Стандарт Безопасности Данных
Индустрии Платежных Карт

Требования и Процедуры Аудита Безопасности

Версия 3.2.1

Май 2018 г.

Об этом документе

Настоящий документ («Официальный перевод на русский язык») является официальным переводом на русский язык документа, описанного как PCI DSS (Стандарт безопасности данных индустрии платёжных карт), который доступен по адресу https://www.pcisecuritystandards.org/document_library, © 2006-2020 Совет PCI SSC («Совет»). Официальный перевод на русский язык предоставляется с разрешения и при поддержке АО «НСПК» («Компания»), как информационная услуга, в рамках соглашения между Советом и Компанией. Настоящий перевод не предоставляет никаких прав на реализацию спецификаций, описанных в настоящем документе; обеспечением таких прав может быть только согласие соблюдать условия лицензионного соглашения, доступного по адресу https://www.pcisecuritystandards.org/document_library. Текст настоящего документа на английском языке доступен по адресу https://www.pcisecuritystandards.org/document_library; он при любых обстоятельствах рассматривается как окончательный вариант настоящего документа. В случае возникновения любых разночтений или несоответствий между данной версией и текстом настоящего документа на английском языке, преимущественную силу имеет текст на английском языке, и, соответствующим образом, данная версия не должна приниматься к сведению. Ни Совет, ни Компания не несут ответственности за любые ошибки или двусмысленность толкований, содержащихся в настоящем документе.

About this document

This document (the “Official Russian Translation") is the official Russian language translation of the document described as PCI DSS, available at https://www.pcisecuritystandards.org/document_library, © 2006-2020 PCI Security Standards Council, LLC (the “Council”). This Official Russian Translation is provided with the approval and support of NSPK JSC (“the Company”), as an informational service only, under agreement between the Council and the Company. No rights to implement the specification(s) described in this document are granted in connection with this translation; such rights may only be secured by agreeing to the terms of the license agreement available at https://www.pcisecuritystandards.org/document_library. The English text version of this document is available at https://www.pcisecuritystandards.org/document_library and shall for all purposes be regarded as the definitive version of this document. To the extent of any ambiguities or inconsistencies between this version and such English text version of this document, the English text version shall control, and accordingly, this version shall not be relied upon for any purpose whatsoever. Neither the Council nor the Company assume any responsibility for any errors or ambiguities contained herein.

Изменения документа

Дата	Версия	Описание	Страница
Октябрь 2008 г.	1.2	В документе «Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности» версии 1.2 содержатся общие и конкретные изменения, отличающие этот документ от его предыдущей версии 1.1 под названием «Стандарт безопасности данных индустрии платежных карт (PCI DSS). Процедуры аудита безопасности». Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 1.1 to 1.2».	
Июль 2009 г.	1.2.1	Добавлено предложение, которое было по ошибке удалено в версиях 1.1 и 1.2 Стандарта PCI DSS.	5
		Исправлена опечатка («then» заменено на «than») в описании процедур тестирования 6.3.7.a и 6.3.7.b.	32
		Удалено выделение серым цветом для столбцов «Выполнено» и «Не выполнено» в описании процедур тестирования 6.5.b.	33
		В заполненной для примера форме «Компенсационные Меры - Форма для заполнения» исправлено предложение в верхней части страницы. Формулировка изменена на: «Используйте эту форму для описания компенсационных мер, принятых в отношении требований, напротив которых поставлен статус «Выполнено» благодаря использованию компенсационных мер».	64
Октябрь 2010 г.	2.0	Внесены изменения в версию 1.2.1. Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 1.2.1 to 2.0».	
Ноябрь 2013 г.	3.0	Внесены изменения в версию 2.0. Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 2.0 to 3.0».	
Апрель 2015 г.	3.1	Внесены изменения в версию 3.0. Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 3.0 to 3.1».	
Апрель 2016 г.	3.2	Внесены изменения в версию 3.1. Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 3.1 to 3.2».	
Май 2018 г.	3.2.1	Внесены изменения в версию 3.2. Изменения Стандарта PCI DSS детально представлены в документе «PCI DSS Summary of Changes from PCI DSS Version 3.2 to 3.2.1».	

Содержание

Введение и обзор Стандарта PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан в целях повышения уровня безопасности данных держателей платежных карт и содействия процессу повсеместного внедрения единообразных мер по защите данных держателей карт. Стандарт PCI DSS содержит основные технические и операционные требования, разработанные для защиты данных держателей карт. Данный Стандарт применяется ко ***всем*** организациям, задействованным в сфере обработки платежных карт: торгово-сервисным предприятиям, процессинговым центрам, эквайерам, эмитентам и сервис-провайдерам. Стандарт PCI DSS также применим ко всем другим организациям, которые хранят, обрабатывают или передают данные держателей карт (ДДК) и/или критичные аутентификационные данные (КАД). Ниже представлен общий обзор 12 требований Стандарта PCI DSS.

