение
	6.4.1.b Проверить настройки механизмов контроля доступа на предмет того, что они внедрены для разделения сред разработки и (или) тестирования и производственной среды (сред).	среда и ДДК могут быть скомпрометированы вследствие менее строгих конфигураций защиты и возможных уязвимостей в среде тестирования или разработки.
6.4.2 Разделить обязанности между работниками сред разработки и (или) тестирования и работниками производственных сред.	**6.4.2** Проследить за процессами и опросить работников, относящихся к средам разработки и (или) тестирования, и работников, относящихся к производственным средам, на предмет того, что обязанности работников сред разработки и (или) тестирования и работников производственных сред разделены.	Уменьшая количество работников, имеющих доступ к производственной среде и ДДК, можно минимизировать риск и упростить контроль за тем, чтобы доступ был ограничен только теми лицами, у которых есть на то служебная необходимость. Цель данного требования состоит в том, чтобы отделить 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 Не использовать производственные данные (действующие PAN) для тестирования или разработки.	**6.4.3** Проверить процессы тестирования и опросить работников на предмет того, что внедрены процедуры, исключающие использование производственных данных (действующих PAN) для тестирования или разработки.	В средах разработки или тестирования обычно реализованы менее жесткие защитные меры. Использование в такой среде производственных данных дает возможность злоумышленникам получить к ним несанкционированный доступ (например, к ДДК).
	6.4.3.b Проверить выборку данных тестовой среды на предмет того, что производственные данные (действующие PAN) не используются для тестирования или разработки.	
6.4.4 Удалить тестовые данные и учетные записи из системных компонентов перед переводом системы в производственный режим.	**6.4.4.a** Проследить за процессами проведения тестирования и опросить работников на предмет того, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	Тестовые данные и учетные записи следует удалить перед переводом системных компонентов в производственный режим, поскольку эти элементы могут использоваться для получения информации о функционировании

Требования PCI DSS	Проверочные процедуры	Пояснение
	6.4.4.b Проверить выборку данных и учетных записей из недавно установленных или обновленных производственных систем на предмет того, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	приложения или системы. Обладая этой информацией, злоумышленники могут скомпрометировать систему и связанные с ней ДДК.
6.4.5 Включить в процедуры контроля изменений следующее:	**6.4.5.a** Проверить документированные процедуры контроля изменений на предмет того, что процедуры требуют: • документировать влияние изменений; • документировать согласования изменений, со стороны уполномоченных лиц; • проводить функциональное тестирование на предмет того, что внесенные изменения не снижают защищенность системы; • предусмотреть процедуры отмены изменений.	Если обновления ПО и оборудования, а также обновления безопасности не управляются должным образом, то влияние таких системных изменений может быть не до конца понято и может привести к нежелательным последствиям.
	6.4.5.b Опросить ответственных работников по выборке системных компонентов, чтобы определить недавние изменения. Отследить эти изменения с помощью соответствующей документации по контролю изменений. Выполнить следующие действия по каждому изученному изменению:	
6.4.5.1 Документирование влияния изменений.	**6.4.5.1** Убедиться, что документация о влиянии изменений включена в документацию по контролю изменений по каждому изменению из выборки.	Влияние изменений должно документироваться, чтобы все заинтересованные лица могли надлежащим образом планировать все изменения в обработке данных.
6.4.5.2 Документирование согласования изменений со стороны уполномоченных лиц.	**6.4.5.2** Проверить, что для каждого изменения из выборки имеется документированное согласование со стороны уполномоченных лиц.	Согласование со стороны уполномоченных лиц указывает на то, что изменение легитимно, авторизовано и санкционировано организацией.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.5.3 Функциональное тестирование, чтобы проверить, что изменения не снижают защищенность системы.	**6.4.5.3.a** Для каждого изменения из выборки убедиться, что функциональное тестирование выполнено для того, чтобы убедиться, что изменение не снижало защищенность системы.	Следует выполнять тщательное тестирование, чтобы проверить, что после внедрения изменения уровень безопасности среды не снизится. Цель тестирования состоит в том, чтобы подтвердить, что все существующие защитные меры по-прежнему работают, что они заменяются защитными мерами такой же надежности или что они усиливаются после любых изменений в среде.
	6.4.5.3.b В отношении изменений разрабатываемого кода убедиться, что все обновления протестированы на соответствие требованию 6.5 PCI DSS перед их развертыванием в производственной среде.	
6.4.5.4 Процедуры отмены изменений.	**6.4.5.4** Убедиться, что по каждому изменению из выборки подготовлена процедура отмены.	По каждому изменению должна существовать документированная процедура отмены, которая позволит вернуть систему в предыдущее состояние в случае сбоя или неблагоприятного воздействия изменения на безопасность приложения или системы.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.6 После выполнения существенных изменений все соответствующие требования PCI DSS должны быть выполнены на всех новых или измененных системах или сетях, и документация обновлена в случае необходимости. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**6.4.6** Проверить по выборке системных компонентов записи изменений, опросить работников и проследить за системами и (или) сетями, которые подверглись изменениям, на предмет того, что применимые требования PCI DSS были выполнены, и документация обновлена в рамках изменений.	Наличие процессов анализа существенных изменений позволяет гарантировать, что все соответствующие защитные меры PCI DSS применены для каждой системы или сети, которые были добавлены или изменены в среде, находящейся в области применимости стандарта. Внедрение этой проверки в процесс управления изменениями гарантирует, что списки устройств и стандарты конфигураций поддерживаются актуальными, и защитные меры применяются там, где это необходимо. В процесс управления изменениями следует включить доказательства того, что требования PCI DSS выполнены или сохранены посредством повторяющегося процесса. Примерами требований PCI DSS, которые могут быть затронуты, являются, среди прочего: • актуализировать схему сети в соответствии с изменениями; • сконфигурировать системы согласно стандартам конфигурации с изменением всех паролей по умолчанию и отключением неиспользуемых сервисов; • защитить системы с помощью необходимых мер, например, мониторинга целостности файлов, антивирусного ПО, обновлений, ведения журналов аудита; • не хранить критичные аутентификационные данные (КАД), хранение всех ДДК документировать и включить в политики и процедуры хранения данных; • включить новые системы в ежеквартальный процесс сканирования на наличие уязвимостей.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5 Управлять распространенными уязвимостями программного кода в процессе разработки ПО следующим образом: • обучать разработчиков не реже одного раза в год 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 были актуальны в соответствии с отраслевыми рекомендациями, существовавшими на момент публикации настоящей версии PCI DSS. Тем не менее, по мере обновления отраслевых рекомендаций по управлению уязвимостями (таких, как Руководство OWASP, Список SANS CWE Top 25, CERT Secure Coding и т. д.) следует использовать их актуальные версии.*	**6.5.a** Проверить политики и процедуры разработки ПО на предмет того, что разработчики обязаны не реже одного раза в год проходить обучение актуальным методикам безопасного программирования, основанным на отраслевых рекомендациях и руководствах. **6.5.b** Проверить документацию об обучении на предмет того, что разработчики проходят обучение актуальным методикам безопасного программирования не реже одного раза в год, в том числе тому, как избегать распространенных уязвимостей программирования. **6.5.c** Убедиться, что имеются реализованные процессы, предназначенные для защиты, по крайней мере, от следующих уязвимостей:	Прикладной уровень подвержен высокому риску и может являться целью как внутренних, так и внешних угроз. Требования 6.5.1–6.5.10 представляют собой минимально необходимые защитные меры, подлежащие выполнению, и организации должны внедрять те методики безопасного программирования, которые применимы к определенным технологиям в их среде. Разработчики приложений должны быть надлежащим образом подготовлены, чтобы определять и устранять проблемы, связанные с этими и другими распространенными уязвимостями программного кода. Осведомленность работников о правилах безопасного программирования позволит свести к минимуму количество уязвимостей, возникающих из-за низкого качества кода. Обучение разработчиков может осуществляться как самой организацией, так и третьими лицами и должно быть применимо к используемой технологии. По мере изменений отраслевых методик безопасного программирования должны соответственно обновляться методики программирования и обучения разработчиков в организации, чтобы бороться с новыми угрозами (например, атаками на извлечение данных из памяти, т.н. memory scraping). Уязвимости, указанные в требованиях 6.5.1–6.5.10, представляют собой лишь минимальный список. Организация самостоятельно обеспечивает соответствие тенденциям в области уязвимостей и внедряет соответствующие меры безопасности в свои методики безопасного программирования.

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *требования 6.5.1–6.5.6, приведенные ниже, распространяются на все приложения (внешние или внутренние).*		
6.5.1 Инъекции, в частности, SQL-инъекции, а также инъекции LDAP, XPath, команд ОС и др.	**6.5.1** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что в методиках программировании учтены уязвимости к инъекциям, в том числе: • введенные пользователями данные проверяются на предмет того, что они не могут изменить значение существующих команд и запросов; • используются параметризованные запросы.	Инъекции кода, в частности SQL-инъекции, являются распространенным способом компрометации приложений. Инъекция происходит, когда предоставленные пользователем данные передаются интерпретатору как часть команды или запроса. Введенные злоумышленником вредоносные данные некорректно обрабатываются интерпретатором, вызывая нежелательные команды или изменяя данные. Это позволяет злоумышленнику атаковать компоненты внутри сети через приложение, инициировать такие атаки, как переполнение буфера, получить доступ к конфиденциальной информации или информации о функциональных возможностях серверного приложения. Следует проверять информацию перед отправкой в приложение (например, проверяя все буквенные символы, сочетания буквенных и цифровых символов и т. д.)
6.5.2 Переполнение буфера	**6.5.2** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают уязвимости переполнения буфера, в том числе: • проверяют границы буфера; • усекают строки ввода.	Переполнение буфера происходит, когда приложение не имеет соответствующих ограничений при проверке буферного пространства. Это может привести к тому, что информация, содержащаяся в буфере, вытесняется за пределы области буферной памяти в область исполняемой памяти. Когда это происходит, злоумышленник получает возможность внедрить в буфер вредоносный код и затем поместить этот вредоносный код в область исполняемой памяти путем переполнения буфера. Затем вредоносный код выполняется, что зачастую позволяет злоумышленнику получить удаленный доступ к приложению и (или) зараженной системе.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.3 Небезопасное криптографическое хранилище.	**6.5.3** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают небезопасность криптографического хранилища следующим образом: • защищают от криптографических уязвимостей; • используют стойкие криптографические алгоритмы и надежные ключи.	Приложения, которые не используют для хранения данных стойкие криптографические функции надлежащим образом, подвергаются повышенному риску компрометации и делают ДДК и (или) учетные данные для аутентификации уязвимее. Если злоумышленник сможет использовать уязвимости криптографических процессов, он, возможно, получит доступ к зашифрованным данным в открытом виде.
6.5.4 Небезопасная передача данных	**6.5.4** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают уязвимости небезопасной передачи данных и обеспечивают надлежащую аутентификацию и шифрование передач всех критичных данных.	Приложения, которые не шифруют надлежащим образом сетевой трафик с применением стойкой криптографии, подвергаются повышенному риску компрометации и делают ДДК уязвимее. Если злоумышленник сможет использовать уязвимости криптографических процессов, он, возможно, сможет получить управление над приложением или даже доступ к зашифрованным данным в открытом виде.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.5 Некорректная обработка ошибок.	**6.5.5** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают уязвимости некорректной обработки ошибок и предотвращают 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 рабочих процессах, или же раскрытие закрытой информации. Злоумышленники используют эти уязвимости, чтобы похитить критичные данные и (или) компрометировать систему. Если злоумышленник сможет вызвать появление ошибок, которые приложение не сможет правильно обработать, существует возможность получения злоумышленником подробной информации о системе, возникновения отказов в обслуживании, нарушения работы системы безопасности или сбоя сервера. Например, сообщение «введен неправильный пароль» говорит злоумышленнику о том, что использовался верный идентификатор пользователя и теперь необходимо сосредоточить свои усилия только на подборе пароля. Следует использовать менее конкретные сообщения об ошибках, например: «данные не могут быть проверены».
6.5.6 Все уязвимости с высоким уровнем критичности, идентифицированные в процессе обнаружения уязвимостей (в соответствии с требованием 6.1 стандарта PCI DSS).	**6.5.6** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают любые уязвимости с высоким уровнем критичности, которые могут повлиять на работу приложения (в соответствии с требованием 6.1 стандарта PCI DSS).	Все уязвимости, которым в процессе ранжирования рисков организации был присвоен высокий уровень критичности (в соответствии с требованием стандарта 6.1) и которые могут повлиять на работу приложения, должны быть идентифицированы и учтены во время разработки приложения.

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *требования 6.5.7–6.5.10, приведенные ниже, распространяются на веб-приложения и интерфейсы приложений (внешние или внутренние):*		Веб-приложениям, как внутренним, так и внешним (общедоступным), свойственны уникальные риски для безопасности, которые связаны с архитектурой веб-приложений, а также относительной простотой и распространенностью компрометации.
6.5.7 Межсайтовый скриптинг (XSS)	**6.5.7** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают межсайтовый скриптинг (XSS), в том числе: • проверяют все параметры перед их включением в код; • используют контекстно-зависимое изолирование.	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 перехвата сеансов пользователя, дефейса веб-сайтов, возможного внедрения червей и т. д.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.8 Ошибки механизмов контроля доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий и отсутствие ограничения прав доступа пользователя к функциям).	**6.5.8** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают ошибки механизмов контроля доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий), в том числе: • обеспечивают надлежащую аутентификацию пользователей; • проверяют входные данные; • не раскрывают пользователям прямые ссылки на внутренние объекты; • пользовательские интерфейсы запрещают доступ к несанкционированным функциям.	Прямая ссылка на объект возникает, когда разработчик раскрывает ссылку на внутренний объект, такой как файл, каталог, запись в базе данных или ключ, в виде URL-адреса или параметра формы. Злоумышленники могут использовать эти ссылки для доступа к другим объектам без авторизации. Следует неукоснительно применять меры контроля доступа на уровне представления и бизнес-логики для всех URL-адресов. Часто защитить критичные функциональные возможности можно, только исключив отображение ссылок или URL-адресов несанкционированным пользователям. Злоумышленники могут использовать эту уязвимость для получения доступа и выполнения несанкционированных операций путем прямого доступа к URL-адресам. Злоумышленник может просканировать структуру директорий веб-сайта (обход директорий), чтобы получить несанкционированный доступ к информации, в т. ч. информации о функционировании сайта для последующей эксплуатации. Если пользовательские интерфейсы разрешают доступ к несанкционированным функциям, это может позволить злоумышленникам получить доступ к привилегированным учетным данным или ДДК. Доступ к прямым ссылкам на критичные ресурсы должен быть разрешен только авторизованным пользователям. Ограничивая доступ к информационным ресурсам, можно предотвратить передачу ДДК на неавторизованные ресурсы.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.9 Подделка межсайтовых запросов (CSRF).	**6.5.9** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают возможность подделки межсайтовых запросов (CSRF) и гарантируют, что приложения не полагаются на учетные данные для авторизации и токены, которые автоматически отправляются 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, совершение покупок или даже вход в приложение).
6.5.10 Противодействие компрометации механизмов аутентификации и управления сеансами	**6.5.10** Проверить политики и процедуры разработки ПО и опросить ответственных работников на предмет того, что методики программирования учитывают возможность атак на механизмы аутентификации и управления сеансами, в том числе, следующим образом: • помечают сеансовые токены (например, cookies) флагом "secure"; • не указывают идентификатор сеанса в URL-адресе; • устанавливают соответствующие ограничения по длительности сеанса и ротации идентификаторов после успешного входа.	Безопасная аутентификация и управление сеансами не позволяют злоумышленнику скомпрометировать подлинные учетные данные, ключи или сеансовые токены, с помощью которых в некоторых случаях злоумышленник может выдать себя за авторизованного пользователя.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.6 Постоянно управлять новыми угрозами и уязвимостями общедоступных веб-приложений и обеспечить этим приложениям защиту от известных атак одним из следующих методов: • проверять общедоступное веб-приложение на наличие уязвимостей, используя методы или инструменты ручного или автоматизированного анализа защищенности приложений не реже одного раза в год, а также после внесения любых изменений; ***Примечание:*** *данный анализ отличается от сканирования на наличие уязвимостей, выполняемого согласно требованию 11.2.* • устанавливать автоматизированное техническое средство (например, межсетевой экран уровня веб-приложений) перед общедоступными веб-приложениями для непрерывной проверки всего трафика, предназначенное для обнаружения и предупреждения веб-атак.	**6.6** Для общедоступных веб-приложений *убедиться следующим образом* в том, что реализован один из следующих методов: • проверить документированные процессы и отчеты о результатах анализа защищенности приложений и опросить работников на предмет того, что анализ (с использованием средств или методов ручного или автоматизированного анализа защищенности приложений) общедоступных веб-приложений проходит следующим образом: – не реже раза в год; – после любых изменений; – организацией, специализирующейся 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 устранения уязвимостей. • Проверить настройки системной конфигурации и опросить ответственных работников на предмет того, что автоматизированное техническое средство (например, межсетевой экран уровня веб-приложений), обнаруживающее и предупреждающее веб-атаки, реализовано следующим образом: – расположено перед общедоступными веб-приложениями, чтобы обнаруживать и предупреждать веб-атаки; – постоянно запущено и обновляется соответствующим образом; – создает журналы регистрации событий; – настроено на блокирование веб-атак или на генерацию соответствующих уведомлений, которые будут незамедлительно изучены.	Общедоступные веб-приложения являются основной целью для злоумышленников, и плохо написанные веб-приложения могут упростить злоумышленникам получение доступа к критичным данным и системам. Анализ приложений или установка межсетевого экрана уровня веб-приложений требуются для того, чтобы снижать количество компрометаций веб-приложений, связанных с недостаточным контролем процессов программирования или управления приложением. • Средства и методы ручной или автоматизированной оценки защищенности приложений используются для анализа и (или) проверки приложений на наличие уязвимостей • Межсетевые экраны уровня веб-приложений используются для фильтрации и блокировки ненужного трафика на уровне приложений. При использовании совместно с межсетевым экраном сетевого уровня, правильно сконфигурированный межсетевой экран уровня веб-приложений предотвращает атаки уровня приложений, если приложения настроены ненадлежащим образом или имеются уязвимости в коде. Это может быть достигнуто за счет сочетания технологии и процесса. Решения, основанные на процессах, должны иметь механизмы, которые способствуют своевременному ответу на уведомления, для того, чтобы отвечать цели данного требования, заключающейся в предотвращении атак. ***Примечание:*** *«организацией, специализирующейся на безопасности приложений», может быть сторонняя компания или внутренняя организация, работники которой специализируются на безопасности приложений и могут доказать независимость от группы разработчиков.*

Требования PCI DSS	Проверочные процедуры	Пояснение
6.7 Гарантировать, что политики безопасности и операционные процедуры разработки и поддержки безопасных систем и приложений документированы, используются и известны всем заинтересованным лицам.	**6.7** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры разработки и поддержки безопасных систем и приложений: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры, чтобы постоянно обеспечивать системам и приложениям безопасную разработку и защиту от уязвимостей.

Внедрять строгие меры контроля доступа

Требование 7. Ограничивать доступ к ДДК в соответствии со служебной необходимостью.

Реализовать системы и процессы, которые ограничивают доступ согласно служебной необходимости и в соответствии со служебными обязанностями, чтобы обеспечить доступ к критичным данным только уполномоченному персоналу.

Служебной необходимостью являются условия, когда права доступа предоставляются только к тому минимальному количеству данных и привилегий, которые необходимы для выполнения служебных 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 служебными обязанностями.	**7.1** Проверить документированную политику контроля доступа на предмет того, что она отражает требования 7.1.1–7.1.4 следующим образом: • определением прав доступа и назначением привилегий для каждой роли; • ограничением доступа привилегированных учетных записей только тем набором прав, который им минимально необходим для выполнения своих должностных обязанностей; • назначением прав доступа согласно роли и должностным обязанностям конкретного работника; • документированным утверждением (в письменной или электронной форме) всех прав доступа уполномоченными сторонами с указанием списка конкретных утвержденных привилегий.	Чем больше людей имеют доступ к ДДК, тем выше риск того, что учетные записи пользователей будут использоваться во вредоносных целях. Ограничивая доступ только теми лицами, которым он необходим в служебных целях, организация может предотвратить ненадлежащее обращение с ДДК, связанное с неопытностью или злым умыслом.

Требования PCI DSS	Проверочные процедуры	Пояснение
7.1.1 Определить необходимые права доступа для каждой роли, включая: • системные компоненты и информационные ресурсы, доступ к которым необходимо предоставить каждой роли для выполнения должностных обязанностей; • необходимый уровень привилегий (например, пользовательский, администраторский и т. д.) для доступа к ресурсам.	**7.1.1** Сделать выборку ролей и проверить их на предмет того, что потребности в правах доступа для каждой роли определены и включают: • системные компоненты и информационные ресурсы, доступ к которым необходимо предоставить каждой роли для выполнения должностных обязанностей; • список прав доступа, необходимых каждой роли для выполнения должностных обязанностей.	Для того чтобы доступ к ДДК ограничивался только теми лицами, которым он необходим, сначала нужно определить: — необходимые права доступа для каждой роли (например, системного администратора, работника колл-центра, продавца), — системы, устройства и данные, доступ к которым необходим для каждой роли, — уровень прав доступа, необходимых каждой роли для реального выполнения своих должностных обязанностей. Как только роли и необходимые им права доступа определены, лицам могут быть предоставлены соответствующие права доступа.
7.1.2 Ограничить права доступа идентификаторам привилегированных пользователей только тем набором прав, который минимально необходим им для выполнения своих должностных обязанностей.	**7.1.2.a** Опросить работников, отвечающих за назначение прав доступа, на предмет того, что доступ идентификаторам привилегированных пользователей: • назначен только тем ролям, которым он явно необходим; • ограничен только тем набором прав, который минимально необходим для выполнения должностных обязанностей.	Назначая привилегированные идентификаторы, важно предоставлять лицам только те права, которые им минимально необходимы для выполнения должностных обязанностей («минимально необходимый набор прав»). Например, администратор баз данных или администратор резервного копирования не должны иметь те же полномочия, что и администратор всей системы. *(Продолжение на следующей странице)*
	7.1.2.b Сделать выборку учетных записей привилегированных пользователей и опросить руководящих работников на предмет того, что назначенные полномочия: • необходимы для выполнения этим лицом своих должностных обязанностей; • ограничен только тем набором прав, который минимально необходим для выполнения должностных обязанностей.	Назначая минимально необходимый набор прав, можно предотвратить ошибочное или случайное изменение конфигурации приложения или его настроек безопасности со стороны пользователей, не обладающих достаточными знаниями о приложении. Устанавливая минимально необходимые права доступа, можно также свести к минимуму ущерб, если постороннее лицо получит доступ к идентификатору пользователя.

Требования PCI DSS	Проверочные процедуры	Пояснение
7.1.3 Назначать права доступа согласно роли и должностным обязанностям конкретного работника.	**7.1.3** Сделать выборку идентификаторов пользователей и опросить руководящих работников на предмет того, что полномочия назначены согласно роли и должностным обязанностям соответствующего работника.	Как только необходимые права доступа для ролей пользователей (согласно требованию 7.1.1 стандарта PCI DSS) определены, права доступа удобно предоставляются лицам согласно их ролям и должностным обязанностям благодаря использованию уже созданных ролей.
7.1.4 Требовать документы, утверждающие права доступа и завизированные уполномоченными лицами, с указанием необходимых прав доступа.	**7.1.4** Сделать выборку учетных записей пользователей и сравнить их с утверждающими документами на предмет того, что: • имеется документ, утверждающий назначенные права доступа; • эти права доступа утверждены уполномоченными лицами; • указанные полномочия соответствуют ролям, назначенным работнику.	Утверждающий документ (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 (или системы) контроля доступа к системным компонентам, которая ограничивает доступ в соответствии со служебной необходимостью пользователя и которая настроена запрещать все, что явным образом не разрешено. Система (или системы) контроля доступа должна:	**7.2** Проверить настройки системы и документацию вендора на предмет того, что система (или системы) контроля доступа реализована следующим образом:	Если отсутствует механизм ограничения доступа согласно служебной необходимости, пользователю, без его ведома, может быть предоставлен доступ к ДДК. Системы контроля доступа автоматизируют процесс ограничения доступа и назначения полномочий. Кроме того, настройка на запрет всего по умолчанию исключает получение кем-либо прав доступа до тех пор, пока не будет установлено правило, напрямую предоставляющее такие права. Организации могут иметь одну или несколько систем контроля доступа для управления доступом пользователей.
7.2.1 охватывать все системные компоненты;	**7.2.1** проверить, что системы контроля доступа внедрены на всех системных компонентах;	
7.2.2 назначать полномочия лицам согласно их ролям и должностным обязанностям;	**7.2.2** проверить, что системы контроля доступа настроены так, чтобы права доступа пользователей назначались согласно их ролям и должностным обязанностям;	***Примечание:*** *некоторые системы контроля доступа по умолчанию настроены на то, чтобы разрешать все, тем самым предоставляя права доступа до тех пор, пока не будет установлено правило, напрямую их запрещающее.*
7.2.3 по умолчанию запрещать любой доступ.	**7.2.3** проверить, что системы контроля доступа настроены так, чтобы по умолчанию запрещать любой доступ.	

Требования PCI DSS	Проверочные процедуры	Пояснение
7.3 Гарантировать, что политики безопасности и операционные процедуры ограничения доступа к ДДК документированы, используются и известны всем заинтересованным лицам.	**7.3** Проверить документацию и опросить работников на предмет того, что политики безопасности и процедуры ограничения доступа к ДДК: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры, чтобы гарантировать, что контроль доступа выполняется непрерывно, предоставляется только по служебной необходимости и с минимально необходимым набором прав.