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

Создание и поддержка защищенной сети и систем	**1.** Установить и поддерживать конфигурацию межсетевых экранов для защиты данных держателей карт **2.** Не использовать пароли и другие системные параметры безопасности, заданные производителем по умолчанию
Защита данных держателей карт	**3.** Защищать хранимые данные держателей карт **4.** Шифровать данные держателей карт при их передаче в открытых общедоступных сетях
Ведение программы по управлению уязвимостями	**5.** Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО или программы **6.** Разрабатывать и поддерживать безопасные системы и приложения
Внедрение строгих мер контроля доступа	**7.** Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью **8.** Определять и подтверждать доступ к системным компонентам **9.** Ограничить физический доступ к данным держателей карт
Регулярный мониторинг и тестирование сети	**10.** Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт **11.** Регулярно выполнять тестирование систем и процессов обеспечения безопасности
Поддержание политики информационной безопасности	**12.** Разработать и поддерживать политику обеспечения информационной безопасности для всех сотрудников организации

Настоящий документ «Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности» устанавливает 12 требований и соответствующих им процедур оценки соответствия данному Стандарту, являющихся единым инструментом оценки безопасности. Этот документ предназначен для использования в ходе оценки соответствия Стандарту

PCI DSS как части процедуры проверки организации на соответствие. В разделах ниже представлены подробные инструкции и лучшие практики, использование которых позволит организациям подготовиться к оценке на соответствие требованиям Стандарта PCI DSS, выполнить такую оценку и отчитаться о ее результатах. Требования Стандарта PCI DSS и Проверочные процедуры описываются, начиная со стр. 15.

Стандарт PCI DSS содержит минимальный набор требований по защите данных держателей карт. Стандарт может быть дополнен мерами и методами дальнейшей минимизации рисков, а также требованиями местного, регионального и отраслевого законодательства. Кроме того, законодательством или нормативно-правовыми актами могут быть предусмотрены особые требования по защите персональных данных, или иных элементов данных (например, имени держателя карты). Стандарт PCI DSS не заменяет собой местные или региональные законы, постановления правительства или иные требования законодательства.

Источники информации

На сайте Совета PCI SSC (PCI Security Standards Council) (www.pcisecuritystandards.org) размещен ряд дополнительных источников информации, которые организации могут использовать при проведении оценки и подтверждении своего соответствия Стандарту PCI DSS. К таким источникам относятся:

- Библиотека документов, содержащая:
  - *Документ «PCI DSS Summary of Changes from PCI DSS Version 2.0 to 3.0» (обзор изменений в Стандарте PCI DSS в версии 3.0 по сравнению с версией 2.0).*
  - *Документ «PCI DSS Quick Reference Guide» (Краткий справочник по Стандарту PCI DSS)*
  - *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms (Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS)*
  - *Дополнения к Стандарту и Руководства*
  - *Документ «Prioritized Approach for PCI DSS» (Концепция приоритетного подхода к достижению соответствия Стандарту PCI DSS)*
  - *Шаблон Отчета о соответствии (ROC) и инструкции по его заполнению*
  - *Листы Самооценки (SAQs) и Инструкции и Руководства по Листам Самооценки (SAQs)*
  - *Аттестаты Соответствия (AOCs)*
- Часто задаваемые вопросы (FAQs)
- Веб-сайт «PCI for Small Merchants»
- Обучающие курсы и информационные вебинары PCI
- Список сертифицированных аудиторов безопасности (QSA) и авторизованных поставщиков услуг сканирования (ASV)
- Список устройств, одобренных согласно PCI PTS, и платежных приложений, прошедших проверку на соответствие стандарту PA-DSS

***Примечание**: «Дополнения к Стандарту» являются сопроводительными документами по отношению к Стандарту PCI DSS, содержащими дополнительные рекомендации по соответствию требованиям Стандарта PCI DSS. Эти рекомендации не заменяют, не исключают и не расширяют ни сам Стандарт PCI DSS, ни какое-либо из его требований.*

Информация об этих и иных источниках информации доступна на сайте *www.pcisecuritystandards.org*.

Сфера применения Стандарта PCI DSS

Стандарт PCI DSS применяется ко ***всем*** организациям, задействованным в сфере обработки платежных карт: торгово-сервисным предприятиям, процессинговым центрам, эквайрерам, эмитентам и сервис-провайдерам. Стандарт PCI DSS также применим ко ***всем*** другим организациям, которые хранят, обрабатывают или передают данные держателей карт и/или критичные аутентификационные данные.

Под данными держателей карт и критичными аутентификационными данными понимается следующее:

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

Основной номер держателя банковской карты является определяющим фактором для данных держателя карты. Если имя держателя карты, сервисный код и/или срок действия хранятся, обрабатываются или передаются вместе с основным номером держателя карты (PAN) или иным образом присутствуют в среде данных держателей карт (CDE), то они должны быть защищены в соответствии с применимыми требованиями Стандарта PCI DSS.

Требования Стандарта PCI DSS применимы к организациям, которые хранят, обрабатывают или передают данные держателей карт и/или критичные аутентификационные данные. Некоторые требования Стандарта PCI DSS также могут быть применены к организациям, которые передали платежные транзакции или управление средой данных держателей карт сторонним организациям[1]. Кроме того, организации, передавшие платежные транзакции или управление средой данных держателей карт сторонним организациям, обязаны обеспечить защиту данных платежных карт такими сторонними организациями в соответствии с применимыми требованиями Стандарта PCI DSS.

Таблица на следующей странице иллюстрирует наиболее часто используемые элементы данных держателей карт и критичных аутентификационных данных, в частности, разрешено или запрещено хранение таких элементов и должен ли быть защищен каждый из таких элементов. Данная таблица не является исчерпывающей. В ней представлены различные типы требований, применимых к каждому элементу данных.

[1] В соответствии с отдельными программами комплаенса платежных систем

		Элемент данных	Хранение разрешено	Приведены ли хранимые данные в нечитаемый вид согласно Требованию 3.4
Данные о платежной карте	**Данные держателя карты**	Основной номер держателя банковской карты (PAN)	Да	Да
		Имя держателя карты	Да	Нет
		Сервисный код	Да	Нет
		Дата истечения срока действия карты	Да	Нет
	Критичные аутентифи-кационные данные[2]	Полные данные дорожки[3]	Нет	Хранение запрещено согласно Требованию 3.2
		CAV2/CVC2/CVV2/CID[4]	Нет	Хранение запрещено согласно Требованию 3.2
		ПИН/ПИН-блок[5]	Нет	Хранение запрещено согласно Требованию 3.2

Требования 3.3 и 3.4 Стандарта PCI DSS применяются исключительно к основному номеру держателя карты (PAN). Если основной номер держателя карты (PAN) хранится вместе с другими элементами данных держателей карт, то согласно Требованию 3.4 Стандарта PCI DSS только PAN должен быть приведен в нечитаемый вид.

Хранить критичные аутентификационные данные после авторизации не разрешается, даже в зашифрованном виде. Данное требование действует, даже если основного номера держателя карты (PAN) нет в среде. Организации должны узнавать у своих эквайреров или конкретных платежных систем напрямую, разрешено ли хранить критичные аутентификационные данные до авторизации, в течение какого времени, а также существуют ли иные требования к использованию и защите таких данных.

---

2 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде).

3 Полные данные дорожки магнитной полосы, аналогичные данные на чипе или ином носителе.

4 Трех- или четырехзначное проверочное значение, напечатанное на лицевой или обратной стороне платежной карты.

5 Персональный идентификационный код, вводимый держателем карты в ходе транзакций с предъявлением карты, и/или зашифрованный ПИН-блок, представленный в транзакционном сообщении.

Взаимосвязь между Стандартами PCI DSS и PA-DSS

Применимость Стандарта PCI DSS к приложениям, соответствующим Стандарту PA-DSS

Факт использования приложения, соответствующего Стандарту безопасности данных платежных приложений (PA-DSS), не значит, что организация становится соответствующей требованиям Стандарта PCI DSS, поскольку такое приложение должно быть внедрено в среду, соответствующую стандарту PCI DSS, и быть настроено согласно руководству «PA-DSS Implementation Guide», предоставляемого разработчиком платежного приложения.

Все приложения, хранящие, обрабатывающие или передающие данные держателей карт, включая приложения, прошедшие проверку на соответствие Стандарту PA-DSS, входят в область оценки организации на соответствие Стандарту PCI DSS. Оценка соответствия Стандарту PCI DSS призвана подтвердить, что платежное приложение, соответствующее Стандарту PA-DSS, надлежащим образом настроено и безопасно внедрено в соответствии с требованиями Стандарта PCI DSS. Если приложение было модифицировано под требования заказчика, то в ходе оценки соответствия Стандарту PCI DSS потребуется более детально изучить такое приложение, поскольку оно может уже не являться вариацией версии, проверенной на соответствие Стандарту PA-DSS.

Требования Стандарта PA-DSS основаны на Требованиях «Стандарта PCI DSS и процедурах оценки безопасности» (определенных в этом документе). В Стандарте PA-DSS детально описаны требования, которым должно соответствовать платежное приложение, чтобы упростить организации достижение соответствия требованиям Стандарта PCI DSS. Поскольку угрозы безопасности постоянно трансформируются, приложения, которые разработчик перестает поддерживать (например, приложению присваивается статус «end of life», т.е. выпуск новых версий ПО прекращается), могут не гарантировать такой же уровень безопасности, как у поддерживаемых приложений.