Требование 8. Идентифицировать и аутентифицировать доступ к системным компонентам

Назначение уникального идентификатора каждому лицу, имеющему доступ, обеспечивает однозначную подотчетность каждого лица в его действиях. Если такая подотчетность реализована, то действия, производимые с критичными данными и системами, производятся известными и авторизованными пользователями и процессами и связь между такими действиями и совершившими их пользователями или процессами может быть отслежена.

Эффективность пароля во многом зависит от устройства и реализации системы аутентификации, в частности от того, насколько часто злоумышленник может пытаться ввести пароль 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 с административными полномочиями, включая учетные записи POS-терминалов, а также ко всем учетным записям, которые используются для просмотра ДДК или доступа ним, или для доступа к системам, содержащим ДДК. Сюда относятся учетные записи производителей и других третьих лиц (например, для поддержки или обслуживания). Данные требования не применимы к учетным записям, используемым клиентами (например, держателями 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 на POS-терминалах, которые обладают доступом только к одному номеру карты в один момент времени для проведения одной транзакции (например, учетные записи кассиров).

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1 Определить и внедрить следующим образом политики и процедуры, обеспечивающие надлежащее управление идентификацией пользователей, не являющихся клиентами, и администраторов на всех системных компонентах:	**8.1.a** Проверить процедуры и подтвердить, что они регламентируют процессы для выполнения каждого из нижеуказанных положений 8.1.1–8.1.8	Уникально идентифицируя каждого пользователя – вместо использования одного идентификатора для нескольких работников – организация может устанавливать индивидуальную ответственность работников за их действия и эффективно вести журнал регистрации событий по каждому из них. Это поможет ускорить разрешение проблем и противодействие им, когда обнаруживаются случаи некорректного использования или злого умысла.
	8.1.b Убедиться следующим образом в том, что реализованы процедуры, предназначенные для управления идентификацией пользователей:	
8.1.1 Назначить всем пользователям уникальные учетные записи, прежде чем предоставить им доступ к системным компонентам или ДДК.	**8.1.1** Опросить административных работников на предмет того, что всем пользователям назначены уникальные учетные записи для доступа к системным компонентам или ДДК.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1.2 Контролировать добавление, удаление и изменение учетных записей пользователей, учетных данных и иных объектов идентификации.	**8.1.2** В выборке учетных записей привилегированных и обычных пользователей проверить связанные с ними авторизации и проверить настройки системы на предмет того, что каждая учетная запись обычного и привилегированного пользователей наделена только теми полномочиями, которые указаны в утверждающем документе.	Чтобы гарантировать, что учетные записи пользователей, получивших доступ к системам, действительны и правомочны, следует применять строгие процессы к любым изменениям учетных записей пользователей и иных учетных данных (в т. ч. добавлению новых, изменению или удалению имеющихся).
8.1.3 Немедленно отзывать доступ у каждого уволенного пользователя.	**8.1.3.a** Сделать выборку пользователей, уволенных за прошедшие шесть месяцев, и проанализировать текущие списки доступа – как *локального, так и удаленного, на предмет того, что учетные записи таких пользователей заблокированы или удалены из списков доступа.*	Если работник уволился из компании и все еще имеет доступ к сети через свою учетную запись, существует риск несанкционированного или злонамеренного доступа к ДДК через старую и (или) неиспользуемую учетную запись со стороны злоумышленника или бывшего работника. Чтобы предотвращать несанкционированный доступ, следует сразу (как можно скорее) после ухода работника отозвать пользовательские учетные данные и другие средства аутентификации.
	8.1.3.b Убедиться, что все физические средства аутентификации (например, смарт-карты, токены и т. д.) были возвращены или деактивированы.	
8.1.4 Удалять и (или) блокировать неактивные учетные записи не позже чем через 90 дней.	**8.1.4** Проверить учетные записи пользователей на предмет того, что любые учетные записи, неактивные более 90 дней, удаляются или блокируются.	Нерегулярно используемые учетные записи часто подвергаются атакам в связи с меньшей вероятностью того, что изменения (например, смена пароля) будут замечены. Следовательно, такими учетными записями легче воспользоваться для доступа к ДДК.
8.1.5 Управлять учетными записями, которые используются третьими сторонами для удаленного доступа, поддержки и обслуживания системных компонентов, следующим образом: • включать только на необходимый промежуток времени и отключать, когда они не используются; • вести мониторинг, когда они используются.	**8.1.5.a** Опросить работников и проверить процессы управления учетными записями, которые используют третьи стороны для доступа, поддержки и обслуживания системных компонентов, на предмет того, что учетные записи, которые используются для удаленного доступа: • отключаются, когда они не используются; • включаются только тогда, когда они нужны третьей стороне и отключаются, когда они не используются.	Предоставляя вендорам доступ в сеть организации круглосуточно и без выходных для того, чтобы они могли по необходимости обслуживать системы организации, организация увеличивает вероятность несанкционированного доступа как со стороны пользователя из среды вендора, так и со стороны злоумышленника, который обнаружит и сможет использовать внешнюю точку входа в сеть, постоянно доступную для подключений. Включение доступа только на необходимые промежутки времени и отключение, когда в нем больше нет необходимости, предотвращает ненадлежащее использование таких подключений.
	8.1.5.b Опросить работников и проверить процессы на предмет того, что во время выполнения работ учетные записи, используемые третьими сторонами для удаленного доступа, контролируются.	

Требования PCI DSS	Проверочные процедуры	Пояснение
		Ведя мониторинг доступа вендоров, можно убедиться в том, что они получают доступ только к необходимым системам и только в согласованный промежуток времени.
8.1.6 Блокировать идентификатор пользователя не более чем после шести неудачных попыток входа подряд.	**8.1.6.a** Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что в параметрах аутентификации установлено требование, чтобы учетная запись пользователя блокировалась не более чем после шести неудачных попыток входа.	Если механизм блокировки учетных записей не реализован, злоумышленник может непрерывно пытаться подобрать пароль вручную или с использованием автоматизированных средств (программ перебора паролей) до тех пор, пока ему это не удастся, и он не получит доступ к учетной записи пользователя. ***Примечание:*** *проверочная процедура 8.1.6.b является дополнительной процедурой, применяемой только для организаций, которые определены как поставщики услуг.*
	8.1.6.b ***Дополнительная проверочная процедура для оценки поставщиков услуг*:** проверить внутренние процессы и клиентскую и (или) пользовательскую документацию и проследить за внедренными процессами на предмет того, что учетные записи пользователей, не являющихся клиентами, временно блокируются не более чем после шести неудачных попыток входа.	
8.1.7 Установить период блокировки идентификатора пользователя равным 30 минутам или до тех пор, пока его не разблокирует администратор.	**8.1.7** Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что учетная запись пользователя блокируется не менее чем на 30 минут, либо до тех пор, пока его не разблокирует администратор.	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.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1.8 Если сеанс был неактивен в течение 15 минут и больше, требовать у пользователя пройти повторную аутентификацию для возобновления работы терминала или сеанса.	**8.1.8** Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что сеанс работы пользователя или система блокируется не позднее чем через 15 минут простоя.	Когда пользователи отлучаются от работающих компьютеров, имеющих доступ к критичным системным компонентам сети или ДДК, эти компьютеры могут использоваться кем-нибудь в отсутствие этих пользователей, что приведет к несанкционированному доступу к учетной записи и (или) некорректному 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, обеспечить надлежащее управление аутентификацией пользователей, не являющихся клиентами, и администраторов на уровне всех системных компонентов, применяя хотя бы один из следующих методов аутентификации всех пользователей: • обладание информацией (например, паролем или парольной фразой); • обладание предметом (например, аппаратным токеном или смарт-картой); • обладание параметрами (например, биометрическими).	**8.2** Чтобы убедиться, что аутентификация пользователей для доступа к среде ДДК осуществляется с помощью уникального идентификатора и дополнительного фактора аутентификации (например, пароля), выполнить следующее: • проверить документацию, описывающую используемый метод (методы) аутентификации; • посмотреть порядок аутентификации по каждому используемому методу аутентификации и типу системного компонента на предмет того, что аутентификация осуществляется согласно указанному в документации методу (методам) аутентификации.	Если данные методы аутентификации использовать совместно с уникальными учетными записями, то можно защитить уникальные учетные записи пользователей от компрометации, поскольку злоумышленнику нужно знать и уникальный идентификатор, и пароль (или другой используемый элемент аутентификации). Стоит учесть, что цифровой сертификат является подходящим вариантом для аутентификации по методу «обладания предметом», если он уникален для каждого конкретного пользователя. Поскольку одним из первых действий, которые злоумышленник предпринимает для компрометации системы, является использование простых или отсутствующих паролей, важно реализовать надежные процессы управления аутентификацией.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.1 Привести все учетные данные для аутентификации (например, пароли и (или) парольные фразы) к нечитаемому виду с использованием стойкой криптографии, когда они передаются или хранятся на любых системных компонентах.	**8.2.1.a** Проверить документацию вендора и настройки системной конфигурации на предмет того, что пароли защищены с использованием стойкой криптографии во время их передачи и хранения.	Многие сетевые устройства и приложения передают незашифрованные пароли (в читаемом виде) по сети и (или) хранят их в незашифрованном виде. Злоумышленник может без труда 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:*** *проверочные процедуры 8.2.1.d и 8.2.1.e являются дополнительными процедурами, применяемыми только для организаций, которые определены как поставщики услуг.*
	8.2.1.b Проверить файлы паролей в выборке системных компонентов на предмет того, что пароли хранятся в нечитаемом виде.	
	8.2.1.c Проверить передачу данных в выборке системных компонентов на предмет того, что пароли передаются в нечитаемом виде.	
	8.2.1.d ***Дополнительная проверочная процедура для оценки поставщиков услуг*:** проверить файлы паролей на предмет того, что пароли пользователей, не являющихся клиентами, хранятся в нечитаемом виде.	
	8.2.1.e ***Дополнительная проверочная процедура для оценки поставщиков услуг:*** проверить передачи данных на предмет того, что пароли пользователей, не являющихся клиентами, передаются в нечитаемом виде.	
8.2.2 Проверить идентификационные данные пользователя перед изменением любых учетных данных для аутентификации (например, перед сбросом пароля, перед предоставлением новых токенов или перед генерацией новых ключей).	**8.2.2** Проверить процедуры аутентификации, выполняемые перед изменением учетных данных для аутентификации, а также действия работников, отвечающих за безопасность, на предмет того, что, если сброс учетных данных для аутентификации запрашивается по телефону, электронной почте, через Интернет или иным удаленным способом, идентификационные данные пользователя проверяются до выполнения запроса.	Многие злоумышленники используют социальную инженерию – например, звонят в службу поддержки для изменения пароля и действуют как легитимный пользователь, чтобы изменить пароль и затем иметь возможность использовать учетную запись пользователя. Рекомендуется использовать секретный вопрос, ответ на который может дать только реальный пользователь, чтобы помочь администраторам идентифицировать пользователя перед сбросом или изменением учетных данных для аутентификации.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.3 Обеспечить соответствие паролей и (или) парольных фраз следующим требованиям: • длина пароля не менее семи символов; • наличие в пароле и цифр, и букв. Как вариант, пароли и (или) парольные фразы должны иметь сложность и стойкость, сравнимые с указанными выше параметрами.	**8.2.3.a** Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что пароли и (или) парольные фразы соответствуют следующим требованиям к сложности и стойкости: • длина пароля не менее семи символов; • наличие в пароле и цифр, и букв. **8.2.3.b** ***Дополнительная проверочная процедура для оценки поставщиков услуг*:** проверить внутренние процессы, а также клиентскую и (или) пользовательскую документацию на предмет того, что пароли и (или) парольные фразы пользователей, не являющихся клиентами, соответствуют, как минимум, следующим требованиям к сложности и стойкости: • длина пароля не менее семи символов; • наличие в пароле и цифр, и букв.	Надежные пароли и (или) парольные фразы являются первой линией обороны в сети, поскольку злоумышленник обычно сначала пытается найти учетные записи с простыми или отсутствующими паролями. Если используются короткие или тривиальные пароли, злоумышленнику относительно просто найти такие уязвимые учетные записи и скомпрометировать сеть с использованием идентификатора реального пользователя. В соответствии с данным требованием в паролях и (или) парольных фразах должно быть не менее семи символов (и букв, и цифр). Если данное минимальное требование не может быть выполнено в силу технических ограничений, организации могут рассмотреть альтернативные решения «эквивалентной надежности». Для дополнительной информации о вариативности и эквивалентной надежности (также используется термин «энтропия») паролей и (или) парольных фраз разных форматов следует обратиться к отраслевым стандартам (например, текущая версия NIST SP 800-63). ***Примечание:*** *проверочная процедура 8.2.3.b является дополнительной процедурой, применяемой только для организаций, которые определены как поставщики услуг.*
8.2.4 Менять пароли и (или) парольные фразы пользователей, как минимум, один раз в 90 дней.	**8.2.4.a** Проверить настройки системной конфигурации в выборке системных компонентов на предмет того, что настройки паролей и (или) парольных фраз пользователей требуют смену пароля, как минимум, один раз в 90 дней.	Пароли и (или) парольные фразы, которые не меняются и действуют в течение длительного времени, дают злоумышленникам больше времени для их подбора.

Требования PCI DSS	Проверочные процедуры	Пояснение
	8.2.4.b ***Дополнительная проверочная процедура для оценки поставщиков услуг****: проверить внутренние* процессы и документацию клиента и (или) пользователя на предмет того, что: • требуется периодическая смена паролей и (или) парольных фраз пользователей, не являющихся клиентами; • пользователи, не являющиеся клиентами, получают инструкции о том, когда и при каких обстоятельствах должен меняться пароль и (или) парольная фраза.	***Примечание:*** *проверочная процедура 8.2.4.b является дополнительной процедурой, применяемой только для организаций, которые определены как поставщики услуг.*

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.5 Запретить пользователю менять пароль и (или) парольную фразу на какие-либо из четырех последних паролей и (или) парольных фраз данного пользователя, использованных им ранее.	**8.2.5.a** Получить и проверить настройки системных конфигураций в выборке системных компонентов на предмет того, что настройки паролей требуют, чтобы новые пароли и (или) парольные фразы отличались от последних четырех использованных паролей.	Если история паролей не ведется, эффективность смены паролей снижается, так как предыдущие пароли могут быть многократно повторно использованы. Запрет повторного использования паролей в течение определенного периода времени снижает вероятность того, что угаданные или подобранные пароли будут использованы в будущем. ***Примечание:*** *проверочная процедура 8.2.5.b является дополнительной процедурой, применяемой только для организаций, которые определены как поставщики услуг.*
	8.2.5.b ***Дополнительная проверочная процедура оценки для поставщиков услуг:*** проверить внутренние процессы и документацию клиента и (или) пользователя на предмет того, что новый пароль и (или) парольная фраза пользователя, не являющегося клиентом, должен отличаться от четырех предыдущих паролей, использованных им ранее.	
8.2.6 Устанавливать каждому пользователю уникальные пароль и (или) парольную фразу для первоначального использования и при их сбросе, а также менять их сразу после первого использования.	**8.2.6** Проверить процедуры управления паролями и понаблюдать за работниками, отвечающими за безопасность, на предмет того, что для первоначальных паролей и (или) парольных фраз новых пользователей и сброшенных паролей и (или) парольных фраз существующих пользователей по каждому пользователю устанавливаются уникальные значения, которые меняются сразу после первого использования.	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, а затем использовать его для доступа к учетным записям.
8.3 Защитить все индивидуальные неконсольные административные доступы и все удаленные доступы в среду ДДК с использованием мультифакторной аутентификации.		Мультифакторная аутентификация требует от пользователя предоставления, как минимум, двух отдельных форм аутентификации (как описано в требовании 8.2) перед тем, как доступ будет предоставлен. Мультифакторная аутентификация обеспечивает дополнительную уверенность в том, что лица, пытающиеся получить доступ, являются теми, за кого себя выдают. При использовании мультифакторной аутентификации злоумышленнику придется скомпрометировать, как минимум, два различных аутентификационных механизма, что повышает сложность компрометации и таким образом уменьшает риск. Мультифакторная аутентификация не

Требования PCI DSS	Проверочные процедуры	Пояснение
		обязательно должна быть одновременно на обоих уровнях - на системном уровне и на уровне приложений - для определенного системного компонента. Мультифакторная аутентификация может выполняться либо при входе в определенную сеть, либо при входе в системный компонент. Примеры технологий мультифакторной аутентификации включают среди прочего удаленную аутентификацию и систему RADIUS с токенами; систему TACACS с токенами и другие технологии, которые поддерживают мультифакторную аутентификацию.
8.3.1 Реализовать мультифакторную аутентификацию для всех неконсольных доступов в среду ДДК для работников с административным доступом. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**8.3.1.a** Проверить сетевые и (или) системные конфигурации, в зависимости от ситуации, на предмет того, что мультифакторная аутентификация требуется для всех неконсольных административных доступов в среду ДДК. **8.3.1.b** Проследить за выборкой случаев входа работников, являющиеся администраторами, в среду ДДК на предмет того, что, как минимум, два из трех методов аутентификации используются.	Это требование распространяется на всех работников, обладающих административным доступом в среду ДДК. Это требование распространяется только на работников, обладающих административным доступом, и только для неконсольного доступа в среду ДДК. Это требование не распространяется на учетные записи приложений или систем, выполняющие автоматические функции. Если организация не использует сегментацию для отделения среды ДДК от остальной сети, администратор может использовать мультифакторную аутентификацию либо при входе в сеть среды ДДК, либо при входе в систему. Если среда ДДК отделена от остальной сети организации, администратору может потребоваться использование мультифакторной аутентификации во время подключения к системе среды ДДК из сети, не входящей в среду ДДК. Мультифакторная аутентификация может быть внедрена на уровне сети или на уровне системы и (или) приложения, внедрение на обоих уровнях не требуется. Если администратор использует мультифакторнную аутентификацию при входе в сеть среды ДДК,

Требования PCI DSS	Проверочные процедуры	Пояснение
		ему не нужно также использовать мультифакторную аутентификацию при входе в определенную систему или приложение внутри среды ДДК.
8.3.2 Реализовать мультифакторнуюаутентификацию, которая должна применяться к удаленному доступу в сеть (как для пользователей, так и для администраторов, включая третьих лиц для поддержки или обслуживания) из внешней сети.	**8.3.2.a** Проверить системные конфигурации серверов и систем удаленного доступа на предмет того, что мультифакторная аутентификация требуется для: • любого удаленного доступа работников, как пользователей, так и администраторов; • любого удаленного доступа третьих лиц и (или) вендоров (включая доступ к приложениям и системным компонентам для поддержки или обслуживания).	Данное требование предназначено для того, чтобы оно применялось ко всем работникам (включая обычных пользователей, администраторов и вендоров поддержки или техобслуживания), которые имеют удаленный доступ к сети, если через такой удаленный доступ можно получить доступ к среде ДДК. Если удаленный доступ осуществляется к сети, которая надлежащим образом сегментирована так, чтобы удаленные пользователи не могли получить доступ к среде ДДК или воздействовать на нее, мультифакторная аутентификация для удаленного доступа к такой сети не является обязательной. Однако мультифакторная аутентификация требуется для любого удаленного доступа к сетям, имеющим доступ к среде ДДК, и рекомендуется для любого удаленного доступа к сетям организации.
	8.3.2.b Проследить за тем, как работники из выборки (например, пользователи и администраторы) осуществляют удаленный доступ к сети, на предмет того, что используются как минимум два из трех методов аутентификации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.4 Документировать политики и процедурыаутентификации и довести их до сведения всех пользователей, включая: • рекомендации по выбору надежных учетных данных для аутентификации; • рекомендации для пользователей по защите учетных данных для аутентификации; • указания не использовать ранее использованные пароли; • указания по смене пароля в случае подозрения на его компрометацию.	**8.4.a** Проверить процедуры и опросить работников на предмет того, что политики и процедуры аутентификации доведены до сведения всех пользователей.	Доводя парольные политики и процедуры и политики и процедуры аутентификации до сведения всех пользователей, можно помочь им понять и соблюдать эти политики. Например, рекомендации по выбору надежных паролей могут включать советы работникам о том, как выбирать трудноугадываемые пароли, которые не содержат словарных слов или информацию о пользователе (например, идентификатор пользователя, имена членов семьи, дата рождения и т. д.). Рекомендации по защите учетных данных для аутентификации могут быть следующими: — не записывать пароли, — не сохранять пароли в незащищенных файлах , — проявлять бдительность в отношении злоумышленников, которые могут попытаться использовать их пароли (например, звоня работнику с просьбой дать его пароль для решения какой-либо проблемы). Рекомендуя пользователям сменить пароли, если есть вероятность, что пароль больше не является надежным, можно пресечь злоумышленникам возможность использовать действующий пароль для получения несанкционированного доступа.
	8.4.b Проверить политики и процедурыаутентификации, доведенные до сведения пользователей, на предмет того, что туда включены: • рекомендации по выбору надежных учетных данных для аутентификации; • рекомендации пользователям по защите своих учетных данных для аутентификации; • указания пользователям не использовать ранее использованные пароли; • указания по смене пароля в случае подозрения на его компрометацию.	
	8.4.c Опросить пользователей из выборки на предмет того, что им известны политики и процедуры аутентификации.	
8.5 Не использовать групповые, общие и стандартные учетные записи и пароли, а также прочие подобные методы аутентификации и обеспечить выполнение следующих положений: • стандартные учетные записи заблокированы или удалены; • общие учетные записи для системного администрирования и иных критичных функций	**8.5.a** Проверить списки учетных записей пользователей в выборке системных компонентов на предмет того, что: • стандартные учетные записи заблокированы или удалены; • общие учетные записи пользователей для системного администрирования и иных критичных функций отсутствуют; • общие и стандартные учетные записи пользователей не используются для администрирования любых системных компонентов.	Если несколько пользователей используют одни и те же учетные данные для аутентификации (например, учетную запись и пароль), проследить за доступом в систему и действиями того или иного пользователя становится невозможно. Это, в свою очередь, не позволит организации устанавливать ответственность за действия конкретного пользователя, или фактически регистрировать события, связанные с этими действиями, поскольку эти действия

Требования PCI DSS	Проверочные процедуры	Пояснение
отсутствуют; • общие и стандартные учетные записи пользователей не используются для администрирования любых системных компонентов.	**8.5.b** Проверить политики и процедуры аутентификации на предмет того, что они явным образом запрещают использование групповых и общих учетных записей и (или) паролей и прочих подобных средств аутентификации. **8.5.c** Опросить системных администраторов на предмет того, что пользователям не выдаются групповые и общие учетные записи и (или) пароли и прочие подобные средства аутентификации, даже если таковые запрашиваются.	могут быть совершены любым членом группы, которой известны учетные данные для аутентификации.
8.5.1 ***Дополнительное требование для поставщиков услуг:*** поставщики услуг, имеющие удаленный доступ к помещениям клиента (например, для поддержки POS систем или серверов), обязаны использовать уникальные учетные данные для аутентификации (например, пароль и (или) парольная фраза) для каждого клиента. ***Примечание:*** *это требование не распространяется на поставщиков услуг хостинга, осуществляющих доступ к своей общей хостинговой среде, в которой размещены среды нескольких клиентов.*	**8.5.1** ***Дополнительная проверочная процедура для оценки поставщиков услуг:*** проверить политики и процедуры аутентификации и опросить сотрудников на предмет того, что для каждого клиента используются отдельные учетные данные.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Чтобы предотвратить компрометацию учетных записей нескольких клиентов через компрометацию единых учетных данных, вендоры, осуществляющие удаленный доступ к средам клиентов, должны использовать разные учетные данные для аутентификации на каждого клиента. Такие технологии, как мультифакторная аутентификация, обеспечивающая уникальность учетных данных для каждого подключения (например, с помощью одноразового пароля), также могут отвечать данному требованию.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.6 Если используются иные механизмы аутентификации (например, физические или логические токены безопасности, смарт-карты, сертификаты и т. д.), организация должна: • назначать механизмы аутентификации для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу; • реализовать физические и (или) логические меры, чтобы для получения доступа такие механизмы мог использовать только тот пользователь, для которого они предназначены.	**8.6.a** Проверить политики и процедуры аутентификации на предмет того, что для использования механизмов аутентификации (например, физических токенов безопасности, смарт-карт и сертификатов) определены процедуры, которые, среди прочего, требуют: • назначать механизмы аутентификации для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу; • установить физические и (или) логические защитные меры, чтобы для получения доступа такие механизмы мог использовать только тот пользователь, для которого они предназначены.	Если механизмы аутентификации пользователя (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, ПИН-код, биометрические данные или пароль), уникальных для каждого пользователя, не позволит злоумышленникам получить доступ с помощью общего механизма аутентификации.
	8.6.b Опросить работников, отвечающих за безопасность, на предмет того, что механизмы аутентификации назначаются для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу.	
	8.6.c Проверить настройки системной конфигурации и (или), по возможности, механизмы физической защиты на предмет того, что механизмы реализованы так, чтобы только авторизованный пользователь мог использовать такие механизмы для получения доступа.	
8.7 Ограничить любой доступ к базе данных, содержащей ДДК (включая доступ со стороны приложений, администраторов и любых других пользователей) следующим образом: • осуществлять доступ, запросы и операции с базами данных только программными методами; • разрешать запросы и прямой	**8.7.a** Проверить настройки конфигурации баз данных и приложений на предмет того, что пользователи проходят аутентификацию перед предоставлением доступа.	Если аутентификация пользователя для доступа к базам данных и приложениям не выполняется, повышается риск несанкционированного или вредоносного 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
	8.7.b Проверить настройки конфигурации баз данных и приложений на предмет того, что любые пользовательские операции с данными (доступ, запрос, перемещение, копирование, удаление) осуществляются только программными методами (например, с использованием хранимых процедур).	

Требования PCI DSS	Проверочные процедуры	Пояснение
доступ к базам данных только администраторам баз данных; • разрешать использовать учетные записи приложений для доступа к БД только приложениям (а не отдельным пользователям или иным процессам).	**8.7.c** Проверить настройки контроля доступа к базам данных и настройки конфигурации приложений для доступа к базам данных на предмет того, что запросы и прямой доступ к базам данных разрешен только администраторам баз данных.	хранимых процедур), а не через прямой доступ конечных пользователей к базе данных (за исключением администраторов баз данных, которым может потребоваться прямой доступ к базе данных для выполнения своих административных обязанностей).
	8.7.d Проверить настройки контроля доступа к базам данных, настройки конфигурации и систем управления базами данных и учетные записи приложений для доступа к базам данных на предмет того, что учетные записи приложений могут использоваться только приложениями (а не отдельными пользователями или иными процессами).	
8.8 Гарантировать, что политики безопасности и операционные процедуры идентификации и аутентификации документированы, используются и известны всем заинтересованным лицам.	**8.8** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры идентификации и аутентификации: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры непрерывного управления идентификацией и авторизацией.

Требование 9. Ограничивать физический доступ к ДДК

Любой физический доступ к данным или системам, содержащим ДДК, предоставляет лицам возможность получить доступ к устройствам или данным, удалить системы или печатные материалы. Такой доступ должен быть соответствующим образом ограничен. В рамках требования 9 термин «работник объекта» относится к постоянным работникам, занятым как полный, так и неполный рабочий день, временным работникам, подрядчикам и консультантам, находящимся на территории организации. Термин «посетитель» относится к вендорам, гостям работников объекта, обслуживающему персоналу и иным лицам, кратковременно находящимся на территории организации, как правило, не более одного дня. Термин «носитель» относится ко всем бумажным и электронным носителям, которые содержат ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.1 Использовать надлежащие средства контроля прохода на территорию, чтобы ограничивать и отслеживать физический доступ к системам среды ДДК.	**9.1** Убедиться, что меры обеспечения физической безопасности имеются в каждом машинном зале, центре обработки данных и иных физических зонах, в которых располагаются системы среды ДДК. • Убедиться, что доступ контролируется с помощью устройств считывания бейджей или иных механизмов, включая бейджи для авторизации и механические замки. • Проследить за попыткой системного администратора войти в консоли случайно выбранных систем среды ДДК на предмет того, что они заблокированы во избежание несанкционированного доступа.	Без механизмов контроля физического доступа (например, бейджей и контроля за входом в помещения) посторонние могут без труда получить доступ к помещениям с целью кражи, отключения, порчи или уничтожения критичных систем и ДДК. Блокировка экрана входа в консоль не позволит посторонним получить доступ к критичной информации, внести изменения в системную конфигурацию, внести уязвимости в сеть или уничтожить записи.
9.1.1 Использовать либо камеры видеонаблюдения, либо механизмы контроля доступа (или оба варианта) для отслеживания каждого случая	**9.1.1.a** Убедиться, что установлены либо камеры видеонаблюдения, либо механизмы контроля доступа (или оба варианта) для наблюдения за точками входа (выхода) в критичные помещения.	Если расследуются нарушения физической безопасности, такие механизмы дают возможность выявлять лица, которые осуществляли физический доступ к критичным

Требования PCI DSS	Проверочные процедуры	Пояснение
физического доступа к критичным помещениям. Проверять собранные данные и сопоставлять их с другими данными. Хранить эти данные не менее трех месяцев, если законодательством не наложены иные ограничения. ***Примечание:*** *термин «критичные помещения» относится к любым центрам обработки данных, серверным комнатам или иным помещениям, в которых расположены системы, хранящие, обрабатывающие или передающие ДДК. Исключением являются места, где присутствуют только POS-терминалы, например, кассовые зоны розничных магазинов.*	**9.1.1.b** Убедиться, что либо камеры видеонаблюдения, либо механизмы контроля доступа (или оба варианта) защищены от физического вмешательства или отключения.	помещениям, а также установить время входа и выхода. Злоумышленники, желающие получить физический доступ к критичным помещениям, часто пытаются отключить или обойти средства мониторинга. Чтобы защитить такие устройства от физического вмешательства, видеокамеры можно разместить за пределами досягаемости и (или) так, чтобы можно было обнаруживать попытки физического вмешательства. Механизмы контроля доступа также могут находиться под наблюдением или быть оснащены физическими средствами защиты от повреждения или отключения злоумышленниками. *(Продолжение на следующей странице)*
	9.1.1.c Убедиться, что данные, полученные с камер видеонаблюдения и (или) механизмов контроля доступа, проверяются, и эти данные хранятся не менее 3 месяцев.	Критичными помещениями являются, например, комнаты с серверами корпоративных баз данных; служебные помещения розничных магазинов, где хранятся ДДК; хранилища с большим объемом ДДК. Каждая организация должна составить список критичных помещений, чтобы обеспечить реализацию надлежащих физических механизмов наблюдения.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.1.2 Внедрить механизмы физического и (или) логического контроля, чтобы ограничить доступ к сетевым разъемам, расположенным в общедоступных местах. *Например, сетевые разъемы, расположенные в общедоступных местах и местах, доступных посетителям, можно отключать и включать только тогда, когда доступ к сети однозначно разрешен. Также можно внедрить процессы, исключающие наличие посетителей без постоянного сопровождения в помещениях с работающими сетевыми разъемами.*	**9.1.2** Опросить ответственных работников и проверить места расположения общедоступных сетевых разъемов на предмет того, что там реализованы меры физического и (или) логического контроля для ограничения доступа к общедоступным сетевым разъемам.	Ограничение доступа к сетевым разъемам (или портам) исключает для злоумышленников возможность подключиться к сетевым разъемам и получить доступ к внутренним сетевым ресурсам. Независимо от типа используемых механизмов контроля (физических, логических или смешанных) они должны обеспечивать достаточную защиту, чтобы исключить подключение к сети лиц или устройств, не имеющих на то явного разрешения.
9.1.3 Ограничить физический доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому или коммуникационному оборудованию и линиям связи.	**9.1.3** Убедиться, что физический доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому или коммуникационному оборудованию и линиям связи должным образом ограничен.	Если доступ к беспроводным компонентам и устройствам не защищен, злоумышленники могут использовать неконтролируемые беспроводные устройства организации для получения доступа к сетевым ресурсам или даже подключать собственные устройства к беспроводной сети, чтобы получить несанкционированный доступ. 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, которые позволяют легко различать работников объекта от посетителей и которые предусматривают: • идентификацию работников объекта или посетителей (например, путем выдачи бейджей); • требования к внесению изменений в права доступа; • изъятие или блокирование средств идентификации у работников объекта или средств идентификации с истекшим сроком действия (например, бейджей) у посетителей.	**9.2.a** Проверить документированные процессы на предмет того, что в них определены процедуры, которые требуют идентифицировать и различать работников объекта и посетителей. Убедиться, что процедуры предусматривают: • идентификацию работников объекта и посетителей (например, путем выдачи бейджей); • требования к внесению изменений в права доступа; • изъятие или блокирование средств идентификации у работников объекта или средств идентификации с истекшим сроком действия (например, бейджей) у посетителей.	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 Проверить методы идентификации (такие как бейджи) и пронаблюдать процессы идентификации и различения работников объекта и посетителей на предмет того, что: • посетители четко идентифицированы; • работники объекта явно отличаются от посетителей.	
	9.2.c Убедиться, что доступ к процессу идентификации (например, к системе выдачи бейджей) ограничивается только уполномоченными работниками.	
9.3 Контролировать физический доступ работников объекта к критичным помещениям следующим образом: • утверждать права доступа согласно персональным должностным обязанностям; • отзывать доступ сразу после увольнения работника; забирать или отключать все средства физического доступа (например, ключи, карты доступа и т. д.).	**9.3.a** Из выборки работников объекта, имеющих физический доступ к критичным помещениям опросить ответственных работников и проверить списки контроля доступа на предмет того, что: • доступ к критичным помещениям утвержден; • доступ необходим для выполнения должностных обязанностей.	Контроль физического доступа к критичным помещениям позволяет обеспечить, чтобы доступ предоставлялся только уполномоченным работникам, которым он необходим для выполнения должностных обязанностей. Если работник увольняется из организации, сразу после увольнения (как можно скорее) следует забрать или отключить все средства физического доступа, чтобы работник не мог получить физический доступ к критичным помещениям.
	9.3.b Проследить за входом работников в критичные помещения на предмет того, что все работники проходят авторизацию перед получением доступа.	
	9.3.c Сделать выборку недавно уволенных работников и проверить списки контроля доступа на предмет того, что у них нет физического доступа к критичным помещениям.	

Требования PCI DSS	Проверочные процедуры	Пояснение
9.4 Внедрить процедуры идентификации и авторизации посетителей, в т. ч.:	**9.4** Проверить наличие механизмов авторизации и контроля доступа посетителей следующим образом:	Средства контроля посетителей снижают риск того, что посторонние лица и злоумышленники получат доступ в помещения организации (и, потенциально, к ДДК). Средства контроля посетителей обеспечивают возможность, чтобы посетители идентифицировались именно как посетители и чтобы за их действиями могли наблюдать работники. Средства контроля также обеспечивают, чтобы продолжительность доступа посетителей была ограничена отведенным им временем посещения. Обязательное изъятие бейджей у посетителей после истечения срока действия или завершения посещения исключает для злоумышленников возможность воспользоваться ранее авторизованным пропуском для получения физического доступа в здание после завершения визита. Журнал регистрации посетителей, где фиксируется минимум информации о посетителе, является простым и недорогим в обслуживании средством, позволяющим идентифицировать физический доступ в здание или помещение и потенциальный доступ к ДДК.
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** Просмотреть процедуры и опросить работников на предмет того, что посетители получают разрешение до получения доступа в помещения, где обрабатываются или хранятся ДДК, и посетителей постоянно сопровождают во время пребывания в этих помещениях.	
	9.4.1 Проследить за использованием бейджей посетителей или других средств идентификации на предмет того, что бейдж не дает возможности получить доступ в помещения, где хранятся ДДК, без сопровождения работников организации.	
9.4.2 Идентифицировать посетителей и выдавать им бейдж или другое средство идентификации с ограниченным сроком действия и позволяющее отличить посетителя от работника объекта.	**9.4.2.a** Осмотреть бейджи лиц, находящихся на территории объекта, на предмет того, что у посетителей есть бейджи или иные средства идентификации и что посетителей легко отличить от работников объекта.	
	9.4.2.b Убедиться, что бейдж посетителя или иное средство идентификации посетителя имеет ограниченный срок действия.	
9.4.3 Требовать от посетителей вернуть выданный бейдж или иное средство идентификации до ухода с объекта или по истечении срока его действия.	**9.4.3** Проследить за процессом ухода посетителей с объекта на предмет того, что от посетителей требуется возврат бейджа или другого средства идентификации при уходе посетителя или окончании срока действия средства идентификации.	
9.4.4 Ведется журнал регистрации посетителей как на входе в помещения, так и на входе в вычислительные центры и центры обработки данных, в которых хранятся или передаются ДДК. В журнале регистрировать имя посетителя, организацию, которую он представляет, а также данные работника объекта, который	**9.4.4.a** Убедиться в том, что ведется журнал регистрации посетителей, в который заносятся записи о физическом доступе на объект, а также в машинные залы и центры обработки данных, где хранятся или передаются ДДК.	
	9.4.4.b Убедиться, что журнал содержит: • имя посетителя; • название организации, которую он представляет; • имя работника объекта, разрешившего посетителю физический доступ.	

Требования PCI DSS	Проверочные процедуры	Пояснение
разрешил физический доступ. Хранить этот журнал не менее трех месяцев, если законодательством не установлены иные ограничения.	**9.4.4.c** Убедиться в том, что журнал хранится не менее трех месяцев.	
9.5 Обеспечить физическую безопасность всех носителей.	**9.5** Убедиться, что процедуры защиты ДДК включают меры физической защиты для всех носителей (в т. ч., среди прочего, компьютеры, съемные электронные носители, бумажные счета, бумажные отчеты и факсы).	Меры физической безопасности носителей предназначены для того, чтобы предотвращать несанкционированный доступ к ДДК на носителях любого типа. Если ДДК не защищены должным образом на съемных и портативных носителях, распечатаны или оставлены без присмотра на чьем-либо столе, существует вероятность их несанкционированного просмотра, копирования или сканирования.
9.5.1 Хранить носители с резервными копиями в безопасном месте, желательно в удаленном подразделении, например, в альтернативном или резервном месте, либо на территории организации, обеспечивающей безопасное хранение. Проверять безопасность этого места не реже раза в год.	**9.5.1.** Проверить, что безопасность места расположения хранилища проверяется не реже одного раза в год, чтобы убедиться,что хранилище для носителей резервных копий является безопасным.	Если хранилище небезопасно, то резервные копии, в которых содержатся ДДК, могут быть легко потеряны, похищены или скопированы для злонамеренных целей. Периодическая проверка хранилища позволяет организации вовремя решать обнаруженные проблемы с безопасностью, сводя к минимуму потенциальный риск.
9.6 Обеспечить строгий контроль за внутренним или внешним перемещением всех видов носителей, в т. ч. следующим образом:	**9.6** Проверить наличие политики контроля перемещения всех видов носителей, а также проверить, что эта политика охватывает все переданные носители, включая переданные частным лицам.	Процедуры и процессы помогают защитить ДДК на носителях, которые передаются пользователям организации или сторонним пользователям. Если таких процедур нет, то данные могут быть потеряны, украдены или использованы в мошеннических целях.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.6.1 классифицировать носители так, чтобы можно было определить уровень критичности хранимых данных;	**9.6.1** Проверить, что носители классифицированы так, чтобы можно было определить уровень критичности данных.	Важно, чтобы носитель был промаркирован таким образом, чтобы его категория была очевидна. Носитель, который не маркирован как конфиденциальный, может быть недостаточно защищен, а также может быть потерян или украден. ***Примечание:*** *это не означает, что необходимо прикреплять к носителям маркировку «Конфиденциальная информация»; цель требования состоит в такой идентификации носителей с критичными данными, которая позволит организации защищать их.*
9.6.2 отправлять носители только надежными курьерами или иным способом доставки, который позволяет точно отслеживать посылку.	**9.6.2.a** Опросить работников и проверить записи на предмет того, что пересылка любого носителя за пределы подразделения регистрируется в журнале, а сама пересылка выполняется только надежными курьерами или иным способом, который можно тщательно отслеживать.	Если носитель отправляется способом, не предусматривающим отслеживание (например, обычной почтой), то он может быть утерян или украден. Использование надежных курьеров для доставки любых носителей с ДДК позволяет организации использовать систему отслеживания, чтобы вести учет местонахождения посылок.
	9.6.2.b Сделать выборку записей за несколько последних дней из журнала перемещения всех носителей за пределы охраняемой территории и проверить выборку на предмет того, что сведения о перемещении носителей документируются.	
9.6.3 Гарантировать, что любой вынос любых носителей за пределы охраняемой территории (включая передачу носителя частным лицам) утверждается руководством.	**9.6.3** Сделать выборку записей за несколько последних дней из журнала перемещения всех носителей. Проверить журналы и опросить ответственных работников на предмет того, что любой вынос носителей за пределы охраняемой территории (включая передачу носителя частным лицам) надлежащим образом утверждается руководством.	Если нет четкого процесса для утверждения любых перемещений носителей за пределы охраняемой территории, то носители нельзя будет ни отслеживать, ни должным образом защищать, их местонахождение будет неизвестно, что приведет к потере или краже носителей.
9.7 Обеспечить строгий контроль хранения и доступности носителей.	**9.7** Получить и проверить политику контроля хранения и обслуживания всех носителей на предмет того, что она требует периодическую инвентаризацию носителей.	Если методы тщательной инвентаризации и контроля за хранением отсутствуют, то факт кражи или утери носителя может оставаться

Требования PCI DSS	Проверочные процедуры	Пояснение
9.7.1 Должным образом вести журналы инвентаризации всех носителей и проводить инвентаризацию носителей не реже одного раза в год.	**9.7.1** Проверить журналы инвентаризации носителей на предмет того, что такие журналы ведутся, а инвентаризация носителей проводится не реже одного раза в год.	незамеченным в течение неопределенного периода времени. Если носители не проходят инвентаризацию, то факт кражи или утери носителя может остаться незамеченным навсегда или в течение длительного периода времени.
9.8 Уничтожать носители, которые более не требуются для служебных нужд или для выполнения требований законодательства, следующим способом:	**9.8** Проверить политику периодического уничтожения носителей на предмет того, что она распространяется на все носители, и содержит следующие требования: • печатные материалы измельчать путем перекрестной резки, сжигать или преобразовывать в целлюлозную массу способом, исключающим их восстановление; • защищать контейнеры для материалов, приготовленных для уничтожения; • уничтожать ДДК на электронном носителе без возможности восстановления (например, с помощью программы безопасного удаления данных в соответствии с отраслевыми стандартами безопасного удаления или путем физического уничтожения носителя).	Если информация, содержащаяся на жестких дисках компьютеров, портативных накопителях, CD- и DVD-дисках или на бумаге, не уничтожается надлежащим образом, злоумышленники могут извлечь эту информацию с утилизированных носителей и получить доступ к ДДК. Например, злоумышленники могут исследовать содержимое мусорных контейнеров на наличие информации, которую они могут использовать для атак. Защита контейнеров для материалов, приготовленных для уничтожения, позволяет предотвратить получение критичной информации при сборе материалов. Например, контейнеры с материалами, подлежащими измельчению, могут быть оборудованы замком для предотвращения доступа к их содержимому или они могут иным образом физически исключать доступ в контейнер. Для безопасного уничтожения электронных носителей можно, например, использовать безопасное стирание, размагничивание или физическое разрушение носителя (например, истирание или измельчение жесткого диска).
9.8.1 Измельчать, сжигать или преобразовывать печатные материалы в целлюлозную массу способом, исключающим возможность восстановления ДДК. Защищать контейнеры для материалов, приготовленных для уничтожения.	**9.8.1.a** Опросить работников и проверить процедуры на предмет того, что печатные материалы измельчаются путем перекрестной резки, сжигаются или преобразовываются в целлюлозную массу способом, исключающим их восстановление.	
	9.8.1.b Осмотреть контейнеры для материалов, приготовленных для уничтожения, на предмет того, что они надежно защищены.	
9.8.2 Привести ДДК, хранимые на электронных носителях, к состоянию, исключающему возможность их восстановления.	**9.8.2** Убедиться в том, что ДДК на электронных носителях уничтожаются без возможности восстановления (например, с помощью программы безопасного удаления данных в соответствии с отраслевыми стандартами безопасного удаления или путем физического уничтожения носителя).	

Требования PCI DSS	Проверочные процедуры	Пояснение
9.9 Защитить устройства, считывающие ДДК путем прямого физического взаимодействия с картой, от физического вмешательства и подмены. ***Примечание:*** *данные требования распространяются на устройства для считывания информации с платежной карты, которые используются в точке продаж для транзакций с предоставлением карты (т. е. при проведении карты через устройство или при вставке в него карты). Данное требование не распространяется на компоненты ручного ввода ключа (например, компьютерные клавиатуры и клавиатуры POS-терминала).*	**9.9** Проверить документированные политики и процедуры на наличие следующих требований: • поддерживать список устройств; • периодически проверять устройства на предмет физического вмешательства или подмены; • обучить работников, чтобы они знали признаки подозрительного поведения и уведомляли о физическом вмешательстве или подмене устройств.	Злоумышленники пытаются красть ДДК путем кражи и (или) подмены считывающих устройств и терминалов. Например, они пытаются украсть устройства, чтобы понять, как их взломать и часто пытаются заменить настоящие устройства на мошеннические, 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 дополнительное устройство для считывания карт поверх настоящего, чтобы данные о платежной карте считывались дважды – сначала поддельным, а затем настоящим компонентом устройства). Таким образом, транзакции могут проходить в обычном режиме, в то время как злоумышленник «снимает» информацию с платежной карты. Для компонентов ручного ввода ключа (например, компьютерных клавиатур и клавиатур POS-терминалов) данное требование является рекомендуемым, но не обязательным. Дополнительную информацию о передовом опыте по предотвращению скимминга можно найти на сайте PCI SSC.
9.9.1 Вести актуальный список устройств. Список должен включать следующую информацию: • марка и модель устройства; • местонахождение устройства (например, адрес объекта или подразделения, в котором	**9.9.1.a** Проверить, что список устройств включает следующую информацию: • марка и модель устройства; • местонахождение устройства (например, адрес объекта или подразделения, в котором находится устройство); • серийный номер устройства или другой уникальный идентификатор.	Поддерживая актуальный список устройств, организация может отслеживать предполагаемое местонахождение устройства и быстро его обнаруживать в случае его утери или пропажи. Список устройств может составляться автоматически (например, через систему

Требования PCI DSS	Проверочные процедуры	Пояснение
находится устройство); • серийный номер устройства или другой уникальный идентификатор.	**9.9.1.b** Сделать выборку устройств из списка и проверить устройства и их местонахождение на предмет того, что список является точным и актуальным.	управления устройствами) или вручную (например, в электронных или бумажных записях). Для устройств, находящихся в постоянном движении, информация о местонахождении может включать в себя имя работника, за которым это устройство закреплено.
	9.9.1.c Опросить работников на предмет того, что список актуализируется каждый раз, когда устройства добавляются, перемещаются, списываются и т. д.	
9.9.2 Периодически проверять поверхность устройств для обнаружения признаков физического вмешательства (например,	**9.9.2.a** Проверить документированные процедуры на предмет того, что в процессах определено следующее: • процедуры осмотра устройств; • частота осмотров.	Регулярно осматривая устройства, организации могут быстрее обнаруживать физическое вмешательство или подмену устройства и, следовательно, снижать потенциальный ущерб

Требования PCI DSS	Проверочные процедуры	Пояснение
прикрепленных к устройствам скиммеров) или подмены (например, проверяя серийный номер или иные характеристики устройств на предмет того, что устройство не было заменено на мошенническое). ***Примечание:*** *признаками того, что устройство подверглось физическому вмешательству или что устройство было подменено, могут служить подозрительные накладки или кабели, подключенные к устройству, отсутствующие или измененные защитные наклейки (пломбы), поврежденный или перекрашенный корпус, изменение серийного номера или иных внешних обозначений.*	**9.9.2.b** Опросить ответственных работников и проследить за процессом осмотра на предмет того, что: • работники знают процедуры осмотра устройств; • все устройства периодически осматриваются на наличие следов физического вмешательства или подмены.	от мошеннических устройств. Способ осмотра зависит от устройства (например, можно использовать фотографию изначально безопасного устройства, чтобы сравнить текущий вид с исходным и обнаружить изменения). Также можно использовать защитный маркер (например, видимый в ультрафиолетовом излучении) для маркировки поверхностей и отверстий устройства, чтобы можно было легко заметить любое физическое вмешательство или подмену. Злоумышленники часто заменяют внешний кожух устройства, чтобы скрыть следы физического вмешательства, и указанные выше способы помогут обнаружить такую замену. Поставщики устройств также часто предоставляют рекомендации по защите и инструкции, которые помогут определить, подвергалось ли устройство физическому вмешательству. Частота осмотров зависит от таких факторов, как местонахождение устройства и наличие за ним наблюдения. Например, устройства, установленные работниками организации в общественном месте и находящиеся без присмотра, требуется осматривать чаще, чем устройства, расположенные в безопасном месте и находящиеся под присмотром. Способ и частота осмотров определяется ТСП согласно его процессу ежегодной оценки рисков.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.9.3 Обучать работников распознавать признаки физического вмешательства или подмены устройств. Обучать в т. ч. следующему: • проверять личность любых третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, до того, как им предоставляется доступ на внесение изменений или устранение проблем с устройствами; • не устанавливать, не заменять или не возвращать устройства без проверки; • знать признаки подозрительного поведения вблизи устройств (например, попыток посторонних лиц отключить или открыть устройства); • сообщать соответствующим работникам (например, руководителю или специалисту по безопасности) о подозрительном поведении, признаках физического вмешательства или подмены устройства.	**9.9.3.a** Проверить учебные материалы для работников в точках продаж на предмет того, что материалы обучают в т. ч. следующему: • проверять личность любых третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, до того, как им предоставляется доступ на внесение изменений или устранение проблем с устройствами; • не устанавливать, не заменять или не возвращать устройства без проверки; • знать признаки подозрительного поведения вблизи устройств (например, попытки посторонних лиц отключить или открыть устройства); • сообщать соответствующим работникам (например, руководителю или специалисту по безопасности) о подозрительном поведении, признаках физического вмешательства или подмены устройства.	Злоумышленники часто выдают себя за уполномоченный обслуживающий персонал для получения доступа к POS-устройствам. Следует проверять все третьи лица, запрашивающие доступ к устройствам, до того, как предоставить им доступ, например, посовещавшись с руководством или позвонив в компанию, обслуживающую POS-терминалы, (например, вендору или эквайреру) для получения подтверждения. Злоумышленники часто пытаются обмануть работников, 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 работники были обучены всегда соблюдать установленные процедуры. Еще один излюбленный трюк злоумышленников – отправка почтой «новой» системы POS-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 работники должны всегда удостоверять у руководителя и поставщика, что оно настоящее и получено из доверенного источника.
	9.9.3.b Опросить работников из выборки в местах установки POS-терминалов на предмет того, что они прошли обучение и знают процедуры того, как: • проверять личность любых третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, до того, как им предоставляется доступ на внесение изменений или устранение проблем с устройствами; • не устанавливать, не заменять или не возвращать устройства без проверки; • знать признаки подозрительного поведения вблизи устройств (например, попыток посторонних лиц отключить или открыть устройства); • сообщать соответствующим работникам (например, руководителю или специалисту по безопасности) о подозрительном поведении, признаках физического вмешательства или подмены устройства.	