Будучи внедренными в среду, отвечающую требованиям Стандарта PCI DSS, безопасные платежные приложения позволят минимизировать вероятность нарушений безопасности, которые могут привести к компрометации основного номера держателя карты (PAN), полных данных дорожки, проверочных кодов карты и проверочных значений (CAV2, CID, CVC2, CVV2), ПИН-кодов и ПИН-блоков, а также мошеннических действий, возникающих в результате таких нарушений безопасности.

Чтобы определить, применяется ли Стандарт PA-DSS к данному платежному приложению, ознакомьтесь с документом «Руководство по программе PA-DSS» («PA-DSS Program Guide»), доступному на сайте www.pcisecuritystandards.org.

Применимость Стандарта PCI DSS к производителям платежных приложений

Стандарт PCI DSS может применяться в отношении производителей платежных приложений, если такие производители хранят, обрабатывают или передают данные держателей карт, или имеют доступ к данным держателей карт своих клиентов (например, в качестве сервис-провайдеров).

Область действия требований Стандарта PCI DSS

Требования безопасности Стандарта PCI DSS применяются ко всем системным компонентам, имеющим отношение или так или иначе связанным со средой данных держателей карт. Среда данных держателей карт включает в себя людей, процессы и технологии, которые хранят, обрабатывают или передают данные держателей карт или критичные аутентификационные данные. К «системным компонентам» относятся сетевые устройства, серверы, вычислительные устройства и приложения. К примерам системных компонентов относятся, в частности:

- Системы, обеспечивающие безопасность (например, серверы аутентификации), способствующие сегментации (например, внутренние межсетевые экраны) или влияющие на безопасность среды данных держателей карт (например, серверы преобразования имен или веб-серверы переадресации).
- Компоненты виртуализации, такие как виртуальные машины, виртуальные коммутаторы и маршрутизаторы, виртуальные устройства, виртуальные приложения/рабочие столы и гипервизоры.
- Сетевые компоненты, в том числе, межсетевые экраны, коммутаторы, маршрутизаторы, беспроводные точки доступа, устройства сетевой безопасности и иные устройства безопасности.
- Типы серверов включая, помимо прочего, веб-серверы, серверы приложений, серверы баз данных, серверы аутентификации, почтовые серверы, прокси-серверы, серверы NTP (Network Time Protocol - протокол сетевого времени) и серверы DNS (Domain Name System - системы доменных имен).
- Приложения, включая все приобретенные или заказные приложения, в том числе внутренние и внешние (например, Интернет-приложения).
- Любой иной компонент или устройство, расположенное в среде данных держателей карт или подключенное к ней.

На первом этапе оценки соответствия требованиям Стандарта PCI DSS необходимо точно определить область аудита. Минимум раз в год и перед каждой ежегодной оценкой соответствия оцениваемая организация должна проверять корректность области действия Стандарта PCI DSS путем указания всех мест хранения и потоков данных держателей карт, а также указывать все системы, к которым подключена среда данных держателей карт, или которые могут повлиять на безопасность среды данных держателей карт в случае своей компрометации (например, серверы аутентификации), чтобы убедиться, что они входят в область оценки на соответствие Стандарту PCI DSS. Системы всех типов и места хранения, включая резервные площадки/площадки восстановления и отказоустойчивые системы, должны рассматриваться как часть процесса определения области аудита.

Для того чтобы проверить корректность определенной среды данных держателей карт, необходимо выполнить следующее:

- Оцениваемая организация выявляет и регистрирует присутствие всех данных держателей карт в своей среде, чтобы убедиться в том, что данные держателей карт отсутствуют вне установленной на текущий момент среды данных держателей карт.
- Как только организация установит и зарегистрирует места нахождения данных держателей карт, организация использует эту информацию, чтобы убедиться в том, что область действия Стандарта PCI DSS определена корректно (например, результаты могут быть представлены в виде схемы или списка мест расположения данных держателей карт).

- Организация признает, что любые обнаруженные данные держателей карт подлежат включению в область оценки на соответствие Стандарту PCI DSS и в среду данных держателей карт. Если организация обнаружит данные, которые не включены в среду данных держателей карт, такие данные должны быть безопасно удалены, перемещены в установленную на данный момент среду данных держателей карт или среда данных держателей карт должна быть переопределена так, чтобы она включала эти данные.

Организация хранит документы, описывающие, как область применения Стандарта PCI DSS была определена. Документы сохраняются для их проверки аудитором и (или) для использования в качестве справочного материала при определении области применения Стандарта PCI DSS в будущем году.