Требования PCI DSS	Проверочные процедуры	Пояснение
9.10 Гарантировать, что политики безопасности и операционные процедуры ограничения физического доступа к ДДК документированы, используются и известны всем заинтересованным лицам.	**9.10** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры ограничения физического доступа к ДДК: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и процедуры постоянного ограничения физического доступа к ДДК и среде ДДК.

Осуществлять регулярный мониторинг и тестирование сетей

Требование 10. Отслеживать и вести мониторинг всего доступа к сетевым ресурсам и ДДК

Механизмы регистрации событий и возможность проследить действия пользователей являются критичными для обнаружения, предотвращения и минимизации воздействия от компрометации данных. Наличие журналов регистрации во всех средах позволяет тщательно отслеживать, создавать оповещения и проводить анализ при возникновении внештатных ситуаций. Без журналов регистрации действий в системе определить причины компрометации трудно, если вообще возможно.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.1 Внедрить журналы регистрации событий, в которых любой доступ к системным компонентам привязывается к конкретному пользователю.	**10.1** Наблюдая за действиями системного администратора и опрашивая его, проверить, что: • включено и действует ведение журналов регистрации событий системных компонентов; • доступ к системным компонентам привязывается к конкретным пользователям.	Важно иметь процесс или систему, где доступ пользователей привязывается к компонентам системы, к которым он осуществлялся. Данная система будет генерировать журналы регистрации событий и позволит отслеживать подозрительную деятельность определенного пользователя.
10.2 Реализовать автоматизированные журналы регистрации событий на всех системных компонентах, чтобы можно было восстановить следующие события:	**10.2** Опрашивая ответственных работников, просматривая журналы аудита и их настройки, выполнить следующее:	Генерация журналов регистрации событий о подозрительной деятельности позволяет предупреждать системного администратора, отправлять данные на другие средства мониторинга (например, в системы обнаружения вторжений), а также отслеживать хронологию событий для расследования инцидентов безопасности. Регистрация следующих событий позволяет организации выявить и отследить потенциально вредоносную деятельность.
10.2.1 все сеансы персонального доступа пользователей к ДДК;	**10.2.1** убедиться, что каждый персональный сеанс доступа к ДДК регистрируется;	Злоумышленники могут получить информацию об учетной записи пользователя с доступом к системам в среде ДДК или создать новую несанкционированную учетную запись для получения доступа к ДДК. Регистрация всех сеансов доступа к ДДК позволяет выявить, какие учетные записи могут быть скомпрометированы или неправильно использованы.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.2.2 все действия, совершенные любым лицом с привилегиями суперпользователя (root) или администратора;	**10.2.2** убедиться в том, что регистрируются все действия, совершенные любым лицом с привилегиями суперпользователя или администратора;	Учетные записи с расширенными правами доступа, такие как «администратор» или «суперпользователь», могут существенно влиять на безопасность или функциональные возможности системы по выполнению операций. Если не регистрировать выполняемые действия, организация не сможет отслеживать проблемы, связанные с ошибками администрирования или ненадлежащим использованием прав доступа в отношении отдельных лиц или действий.
10.2.3 доступ ко всем журналам регистрации событий;	**10.2.3 убедиться, что регистрируется доступ ко всем журналам регистрации событий;**	Злоумышленники часто пытаются изменить записи в журнале, чтобы скрыть свои действия. Регистрация сеансов доступа позволяет организации связывать несоответствия или возможные изменения записей в журнале с конкретной учетной записью. Имея доступ к журналам изменений, добавлений и удалений, есть возможность отследить несанкционированные действия сотрудников.
10.2.4 неуспешные попытки логического доступа;	**10.2.4** убедиться, что регистрируются неуспешные попытки логического доступа;	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, перебирая или угадывая пароли.
10.2.5 использование и изменение механизмов идентификации и аутентификации, включая, помимо прочего, создание новых учетных записей, повышение привилегий, а также все изменения, добавления, удаления учетных записей с правами суперпользователя или администратора	**10.2.5.a** убедиться в том, что регистрируется использование механизмов идентификации и аутентификации;	Не зная того, кто входил в систему на момент возникновения инцидента, невозможно выявить учетные записи, которые могли быть использованы. Кроме того, злоумышленники могут также пытаться манипулировать механизмами аутентификации, чтобы обойти их или выдать себя за другого пользователя.
	10.2.5.b убедиться в том, что регистрируется любое повышение привилегий;	
	10.2.5.c убедиться в том, что регистрируются любые изменения, добавления или удаления в отношении любых учетных записей с правами суперпользователя или администратора.	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.2.6 запуск, остановка или приостановка ведения журналов регистрации событий;	**10.2.6** убедиться в регистрации следующих событий: • запуск журналов аудита; • остановка или приостановка журналов аудита;	Выключение (или приостановка ведения) журналов аудита перед выполнением подозрительных действий является распространенной практикой среди злоумышленников, которые стремятся избежать обнаружения. Запуск журнала аудита может указывать на то, что функции журнала были отключены пользователем в целях сокрытия своих действий.
10.2.7 создание и удаление объектов системного уровня.	**10.2.7** убедиться, что регистрируется создание и удаление объектов системного уровня.	Вредоносное ПО часто создает или заменяет объекты системного уровня на целевой системе, чтобы получить контроль над определенной функцией или операцией в этой системе. Регистрация создания или удаления объектов системного уровня, таких как таблицы баз данных или хранимые процедуры, упрощает определение легитимности таких изменений.
10.3 Записывать в журналах регистрации событий для каждого события каждого системного компонента, как минимум, следующее:	**10.3** Опрашивая работников и просматривая журналы аудита, выполнить следующие действия для каждого контролируемого события (из требования 10.2):	Записывая указанные данные 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 записывается в журнал;	
10.3.2 тип события;	**10.3.2** убедиться в том, что тип события записывается в журнал;	
10.3.3 дата и время;	**10.3.3** убедиться в том, что отметка о дате и времени записывается в журнал;	
10.3.4 успешное или неуспешное завершение события;	**10.3.4** убедиться в том, что отметка об успешном или неуспешном завершении события записывается в журнал;	
10.3.5 источник события;	**10.3.5** убедиться в том, что источник события записывается в журнал;	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.3.6 идентификатор или название данных, системного компонента или ресурса, на которые воздействовало событие.	**10.3.6** убедиться, что идентификатор или название данных, системного компонента или ресурса, на которые воздействовало событие, включены в записи журнала.	
10.4 Синхронизировать все часы и системное время в критичных системах с помощью механизмов синхронизации времени и обеспечить выполнение следующих требований при получении, распространении и хранении данных о времени. ***Примечание:*** *примером механизма синхронизации времени является сетевой протокол службы времени (NTP).*	**10.4** Проверить стандарты конфигурации и относящиеся к ним процессы на предмет того, что для синхронизации часов внедрена и поддерживается в актуальном состоянии 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 регистрации событий из различных систем и установить точную последовательность событий (что имеет большое значение при расследовании нарушений). Для групп, расследующих инциденты, точность и согласование времени на всех системах и времени совершения каждого действия является критичным для того, чтобы определить, каким образом были скомпрометированы системы.
10.4.1 Установить точное и согласованное время в критичных системах.	**10.4.1.a** Проверить процесс получения, распространения и хранения точного времени в организации, на предмет того, 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); • при наличии более одного назначенного сервера времени, серверы времени связываются друг с другом для поддержания точного времени; • системы получают информацию о времени только от назначенных центральных серверов времени.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	10.4.1.b Проверить системные параметры времени в выборке системных компонентов на предмет того, 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); • при наличии более одного назначенного сервера времени, серверы времени связываются друг с другом для поддержания точного времени; • системы получают информацию о времени только от назначенных центральных серверов времени.	
10.4.2 Защитить данные о времени.	**10.4.2.a** Проверить системные конфигурации и настройки синхронизации времени на предмет того, что доступ к данным о времени ограничивается только работниками, у которых есть служебная необходимость в таком доступе.	
	10.4.2.b Проверить системные конфигурации, настройки, журналы и процессы синхронизации времени на предмет того, что любые изменения в настройках времени на критичных системах регистрируются, отслеживаются и контролируются.	
10.4.3 Получать настройки времени из общепризнанных в отрасли источников.	**10.4.3** Проверить системные конфигурации на предмет того, что серверы времени принимают обновления времени от специализированных, общепризнанных отраслевых внешних источников (чтобы злоумышленник не мог изменить время). Как вариант, данные обновления можно зашифровать с помощью симметричного ключа, а также можно создать списки контроля доступа, определяющие IP-адреса клиентских машин, которым будут предоставляться обновления времени (чтобы предотвратить несанкционированное использование внутренних серверов времени).	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.5 Защитить журналы регистрации событий от изменений:	**10.5** Опросить системных администраторов и проверить системные конфигурации и права доступа на предмет того, что журналы регистрации событий защищены от изменений следующим образом:	Злоумышленники, проникшие в сеть, зачастую пытаются внести изменения в журналы аудита для того, чтобы скрыть свои действия. При недостаточной защите журналов аудита 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 журналов регистрации событий только теми работниками, которым такой доступ необходим в соответствии с их должностными обязанностями;	**10.5.1** доступ к журналу регистрации событий предоставлен только тем работникам, которым такой доступ необходим в соответствии с их должностными обязанностями.	Надежная защита журналов регистрации событий подразумевает строгий контроль доступа (ограничение доступа к журналам по принципу служебной необходимости) и использование физического или сетевого разделения, чтобы затруднить поиск и модификацию журналов. Оперативно сохраняя резервные копии журналов регистрации событий на централизованный сервер протоколирования или на носитель, где их изменение затруднено, можно защитить журналы даже в случае компрометации системы, их генерирующей.
10.5.2 защищать файлы журналов регистрации событий от несанкционированных изменений;	**10.5.2** актуальные журналы регистрации событий защищены от несанкционированного изменения с помощью механизмов контроля доступа, физического разделения и (или) разделения на уровне сетей;	
10.5.3 оперативно сохранять резервные копии журналов регистрации событий на централизованный сервер протоколирования или носитель, на котором их трудно изменить;	**10.5.3** резервные копии журналов регистрации событий оперативно сохраняются на централизованный сервер протоколирования или отдельный носитель, на котором их трудно изменить;	
10.5.4 сохранять копии журналов регистрации событий доступных из внешней сети технологий на безопасный и централизованный внутренний сервер протоколирования или носитель;	**10.5.4** журналы регистрации событий сохраняются с доступных из внешней сети технологий (например, беспроводных устройств, межсетевых экранов, DNS, почтовых серверов) на безопасный и централизованный внутренний сервер протоколирования или носитель.	Если ведутся журналы регистрации событий с доступных из внешней сети технологий, 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, загружаться или копироваться с внешних систем на безопасную внутреннюю систему или носитель.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.5.5 применять ПО для мониторинга целостности файлов или обнаружения изменений в журналах регистрации событий, чтобы данные существующих журналов нельзя было изменить без автоматического создания уведомления (однако добавление новых данных не должно создавать уведомление).	**10.5.5** проверить системные настройки, отслеживаемые файлы и результаты мониторинга на предмет того, что в журналах применяется ПО для мониторинга целостности файлов или обнаружения несанкционированных изменений в журналах.	Системы мониторинга целостности файлов или обнаружения несанкционированных изменений выполняют проверку на внесение изменений в критичные файлы и генерируют уведомления при обнаружении изменений. В целях мониторинга целостности файлов организация обычно выполняет мониторинг файлов, которые не меняются нечасто, но изменение которых может свидетельствовать о компрометации.
10.6 Проверять журналы и события безопасности всех системных компонентов, чтобы выявлять аномалии или подозрительную активность. ***Примечание:*** *для выполнения данного требования могут использоваться средства сбора и анализа журналов регистрации событий, а также средства оповещения.*	**10.6** Выполнить следующее.	Большое количество компрометаций происходит за несколько дней или даже месяцев до обнаружения. Регулярная проверка журналов вручную или автоматически позволяет выявлять и заблаговременно противодействовать несанкционированному доступу к среде ДДК. Проверку журналов не обязательно выполнять вручную. Средства сбора и анализа журналов регистрации событий, а также средств оповещения могут облегчить проверку благодаря тому, что они указывают на события, которые требуют проверки.
10.6.1 Проверять не реже одного раза в день: • все события безопасности; • журналы всех системных компонентов, которые хранят, обрабатывают или передают ДДК и (или) КАД; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, межсетевых экранов, систем	**10.6.1.a** Проверить политики и процедуры безопасности на предмет того, что имеются процедуры, требующие проверять следующие записи вручную или автоматически не реже одного раза в день: • все события безопасности; • журналы всех системных компонентов, которые хранят, обрабатывают или передают ДДК и (или) КАД; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, межсетевых экранов, систем обнаружения или предотвращения вторжений, серверов аутентификации, серверов перенаправления для электронной коммерции и т. д.).	Ежедневная проверка журналов регистрации событий минимизирует время, необходимое для обнаружения компрометации. Чтобы обнаруживать потенциальные проблемы, необходимо ежедневно проверять события безопасности (например, уведомления или предупреждения о подозрительной или аномальной активности), журналы критичных системных компонентов и журналы систем, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения или предотвращения вторжений, систем мониторинга целостности файлов). Следует учитывать, что значение

Требования PCI DSS	Проверочные процедуры	Пояснение
обнаружения или предотвращения вторжений, серверов аутентификации, серверов перенаправления для электронной коммерции и т. д.).	**10.6.1.b** Проследить за процессами и опросить работников на предмет того, что не реже раза в день проверяются: • все события безопасности; • журналы всех системных компонентов, которые хранят, обрабатывают или передают ДДК и (или) КАД; • журналы всех критичных системных компонентов; • журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, межсетевых экранов, систем обнаружения или предотвращения вторжений, серверов аутентификации, серверов перенаправления для электронной коммерции и т. д.).	термина «событие безопасности» зависит от организации и может включать ограничения по типу технологий, местонахождении и функции устройства. Организациям также рекомендуется определить так называемый «нормальный» трафик в целях идентификации аномального поведения.
10.6.2 Периодически изучать журналы других системных компонентов на основании политик и стратегии управления рисками организации, определяемых в рамках ежегодной оценки рисков.	**10.6.2.a** Проверить политики и процедуры безопасности на предмет того, что имеются процедуры, требующие периодически изучать журналы всех остальных системных компонентов (вручную или автоматически) на основании политик и стратегии управления рисками.	Периодически следует проверять журналы всех остальных системных компонентов, чтобы выявлять признаки потенциальных проблем или попыток получить доступ к критичным системам через другие, менее критичные системы. Частота проведения проверок определяется организацией в рамках ежегодной оценки рисков.
	10.6.2.b Проверить документацию организации по оценке рисков и опросить работников на предмет того, что проверки выполняются 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 предмет того, что имеются процедуры, требующие изучать исключения и аномалии, обнаруженные 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 Проследить за процессами и опросить работников на предмет того, что исключения и аномалии изучаются.	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.7 Сохранять историю журналов регистрации событий не менее одного года, причем в оперативном доступе должна находиться история не менее чем за последние три месяца (например, в прямом доступе, в архиве, либо с возможностью восстановления из резервной копии).	**10.7.a** Проверить политики и процедуры на предмет того, что они определяют: • политики хранения журналов аудита; • процедуры хранения журналов аудита в течение не менее одного года, в том числе в оперативном доступе не менее трех месяцев.	То, что журналы должны храниться, по крайней мере, в течение года, связано с тем фактом, что на обнаружение компрометации требуется время. У экспертов, таким образом, имеется достаточно материалов с хронологией событий, позволяющих более точно определить продолжительность существования потенциальной компрометации и систем, потенциально подверженных ее воздействию. Располагая журналами за три месяца, организация может быстро выявить компрометацию и минимизировать ущерб. Хранение журналов в оффлайновых местах расположения может затруднить получение к ним оперативного доступа и привести к увеличению времени, необходимого, чтобы восстановить данные журнала, выполнить анализ и выявить системы или данные, подвергшиеся воздействию компрометации.
	10.7.b Опросить работников и проверить журналы аудита на предмет того, что журналы доступны, по крайней мере, в течение одного года.	
	10.7.c Опросить работников и проследить за процессами на предмет того, что для проведения анализа можно незамедлительно восстановить журналы аудита как минимум за последние три месяца.	
10.8 ***Дополнительное требование для поставщиков услуг:*** внедрить процесс своевременного обнаружения и отчетности об ошибках в критичных системах контроля безопасности, включая среди прочего ошибки: • межсетевых экранов; • систем обнаружения и (или) предотвращения вторжений; • систем мониторинга целостности файлов; • антивирусного ПО; • физических механизмов	**10.8.a** Проверить документированные политики и процедуры на предмет того, что определены процессы своевременного обнаружения и отчетности об ошибках в критичных системах контроля безопасности, включая среди прочего ошибки: • межсетевых экранов; • систем обнаружения или предотвращения вторжений; • систем мониторинга целостности файлов; • антивирусного ПО; • физических механизмов контроля доступа; • логических механизмов контроля доступа; • механизмов ведения журналов регистрации событий; • средств сегментации (если они используются)	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Если формализованные процессы обнаружения ошибок и оповещения отсутствуют, в случае возникновения ошибок в критичных механизмах контроля безопасности данные ошибки могут остаться невыявленными в течение длительного времени, и злоумышленники получат достаточно времени для компрометации систем и хищения критичных данных из среды ДДК. Определенные типы ошибок могут

Требования PCI DSS	Проверочные процедуры	Пояснение
контроля доступа; • логических механизмов контроля доступа; • механизмов ведения журналов регистрации событий; • средств сегментации (если они используются) ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**10.8.b** Проверить процессы обнаружения и оповещения и опросить работников на предмет того, что эти процессы внедрены на всех критичных механизмах контроля безопасности, и в случае обнаружения ошибок в данных механизмах происходит оповещение.	различаться в зависимости от функциональности устройства и используемой технологии. Типовые ошибки включают прекращение выполнения системой функции обеспечения безопасности или выполнение функции не в том виде, в котором она запланирована, например, межсетевой экран удаляет все свои правила или переходит в автономный режим.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.8.1 ***Дополнительное требование для поставщиков услуг:*** своевременно реагировать на ошибки в любых критичных механизмах контроля безопасности. Процессы реагирования на ошибки в механизмах контроля безопасности должны включать: • восстановление функций обеспечения безопасности; • определение и документирование продолжительности (дата и время начала и окончания) ошибки в обеспечении безопасности; • определение и документирование причины (причин) ошибки, включая изначальную причину, и документирование мер, необходимых для исправления изначальной причины; • определение и решение любых вопросов безопасности, которые возникают во время ошибки; • выполнение оценки рисков, чтобы определить необходимость дальнейших действий при ошибке в обеспечении безопасности; • применение мер для предотвращения причины ошибки и недопущения ее	**10.8.1.a** Проверить документированные политики и процедуры и опросить персонал на предмет того, что процессы реагирования на ошибки в механизмах контроля безопасности определены, внедрены и включают: • восстановление функций обеспечения безопасности; • определение и документирование продолжительности (дата и время начала и окончания) ошибки в обеспечении безопасности; • определение и документирование причины (причин) ошибки, включая изначальную причину, и документирование мер, необходимых для исправления изначальной причины; • определение и решение любых вопросов безопасности, которые возникают во время ошибки; • выполнение оценки рисков, чтобы определить необходимость дальнейших действий при ошибке в обеспечении безопасности; • применение мер для предотвращения причины ошибки и недопущения ее повторения; • возобновление мониторинга механизмов контроля безопасности.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Если реагирование на оповещения об ошибках в критичных механизмах контроля безопасности не осуществляется быстро и эффективно, злоумышленники могут воспользоваться этим временем для внедрения вредоносного ПО, получить контроль над системой или похитить данные из среды организации. Документированные свидетельства (например, записи о проблемах в системе управления) должны поддерживать действующими процессы и процедуры реагирования на ошибки в обеспечении безопасности. Кроме того, работники должны знать свои обязанности в случае возникновения ошибки. Ответные действия на ошибки должны быть зафиксированны в виде документированных свидетельств.

Требования PCI DSS	Проверочные процедуры	Пояснение
повторения; • возобновление мониторинга механизмов контроля безопасности. ***Примечание**: до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием*.	**10.8.1.b** Проверить записи на предмет того, что ошибки в механизмах контроля безопасности задокументированы и включают: • определение причины (причин) ошибки, включая изначальную причину; • продолжительность (дата и время начала и окончания) ошибки в обеспечении безопасности; • меры, необходимые для исправления изначальной причины.	
10.9 Гарантировать, что политики безопасности и операционные процедуры мониторинга любого доступа к сетевым ресурсам и ДДК документированы, используются и известны всем заинтересованным лицам.	**10.9** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры мониторинга любого доступа к сетевым ресурсам и ДДК: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и повседневные операционные процедуры непрерывного мониторинга любого доступа к сетевым ресурсам и ДДК.

Требование 11. Регулярно тестировать системы и процессы безопасности.

Уязвимости постоянно обнаруживаются злоумышленниками и исследователями, а также появляются вместе с новым программным обеспечением. Системные компоненты, процессы и заказные программы необходимо часто тестировать на предмет того, что защитные меры соответствуют постоянно меняющейся среде.