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

Сегментация сети

Сетевая сегментация среды данных держателей карт или отделение части такой среды от остальной сети организации не является требованием Стандарта PCI DSS. Тем не менее, сегментацию рекомендуется выполнять, поскольку она позволяет уменьшить:

- Область оценки на соответствие Стандарту PCI DSS
- Затраты на оценку соответствия Стандарту PCI DSS
- Стоимость и сложность внедрения и обеспечения функционирования мер безопасности, требуемых PCI DSS
- Риск для организации (риск уменьшается путем консолидации данных держателей карт в меньшем количестве мест хранения, за которыми осуществляется более жесткий контроль)

Без надлежащей сегментации сети вся сеть целиком (или как ее иногда называют: «плоская сеть») попадает в область оценки на соответствие Стандарту PCI DSS. Сегментация сети может быть реализована путем применения ряда физических или логических средств, таких как надлежащая конфигурация внутренних межсетевых экранов, маршрутизаторов с надежным списком контроля доступа или иных технологий, которые ограничивают доступ к определенным сегментам сети. Чтобы системный компонент считался не входящим в область оценки соответствия PCI DSS, он должен быть изолирован (сегментирован) от среды держателей карт (CDE) таким образом, чтобы даже взлом такого компонента не повлиял бы на безопасность среды держателей карт.

Важной предпосылкой к сокращению области среды данных держателей карт является понимание бизнес-потребностей и процессов, связанных с хранением, обработкой или передачей данных держателей карт. Размещение данных держателей карт в наименьшем количестве мест хранения путем удаления ненужных данных может потребовать реорганизации устоявшихся практик ведения бизнеса.

Документирование потоков данных держателей карт в виде диаграммы потоков данных помогает лучше понять все потоки данных держателей карт и обеспечивает эффективность сегментации сети для изолирования среды данных держателей карт.

Если сегментация сети используется для уменьшения области применения PCI DSS, аудитор должен удостовериться в том, что сегментация выполняется надлежащим образом и тем самым позволяет уменьшить область оценки. Корректно выполненная сегментация сети изолирует системы, которые хранят, обрабатывают или передают данные держателей карт, от остальных систем. Корректность каждой отдельной реализации сетевой сегментации зависит от многих факторов, таких как сетевые настройки, используемые технологии и иные реализуемые защитные меры.

Приложение D: «Сегментация и выборочная оценка помещений организации/системных компонентов» содержит дополнительную информацию о влиянии сетевой сегментации и выборки на область оценки PCI DSS.

Беспроводные технологии

В случае использования беспроводных технологий для хранения, обработки или передачи данных держателей карт (например, в ходе выполнения транзакций через POS-терминалы, при применении технологии ускорения обслуживания потребителей «line-busting») или если беспроводная локальная сеть (WLAN) подключена или является частью среды держателей карт, в силу вступают и должны быть выполнены требования и процедуры тестирования PCI DSS для беспроводных сред (например, требования 1.2.3, 2.1.1 и 4.1.1). Перед внедрением беспроводных технологий организация должна тщательно проанализировать необходимость их использования и оценить связанные с этим риски. Рекомендуется использовать беспроводные технологии только для передачи некритичных данных.

Привлечение сторонних сервис-провайдеров / внешних подрядчиков

Сервис-провайдеры и ТСП могут воспользоваться услугами сторонних организаций по обработке, хранению и передаче данных держателей карт или управлению маршрутизаторами, межсетевыми экранами, базами данных, системами физической безопасности и/или серверами. Однако это может оказать негативное влияние на безопасность среды данных держателей карт.

Стороны должны четко определить, какие службы и системные компоненты входят в область оценки сервис-провайдера на соответствие требованиям PCI DSS, какие требования предъявляются к сервис-провайдеру, а какие находятся в области ответственности клиентов сервис-провайдеров и должны быть проверены в рамках оценки соответствия PCI DSS клиента. Например, хостинг-провайдер должен четко определить, какие IP-адреса просканированы в рамках ежеквартального сканирования на наличие уязвимостей, и за ежеквартальное сканирование каких адресов ответственны клиенты.

Сервис-провайдеры несут ответственность за подтверждение своего соответствия стандарту PCI DSS и такие требования могут предъявляться к сервис-провайдерам платежными системами. Сервис-провайдерам следует обращаться к платежной системе или своему эквайреру для определения соответствующего способа подтверждения соответствия.

Сервис-провайдер (третья сторона) может подтвердить соответствие требованиям двумя способами:

1) **Ежегодная оценка:** Сервис-провайдеры могут самостоятельно пройти ежегодную оценку (ежегодные оценки) соответствия стандарту PCI DSS и предоставить доказательство соответствия своим клиентам, или
2) **Многократные оценки, оценки по требованию:** если сервис-провайдеры не проводят собственные ежегодные оценки соответствия стандарту PCI DSS, они обязуются проходить оценки по запросу своих клиентов и/или участвовать в каждой оценке соответствия стандарту PCI DSS своих клиентов, предоставляя результаты каждой оценки соответствующему клиенту (клиентам).