Требования PCI DSS	Проверочные процедуры	Пояснение
11.1 Внедрить процессы ежеквартальной проверки на наличие беспроводных точек доступа (802.11), а также выявления и идентификации санкционированных и несанкционированных беспроводных точек доступа. ***Примечание:*** *в данном процессе могут использоваться, среди прочего, следующие методы: сканировать беспроводные сети, выполнять физическую или логическую проверку системных компонентов и инфраструктуры, реализовать контроль доступа к сети или беспроводные системы обнаружения или предотвращения вторжений.* *Какие бы методы ни использовались, они должны быть достаточны, чтобы обнаруживать как санкционированные, так и несанкционированные устройства.*	**11.1.a** Проверить политики и процедуры на наличие в них процессов, предписывающих ежеквартально выявлять и идентифицировать санкционированные и несанкционированные беспроводные точки доступа. **11.1.b** Проверить используемую методологию на предмет того, что она достаточна, чтобы выявить и идентифицировать любые несанкционированные беспроводные точки доступа, в т. ч., как минимум, указанные ниже: • 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** Если используется сканирование беспроводных сетей, проверить результаты недавних сканирований беспроводных сетей на предмет того, что: • идентифицируются санкционированные и несанкционированные беспроводные точки доступа; • сканирование всех системных компонентов и помещений проводится, по крайней мере, ежеквартально.	Установка и (или) использование беспроводных технологий в сети являются одними из наиболее часто используемых злоумышленниками способов для получения доступа к сети и ДДК. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может без труда и незаметно проникать в сеть. Несанкционированные 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 несанкционированное устройство может выполнять роль несанкционированной точки доступа в среду. Зная, какие беспроводные устройства санкционированы, администраторы могут быстро обнаруживать несанкционированные беспроводные устройства, а, реагируя на обнаружение несанкционированных беспроводных точек доступа, организация может заблаговременно снизить уязвимость среды ДДК к действиям злоумышленников. Поскольку подключить к сети беспроводную точку доступа несложно, определить ее наличие трудно, а риск от

Требования PCI DSS	Проверочные процедуры	Пояснение
	11.1.d Если используется автоматизированный мониторинг (например, беспроводные системы обнаружения или предотвращения вторжений, контроль сетевого доступа и т. п.), проверить его на предмет того, что он генерирует уведомления и передает их работникам.	несанкционированных беспроводных устройств повышен, эти процессы следует выполнять даже при наличии политики, запрещающей использование беспроводных технологий. Размер и сложность определенной среды обуславливает необходимость использования соответствующих инструментов и процессов, которые достаточно надежно исключат возможность установки несанкционированной точки доступа в среде. *(Продолжение на следующей странице)*
11.1.1 Вести список санкционированных беспроводных точек доступа и документировать по ним служебное обоснование.	**11.1.1** Проверить документацию на предмет того, что ведется список санкционированных беспроводных точек доступа и по всем ним документируется служебное обоснование.	***Например:*** *если один автономный розничный киоск стоит в торговом центре, где все коммуникационные компоненты содержатся в опломбированном корпусе, защищенном от физического вмешательства, то чтобы быть уверенным, что к киоску не подключены и на нем не установлены несанкционированные беспроводные точки доступа, возможно, будет достаточно провести тщательный физический осмотр киоска. Однако в среде с несколькими узлами (например, в большом розничном магазине, колл-центре, серверной комнате или центре обработки данных) проведение тщательного физического осмотра затруднительно. В этом случае для выполнения требования можно использовать несколько методов, например физический осмотр системы и анализ беспроводных сетей.*
11.1.2 Внедрить процедуры реагирования на инцидент, заключающийся в обнаружении несанкционированных беспроводных точек доступа.	**11.1.2.a** Проверить план реагирования на инциденты (требование 12.10) на предмет того, что она определяет план реагирования на случай, когда обнаруживается несанкционированная беспроводная точка доступа.	
	11.1.2.b Опросить ответственных работников и (или) проверить результаты недавних сканирований и меры, предпринятые в связи с ними, на предмет того, что при обнаружении несанкционированных беспроводных точек доступа предпринимаются соответствующие меры.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.2 Проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал**,** а также после значительных изменений в сети (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов). ***Примечание:*** *в рамках ежеквартального сканирования можно объединить несколько отчетов о результатах сканирования, чтобы подтвердить, что все системы были просканированы, и все соответствующие уязвимости обработаны. Может потребоваться дополнительная документация, чтобы подтвердить, что неустраненные уязвимости находятся в процессе устранения.* *Для первоначального соответствия стандарту PCI DSS успешное прохождение четырех ежеквартальных сканирований необязательно, если аудитор убедился в следующем: 1) последнее сканирование было пройдено успешно, 2) в организации имеются документированные политики и процедуры, которые регламентируют необходимость ежеквартального сканирования, 3) обнаруженные уязвимости были устранены и это подтверждено повторным сканированием (сканированиями). В течение всех последующих лет после первоначального подтверждения соответствия стандарту PCI DSS успешное прохождение всех четырех ежеквартальных сканирований обязательно.*	**11.2** Проверить отчеты о результатах сканирования и сопутствующую документацию на предмет того, что внешнее и внутреннее сканирование сети на наличие уязвимостей проводится следующим образом:	Сканирование на наличие уязвимостей выполняется с использованием сочетания автоматизированных или ручных средств, техник и (или) методов,которые проверяют внутренние и внешние сетевые устройства и серверы и предназначены для того, чтобы выявлять потенциальные уязвимости, которые могут быть обнаружены и использованы злоумышленниками. Стандартом PCI DSS требуется три типа сканирования на наличие уязвимостей: • ежеквартальное внутреннее сканирование на наличие уязвимостей, проводимое квалифицированными работниками (статус авторизованного поставщика услуг сканирования (ASV) по требованиям стандарта PCI SSC не требуется); • ежеквартальное внешнее сканирование на наличие уязвимостей, которое должны выполнять организации, имеющие статус авторизованного поставщика услуг сканирования (ASV); • внутреннее и внешнее сканирования, по необходимости, после значительного изменения в сети. После обнаружения уязвимостей организация устраняет их и проводит повторное сканирование пока не устранит их полностью. Своевременное выявление и устранение уязвимостей снижает вероятность того, что злоумышленник будет использовать уязвимость и скомпрометирует системный компонент или ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
11.2.1 Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей. Обрабатывать уязвимости и сканировать повторно, чтобы проверить, что все уязвимости с высоким уровнем критичности устанены в соответствии с принятой в организации оценкой критичности уязвимостей (согласно требованию 6.1). Сканирование должны выполнять квалифицированные работники.	**11.2.1.a** Проверить отчеты сканирования на предмет того, что за последние 12 месяцев было проведено 4 ежеквартальных внутренних сканирования.	Установленный процесс выявления уязвимостей во внутренних системах требует ежеквартального сканирования уязвимостей. Уязвимости, которые представляют максимальный уровень критичности для среды (например, те, которым согласно требованию 6.1 присвоен высокий уровень критичности), должны быть устранены в первую очередь. Внутреннее сканирование на наличие уязвимостей могут выполнять квалифицированные работники, которые являются достаточно независимыми относительно сканируемых компонентов системы (например, нельзя, чтобы за сканирование межсетевого экрана отвечал его администратор), либо организация может проводить внутреннее сканирование услугами другой организации, которая занимается сканированием на наличие уязвимостей.
	11.2.1.b Проверить отчеты о результатах сканирования на предмет того, что все уязвимости с высоким уровнем критичности обработаны, и процесс сканирования включает повторное сканирование, чтобы проверить, что все уязвимости с высоким уровнем критичности (согласно определению в требовании 6.1 PCI DSS) устранены.	
	11.2.1.c Опросить работников на предмет того, что сканирование проводилось квалифицированными работниками организации либо квалифицированной третьей стороной, а также, если применимо, проверить тестировщиков на организационную независимость (наличие у них статуса QSA или ASV не требуется).	
11.2.2 Проводить ежеквартальное внешнее сканирование на наличие уязвимостей с привлечением авторизованного поставщика услуг сканирования (ASV), утвержденного Советом PCI SSC. По необходимости, повторять сканирование, пока оно не будет пройдено успешно. ***Примечание:*** *для ежеквартального внешнего сканирования на наличие уязвимостей использовать авторизованного поставщика услуг сканирования (ASV), утвержденного Советом PCI SSC.*	**11.2.2.a** Проверить результаты четырех последних внешних сканирований на наличие уязвимостей и проверить, проведены ли четыре последние внешние ежеквартальные сканирования в течение последних 12 месяцев.	Поскольку внешние сети подвержены более высокому риску компрометации, ежеквартальное сканирование на наличие уязвимостей в таких сетях должны выполнять специалисты авторизованного поставщика услуг сканирования, утвержденного Советом PCI SSC. Надежная программа сканирования на наличие уязвимостей обеспечивает выполнение сканирования и своевременное выявление уязвимостей.
	11.2.2.b Проверить результаты каждого ежеквартального сканирования (в т. ч. повторных сканирований) на предмет того, что они отвечают требованиям «Руководства для авторизованных поставщиков услуг сканирования» к успешно пройденному сканированию (например, отсутствуют уязвимости с оценкой 4.0 и выше по системе CVSS и нет ошибок, в результате которых автоматическое сканирование было прервано).	

Требования PCI DSS	Проверочные процедуры	Пояснение
См. «Руководство для авторизованных поставщиков услуг сканирования» (ASV Program Guide), опубликованное на веб-сайте Совета PCI SSC, для получения информации об обязанностях заказчиков сканирования, подготовке к сканированию и т. д.	**11.2.2.c** Проверить отчеты о результатах сканирования на предмет того, что сканирование производилось авторизованным поставщиком услуг сканирования, утвержденным Советом PCI SSC.	
11.2.3 Проводить внутреннее и внешнее сканирования и, при необходимости, повторять сканирование после любого значительного изменения в сети. Сканирование должны выполнять квалифицированные работники.	**11.2.3.a** Проверить и сопоставить документацию по контролю изменений и отчеты о результатах сканирования на предмет того, что выполнялось сканирование системных компонентов после любых значительных изменений.	Понятие «значительного изменения» сильно зависит от конфигурации конкретной среды. Если после обновления или модификации может появиться доступ к ДДК или безопасность среды ДДК может быть снижена, то изменение считается значительным. Сканирование среды после любых значительных изменений гарантирует, что изменения внедрены надлежащим образом, и безопасность среды не была нарушена в результате этих изменений. Необходимо просканировать все системные компоненты, на которые повлияло изменение.
	11.2.3.b Проверить отчеты о сканировании на предмет того, что процесс сканирования предусматривает повторять сканирования: • для внешнего сканирования – до тех пор, пока не устранены уязвимости с оценкой 4.0 и более по системе CVSS; • для внутреннего сканирования – до тех пор, пока не будут устранены все уязвимости с высоким уровнем критичности, согласно определению в требовании 6.1 PCI DSS.	
	11.2.3.c Убедиться, что сканирование проводилось квалифицированными работниками организации или третьей стороны, а также, если применимо, проверить тестировщиков на организационную независимость (наличие у них 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 среды	**11.3** Проверить методологию проведения тестов на проникновение и опросить ответственных работников на предмет того, что она: • основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115); • охватывает весь периметр среды ДДК и критичные системы;	Цель теста на проникновение — смоделировать реальную атаку, чтобы выявить, насколько глубоко злоумышленник сможет проникнуть в среду. Благодаря этому, организация может лучше разобраться в своих потенциальных уязвимостях и разработать стратегию защиты от атак. Тест на проникновение отличается от сканирования на наличие уязвимостей тем, что

Требования PCI DSS	Проверочные процедуры	Пояснение
ДДК и критичные системы; • включает тестирование как снаружи сети, так и внутри сети; • включает тестирование для проверки любых средств сегментации и сокращения области применимости; • 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 операционные системы и сетевые компоненты; • включает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев; • регламентирует хранение результатов тестов на проникновение и мер, предпринятых для устранения уязвимостей.	• включает тестирование как снаружи сети, так и внутри сети; • включает тестирование для проверки любых средств сегментации и сокращения области применимости; • 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 операционные системы и сетевые компоненты; • включает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев; • регламентирует хранение результатов тестов на проникновение и мер, предпринятых для устранения уязвимостей.	первый является активным процессом и он может включать эксплуатацию обнаруженных уязвимостей. Сканирование на наличие уязвимостей может быть первым, но точно не единственным шагом, который выполняет специалист по тестам на проникновение, чтобы определить стратегию тестирования. Даже если сканирование на наличие уязвимостей не обнаруживает известные уязвимости, специалист по тестам на проникновение часто получает достаточно информации о системе, чтобы выявить потенциальные проблемы безопасности. Тесты на проникновение обычно выполняются вручную. Даже используя автоматизированные средства, тестировщик должен применять свои знания систем для проникновения в среду. Часто тестировщик использует несколько типов эксплойтов вместе, чтобы обойти несколько уровней защиты. Например, если тестировщик находит способ получить доступ к серверу приложений, он использует скомпрометированный сервер как площадку для новой атаки, где использует ресурсы, доступ к которым имеет сервер. Таким образом, тестировщик может имитировать методы, которыми пользуются злоумышленники, для выявления потенциальных уязвимостей среды. *Методы тестирования на проникновение зависят от организации, а тип, глубина и сложность тестирования зависят от конкретной среды и оценки рисков организации.*

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3.1 Проводить *внешний* тест на проникновение не реже одного раза в год и после любых значительных модификаций или обновлений инфраструктуры или приложений (например, обновления операционной системы, добавления подсети или веб-сервера к среде).	**11.3.1.a** Проверить объем работ и результаты последнего внешнего теста на проникновение на предмет того, что тест на проникновение осуществляется: • в соответствии с определенной методологией; • не реже раза в год; • после любых значительных изменений в среде.	Тесты на проникновение, выполняемые по графику и после значительных изменений в среде – это превентивная мера, позволяющая уменьшить риск доступа злоумышленников к среде ДДК. Понятие «значительного» обновления или модификации сильно зависит от конфигурации конкретной среды. Если после обновления или модификации может появиться доступ к ДДК или безопасность среды ДДК может быть снижена, то изменение считается значительным. Выполнение тестов на проникновение после обновления или модификации сети гарантирует, что существующие механизмы по-прежнему работают.
	11.3.1.b Убедиться, что тест на проникновение проводили квалифицированные работники организации либо квалифицированная третья сторона и, если применимо, что они организационно независимы (наличие у них статуса QSA или ASV не требуется).	
11.3.2 Выполнять *внутренний* тест на проникновение не реже одного раза в год и после любых значительных модификаций или обновлений инфраструктуры или приложений (например, обновления операционной системы, добавления подсети или веб-сервера к среде).	**11.3.2.a** Проверить объем работ и результаты последнего внутреннего теста на проникновение на предмет того, что тест на проникновение проводится: • в соответствии с определенной методологией; • не реже раза в год; • после любых значительных изменений в среде.	
	11.3.2.b Убедиться, что тест на проникновение проводили квалифицированные работники организации либо квалифицированная третья сторона и, если применимо, что они организационно независимы (наличие у них статуса QSA или ASV не требуется).	
11.3.3 Устранять потенциально эксплуатируемые уязвимости, обнаруженные во время теста на проникновение, и повторить тест, чтобы проверить устранение.	**11.3.3** Проверить результаты теста на проникновение на предмет того, что заявленные потенциально эксплуатируемые уязвимости были устранены и это подтверждено повторным тестом.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3.4 Если для изоляции среды ДДК от других сетей используется сегментация, проводить тест на проникновение не реже одного раза в год и после любого изменения средств/методов сегментации на предмет того, что методы сегментации действительно работают и изолируют от остальных все системы, находящиеся в среде ДДК.	**11.3.4.a** Проверить средства сегментации и методологию теста на проникновение и подтвердить, что процедуры теста на проникновение предусматривают тестирование всех методов сегментации на предмет того, что методы сегментации действительно работают и изолируют от остальных все системы,находящиеся в среде ДДК.	Тест на проникновение – это важный инструмент проверки, что реализованная сегментация действительно изолирует среду ДДК от других сетей. Тест на проникновение необходимо нацелить на средства сегментации, используемые как на границе, так и внутри сети организации, но вне среды ДДК. Он должен подтвердить, что невозможно преодолеть средства сегментации и получить доступ к среде ДДК. Например, проверив сеть и (или) просканировав ее на наличие открытых портов, можно убедиться, что между сетями, входящими в область применимости, и остальными сетями подключений нет.
	11.3.4.b Проверить результаты последнего теста на проникновение на предмет того, что: • тест на проникновение для проверки средств сегментации осуществляется не реже одного раза в год и после любого изменения средств и (или) методов сегментации; • тест на проникновение распространяется на все используемые средства и (или) методы сегментации; • тест на проникновение проверяет, действительно ли механизмы и (или) методы сегментации работают и изолируют все системы, находящиеся в среде ДДК, от остальных.	
	11.3.4.c Убедиться, что тест на проникновение проводили квалифицированные работники организации либо квалифицированная третья сторона и, если применимо, что они организационно независимы (наличие у них статуса QSA или ASV не требуется).	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3.4.1 ***Дополнительное требование для поставщиков услуг:*** если применяется сегментация, подтвердить область применимости PCI DSS путем тестирования на проникновение в отношении средств сегментации, как минимум, каждые 6 месяцев и после любого изменения средств и (или) методов сегментации. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**11.3.4.1.a** Проверить результаты последнего теста на проникновение на предмет того, что: • тест на проникновение для проверки средств сегментации осуществляется, как минимум, каждые 6 месяцев и после любого изменения средств и (или) методов сегментации; • тест на проникновение распространяется на все используемые средства и (или) методы сегментации; • тест на проникновение проверяет, действительно ли механизмы и (или) методы сегментации эффективно работают и изолируют все системы, находящиеся в среде ДДК, от остальных.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Для поставщиков услуг проверка области применимости PCI DSS должна осуществляться как можно чаще для подтверждения того, что область применимости PCI DSS остается актуальной и соответствует изменениям бизнес-целей.
	11.3.4.1.b Убедиться, что тест на проникновение проводили квалифицированные работники организации либо квалифицированная третья сторона и, если применимо, что они организационно независимы (наличие у них статуса QSA или ASV не требуется).	
11.4 Использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Осуществлять мониторинг всего сетевого трафика по периметру среды ДДК и в критичных точках внутри среды ДДК, и оповещать работников о подозрениях на компрометацию. Поддерживать в актуальном состоянии системы обнаружения и предотвращения вторжений, их	**11.4.a** Проверить системные конфигурации и схемы сети на предмет того, что методы мониторинга (например, системы обнаружения и (или) предотвращения вторжений) используются для всего трафика: • по периметру среды ДДК; • в критичных точках внутри среды ДДК.	Методы обнаружения и (или) предотвращения вторжений (например, система обнаружения или предотвращения вторжений, IDS/IPS) сопоставляют поступающий в сеть трафик с тысячами известных сигнатур и (или) моделей вредоносного поведения (инструментарий злоумышленников, троянское и другое вредоносное ПО и т. д.), отправляют предупреждения и (или) блокируют попытку проведения атаки. Не используя превентивные меры для обнаружения несанкционированной деятельности, можно не заметить атаки на
	11.4.b Проверить системные конфигурации и опросить ответственных работников на предмет того, что средства обнаружения и (или) предотвращения вторжений уведомляют работников о подозрениях на компрометацию.	

Требования PCI DSS	Проверочные процедуры	Пояснение
сигнатуры и правила.	**11.4.c** Проверить конфигурации систем обнаружения или предотвращения вторжений (IDS/IPS) и документацию вендоров на предмет того, что, чтобы обеспечить оптимальную защиту, средства обнаружения и (или) предотвращения вторжений настроены, поддерживаются и обновляются в соответствии с рекомендациями вендора.	компьютерные ресурсы (или их ненадлежащее использование) в момент выполнения. Для блокирования попыток вторжений необходимо вести мониторинг уведомлений, генерируемых данными средствами.
11.5 Внедрить средство обнаружения изменений (например, мониторинг целостности файлов), чтобы уведомлять работников о несанкционированных изменениях (включая, изменения, добавления и удаления) критичных системных файлов, конфигурационных файлов или файлов данных. Настроить программное обеспечение так, чтобы оно сопоставляло критичные файлы не реже одного раза в неделю. ***Примечание:*** *в рамках системы обнаружения изменений критичные файлы – это файлы, которые изменяются нечасто, но изменение которых может служить признаком компрометации или риска компрометации системы. Средства обнаружения изменений (например, ПО для мониторинга целостности файлов) обычно содержат предустановленный перечень критичных файлов для соответствующей операционной системы. Иные критичные файлы, такие как файлы заказных приложений, должна проверить и определить сама организация (т. е. ТСП или поставщик услуг).*	**11.5.a** Проверить, используется ли средство обнаружения изменений путем проверки системных настроек и наблюдения за файлами, а также проверить результаты мониторинга. Примеры файлов, подлежащих мониторингу: ▪ системные исполняемые файлы; ▪ исполняемые файлы приложений; ▪ файлы конфигураций и параметров; ▪ централизованно хранимые файлы хронологии, архивирования, аудита и журналов регистрации событий; ▪ дополнительные критичные файлы, определяемые организацией (например, путем оценки рисков или другими способами).	Средства обнаружения изменений, например, инструменты для мониторинга целостности файлов проверяют критичные файлы на изменения, добавления и удаления и уведомляют при обнаружении изменений. Если такое средство внедрено ненадлежащим образом, а его отчет не проверяется, то злоумышленник может добавить, удалить или изменить содержимое конфигурационных файлов, программы операционной системы или исполняемые файлы приложений. Незамеченные несанкционированные изменения могут ухудшить работу защитных мер и привести к краже ДДК без заметного влияния на процессы обработки.
	11.5.b Проверить, что средство настроено на оповещение работников о несанкционированных изменениях (включая, изменения, добавления и удаления) критичных файлов, а также на сопоставление критичных файлов не реже одного раза в неделю.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.5.1 Внедрить процесс реагирования на любые уведомления от средства обнаружения изменений.	**11.5.1** Опросить работников на предмет того, что все уведомления изучаются и обрабатываются.	
11.6 Гарантировать, что политики безопасности и операционные процедуры мониторинга и проверки безопасности документированы, используются и известны всем заинтересованным лицам.	**11.6** Проверить документацию и опросить работников на предмет того, что политики безопасности и операционные процедуры мониторинга и проверки безопасности: • документированы; • используются; • известны всем заинтересованным лицам.	Работники должны знать и соблюдать политики безопасности и операционные процедуры мониторинга и проверки безопасности.

Поддерживать политику информационной безопасности

Требование 12. Поддерживать политику информационной безопасности для всех работников.

Строгая политика безопасности определяет характер безопасности по всей организации и информирует работников о том, что от них требуется. Все работники должны знать о критичности данных и своих обязанностях по их защите. В рамках требования 12 термин «работники» относится к постоянным работникам, работающим как полный, так и неполный рабочий день, временным работникам, подрядчикам, консультантам, находящимся на территории организации или иным образом имеющим доступ к среде ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.1 Разработать, опубликовать, поддерживать и распространять политику информационной безопасности.	**12.1** Проверить политику информационной безопасности на предмет того, что она опубликована и распространена среди всех работников, к которым она относится (включая вендоров и деловых партнеров).	Политика информационной безопасности компании определяет план действий, реализующих защитные меры для наиболее ценных ресурсов. Все работники должны знать о критичности данных и своих обязанностях по их защите.
12.1.1 Пересматривать политику информационной безопасности не реже раза в год и обновлять в случае изменения среды организации.	**12.1.1** Убедиться, что политика информационной безопасности пересматривается не реже раза в год и обновляется по необходимости, чтобы отражать изменения целей организации или структуры рисков.	Угрозы для безопасности и методы защиты быстро развиваются. Если политика информационной безопасности не обновляется с учетом этих изменений, то организация не реализует актуальные меры защиты от новых угроз.
12.2 Внедрить процесс оценки рисков, который: • осуществляется не реже раза в год и после значительного изменения среды (например, покупки, слияния, перемещения и т. д.); • выявляет критичные активы, угрозы и уязвимости; • завершается формализованным и документированным анализом рисков. *К примерам методологий оценки рисков относятся, среди прочего, OCTAVE, ISO 27005 и NIST SP 800-30.*	**12.2.a** Убедиться, что ежегодный процесс оценки рисков документирован и включает: • определение критичных активов, угроз и уязвимостей; • завершение в виде формализованного и документированного анализа рисков. **12.2.b** Проверить документацию по оценке рисков на предмет того, что оценка рисков проводится, по крайней мере, раз в год и после значительных изменений в среде.	Оценка рисков позволяет организации выявить угрозы и связанные с ними уязвимости, которые могут негативно отразиться на деятельности организации. Примеры различных факторов риска включают в себя киберпреступность, веб-атаки и вредоносные программы на POS-терминалах. После этого можно эффективно выделить ресурсы на внедрение защитных средств, которые помогут снизить вероятность реализации угроз и (или) потенциальное воздействие от реализованной угрозы. Оценивая риски, по крайней мере, раз в год и после значительных изменений, организация может учитывать структурные изменения, новые угрозы, тенденции и технологии.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3 Разработать политики использования критичных технологий и определить надлежащее пользование этих технологий. ***Примечание:*** *к критичным технологиям относятся среди прочего: технологии удаленного доступа, беспроводные технологии, ноутбуки, планшеты, съемные носители информации, электронная почта и сеть Интернет.* Гарантировать, что политики использования критичных технологий предусматривают:	**12.3** Проверить политики использования критичных технологий, опросить ответственных работников и удостовериться, что реализованы и выполняются политики, которые:	Политики использования могут либо запрещать использование определенных устройств и других технологий, если этого требует политика организации, либо содержать инструкции для работников по надлежащему использованию и реализации технологий. Если политики использования отсутствуют, работники, вероятно, будут использовать технологии с нарушениями политики организации, позволяя злоумышленникам получать доступ к критичным системам и ДДК.
12.3.1 явное утверждение со стороны уполномоченных лиц;	**12.3.1** предусматривают процессы, согласно которым уполномоченные лица явным образом разрешают использовать технологию;	Если для реализации технологий не требуется надлежащего разрешения, работники могут непреднамеренно внедрить решение в соответствии с предполагаемыми потребностями организации, при этом создав огромную брешь в системе безопасности и создать угрозу для критичных систем и данных от злоумышленников.
12.3.2 аутентификацию для пользования технологией;	**12.3.2** предусматривают процессы аутентификации по идентификатору пользователя и паролю, либо иному средству аутентификации (например, токену) для пользования любой технологией;	Если технология реализована без надлежащей аутентификации (идентификаторов пользователей и паролей, электронных ключей, VPN и т. д.), злоумышленник легко может воспользоваться такой незащищенной технологией, чтобы получить доступ к критичным системам и ДДК.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3.3 перечень всех таких используемых устройств и работников, имеющих к ним доступ;	**12.3.3** включают: • список всех критичных устройств; • список работников, уполномоченных использовать такие устройства;	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве «черного хода». Работники также могут обойти процедуры и установить свои устройства. Тщательная инвентаризация и надлежащая маркировка устройств позволят быстро идентифицировать несанкционированно установленные устройства.
12.3.4 способ быстро и точно устанавливать владельца, его контактные данные и назначение устройства (например, **путем** маркировки, кодирования и (или) инвентаризации устройств);	**12.3.4** определяют способ быстро и точно устанавливать владельца, его контактные данные и назначение устройства (например, **путем** маркировки, кодирования и (или) инвентаризации устройств);	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве «черного хода». Работники также могут обойти процедуры и установить свои устройства. Тщательная инвентаризация и надлежащая маркировка устройств позволят быстро идентифицировать несанкционированно установленные устройства. Рекомендуется разработать формализованную процедуру именования устройств и вести учет всех устройств с помощью механизмов инвентаризации. Допускается 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** определяют допустимые способы использования технологий;	Определяя допустимые способы использования и варианты размещения устройств и технологий, утвержденных руководством, организация может лучше управлять и контролировать уязвимостями в конфигурациях и операционных механизмах. Это необходимо, чтобы исключить возможность появления «черных ходов», которыми могут воспользоваться злоумышленники для получения доступа к критичным системам и ДДК.
12.3.6 допустимые места размещения технологий в сети;	**12.3.6** определяют допустимые места размещения технологий в сети;	
12.3.7 перечень одобренных организацией продуктов;	**12.3.7** включают перечень одобренных организацией продуктов;	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3.8 автоматическое отключение сеансов удаленного доступа после определенного периода бездействия;	**12.3.8.a** требуют автоматического отключения сеансов удаленного доступа после определенного периода бездействия;	Технологии удаленного доступа часто выступают в роли «черных ходов» к критичным ресурсам и ДДК. Отключая технологии удаленного доступа, когда ими не пользуются (например, те, что используются для поддержки систем вендорами POS-терминалов, иными вендорами или деловыми партнерами), можно уменьшить доступ к сети и сократить риски для безопасности сетей.
	12.3.8.b требуют настроить конфигурации технологий удаленного доступа так, чтобы сеансы автоматически отключались после определенного периода бездействия;	
12.3.9 включение технологий удаленного доступа для вендоров и деловых партнеров, только когда им необходим такой доступ, и немедленное выключение после использования;	**12.3.9** требуют включать технологии удаленного доступа для вендоров и деловых партнеров, только когда им необходим такой доступ, и немедленно выключать после использования;	

Требования PCI DSS	Проверочные процедуры	Пояснение
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 использования должны требовать защищать данные в соответствии со всеми применимыми требованиями стандарта PCI DSS.	**12.3.10.a** запрещают копирование, перемещение и хранение ДДК на локальных жестких дисках и съемных электронных носителях, если доступ к этим данным осуществляется через технологии удаленного доступа; **12.3.10.b** требуют от должным образом уполномоченных работников, чтобы они защищали ДДК в соответствии с требованиями PCI DSS.	Чтобы работники знали о своем обязательстве не хранить или не копировать ДДК на свои персональные компьютеры или другие носители информации, политика организации должна явно запрещать действия такого рода, исключая работников, которым так делать явно разрешено. Хранение или копирование ДДК на локальный жесткий диск или иной носитель должно осуществляться в соответствии со всеми применимыми требованиями стандарта PCI DSS.
12.4 Гарантировать, что политика и процедуры безопасности четко определяют обязанности по обеспечению информационной безопасности для всех работников.	**12.4** Убедиться, что политики информационной безопасности четко определяют обязанности по обеспечению информационной безопасности для всех работников. **12.4.b** Опросить выборку ответственных работников на предмет того, что они понимают политику безопасности.	Если роли и обязанности по обеспечению информационной безопасности четко не определены, то взаимодействие между работниками, отвечающими за безопасность, будет неэффективным, что может привести к небезопасному внедрению технологий или использованию устаревших или небезопасных технологий.
12.4.1 ***Дополнительное требование для поставщиков услуг:*** исполнительные органы управления должны определить обязанности по защите ДДК и программу обеспечения соответствия требованиям стандарта PCI DSS, которая включает: • общую ответственность за	**12.4.1.a** Проверить документацию на предмет того, что исполнительные органы управления назначили ответственных за поддержание соответствия требованиям стандарта PCI DSS в организации.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Распределение обязанностей по обеспечению соответствия требованиям стандарта PCI DSS иполнительными органами управления обеспечивает наличие осведомленности о программе обеспечения соответствия требованиям стандарта PCI DSS на уровне

Требования PCI DSS	Проверочные процедуры	Пояснение
поддержание соответствия требованиям стандарта PCI DSS; • определение устава программы обеспечения соответствия требованиям стандарта PCI DSS и взаимодействия с исполнительными органами управления. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**12.4.1.b** Проверить устав программы обеспечения соответствия требованиям стандарта PCI DSS на предмет того, что он описывает принципы работы данной программы и взаимодействия с исполнительными органами управления.	управления и дает возможность задавать необходимые вопросы для определения эффективности программы и оказывать влияние на стратегические приоритеты. Общие обязанности по программе обеспечения соответствия требованиям стандарта PCI DSS могут быть назначены на отдельных работников и (или) подразделения организации внутри организации. Исполнительные органы управления могут включать руководителей компании и отделов, совет директоров и аналогичные должности. Конкретные названия должностей будут зависеть от определенной организационной структуры. Уровень детализации информации для руководящих должностей должен соответствовать определенной организации и целевой аудитории.
12.5 Назначить лицу или группе лиц следующие обязанности по управлению информационной безопасностью:	**12.5** Проверить политики и процедуры информационной безопасности на предмет того, что они: • официально делегируют ответственность за информационную безопасность руководителю службы безопасности (Chief Security Officer) или другому члену руководства, компетентному в вопросах обеспечения информационной безопасности; • явным образом и официально назначают следующие обязанности по информационной безопасности:	Каждое лицо или группа лиц, которые отвечают за управление информационной безопасностью, обязаны четко знать свои обязанности и связанные с ними задачи. Задачи и обязанности доводятся до сведения через соответствующие политики. Если такой подотчетности нет, то уязвимости в процессах могут открыть доступ к критичным ресурсам или ДДК. Организациям также следует рассмотреть вопрос о переходе и (или) планы преемственности для ключевых работников для избежания потенциальных пробелов в обязанностях по безопасности, которые могут возникнуть из-за того, что обязанности не были распределены и поэтому не выполняются.
12.5.1 разработка, документирование и распространение политик и процедур безопасности;	**12.5.1** разработка, документирование и распространение политик и процедур безопасности;	
12.5.2 мониторинг и анализ уведомлений и информации о безопасности; доведение их до сведения соответствующих работников;	**12.5.2** мониторинг и анализ уведомлений и информации о безопасности; доведение их до сведения соответствующих работников;	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.5.3 определение, документирование и распространение процедур реагирования на инциденты информационной безопасности и процедур эскалации, чтобы обеспечить своевременную и эффективную обработку всех ситуаций;	**12.5.3** определение, документирование и распространение процедур реагирования на инциденты информационной безопасности и процедур эскалации;	
12.5.4 администрирование учетных записей пользователей (в т. ч. их добавление, удаление и изменение);	**12.5.4** администрирование учетных записей пользователей (в т. ч. их добавление, удаление и изменение);	
12.5.5 мониторинг и контроль любого доступа к данным;	**12.5.5** мониторинг и контроль любого доступа к данным.	
12.6 Внедрить официальную программу повышения осведомленности работников по вопросам безопасности, чтобы они знали политику и процедуры защиты ДДК.	**12.6.a** Проверить программу повышения осведомленности работников по вопросам безопасности на предмет того, что она предусматривает информирование всех работников о политике и процедурах защиты ДДК.	Если работники не знают о своих обязанностях по обеспечению информационной безопасности, реализованные защитные меры и процессы могут стать неэффективными из-за ошибок или умышленных действий.
	12.6.b Проверить процедуры и документацию программы повышения осведомленности работников по вопросам безопасности и проверить их следующим образом:	
12.6.1 Обучать работников при приеме на работу, а также не реже одного раза в год. ***Примечание:*** *методы обучения могут зависеть от роли работника и уровня его доступа к ДДК.*	**12.6.1.a** Убедиться в том, что в программе повышения осведомленности по вопросам информационной безопасности используются различные методы доведения информации и обучения работников (например, плакаты, письма, заметки, системы Интернет-обучения, специальные кампании).	Если программа повышения осведомленности по вопросам информационной безопасности не предусматривает переподготовку, работники могут забыть важнейшие процессы и процедуры обеспечения безопасности или пренебречь ими, что приведет к уязвимости критичных ресурсов и ДДК.
	12.6.1.b Убедиться, что работники проходят обучение, повышающее их осведомленность в вопросах информационной безопасности, при приеме на работу и не реже раза в год.	
	12.6.1.c Опросить выборку работников на предмет того, что они прошли обучение, повышающее их осведомленность в вопросах информационной безопасности, и понимают важность защиты ДДК.	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.6.2 Требовать, чтобы работники подтверждали не реже раза в год, что они прочли и поняли политику и процедуры информационной безопасности.	**12.6.2** Убедиться, что программа повышения осведомленности по вопросам информационной безопасности требует, чтобы работники не реже раза в год подтверждали (в письменной или электронной форме), что они прочли и поняли политику информационной безопасности.	Требование от работника подтверждения в письменном или электронном виде, помогает гарантировать, что он действительно прочитал и понял политики и процедуры информационной безопасности, а также то, что он действует и будет продолжать действовать в соответствии с этими политиками.
12.7 Тщательно проверять потенциальных работников до приема на работу, чтобы минимизировать риск инсайдерских атак. (Примерами проверки биографических данных являются изучение списка предыдущих мест работы, сведений о судимости, кредитной истории, рекомендаций). ***Примечание:*** *для кандидатов на определенные должности, такие как кассиры в магазине, которые имеют доступ только к одному номеру карты в момент выполнения транзакции, это требование носит исключительно рекомендательный характер.*	**12.7** Сделать запрос в руководство отдела кадров на предмет того, что до приема на работу потенциальных работников, которым будет предоставляться доступ к ДДК или среде ДДК, их биографические данные тщательно проверяются (в рамках местного законодательства).	Тщательное изучение биографии потенциальных работников, которые имеют доступ к ДДК, до их приема на работу, снижает риск несанкционированного использования PAN и других ДДК лицами с сомнительным или криминальным прошлым.
12.8 Внедрить и поддерживать следующие политики и процедуры управления поставщиками услуг, у которых есть доступ к ДДК или которые могут воздействовать на безопасность ДДК:	**12.8** Просмотреть и проверить следующим образом политики, процедуры и сопутствующую документацию на предмет того, что реализованы процессы для управления поставщиками услуг, у которых есть доступ к ДДК или которые могут воздействовать на безопасность ДДК:	Если ТСП или поставщик услуг дают доступ к ДДК другому поставщику услуг, то необходимо выполнить определенные требования, чтобы обеспечить защиту таких данных со стороны поставщика услуг. Примерами различных типов поставщиков услуг являются хранилища резервных копий на магнитной ленте, поставщики управляемых услуг, такие как поставщики услуг хостинга или услуг защиты, организации, которые получают данные для выявления мошеннического поведения и т.д.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.8.1 поддержка перечня поставщиков услуг, включая описание предоставляемых услуг;	**12.8.1** проверить, что перечень поставщиков услуг поддерживается в актуальном состоянии и включает описание предоставляемых услуг;	Ведение перечня поставщиков услуг помогает оценить потенциальные риски, внешние по отношению к организации.
12.8.2 поддержка письменного соглашения, в котором поставщики услуг подтверждают, что они отвечают за безопасность ДДК, которые они хранят, обрабатывают или передают от имени клиента, или отвечают в той мере, в которой они могут воздействовать на безопасность среды ДДК клиента; ***Примечание:*** *точная формулировка подтверждения зависит от договора между двумя сторонами, деталей предоставляемой услуги и обязанностей каждой из сторон. Формулировка подтверждения не обязательно должна соответствовать точной формулировке, указанной в данном требовании.*	**12.8.2** проверить письменные соглашения на предмет того, что поставщики услуг в них подтверждают, что они отвечают за безопасность ДДК, которые они хранят, обрабатывают или передают по поручению клиента, или отвечают в той мере, в которой они могут воздействовать на безопасность среды ДДК клиента;	Подтверждение от поставщиков услуг свидетельствует об их готовности поддерживать надлежащий уровень безопасности ДДК, которые они получают от своих клиентов. Мера ответственности поставщика услуг за безопасность карточных данных будет зависеть от определенных услуг и соглашений между поставщиком и оцениваемой организацией. В сочетании с требованием 12.9 данное требование нацелено на то, чтобы между сторонами установилось единое понимание своих обязанностей в рамках стандарта PCI DSS. Например, соглашение может включать соответствующие требования PCI DSS, которые необходимо соблюдать при предоставлении услуг.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.8.3 процесс привлечения поставщиков услуг, который включает в себя проверку благонадежности, проводимую до начала работу с поставщиком услуг;	**12.8.3** проверить, что политики и процедуры документированы, соблюдаются и включают необходимость должного выполнения предварительных проверок благонадежности любого поставщика услуг;	Данный процесс гарантирует, что возможность привлечения поставщика услуг тщательно изучается внутри организации и включает в себя анализ рисков до установления официальных отношений с этим поставщиком. Конкретные процессы и цели проверки благонадежности зависят от организации и учитывают, например, следующие факторы: — как предоставляется отчетность; — как организация уведомляет о нарушениях ИБ; — как реагирует на инциденты; — как разделены между сторонами обязанности по соблюдению требований PCI DSS; — как поставщик подтверждает и доказывает свое соответствие требованиям PCI DSS и т. д.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.8.4 поддержка программы отслеживания статуса соответствия поставщиков услуг требованиям PCI DSS не реже раза в год;	**12.8.4** проверить, что в организации поддерживается программа, требующая отслеживать статус соответствия поставщиков услуг требованиям PCI DSS не реже раза в год;	Зная статус соответствия поставщиков услуг требованиям стандарта PCI DSS, организация может быть уверена в том, что поставщики соблюдают те же требования, что и она сама. Если поставщик предоставляет широкий спектр услуг, данное требование применяется только к услугам, которые предоставляются организации и входят в область оценки соответствия стандарту PCI DSS организации. Конкретная информация, которая должна поддерживаться организацией, зависит от действующих соглашений с ее поставщиками, вида услуг и т. д. Цель данного требования – организация должна понимать требования PCI DSS, на выполнение которых согласились поставщики.
12.8.5 поддержка информации о том, за какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	**12.8.5** проверить, что организация поддерживает информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация.	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.9 ***Дополнительное требование только для поставщиков услуг*:** поставщики услуг должны письменно подтверждать, что они отвечают за безопасность ДДК, которые они хранят, обрабатывают или передают от имени клиента, или отвечают в той мере, в которой они могут воздействовать на безопасность среды ДДК клиента. ***Примечание:*** *точная формулировка подтверждения зависит от договора между двумя сторонами, деталей предоставляемой услуги и обязанностей каждой из сторон. Формулировка подтверждения не обязательно должна соответствовать точной формулировке, указанной в данном требовании.*	**12.9** ***Дополнительная проверочная процедура только для поставщиков услуг:*** проверить политики и процедуры поставщиков услуг, а также шаблоны письменного соглашения на предмет того, что поставщики услуг письменно подтверждают клиентам, что они будут соблюдать все применимые требования PCI DSS в той части, в которой у поставщиков услуг присутствуют ДДК или иначе они хранятся, обрабатываются или передаются по поручению клиентов, или в которой поставщики услуг могут влиять на безопасность среды ДДК клиентов.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* В сочетании с требованием 12.8.2 данное требование нацелено на то, чтобы между поставщиками услуг и их клиентами установилось единое понимание своих обязанностей в рамках стандарта PCI DSS. Подтверждение от поставщиков услуг свидетельствует об их готовности поддерживать надлежащий уровень безопасности ДДК, которые они получают от своих клиентов. Внутренние политики и процедуры поставщиков услуг, связанные с процессом взаимодействия с клиентами и шаблонами, используемыми для письменных соглашений, должны включать положения о том, что поставщики услуг подтверждают клиентам соблюдение применимых к ним требований PCI DSS. Форма письменного обязательства поставщика услуг должна быть согласована между ним и его клиентами.
12.10 Внедрить план реагирования на инциденты. Организация должна быть готова к немедленному реагированию на нарушение безопасности системы.	**12.10** Проверить план и процедуры реагирования на инциденты на предмет того, что организация готова немедленно отреагировать на нарушение безопасности системы следующим образом:	Если ответственные лица не доводят до сведения, не читают и не понимают должным образом план реагирования на инциденты безопасности, то замешательство и отсутствие единого подхода к реагированию могут: — увеличить время вынужденного простоя, — привести к появлению в СМИ нежелательной информации, — наложить дополнительные юридические обязательства.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.10.1 Разработать план реагирования на инциденты, применяемый в случае нарушения безопасности системы. План должен учитывать, как минимум, следующее: • роли, обязанности, порядок оповещения, алгоритм установления контактов в случае компрометации данных, в т. ч., как минимум, оповещение международных платежных систем; • процедуры реагирования на конкретные инциденты; • процедуры восстановления и обеспечения непрерывности деятельности организации; • процессы резервного копирования данных; • анализ требований законодательства об оповещении о фактах компрометации; • покрытие всех критичных системных компонентов; • процедуры реагирования на инциденты или ссылки на такие процедуры, предусмотренные международными платежными системами.	**12.10.1.a** Проверить, что план реагирования на инциденты включает в себя: • роли, обязанности, порядок оповещения в случае компрометации данных, в т. ч., как минимум, оповещение международных платежных систем; • процедуры реагирования на конкретные инциденты; • процедуры восстановления и обеспечения непрерывности деятельности организации; • процессы резервного копирования данных; • анализ требований законодательства об оповещении о фактах компрометации (например, Закона Калифорнии №1386, который требует, чтобы каждая организация, в базе данных которой находятся жители штата Калифорния, уведомляла пострадавших клиентов, если она выявила у себя компрометацию или подозрение на компрометацию); • покрытие всех критичных системных компонентов; • процедуры реагирования на инциденты или ссылки на такие процедуры, предусмотренные международными платежными системами.	План реагирования на инциденты должен быть подробным и содержать все ключевые элементы, которые позволят организации эффективно реагировать, если возникает нарушение безопасности, которое подвергает риску ДДК.
	12.10.1.b Опросить работников и проверить документацию по выборке ранее зарегистрированных инцидентов или уведомлений безопасности на предмет того, что были выполнены документированные план реагирования на инцидент и процедуры.	
12.10.2 Проверять и тестировать план, включая все элементы, перечисленные в требовании 12.10.1, не реже раза в год.	**12.10.2** Опросить работников и проверить документацию по тестированию на предмет того, что план тестируется не реже раза в год, и тестирование включает все элементы, перечисленные в требовании 12.10.1.	Без надлежащего тестирования можно пропустить ключевые пункты, которые могут сделать систему уязвимее во время инцидента.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.10.3 Назначить специальных работников, готовых реагировать на уведомления круглосуточно и без выходных.	**12.10.3** Проверить политики, наблюдать за работниками и опросить ответственные лица на предмет того, что назначенные работники готовы круглосуточно и без выходных отслеживать и реагировать на следующие события: — инциденты, — любые признаки несанкционированной деятельности, — обнаружение несанкционированных беспроводных точек доступа, — критичные предупреждения систем обнаружения вторжений (IDS), — сообщения о несанкционированных изменениях в критичных системных файлах или файлах данных.	Если отсутствует обученная группа быстрого реагирования на инциденты, сети может быть нанесен серьезный ущерб, а критичные данные и системы могут быть повреждены из-за ненадлежащего обращения с целевыми системами. Это может помешать расследованию инцидента.
12.10.4 Обеспечить надлежащее обучение работников, ответственных за реагирование на нарушения безопасности.	**12.10.4** Проверить политики и опросить ответственных работников на предмет того, что работники, которые отвечают за реагирование на нарушения безопасности, проходят периодическое обучение.	
12.10.5 Отслеживать уведомления от систем мониторинга безопасности, включая, среди прочего, системы обнаружения и предотвращения вторжений, межсетевые экраны и системы мониторинга целостности файлов.	**12.10.5** Пронаблюдать и проверить процессы на предмет того, что мониторинг и реагирование на уведомления от систем мониторинга безопасности предусмотрены планом реагирования на инциденты.	Данные системы мониторинга предназначены для того, чтобы отслеживать потенциальные риски для данных, и необходимы, чтобы оперативно предотвращать инциденты. Организация должна включать такие системы в процессы реагирования на инциденты.
12.10.6 Разработать процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в отрасли.	**12.10.6** Проверить политики, опросить ответственных работников и пронаблюдать процесс на предмет того, что разработан процесс изменения и дополнения плана реагирования на инциденты в соответствии с полученным опытом и разработками в отрасли.	Учитывая после инцидента полученный опыт в плане реагирования на инциденты, можно поддерживать план в актуальном состоянии 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*:** проводить проверку, как минимум, ежеквартально, чтобы убедиться в том, что работники соблюдают политику обеспечения безопасности и операционные процедуры. Проверка должна охватывать следующие процессы: • ежедневная проверка журналов регистрации событий; • проверка правил межсетевых экранов; • применение стандартов конфигураций для новых систем; • реагирование на уведомления безопасности; • процессы управления изменениями. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**12.11.a** Проверить политики и процедуры на предмет того, что определены процессы проверки и подтверждения того, что работники соблюдают политику обеспечения безопасности и операционные процедуры, и данные процессы охватывают следующее: • ежедневная проверка журналов регистрации событий; • проверка правил межсетевых экранов; • применение стандартов конфигураций для новых систем; • реагирование на уведомления безопасности; • процессы управления изменениями. **12.11.b** Опросить ответственных работников и проверить записи проверок на предмет того, что проверки проводятся, как минимум, ежеквартально.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Регулярные подтверждения того, что политика обеспечения безопасности и процедуры соблюдаются, обеспечивают надлежащую работу защитных мер. Целью данных проверок является не повторное выполнение других требований, а подтверждение того, что работники соблюдают процедуры надлежащим образом.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.11.1 ***Дополнительное требование только для поставщиков услуг*:** вести документацию по ежеквартальной проверке процессов, включающую: • документирование результатов проверок; • проверку и утверждение результатов работником, ответственным за поддержание соответствия требованиям стандарта PCI DSS. ***Примечание:*** *до 31 января 2018 года это требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*	**12.11.1** Проверить документацию по ежеквартальным проверкам на предмет того, что они включают: • доументирование результатов проверок; • проверку и утверждение результатов работником, ответственным за поддержание соответствия требованиям стандарта PCI DSS.	***Примечание:*** *это требование применимо только для организаций, которые определены как поставщики услуг.* Цель этих независимых проверок – подтверждение того, что деятельность по обеспечению безопасности осуществляется на постоянной основе. Данные проверки также могут быть использованы для подтверждения того, что необходимые доказательства (например, журналы регистрации событий, отчеты об сканировании на наличие уязвимостей, проверки межсетевых экранов и т.д.) ведутся, чтобы способствовать подготовке организации к следующей оценке соответствия требованиям стандарта PCI DSS.

Приложение A. Дополнительные требования PCI DSS

Это приложение содержит дополнительные требования PCI DSS для различных типов организаций. Приложение включает следующие разделы:

- Приложение A1. Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой;
- Приложение A2. Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS;
- Приложение A3: Дополнительная проверка организаций зоны повышенного риска.

Пояснения и информация о применимости требований приводится в каждом разделе.

Приложение A1. Дополнительные требования PCI DSS для поставщиков услуг хостинга с общей средой

Согласно требованиям 12.8 и 12.9 все поставщики услуг, имеющие доступ к ДДК (включая поставщиков услуг хостинга с общей средой) обязаны выполнять требования PCI DSS. В дополнение к этому, требование 2.6 говорит о том, что поставщики услуг хостинга с общей средой должны защищать среды и ДДК каждой размещенной на хостинге организации. Поэтому, поставщики услуг хостинга с общей средой должны дополнительно соответствовать требованиям, перечисленным в этом приложении.

Требования A1	Проверочные процедуры	Пояснение
A1 Обеспечить защиту среды и данных каждой размещенной организации (т. е. ТСП, поставщика услуг или иной) согласно требованиям A1.1 - A1.4: Поставщик услуг хостинга должен выполнять эти и все остальные соответствующие требования PCI DSS. ***Примечание:*** *даже если поставщик услуг хостинга отвечает этим требованиям, это не гарантирует, что организация, которая пользуется его услугами, соответствует требованиям. Каждая организация должна соответствовать требованиям стандарта PCI DSS и, в зависимости от обстоятельств, подтверждать свое соответствие применимым для нее способом.*	**A1** Для оценки соответствия требованиям PCI DSS именно поставщиков услуг хостинга с общей средой: — сделать выборку серверов (под управлением Microsoft Windows и Unix (Linux) из репрезентативной выборки размещенных ТСП и поставщиков услуг; — выполнить проверки, перечисленные в пунктах A1.1 - A1.4 на предмет того, что эти поставщики защищают среду и данные размещенных у них организаций (ТСП и поставщиков услуг).	*Приложение A* к стандарту PCI DSS предназначено для поставщиков услуг хостинга с общей средой, которые желают предоставлять своим клиентам (ТСП и (или) поставщику услуг) хостинговую среду, которая соответствует требованиям стандарта PCI DSS.

Требования A1	Проверочные процедуры	Пояснение
A1.1 Гарантировать, что каждая организация исполняет только те процессы, у которых есть доступ к ее среде ДДК.	**A1.1** Если поставщик услуг хостинга с общей средой позволяет организациям (например, ТСП или поставщикам услуг) запускать свои приложения, убедиться, что эти приложения выполняются с использованием уникальной пользовательской учетной записи организации. Например: • ни одна организация в системе не может использовать совместно используемую учетную запись пользователя веб-сервера. • Все CGI-скрипты, используемые организацией, должны создаваться и выполняться под уникальной пользовательской учетной записью организации.	Если ТСП или поставщику услуг разрешается выполнять свои собственные приложения на совместно используемом сервере, то они должны выполняться под учетной записью этого ТСП или поставщика услуг, а не под учетной записью привилегированного пользователя.
A1.2 Ограничить доступ и привилегии каждой организации только ее собственной средой ДДК.	**A1.2.a** Проверить, что ни один прикладной процесс не выполняется под учетной записью привилегированного пользователя (root или admin).	Для того чтобы гарантировать, что каждые ТСП или поставщик услуг имеют доступ только к собственной среде, следует учесть следующее: 1. полномочия пользовательской учетной записи ТСП или поставщика услуг на веб-сервере; 2. разрешения на чтение, запись и исполнение файлов; 3. разрешения на запись в системные исполняемые файлы; 4. разрешения на доступ к файлам журналов регистрации событий поставщика услуг или ТСП; 5. меры для защиты системных
	A1.2.b Проверить, что у каждой организации (ТСП, поставщика услуг) есть права на чтение, запись и выполнение только тех файлов и папок, владельцем которых она является, или необходимых системных файлов (доступ к которым ограничен через установку прав доступа к файлам, списки контроля доступа, окружений chroot, jailshell и т. п.). **Важно!** Групповой доступ к файлам организации запрещен.	
	A1.2.c Проверить, что у пользователей организации нет доступа с правом записи к совместно используемым системным двоичным файлам.	
	A1.2.d Проверить, что просмотр записей журналов регистрации событий доступен только владеющей ими организации.	