Если третье лицо проводит собственную оценку соответствия стандарту PCI DSS, оно должно предоставить своим клиентам достаточные доказательства того, что область оценки сервис-провайдера включает услуги, относящиеся к клиенту, и что соответствующие требования PCI DSS были проверены, а соответствие им - подтверждено. Конкретные виды доказательств, которые сервис-провайдер должен предоставить своим клиентам, зависят от действующих соглашений/контрактов между этими сторонами. Например, Аттестат соответствия (AOC) и (или) соответствующие разделы Отчета о соответствии (ROC) сервис-провайдера (отредактированного для защиты конфиденциальной информации) могут содержать всю или некоторую необходимую информацию.

Кроме того, ТСП и сервис-провайдеры должны контролировать статус соответствия PCI DSS всех сторонних сервис-провайдеров, которые имеют доступ к данным держателей карт. *Подробная информация приведена в требовании 12.8.*

Лучшие практики по внедрению Стандарта PCI DSS в рабочие процессы

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

1. Мониторинг мер безопасности (таких как межсетевые экраны, системы обнаружения и предотвращения вторжений, мониторинг целостности файлов, антивирус, управление доступом и т.д.), чтобы гарантировать их эффективную и надлежащую работу.
2. Своевременное обнаружение и реагирование на любые отказы средств контроля безопасности. Процессы реагирования на отказы средств контроля безопасности должны включать:
    - Восстановление средства безопасности
    - Определение причины отказа
    - Определение и решение любых проблем с безопасностью, возникших во время отказа средств контроля безопасности
    - Внедрение мер (например, процесса или технического средства) для предотвращения повторного возникновения причины отказа
    - Возобновление мониторинга средств контроля безопасности, по возможности с более тщательным мониторингом в течение некоторого времени для проверки эффективности работы средства контроля
3. Оценка изменений среды (например, добавление новых систем, внесение изменений в систему или конфигурацию сети) до окончательного внесения изменений, а также:
    - Определение потенциального влияния на область действия Стандарта PCI DSS (например, новое правило межсетевого экрана, разрешающее соединение между системой в среде держателей карт и другой системой, может привести к добавлению других систем или сетей в область оценки PCI DSS).
    - Определение требований PCI DSS, применимых к системам и сетям, на которые распространяются изменения (например, если новая система входит в область оценки PCI DSS, необходимо будет выполнить ее конфигурацию согласно стандартам конфигурации системы, включая мониторинг целостности файлов, установку антивируса, установку патчей, ведение журнала аудита и т.д., и включить в план ежеквартального сканирования на наличие уязвимостей).
    - Обновление области применения PCI DSS и внедрение необходимых средств контроля безопасности.
4. Внесение изменений в организационную структуру (например, слияние или приобретение компаний) должно приводить к официальному пересмотру области применения PCI DSS и применения требований.
5. Выполнение регулярной оценки и проведение опросов с целью подтверждения того, что требования PCI DSS соблюдаются, а сотрудники следуют процессам обеспечения безопасности. Такие регулярные оценки должны распространяться на все подразделения и филиалы, в том числе магазины розничной торговли, центры обработки данных и т.д., и включать оценку системных компонентов (или выборок системных компонентов) с целью подтверждения того, что требования PCI DSS выполняются (например, применены стандарты конфигурации, антивирус обновлен до актуальной версии, установлены последние патчи, проводится мониторинг журнала аудита и т.д.). Частота проведения оценок определяется организацией в

зависимости от размера и сложности среды.

Подобные оценки также могут использоваться для проверки наличия соответствующих свидетельств – например, журналов аудита, отчетов о результатах сканирования на наличие уязвимостей, результатов пересмотра правил межсетевого экрана и т.д. – для упрощения подготовки организации к следующей оценке на соответствие требованиям.

6. Выполнение проверки аппаратных и программных технологий не реже одного раза в год для подтверждения наличия их поддержки производителем и способности соблюдать требования организации по безопасности, включая требования PCI DSS. Если будет выявлено, что производитель больше не поддерживает технологии, или что технологии более не соответствуют требованиям организации по безопасности, организация должна подготовить план устранения несоответствий, включающий (при необходимости) замену технологий.

Кроме указанных выше действий организациям также предлагается рассмотреть возможность внедрения разделения обязанностей по обеспечению безопасности таким образом, чтобы обязанности, включающие в себя функции обеспечения безопасности и/или выполнения оценки, были отделены от обязанностей, предусматривающих функции оперативного управления. В средах, где один сотрудник выполняет несколько обязанностей (например, администрирование и выполнение действий по обеспечению безопасности), обязанности могут быть распределены таким образом, чтобы никакой сотрудник не обладал полным контролем над процессом без независимого контроля. Например, ответственность за конфигурирование и ответственность за согласование изменений может быть назначена разным сотрудникам.