Требования A1	Проверочные процедуры	Пояснение
	A1.2.e Чтобы проверить, что ни одна организация не может монопольно задействовать ресурсы сервера для эксплуатации уязвимостей (таких как условия возникновения ошибок, состояния гонки, условия перезапуска, которые могут привести, например, к переполнениям буфера) убедиться в наличии ограничений на использование следующих системных ресурсов: • дисковое пространство; • канал; • память; • использование процессорного времени.	ресурсов от монополизации поставщиком услуг или ТСП.
A1.3 Убедиться, что ведение журналов регистрация событий включено, а сами журналы являются уникальными для среды ДДК каждой организации и соответствуют требованию 10 PCI DSS.	**A1.3** Проверить, что поставщик услуг хостинга с общей средой обеспечивает ведение журналов регистрации событий для каждого ТСП и поставщика услуг следующим образом: • журналы для распространенных приложений сторонних производителей включены; • журналы активны по умолчанию; • журналы доступны владеющей организации для изучения; • месторасположения журналов доведены до сведения владеющей организации.	Журналы должны быть доступны в общей среде размещения данных так, чтобы ТСП и поставщики услуг имели доступ к журналам регистрации событий для своей среды ДДК и могли их изучать.
A1.4 Внедрить процессы, позволяющие провести своевременное расследование с использованием компьютерной экспертизы в случае компрометации любых ТСП или поставщика услуг, размещенных на хостинге.	**A1.4** Убедиться, что у поставщиков услуг хостинга с общей средой есть политики в письменной форме, которые требуют своевременно проводить расследование с использованием компьютерной экспертизы соответствующих серверов в случае компрометации.	Поставщики услуг хостинга должны определить процессы, как быстро реагировать в случае компрометации, если требуется расследование с использованием компьютерной экспертизы вплоть до такого уровня детализации, чтобы можно было получить подробные сведения о конкретном ТСП или поставщике услуг.

Приложение A2. Дополнительные требования PCI DSS для организаций, использующих SSL и (или) ранние версии TLS

Организации, использующие SSL и (или) ранние версии TLS, должны работать в направлении обновления этих протоколов до стойких криптографических протоколов в максимально короткие сроки. Кроме того, SSL и (или) ранние версии TLS не должны внеряться в средах, где эти протоколы на данный момент не используются. На момент публикации, известные уязвимости сложно использовать в платежных средах POS POI. Однако, новые уязвимости могут появится в любой момент, и организация должна самостоятельно следовать тенденциям, связанным с уязвимостями, и определять подвержена она или нет всем известным эксплойтам.

Требования стандарта PCI DSS, которые напрямую связаны с темой данного приложения, включают:

Требование 2.2.3	Внедрить дополнительные защитные меры для любых необходимых служб, протоколов и управляющих программ, которые признаны небезопасными.
Требование 2.3	При использовании любого неконсольного административного доступа к системе всегда шифровать канал с использованием стойкой криптографии.
Требование 4.1	Использовать стойкую криптографию и безопасные протоколы, чтобы защитить критичные ДДК при их передаче через открытые общедоступные сети.

SSL и (или) ранние версии TLS не должны использоваться как мера обеспечения безопасности для выполнения данных требований. Для поддержки организаций, работающих над переходом с SSL и (или) ранних версий TLS, включены следующие положения:

- Новые внедрения не должны использовать SSL и (или) ранние версии TLS как защитную меру.
- Все поставщики услуг должны обеспечить поддержку безопасных протоколов до 30 июня 2016 года.
- После 30 июня 2018 года все организации должны прекратить использование SSL и (или) ранних версий TLS как защитной меры и использовать только безопасные версии протоколов (допущение для определенных POS POI-терминалов описано в последнем абзаце списка).
- До 30 июня 2018 года существующие внедрения, которые используют SSL и (или) ранние версии TLS, должны иметь действующий формализованный План снижения риска и перехода на безопасные версии протоколов.
- На POS POI-терминалах (и местах терминации SSL и (или) TLS, с которыми они соединяются), для которых может быть проверено, что они не подвержены любым из известных эксплойтов для SSL и ранних версий TLS, возможно продолжение использования этих протоколов как защитной меры после 30 июня 2018 года.

Требования этого приложения распространяются на организации, использующие SSL и (или) ранние версии TLS как защитную меру, чтобы защитить среду ДДК и (или) ДДК (например, SSL и (или) ранние версии TLS, используемые для выполнения требований 2.2.3, 2.3 или 4.1). Для получения дополнительных пояснений по использованию SSL и (или) ранних версий TLS следует обратиться к *«Вспомогательному документу к стандарту PCI DSS по переходу с SSL и (или) ранних версий TLS».*

Требования A2	Проверочные процедуры	Пояснение
A2.1 Там, где SSL и (или) ранние версии TLS используются на POS POI-терминалах (и местах терминации SSL и (или) TLS, с которыми они соединяются), организация должна применить любую одну из следующих мер**:** • подтвердить, что устройства не подвержены всем известным эксплойтам для этих протоколов; • иметь действующий формализованный План снижения риска и перехода на безопасные версии протоколов.	**A2.1** *Для POS POI-терминалов (и мест терминации SSL и (или) TLS, с которыми они соединяются), использующих SSL и (или) ранние версии TLS, выполнить одну из следующих проверок:* • подтвердить, что в организации есть документация (например, документация от вендоров, документация системных и (или) сетевых конфигураций и т.д.), которая подтверждает, что устройства не подвержены всем известным эксплойтам для SSL и (или) ранних версий TLS; • выполнить проверочную процедуру A2.2, описанную ниже.	На POI-терминалах возможно продолжение использования SSL и (или) ранних версий TLS, если продемонстрировано, что устройство не подвержено известным на данный момент экспойтам. Однако, SSL является устаревшей технологией, и в нем могут быть найдены новые уязвимости в безопасности в будущем. Поэтому настоятельно рекомендуется обновление среды POI-терминалов до безопасных протоколов как можно скорее. Если SSL и (или) ранние версии TLS не требуются в среде, использование и возврат к данным версиям протоколов следует исключить. Если среда POS POI-терминалов подвержена известным эксплойтам, следует немедленно начать планирование перехода на безопасные альтернативы. ***Примечание:*** *допущение для POS POI-терминалов о том, что они на данный момент не подвержены эксплойтам, основывается на текущих известных рисках. Если появятся новые эксплойты, которым среды POI-терминалов подвержены, эти среды необходимо будет обновить.*

Требования A2	Проверочные процедуры	Пояснение
A2.2 Организации с существующими внедрениями (отличными от разрешенных в A2.1), которые используют SSL и (или) ранние версии TLS, должны иметь действующий формализованный План снижения риска и перехода на безопасные версии протоколов.	**A2.2** Проверить, что документированный План снижения риска и перехода на безопасные версии протоколов включает: • описание использования, включая информацию о том, какие данные передаются, типы и количество систем, которые используют и (или) поддерживают SSL и (или) ранние версии TLS, тип среды; • результаты оценки рисков и действующие меры по снижению рисков; • описание процессов по отслеживанию новых уязвимостей, связанных с SSL и (или) ранними версиями TLS; • описание процессов контроля изменений, которые используются чтобы гарантировать, что SSL и (или) ранние версии TLS не внедряются в новые среды; • обзор плана проекта перехода на безопасные версии протоколов, включая дату завершения перехода не позднее 30 июня 2018 года.	План снижения риска и перехода на безопасные версии протоколов – это документ, подготовленный организацией, который подробно описывает планы перехода на безопасные версии протоколов и меры по снижению риска, связанного с SSL и (или) ранними версиями TLS, до завершения перехода. Для получения дополнительных пояснений по Плану снижения риска и перехода на безопасные версии протоколов следует обратиться к *«Вспомогательному документу к стандарту PCI DSS по переходу с SSL и (или) ранних версий TLS».*

Требования A2	Проверочные процедуры	Пояснение
A2.3 ***Дополнительное требование только для поставщиков услуг:*** все поставщики услуг должны обеспечить поддержку безопасных протоколов до 30 июня 2016 года. ***Примечание:*** *до 30 июня 2016 года поставщик услуг должен* ***или*** *предоставлять возможность использования безопасного протокола для доступа к своему сервису,* ***или*** *иметь документированный План снижения риска и перехода на безопасные версии протоколов (согласно A2.2), который включает плановую дату предоставления возможности использования безопасного протокола не позднее 30 июня 2016 года.*	**A2.3** Проверить системные конфигурации и сопутствующую документацию на предмет того, что поставщик услуг предоставляет возможность использования безопасного протокола для доступа к своему сервису.	Для получения дополнительных пояснений следует обратиться к термину «Поставщик услуг» в документе «Глоссарий. Основные определения, аббревиатуры и сокращения стандартов PCI DSS и PA-DSS».

Приложение A3: Дополнительная проверка организаций зоны повышенного риска

Требования этого приложения распространяются только на организациии, определенные международными платежными системами или эквайрером как требующие дополнительной проверки существующих требований PCI DSS. Примеры организаций, к которым ***могут*** применятся требования этого приложения, включают:

- организации, которые хранят, обрабатывают и (или) передают большие объемы ДДК;
- организации, предоставляющие услуги по агрегированию ДДК;
- организации, которые понесли значительные или повторяющиеся утечки ДДК.

Эти действия по дополнительной проверке призваны обеспечить большую уверенность в том, что требования PCI DSS выполняются эффективно и непрерывно посредством проверки привычных бизнес-процессов и усиленной проверки и рассмотрения области применимости.

Действия по дополнительной проверке в этом документе разделены на следующие направления:

- **A3.1** внедрить программу соответствия требованиям стандарта PCI DSS;
- **A3.2** задокументировать и проверить область применимости требований стандарта PCI DSS;
- **A3.3** проверить, встроены ли требования PCI DSS в привычные бизнес-процессы;
- **A3.4** контролировать и управлять логическим доступом к среде ДДК;
- **A3.5** выявлять и реагировать на подозрительные события.

Примечание: *некоторые требования включают временные периоды (например, как минимум ежеквартально или каждые шесть месяцев), в течение которых определенные действия должны быть выполнены. При первоначальной проверке соответствия требованиям этого документа не требуется, чтобы действие выполнялось для каждого временного периода в течение предыдущего года, если аудитор подтверждает, что:*

1) *действие выполнялось в соответствии с применимым требованием в течение последнего периода (например, последний квартал или шесть месяцев),*
2) *и организация имеет документированные политики и процедуры для продолжения выполнения действия в соответствии с определенными временными периодами.*

В последующие годы после первоначальной проверки действие должно выполняться для каждого временного периода, для которого это необходимо (например, ежеквартальное действие должно быть выполнено в каждом из четырех кварталов предыдущего года).

Примечание: *организация должна пройти оценку по требованиям этого приложения* ***ТОЛЬКО по предписанию эквайрера или международной платежной системы****.*

Требования A3	Проверочные процедуры	Пояснение
A3.1 Внедрить программу соответствия требованиям стандарта PCI DSS		
A3.1.1 Исполнительные органы управления должны определить обязанности по защите ДДК и программу обеспечения соответствия требованиям стандарта PCI DSS, которая включает: • общую ответственность за поддержание соответствия требованиям стандарта PCI DSS; • определение устава программы обеспечения соответствия требованиям стандарта PCI DSS; • предоставление актуальной информации исполнительным органам управления и совету директоров по инициативам и вопросам обеспечения соответствия требованиям стандарта PCI DSS, включая деятельность по устранению несоответствий, как минимум, ежегодно. ***Связанные требования стандарта PCI DSS:*** *Требование 12*	**A3.1.1.a** Проверить документацию на предмет того, что исполнительные органы управления назначили ответственных за поддержание соответствия требованиям стандарта PCI DSS в организации.	Распределение обязанностей по обеспечению соответствия требованиям стандарта PCI DSS иполнительными органами управления обеспечивает наличие осведомленности о программе обеспечения соответствия требованиям стандарта PCI DSS на уровне управления и дает возможность задавать необходимые вопросы для определения эффективности программы и оказывать влияние на стратегические приоритеты. Общие обязанности по программе обеспечения соответствия требованиям стандарта PCI DSS могут быть назначены на отдельных работников и (или) подразделения организации внутри организации.
	A3.1.1.b Проверить устав программы обеспечения соответствия требованиям стандарта PCI DSS на предмет того, что он описывает условия, на которых построена программа обеспечения соответствия требованиям стандарта PCI DSS.	
	A3.1.1.c Проверить протоколы совещаний и (или) презентации для исполнительных органов управления и совета директоров на предмет того, что информация об инициативах по обеспечению соответствия требованиям стандарта PCI DSS и устранению несоответствий предоставляется, как минимум, ежегодно.	

Требования A3	Проверочные процедуры	Пояснение
A3.1.2 Формализованная программа обеспечения соответствия требованиям стандарта PCI DSS должна существовать и включать: • определение действий по поддержанию и контролю общего соответствия требованиям стандарта PCI DSS, включая привычные бизнес-процессы; • ежегодный процесс оценки соответствия требованиям стандарта PCI DSS; • процессы постоянной проверки выполнения требований стандарта PCI DSS (например, ежедневно, еженедельно, ежеквартально и т.д., в соответствии с требованием); • процесс анализа влияния на деятельность компании для определения потенциального влияния стратегических бизнес-решений на соответствие PCI DSS. ***Связанные требования стандарта PCI DSS:*** *Требования 1 - 12*	**A3.1.2.a** Проверить политики и процедуры информационной безопасности на предмет того, что процессы четко определены для: • поддержания и мониторинга общего соответствия требованиям стандарта PCI DSS, включая привычные бизнес-процессы; • ежегодной оценки (оценок) соответствия требованиям стандарта PCI DSS; • постоянной проверки выполнения требований стандарта PCI DSS; • анализа влияния на деятельность компании для определения потенциального влияния стратегических бизнес-решений на соответствие PCI DSS.	Формализованая программа соответствия стандарту PCI DSS позволяет организации контролировать состояние защитных мер, проявлять инициативу в случае ошибок контроля и эффективно передавать информацию о действиях и состоянии соответствия требованиям стандарта PCI DSS внутри организации. Программа соответствия требованиям стандарта PCI DSS может быть отдельным документом или частью общей программы по обеспечению соответствия и (или) управления, и должна включать четко определенную методологию, которая показывает последовательную и эффективную оценку. Примеры методологий включают Цикл Деминга (PDCA), ISO 27001, COBIT, DMAIC и концепция Шести Сигм.
	A3.1.2.b Опросить работников и проверить действия по поддержанию соответствия на предмет того, что определенные процессы выполняются для следующих действий: • поддержание и контроль общего соответствия требованиям стандарта PCI DSS, включая привычные бизнес-процессы; • ежегодная оценка (оценки) соответствия требованиям стандарта PCI DSS; • постоянная проверка выполнения требований стандарта PCI DSS; • анализ влияния на деятельность компании для определения потенциального влияния стратегических бизнес-решений на соответствие PCI DSS.	Поддержание и контроль общего соответствия требованиям стандарта PCI DSS в организации включает определение действий, которые будут выполняться ежедневно, еженедельно, ежемесячно, ежеквартально или ежегодно, и подтверждение того, что эти действия выполняются соответствующим образом (например, с помощью самооценки безопасности или Цикла Деминга (PDCA)). Примеры стратегических бизнес-решений, которые следует проанализировать для определения потенциального влияния на соответствие PCI DSS, могут включать сделки по слиянию и поглощению, приобретение новых технологий или новые каналы приема платежей.

Требования A3	Проверочные процедуры	Пояснение
A3.1.3 Роли и обязанности по обеспечению соответствия требованиям стандарта PCI DSS должны быть четко определены и формализованно назначены на одного или нескольких работников, включая, как минимум, следующее: • управление PCI DSS с точки зрения привычных бизнес-процессов; • управление ежегодной оценкой соответствия требованиям стандарта PCI DSS; • управление постоянной проверкой выполнения требований стандарта PCI DSS (например, ежедневно, еженедельно, ежеквартально и т.д., в соответствии с требованием); • управление анализом влияния на деятельность компании для определения потенциального влияния стратегических бизнес-решений на соответствие PCI DSS. ***Связанные требования стандарта PCI DSS:*** *Требование 12*	**A3.1.3.a** Проверить политики и процедуры информационной безопасности и опросить работников на предмет того, что роли и обязанности четко определены, и служебные обязанности назначены с учетом, как минимум, следующего: • управление PCI DSS с точки зрения привычных бизнес-процессов; • управление ежегодной оценкой соответствия требованиям стандарта PCI DSS; • управление постоянной проверкой выполнения требований стандарта PCI DSS (например, ежедневно, еженедельно, ежеквартально и т.д., в соответствии с требованием); • управление анализом влияния на деятельность компании для определения потенциального влияния стратегических бизнес-решений на соответствие PCI DSS. **A3.1.3.b** Опросить ответственных работников на предмет того, что они знают и выполняют назначенные на них обязанности по обеспечению соответствия требованиям стандарта PCI DSS.	Формализованное определение конкретных ролей и обязанностей по обеспечению соответствия требованиям стандарта PCI DSS позволяет обеспечить ответственность и контроль текущей деятельности по обеспечению соответствия требованиям стандарта PCI DSS. Эти роли могут быть назначены на одного работника или на несколько работников в различных аспектах. Роли следует назначать на работников, имеющих полномочия принимать решения на основе оценки рисков, на которых возложена ответственность за выполнение этой определенной функции. Служебные обязанности должны быть формализованы, и работники, на которых возложены данные функции, должны быть в состоянии продемонстрировать понимание своих обязанностей и ответственности.
A3.1.4 Обеспечить актуальное обучение по стандарту PCI DSS и (или) информационной безопасности не реже раза в год для работников, на которых возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS (как	**A3.1.4.a** Проверить политики и процедуры информационной безопасности на предмет того, что обучение по стандарту PCI DSS и (или) информационной безопасности необходимо проходить не реже раза в год каждому работнику, на которого возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS.	Для работников, ответственных за обеспечение соответствия требованиям стандарта PCI DSS, требуется обучение, превосходящее типовое обучение по вопросам безопасности. Работникам, на которых возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS,

Требования A3	Проверочные процедуры	Пояснение
указано в A3.1.3). ***Связанные требования стандарта PCI DSS:*** *Требование 12*	**A3.1.4.b** Опросить работников и проверить сертификаты о прохождении обучения или другие записи на предмет того, что работники, на которых возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS, проходят актуальное обучение по стандарту PCI DSS и (или) подобное обучение по информационной безопасности не реже раза в год.	следует проходить специализированное обучение в дополнение к типовому обучению по вопросам безопасности, которое сосредоточено на конкретных вопросах безопасности, навыках, процессах или методологиях, которыми они должны руководствоваться для эффективного выполнения своих обязанностей по обеспечению соответствия требованиям стандарта PCI DSS. Обучение может быть проведено третьими лицами (например, SANS или PCI SSC (программы «PCI Awareness», «PCIP», «ISA»), международными платежными системами или эквайерами), или обучение может быть внутренним. Содержание обучания должно быть применимо к определенной функции работника и актуально, включая последнюю информацию об угрозах безопасности и (или) версиях стандарта PCI DSS. Для получения дополнительных пояснений по разработке соответствующего содержания обучения по вопросам безопасности для определенных служебных ролей следует обратиться к дополнительному документу PCI SSC *«Передовой опыт по внедрению обучающей программы по вопросам безопасности».*
A3.2 Задокументировать и проверить область применимости требований стандарта PCI DSS		
A3.2.1 Документировать и подтверждать правильность области применимости требований стандарта PCI DSS, как минимум, ежеквартально и после значительных изменений среды, находящейся в области применимости требований	**A3.2.1.a** Проверить документированные результаты анализа области применимости стандарта PCI DSS и опросить работников на предмет того, что анализ выполняется: • как минимум, ежеквартально; • после значительных изменений среды, находящейся в области применимости требований стандарта PCI DSS.	Проверку области применимости требований стандарта PCI DSS следует выполнять настолько часто, насколько это возможно, чтобы обеспечивать актуальность области применимости требований стандарта PCI DSS и соответствие изменениям бизнес-целей.

Требования A3	Проверочные процедуры	Пояснение
стандарта PCI DSS. Как минимум, ежеквартальная проверка области применимости требований стандарта PCI DSS должна включать: • определение всех сетей и системных компонентов, входящих в область применимости требований стандарта PCI DSS; • определение всех сетей, не входящих в область применимости требований стандарта PCI DSS, и обоснование того, почему сети не включены в данную область, в том числе описание всех используемых средств сегментации; • определение всех связанных организаций, например, сторонних организаций, имеющих доступ к среде ДДК. ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS"*	**A3.2.1.b** Проверить документированные результаты ежеквартального анализа области применимости стандарта PCI DSS на предмет того, что выполняется следующее: • определение всех сетей и системных компонентов, входящих в область применимости требований стандарта PCI DSS; • определение всех сетей, не входящих в область применимости требований стандарта PCI DSS, и обоснование того, почему сети не включены в данную область, в том числе описание всех используемых средств сегментации; • определение всех связанных организаций, например, сторонних организаций, имеющих доступ к среде ДДК.	

Требования A3	Проверочные процедуры	Пояснение
A3.2.2 Определять влияние каждого из изменений систем или сетей на область применимости требований стандарта PCI DSS, включая добавления новых систем и новые сетевые соединения. Процессы должны включать: • выполнение формализованной оценки влияния с точки зрения стандарта PCI DSS; • определение применимых требований стандарта PCI DSS к системе или сети; • актуализация области применимости стандарта PCI DSS при необходимости; • документальное утверждение результатов оценки влияния ответственным работником (как указано в A3.1.3). ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS", Требования 1 - 12 стандарта PCI DSS*	**A3.2.2** Проверить документацию по изменениям и опросить работников на предмет того, что для каждого изменения систем или сетей: • формализованная оценка влияния с точки зрения стандарта PCI DSS была выполнена; • применимые требования стандарта PCI DSS к системе или сети были определены; • область применимости стандарта PCI DSS, если это необходимо при изменении, была актуализирована; • утверждение ответственным работником (как указано в A3.1.3) было получено и задокументировано.	Изменения систем или сетей могут оказывать значительное влияние на область применимости требований стандарта PCI DSS. Например, изменение правил межсетевого экрана может привести к тому, что все сетевые сегменты попадут в область применимости, или в среду ДДК могут быть добавлены новые системы, которые придется защищать соответствующим образом. Процесс определения потенциального влияния изменения систем или сетей, которое оно может оказывать на область применимости требований стандарта PCI DSS в организации, может быть выполнен в рамках выделенной программы по обеспечению соответствия требованиям стандарта PCI DSS или являться частью общей программы по обеспечению соответствия.

Требования A3	Проверочные процедуры	Пояснение
A3.2.2.1 После завершения изменения проверять все соответствующие требования стандарта PCI DSS на всех новых или измененных системах и сетях, и при необходимости актуализировать документацию. Примеры требований стандарта, которые необходимо проверить, включают, среди прочего: • актуализировать схему сети в соответствии с изменениями; • сконфигурировать системы согласно стандартам конфигурации с изменением все паролей по умолчанию и отключением неиспользуемых сервисов; • защитить системы с помощью необходимых мер, например, мониторинга целостности файлов, антивирусного ПО, обновлений, ведения журналов аудита; • проверить, что критичные аутентификационные данные (КАД) не хранятся, и хранение всех ДДК задокументировано и приведено в соответствие политике и процедурам хранения данных; • включить новые системы в ежеквартальный процесс сканирования на наличие уязвимостей. ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS", Требования 1 - 12 стандарта PCI DSS*	**A3.2.2.1** Для выборки изменений систем и сетей проверить записи об изменениях, опросить работников и изучить затронутые системы и (или) сети на предмет того, что применимые требования стандарта PCI DSS были выполнены, и документация актуализирована в рамках изменений.	Важно наладить процессы анализа всех изменений для подтверждения того, что все соответствующие требования стандарта PCI DSS применяются к любым системам и сетям, включенным в результате изменения в среду, находящуюся в области применимости стандарта PCI DSS. Включение этой проверки в процессы управления изменениями позволяет обеспечить наличие актуальных списков устройств и стандартов конфигурации и применение защитных мер там, где это необходимо. Процесс управления изменениями должен включать подтверждение того, что требования стандарта PCI DSS выполнены или сохранены посредством повторяющегося процесса.

Требования A3	Проверочные процедуры	Пояснение
A3.2.3 После изменения организационной структуры, например, сделки организации по слиянию или поглощению, смены или переназначения работников, ответственных за защитные меры, проводить формализованную (внутреннюю) проверку влияния на область применимости требований стандарта PCI DSS и применимость защитных мер. ***Связанные требования стандарта PCI DSS:*** *Требование 12*	**A3.2.3** Проверить политики и процедуры на предмет того, что после изменения организационной структуры проводится формализованная проверка влияния на область применимости требований стандарта PCI DSS и применимость защитных мер.	Структура и руководство организации определяют требования и порядок для эффективной и безопасной деятельности. Изменения этой структуры могут оказывать негативное воздействие на существующие защитные меры и среду их функционирования путем перераспределения и удаления средств, которые раньше обеспечивали выполнение требований стандарта PCI DSS, или появления новых обязанностей, выполнение которых пока не контролируется. Следовательно, важно пересматривать область применимости требований стандарта PCI DSS и защитные меры после изменений, чтобы обеспечить реализацию данных мер.
A3.2.4 Если применяется сегментация, подтверждать область применимости стандарта PCI DSS путем тестирования на проникновение в отношении средств сегментации, как минимум, каждые 6 месяцев и после любого изменения средств и (или) методов сегментации. ***Связанные требования стандарта PCI DSS:*** *Требование 11*	**A3.2.4** Проверить результаты последнего тестирования на проникновение на предмет того, что: • тест на проникновение для проверки средств сегментации осуществляется, как минимум, каждые 6 месяцев и после любого изменения средств и (или) методов сегментации; • тест на проникновение распространяется на все используемые средства и (или) методы сегментации; • тест на проникновение проверяет, действительно ли механизмы и (или) методы сегментации эффективно работают и изолируют все системы, находящиеся в среде ДДК, от остальных.	Если сегментация применяется для изоляции сетей, находящихся в области применимости стандарта PCI DSS, от остальных сетей, эти средства сегментации должны быть проверены путем тестирования на проникновение для того, чтобы подтвердить, что они продолжают работать по назначению и эффективно. Методы тестирования на проникновение должны соответствовать существующей методологии тестирования на проникновение, как указано в Требовании 11 стандарта PCI DSS. Для получения дополнительных пояснений по эффективному тестированию на проникновение следует обратиться к дополнительному документу PCI DSS *«Руководство по тестированию на проникновение»*.