Примечание: *Для ряда организаций данные практики также являются требованиями для обеспечения постоянного соответствия стандарту PCI DSS.*
Например, описанные выше принципы включены в некоторые требования PCI DSS, а в «Дополнительных проверках для определенных организаций (DESV)» (Приложение A3 Стандарта PCI DSS) от определенных организаций требуется соблюдение этих принципов.

Все организации должны рассмотреть внедрение данных практик в свою среду, даже если от организации не требуется подтверждать их соблюдение.

Для Аудиторов: Выборочная оценка помещений организации/системных компонентов

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

Тогда как аудитору разрешается делать выборочную проверку помещений организации и (или) системных компонентов в рамках проверки организации на соответствие требованиям PCI DSS, организациям запрещается применять требования PCI DSS только к части среды (так, например, требования о выполнении ежеквартального сканирования на наличие уязвимостей применяются ко всем системным компонентам). Аналогично аудитору не разрешается проводить проверку организации на соответствие только части требований PCI DSS.

После рассмотрения области оценки в целом и уровня сложности оцениваемой среды аудитор может самостоятельно сделать репрезентативную выборку помещений организации или системных компонентов для выполнения оценки соответствия организации требованиям PCI DSS. Сначала следует определить, какие помещения организации будут оцениваться, а затем уже - какие системные компоненты внутри каждого такого помещения. Выборка должна быть репрезентативной как для всех типов и местоположений помещений организации, так и для типов системных компонентов внутри выбранных помещений. Размер выборки должен быть достаточным для того, чтобы аудитор мог удостовериться, что средства контроля применяются надлежащим образом.

К примерам помещений организации относятся (но не ограничиваются ими): офисы организации, магазины, франчайзинговые точки продаж, центры обработки данных и другие объекты в разных местах расположения. Системные компоненты из каждого выбранного помещения организации должны быть включены в выборку. Например, для каждого выбранного помещения организации необходимо включать различные типы операционных систем, функции и приложения, относящиеся к проверяемой области.

Так, аудитор может определить, что выборка внутри помещения организации включает в себя сервера Sun, на которых функционирует веб-сервер Apache, Windows-серверы, на которых функционирует система Oracle, мейнфреймы, на которых функционируют устаревшие платежные приложения обработки карт, серверы передачи данных под управлением HP-UX и Linux-серверы с системой MySQL. Если все приложения работают на базе одной операционной системы (например, Windows 7 или Solaris 10), в выборку все равно должен входить ряд различных приложений (например, серверы базы данных, веб-серверы, серверы передачи данных).

При самостоятельном выборе помещений организации или системных компонентов аудитор должен учитывать следующее:

- При наличии стандартизированных в соответствии с PCI DSS процессов и средств контроля безопасности, которые должны соблюдаться для всех помещений организации или системных компонентов, выборка может быть меньшего объема, чем в случае отсутствия таких процессов или средств контроля безопасности. Выборка должна быть достаточно большой, чтобы аудитор мог убедиться, что все помещения организации или системные компоненты настроены и функционируют в соответствии со стандартными процессами. Аудитор должен убедиться, что стандартизированные и централизованные средства контроля безопасности применяются и работают эффективно.
- В случае наличия более одного процесса безопасности и (или) операционного процесса (например, для разных типов помещений организации/системных компонентов), выборка должна быть настолько большой, чтобы включать помещения организации/системные компоненты, привязанные к каждому процессу.

- В случае отсутствия стандартизированных процессов/средств контроля в соответствии с PCI DSS и когда каждое помещение/системный компонент регулируется нестандартизированными процессами, размер выборки должен быть больше, чтобы аудитор мог убедиться, что требования PCI DSS корректно реализованы для каждого помещения организации или для каждого системного компонента.
- Выборка системных компонентов должна включать каждый используемый тип и сочетание. Например, выборка приложений должна включать все версии и платформы для каждого типа приложений.

Для каждого случая применения выборки аудитор должен:

- Документировать обоснование примененного метода выборки и ее размера.
- Документировать и проверить стандартизованные процессы PCI DSS и средства контроля, используемые при определении размера выборки.
- Объяснить, насколько сделанная выборка репрезентативна.

Также см.: Приложение D: Сегментация и выборочная оценка помещений организации/системных компонентов

Аудитор должен перепроверять обоснование примененного метода выборки при каждой оценке. При применении выборки в рамках каждой оценки должны выбираться разные помещения организации и системные компоненты.