Требования A3	Проверочные процедуры	Пояснение
A3.2.5 Внедрить методологию обнаружения даннных для подтверждения области применимости стандарта PCI DSS и выявления всех источников и местоположения незашифрованных PAN, как минимум, ежеквартально и после существенных изменений среды ДДК или процессов. Методология обнаружения даннных должна учитывать возможность появления незашифрованных PAN в системах и сетях, которые в настоящее время находятся за пределами определенной среды ДДК. ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS"*	**A3.2.5.a** Проверить документированную методологию обнаружения даннных на предмет того, что: • методология обнаружения даннных включает процессы выявления всех источников и местоположения незашифрованных PAN; • методология учитывает возможность появления незашифрованных PAN в системах и сетях, которые в настоящее время находятся за пределами определенной среды ДДК.	Стандарт PCI DSS требует, чтобы в рамках исследования его области применимости оцениваемые организации выявляли и документировали наличие всех незашифрованных PAN в их среде. Внедрение методологии обнаружения даннных, которая выявляет все источники и местоположения незашифрованных PAN и учитывает возможность наличия незашифрованных PAN в системах и сетях, которые в настоящее время находятся за пределами определенной среды ДДК или внутри определенной среды ДДК в неожиданных местах (например, в журнале ошибок или файле дампа памяти), позволяет обеспечить обнаружение и правильную защиту ранее неизвестных местоположений незашифрованных PAN. Процесс обнаружения данных может быть реализован с помощью различных способов, включая, среди прочего: • имеющееся в продаже ПО по обнаружению данных; • разработанную организацией программу по обнаружению данных; • ручной поиск. Независимо от используемого способа, целью является обнаружение всех источников и местоположения незашифрованных PAN (не только в определенной среде ДДК).
	A3.2.5.b Проверить результаты последних попыток обнаружения данных и опросить ответственных работников на предмет того, что поиск данных выполняется, как минимум, ежеквартально и после существенных изменений среды ДДК или процессов.	

Требования A3	Проверочные процедуры	Пояснение
A3.2.5.1 Обеспечить эффективность используемых методов обнаружения данных, напрмер, методы должны позволять обнаруживать незашифрованные PAN на системных компонентах всех видов (например, в каждой операционной системе или платформе) и в используемых форматах файлов. Эффективность методов обнаружения данных должна подтверждаться не реже раза в год. ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS"*	**A3.2.5.1.a** Опросить работников и изучить документацию на предмет того, что: • в организации реализован процесс тестирования эффективности методов, используемых для обнаружения данных; • процесс включает проверку того, что методы могут обнаруживать незашифрованные PAN на системных компонентах всех видов и в используемых форматах файлов. **A3.2.5.1.b** Проверить результаты последних тестирований эффективности на предмет того, что эффективность методов, используемых для обнаружения данных, подтверждается не реже раза в год.	Процесс тестирования эффективности методов, используемых для обнаружения данных, обеспечивает полноту и точность обнаружения ДДК. Для полноты, как минимум, выборка системных компонентов из сетей, находящихся в области применимости стандарта PCI DSS, и из сетей, находящихся за ее пределами, должна быть включена в процесс обнаружения данных. Точность может быть проверена через подтверждение того, что тестовые PAN, помещенные в выборку системных компонентов и используемые форматы файлов, выявлены с помощью метода обнаружения данных.
A3.2.5.2 Внедрить процедуры реагирования на выявление незашифрованных PAN за рамками среды ДДК, которые включают: • процедуры определения действий в случае выявления незашифрованных PAN за рамками среды ДДК, включая их поиск, безопасное удаление и (или) перенос в текущую определенную среду ДДК при необходимости; • процедуры определения того, как данных оказались за рамками среды ДДК; • процедуры устранения утечки данных или недостатков процесса, в результате которых данные	**A3.2.5.2.a** Проверить документированные процедуры реагирования на предмет того, что эти процедуры реагирования на процедуры реагирования на выявление незашифрованных PAN за рамками среды ДДК определены и включают: • процедуры, определяющие действия в случае выявления незашифрованных PAN за рамками среды ДДК, включая их поиск, безопасное удаление и (или) перенос в текущую определенную среду ДДК при необходимости; • процедуры определения того, как данных оказались за рамками среды ДДК; • процедуры устранения утечки данных или недостатков процесса, в результате которых данные оказываются за рамками среды ДДК; • процедуры отпределения источников данных; • процедуры определения, хранятся ли данные треков вместе с PAN.	Наличие документированных процедур реагирования на событие обнаружения незашифрованного PAN за рамками среды ДДК позволяет определить необходимые действия по устранению уязвимостей и предотвратить утечки в будущем. Например, если PAN был найден за рамками среды ДДК, следует выполнить анализ, чтобы: • определить, был ли он сохранен независимо от других данных (или это часть полных данных трека); • определить источник данных; • определить недостатки контроля, в результате которых данные оказались за рамками среды ДДК.

Требования A3	Проверочные процедуры	Пояснение
оказываются за рамками среды ДДК; • процедуры отпределения источников данных; • процедуры определения, хранятся ли данные треков вместе с PAN.	**A3.2.5.2.b** Опросить персонал и проверить записи о реагировании на предмет того, что устранение уязвимостей выполняется, когда незашифрованный PAN выявляется за рамками среды ДДК.	
A3.2.6 Внедрить механизмы выявления и предотвращения утечки незашифрованного PAN за рамки среды ДДК через неавторизованный канал, метод или процесс, включая генерацию журналов аудита и уведомлений. ***Связанные требования стандарта PCI DSS:*** *раздел "Область применимости требований стандарта PCI DSS"*	**A3.2.6.a** Проверить документацию и изучить внедренные механизмы на предмет того, что механизмы: • внедрены и работают; • сконфигурированы так, чтобы выявлять и продотвращать утечку незашифрованного PAN за рамки среды ДДК через неавторизованный канал, метод или процесс; • генерируют журналы и уведомления при обнаружении утечки незашифрованного PAN за рамки среды ДДК через неавторизованный канал, метод или процесс. **A3.2.6.b** Проверить журналы аудита и уведомления и опросить ответственных работников на предмет того, что уведомления изучаются.	Механизмы выявления и предотвращения неавторизированной утечки незашифрованного PAN могут включать подходящие инструменты, такие как технологии предотвращения утечки информации (DLP), и ручные процессы и процедуры. Механизмы должны охватывать, среди прочего, электронную почту, загрузки со съемных носителей и документы, выводимые на печать. Использование данных механизмов позволяет организации выявлять и предотвращать ситуации, которые могут привести к утечке данных.
A3.2.6.1 Внедрить процедуры реагирования на обнаружение попыток переноса незашифрованного PAN из среды ДДК через неавторизованный канал, метод или процесс. Процедуры реагирования должны включать: • процедуры своевременного изучания уведомлений ответственными работниками; • процедуры устранения утечек данных или недостатков процессов при необходимости, чтобы предотвратить утечку данных.	**A3.2.6.1.a** Проверить документированные процедуры реагирования на предмет того, что процедуры реагирования на попытки переноса незашифрованного PAN из среды ДДК через неавторизованный канал, метод или процесс включают: • процедуры своевременного изучения уведомлений ответственными работниками; • процедуры устранения утечек данных или недостатков процессов при необходимости, чтобы предотвратить утечку данных. **A3.2.6.1.b** Опросить работников и изучить записи действий, выполняемых при обнаружении переноса незашифрованного PAN из среды ДДК через неавторизованный канал, метод или процесс, и проверить, что исправление выполняется.	Попытки переноса незашифрованного PAN из среды ДДК через неавторизованный канал, метод или процесс могут свидетельствовать о намерении злоумышленника украсть данные или действиях неавторизированног работника, который не осведомлен о правильных методах или просто не выполняет их. Своевременное изучение этих событий может выявить, где необходимо устранение уязвимостей, и предоставить важную информацию для понимания того, откуда могут появиться угрозы.

Требования A3	Проверочные процедуры	Пояснение
A3.3 Проверить, встроены ли требования PCI DSS в привычные бизнес-процессы.		
A3.3.1 Внедрить процесс немедленного обнаружения и оповещения об ошибках в критичных защитных мерах. Примеры критичных защитных мер включают, среди прочего: • межсетевые экраны; • системы обнаружения и (или) предотвращения вторжений; • системы мониторинга целостности файлов; • антивирусное ПО; • физические механизмы контроля доступа; • логические механизмы контроля доступа; • механизмы ведения журналов регистрации событий; • средства сегментации (если они используются). ***Связанные требования стандарта PCI DSS:*** *Требования 1-12*	**A3.3.1.a** Проверить документированные политики и процедуры на предмет того, что определены процедуры немедленного обнаружения и оповещения об ошибках в критичных защитных мерах. **A3.3.1.b** Проверить процессы обнаружения и оповещения и опросить работников на предмет того, что процессы для всех критичных защитных мер внедрены, и в случае ошибки в критичной защитной мере происходит генерация оповещения.	При отсутствии формализованных процессов быстрого (в максимально короткий срок) обнаружения и оповещения об ошибках в критичных защитных мерах, ошибки могут остаться невыявленными в течение длительного времени, и злоумышленники получат достаточно времени для компрометации систем и хищения критичных данных из среды ДДК.

Требования A3	Проверочные процедуры	Пояснение
A3.3.1.1 Своевременно реагировать на ошибки в любых критичных защитных мерах. Процессы реагирования на ошибки в защитных мерах должны включать: • восстановление функций обеспечения безопасности; • определение и документирование продолжительности (дата и время начала и окончания) ошибки в обеспечении безопасности; • определение и документирование причины (причин) ошибки, включая изначальную причину, и документирование мер, необходимых для исправления изначальной причины; • определение и решение любых проблем безопасности, которые возникают во время ошибки; • выполнение оценки риска, чтобы определить необходимость дальнейших действий при ошибке в обеспечении безопасности; • реализация мер для предотвращения причины ошибки и недопущения ее повторения; • возобновление мониторинга защитных мер. ***Связанные требования стандарта PCI DSS:*** *Требования 1-12*	**A3.3.1.1.a** Проверить документированные политики и процедуры и опросить работников на предмет того, что процессы определены и внедрены для реагирования на ошибки в защитных мерах, и включают: • восстановление функций обеспечения безопасности; • определение и документирование продолжительности (дата и время начала и окончания) ошибки в обеспечении безопасности; • определение и документирование причины (причин) ошибки, включая изначальную причину, и документирование мер, необходимых для исправления изначальной причины; • определение и решение любых проблем безопасности, которые возникают во время ошибки; • выполнение оценки риска, чтобы определить необходимость дальнейших действий при ошибке в обеспечении безопасности; • реализация мер для предотвращения причины ошибки и недопущения ее повторения; • возобновление мониторинга защитных мер. **A3.3.1.1.b** Проверить записи на предмет того, что ошибки в защитных мерах задокументированы и включают: • определение причины (причин) ошибки, включая изначальную причину; • продолжительность (дата и время начала и окончания) ошибки в обеспечении безопасности; • меры, необходимые для исправления изначальной причины.	Документированные свидетельства (например, записи в системе управления) должны поддерживать действующими процессы и процедуры реагирования на ошибки в обеспечении безопасности. Кроме того, работники должны знать свои обязанности в случае возникновения ошибки. Ответные действия на ошибки должны быть зафиксированны в виде документированных свидетельств.
A3.3.2 Проверять аппаратные и программные технологии не реже раза в год, чтобы убедиться в том, что они продолжают соответствовать требованиям стандарта PCI DSS в организации. (Например, проверка	**A3.3.2.a** Проверить документированные политики и процедуры и опросить работников на предмет того, что процессы пересмотра аппаратных и программных технологий для проверки того, что они продолжают соответствовать требованиям PCI DSS в организации, определены и внедрены.	Технологии аппаратного и программного ПО постоянно изменяются, и организации должны знать об изменениях в технологиях, которые они используют, также как и угрозы для этих технологий. Организациям также необходимо знать об изменениях, сделанных вендорами в

Требования A3	Проверочные процедуры	Пояснение
технологий, которые уже не поддерживаются разработчиком и (или) не соответствуют требованиям безопасности в организации). Процесс включает план исправления технологий, которые уже не соответствуют требованиям стандарта PCI DSS в организации, вплоть до замены технологии в случае необходимости. ***Связанные требования стандарта PCI DSS:*** *Требования 2, 6*	**A3.3.2.b** Проверить результаты последних проверок на предмет того, что они выполняются не реже раза в год. **A3.3.2.c** Для всех технологий, которые были определены как несоответствующие требованиям стандарта PCI DSS в организации, проверить наличие действующего плана исправления технологии.	этих технологиях или процессах поддержки, чтобы понимать, как эти изменения могут повлиять на использование технологии организацией. Регулярные проверки технологий, которые влияют на защитные меры стандарта PCI DSS, могут быть полезны в стратегиях закупок, использования и внедрения и обеспечивают сохранение эффективности защитных мер, основанных на этих технологиях.
A3.3.3 Выполнять проверки, как минимум, ежевкартально на предмет того, что привычные бизнес-процессы соблюдаются. Проверки должны выполняться работником, на которого возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS (как указано в A3.1.3), и включать следующее: • подтверждение того, что все привычные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1) выполняются; • подтверждение того, что работники соблюдают политики безопасности и операционные процедуры (например, ежедневные проверки журналов, проверки набора правил межсетевых экранов, стандарты конфигурации для новых систем и т.д.); • документирование того, как проводились проверки, включая как проверялось, что все	**A3.3.3.a** Проверить политики и процедуры на предмет того, что процессы обзора и проверки привычных бизнес-процессов определены. Проверить, что процедуры включают: • подтверждение того, что все привычные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1) выполняются; • подтверждение того, что работники соблюдают политики безопасности и операционные процедуры (например, ежедневные проверки журналов, проверки набора правил межсетевых экранов, стандарты конфигурации для новых систем и т.д.); • документирование того, как проводились проверки, включая как проверялось, что все привычные бизнес-процессы реализованы; • сбор документированных свидетельств, как требуется для ежегодной оценки соответствия требованиям стандарта PCI DSS; • проверква и утверждение результатов работником, на которого возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS (как указано в A3.1.3); • хранение записей и документации, охватывающих все привычные бизнес-процессы, как минимум, 12 месяцев.	Внедрение мер стандарта PCI DSS в привычные бизнес-процессы является эффективным способом гарантировать, что безопасность составляет часть обычных рабочих операций на постоянной основе. Поэтому важно выполнять независимые проверки, чтобы обеспечить функционирование мер привычных бизнес-процессов надлежащим образом. Целью этих независимых проверок является изучение свидетельства, которое подтверждает выполнение привычных бизнес-процессов. Эти проверки также могут быть использваны для подтверждения того, что необходимое свидетельство сохраняется (например, журналы аудита, отчеты о сканировании на наличие уязвимостей, проверки межсетевых экранов и т.д.), чтобы помочь организации в подготовке к следующей оценке соответствия требованиям стандарта PCI DSS.

Требования A3	Проверочные процедуры	Пояснение
привычные бизнес-процессы реализованы; • сбор документированных свидетельств, как требуется для ежегодной оценки соответствия требованиям стандарта PCI DSS; • проверква и утверждение результатов работником, на которого возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS (как указано в A3.1.3); • хранение записей и документации, охватывающих все привычные бизнес-процессы, как минимум, 12 месяцев. ***Связанные требования стандарта PCI DSS:*** *Требования 1-12*	**A3.3.3.b** Опросить ответственных работников и проверить записи проверок на предмет того, что: • проверки выполняются работником, на которого возложены обязанности по обеспечению соответствия требованиям стандарта PCI DSS; • проверки выполняются, как минимум, ежеквартально.	
A3.4 Контролировать и управлять логическим доступом к среде ДДК		
A3.4.1 Проверять учетные записи и права доступа к системным компонентам, находящимся внутри области применимости стандарта PCI DSS, как минимум, каждые шесть месяцев, чтобы убедиться, что учетные записи и доступы продолжают соответствовать должностным обязанностям и авторизованы. ***Связанные требования стандарта PCI DSS:*** *Требование 7*	**A3.4.1** Опросить ответственных работников и проверить сопроводительную документацию на предмет того, что: • учетные записи и права доступа проверяются, как минимум, каждые шесть месяцев; • проверки подтверждают, что доступ соответствует должностным обязанностям, и все доступы авторизованы.	Требования к доступу изменяются с течением времени, так как у работников сменяются роли, или они увольняются. Органам управления необходимо регулярно изучать, перепроверять и актуализировать доступы пользователей в соответствии с необходимостью, чтобы обеспечивать соответствие изменениям в составе работников, включая третьи стороны, и должностные обязанности пользователей.

Требования A3	Проверочные процедуры	Пояснение
A3.5 Выявлять и реагировать на подозрительные события		
A3.5.1 Внедрить методологию своевременного выявления признаков атак и нежелательного поведения в отношении систем (например, использование согласованных ручных проверок и (или) централизованно управляемых или автоматических инструментов сопоставления журналов), включающую, как минимум, следующее: • выявление аномалий или подозрительной активности, если они происходят; • генерация своевременных уведомлений при обнаружении подозрительной активности или аномалии для ответственных работников; • реагирование на уведомления в соответствии с документированными процедурами реагирования. ***Связанные требования стандарта PCI DSS:*** *Требования 10, 12*	**A3.5.1.a** Изучить документацию и опросить работников на предмет того, что методология определена и внедрена для своевременного выявления признаков атак и нежелательного поведения в отношении систем, и включает следующее: • выявление аномалий или подозрительной активности, если они происходят; • генерация своевременных уведомлений при обнаружении подозрительной активности или аномалии для ответственных работников; • реагирование на уведомления в соответствии с документированными процедурами реагирования. **A3.5.1.b** Проверить процедуры реагирования на происшествия и опросить ответственных работников на предмет того, что: • дежурные работники получают уведомления своевременно; • реагирование на уведомления происходит в соответствии в документированными процедурами реагирования.	Способность выявления признаков атак и нежелательного поведения внутри систем имеет важнейшее значение для предотвращения, выявления или уменьшения влияния от компрометации данных. Наличие журналов в среде позволяет тщательно отслеживать, оповещать и анализаровать, если что-то пойдет неправильно. Определить причину компрометации очень сложно, если не невозможно, без процесса подкрепления информации из критичных системных компонентов информацией из систем, которые выполняют защитные функции, таких как межсетевые экраны, системы обнаружения или предотвращения вторжений и системы мониторинга целостности файлов. Поэтому журналы для всех критичных системных компонентов и систем должны вестись, сопоставляться и сохранятся. В этом случае возможно использование ПО и служебных методологий для обеспечения анализа, оповещения и отчетности в реальном времени, таких как SIEM (управление информационной безопасностью и событиями безопасности), мониторинг целостности файлов (FIM) или выявление изменений.

Приложение B. Компенсационные меры

Компенсационные меры могут использоваться для большинства требований PCI DSS, если организация не может выполнить то или иное требование явно, согласно его формулировке, в силу обоснованных технических или документированных служебных ограничений, но достаточно снизила риск, который связан с данным требованием, путем реализации иных, компенсационных мер.

Компенсационные меры должны удовлетворять следующим требованиям:

1. отвечать цели и строгости исходного требования PCI DSS;
2. обеспечивать защиту и снижать риск так же, как это делает исходное требование PCI DSS. (см. *«PCI DSS: Понимание назначения требований»* (Navigating PCI DSS), чтобы определить цель каждого требования PCI DSS);
3. обеспечивать дополнительный уровень защиты по сравнению с другими требованиями PCI DSS (защитная мера, которая просто соответствует другим требованиям PCI DSS, не является компенсационной).

   Анализируя дополнительный уровень защиты компенсационной меры, учитывать следующее:

Примечание: *пункты a – c, приведенные ниже, являются лишь примерами. Все компенсационные меры должны быть проверены, а их достаточность – подтверждена аудитором, который проводит проверку на соответствие PCI DSS. Действие компенсационной меры зависит от среды, в которой она внедрена, контекста защитных мер и конфигурации компенсационной меры. Следует помнить, что одна и та же компенсационная мера не может работать одинаково хорошо во всех 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 защиты паролей уже являются требованиями PCI DSS для объекта проверки (паролей).

b) Существующие требования PCI DSS МОЖНО рассматривать как компенсационные меры, если они применимы в другой области, но не для объекта проверки. Например, мультифакторная аутентификация является требованием PCI DSS для удаленного доступа. Использование мультифакторной аутентификации *во внутренней сети может рассматриваться как компенсационная мера для неконсольного административного доступа, если невозможно обеспечить передачу зашифрованных паролей. Мультифакторная аутентификация может быть приемлемой компенсационной мерой, если она: 1) соответствует цели изначального требования, снижая риск перехвата незашифрованных административных паролей, и; 2) 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 привести ДДК к нечитаемому виду в соответствии с требованием 3.4 (например, путем шифрования), компенсационная мера может включать устройство или набор устройств, приложений и защитных мер, обеспечивающих все перечисленные ниже условия: 1) сегментацию внутренней сети; 2) фильтрацию по IP- или MAC-адресам; 3) мультифакторную аутентификации во внутренней сети.

4. адекватно учитывать дополнительный риск, который вызван несоблюдением требования PCI DSS.

Аудитор должен тщательно оценивать компенсационные меры каждый раз, когда он выполняет ежегодную оценку соответствия организации требованиям PCI DSS. Во время 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

Использовать эту таблицу для описания компенсационных мер по любым требованиям, выполненным с использованием компенсационных мер. Важно! Документировать компенсационные меры также 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	Перечислить ограничения, препятствующие выполнению исходного требования стандарта.	
2. Цель	Определить цель исходного требования; указать цель, которая достигнута с помощью компенсационной меры.	
3. Выявленный риск	Описать любой дополнительный риск от невыполнения исходного требования.	
4. Определение компенсационных мер	Описать компенсационные меры и объяснить, как с их помощью достигаются цели исходного требования и снижается дополнительный риск (при его наличии).	
5. Проверка компенсационных мер	Описать, каким образом были проверены и протестированы компенсационные меры.	
6. Поддержка	Определить процесс и защитные меры, которые поддерживают компенсационные меры.	

Компенсационные меры – Форма для заполнения. Пример заполнения

Использовать эту таблицу, чтобы описать компенсационные меры по любым требованиям, у которых указан статус «Выполнено» с использованием компенсационных мер».

Номер требования: *8.1.1. – Все ли пользователи идентифицированы с использованием уникальной учетной записи до получения доступа к системным компонентам или ДДК?*

	Требуемая информация	Объяснение
1. Ограничения	Перечислить ограничения, препятствующие выполнению исходного требования стандарта.	*Компания XYZ использует изолированные Unix-серверы без LDAP, таким образом, на каждом из них требуется учетная запись суперпользователя (root). Компания XYZ не может управлять входом под учетной записью root и записывать все ее действия по каждому пользователю.*
2. Цель	Определить цель исходного требования; указать цель, которая достигнута с помощью компенсационной меры.	*Учетные записи делают уникальными для двух целей. 1. С точки зрения безопасности недопустимо использовать общие учетные данные. 2. Если используются общие учетные записи, нельзя точно установить, кто отвечает за то или иное действие.*
3. Выявленный риск	Описать любой дополнительный риск от невыполнения исходного требования.	*Появляется дополнительный риск для системы контроля доступа, так как нет гарантии, что можно отследить всех пользователей без уникальных учетных записей.*
4. Определение компенсационных мер	Описать компенсационные меры и объяснить, как с их помощью достигаются цели исходного требования и снижается дополнительный риск (при его наличии).	*Компания XYZ требует, чтобы все пользователи получали доступ к серверам с помощью своих обычных учетных записей, и затем использовали команду «sudo», чтобы запустить какие-либо административные команды. Это позволяет использовать привилегии учетной записи с правами суперпользователя («root»), чтобы запускать заранее установленные команды, которые записываются утилитой «sudo» в журнал безопасности. Таким образом, действия каждого пользователя можно отслеживать через индивидуальную учетную запись, не разглашая пароль учетной записи с правами суперпользователя («root»).*

5. Проверка компенсационных мер	Описать, каким образом были проверены и протестированы компенсационные меры.	*Компания XYZ показала аудитору, что команда «sudo» сконфигурирована правильно с помощью файла «sudoers», так что только заранее установленные команды могут запускаться определенными пользователями, и все действия, выполняемые этими работниками с помощью «sudo», записываются в журналы, чтобы определить пользователя, который выполняет действия с правами суперпользователя ("root").*
6. Поддержка	Определить процесс и защитные меры, которые поддерживают компенсационные меры.	*У компании XYZ есть документированные процессы и процедуры, которые проверяют, что конфигурации для sudo не заменены, не модифицированы или не удалены таким образом, что пользователи смогут выполнять команды с правами суперпользователя без идентификации, отслеживания и регистрации.*

Приложение D. Сегментация и выборка подразделений организации и системных компонентов