Компенсационные меры

Ежегодно аудитор должен документировать, пересматривать и проверять все компенсационные меры и включать их в Отчет о соответствии согласно *Приложению B:* «Компенсационные меры» и *Приложению C: «Компенсационные меры - Форма для заполнения».*

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

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

Инструкции по заполнению и требования к содержанию Отчета о соответствии

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

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

Процесс проведения оценки соответствия Стандарту PCI DSS

Процесс оценки соответствия стандарту PCI DSS включает выполнение следующих этапов:

1. Подтвердить объем оценки на соответствие Стандарту PCI DSS.
2. Провести оценку среды на соответствие PCI DSS, следуя проверочным процедурам для каждого требования.
3. Заполнить соответствующий отчет о проведении оценки (Лист Самооценки (SAQ) или Отчет о соответствии (ROC)), указав все компенсационные меры согласно применимым рекомендациям и инструкциям индустрии платежных карт.
4. Заполнить Аттестат Соответствия (Attestation of Compliance) в полном объеме для сервис-провайдеров или ТСП, в зависимости от типа оцениваемой организации. Аттестаты соответствия доступны на сайте PCI SSC.
5. Направить Лист Самооценки (SAQ) или Отчет о соответствии (ROC) и Аттестат Соответствия (Attestation of Compliance) вместе со всей требуемой документацией (например, отчетами о ASV-сканировании) эквайреру (для ТСП) или платежной системе, или иной запрашивающей стороне (для сервис-провайдеров).
6. При необходимости устранить нарушения в отношении требований, которые не выполнены и предоставить обновленный отчет.

Версии Стандарта PCI DSS

На дату публикации данного документа версия стандарта PCI DSS v3.2 действительна до 31 декабря 2018 г., после чего она считается неактуальной. Все оценки по стандарту PCI DSS после указанной даты должны быть выполнены согласно версии PCI DSS v.3.2.1 или более поздней.

Приведенная ниже таблица резюмирует данные по версиям стандарта PCI DSS и датам их вступления в силу.[6]

Версия	Дата публикации	Дата вывода из действия
PCI DSS, версия 3.2.1 (настоящий документ)	Май 2018 г.	Не установлена
PCI DSS, версия 3.2	Апрель 2016 г.	31 декабря 2018 г.

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

Подробное описание требований Стандарта PCI DSS и процедур оценки безопасности

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

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

Примечание: *Требования стандарта PCI DSS не считаются выполненными, если средства контроля не были внедрены либо были запланированы на будущее. После того как все невыполненные требования будут выполнены организацией, аудитор должен провести повторную проверку для подтверждения того, что проблемы устранены и все требования выполнены.*

Ознакомьтесь со следующими информационными материалами (доступными на веб-сайте PCI SSC), для документального оформления оценки PCI DSS:

- *См. инструкции по заполнению Отчета о соответствии (ROC) в документе «Шаблон отчета о соответствии стандарту PCI DSS» (PCI DSS ROC Reporting Template).*
- *См. инструкции по заполнению Листов Самооценки (SAQ) в документе «Инструкции и рекомендации по заполнению Листов Самооценки PCI DSS» (PCI DSS SAQ Instructions and Guidelines).*
- *См. инструкции по подаче отчетов о соответствии стандарту PCI DSS в Аттестатах о соответствии стандарту PCI DSS (PCI DSS Attestations of Compliance).*

Создание и поддержка защищенной сети и систем

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

Межсетевые экраны — это устройства, контролирующие сетевой трафик между (внутренней) локальной сетью организации и недоверенными (внешними) сетями, а также входящий и исходящий трафик из более критичных областей во внутренних доверенных сетях организации. Среда данных держателей карт является примером области повышенной критичности внутри доверенной сети организации.

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

Все системы должны быть защищены от неавторизованного доступа из недоверенных сетей, будь то подключение через Интернет систем электронной коммерции, доступ сотрудников к Интернету посредством веб-браузеров, доступ сотрудников к электронной почте, выделенные подключения со сторонними организациями, подключения по беспроводным сетям или через иные источники. Часто, казалось бы, незначительные пути к и из недоверенных сетей могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны - основные механизмы обеспечения безопасности любой компьютерной сети.

Другие системные компоненты могут обеспечивать функциональные возможности межсетевого экрана, если они отвечают минимальным требованиям к межсетевым экранам, приведенным в Требовании 1. Если для обеспечения функциональности межсетевого экранирования внутри среды данных держателей карт используются иные системные компоненты, то они должны быть включены в область оценки на соответствие Требованию 1.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1 Разработать и реализовывать стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя следующее:	**1.1** Изучите стандарты конфигурации межсетевых экранов и маршрутизаторов, а также иную нижеуказанную документацию для проверки того, что стандарты включают в себя все необходимые требования и внедрены следующим образом:	Межсетевые экраны и маршрутизаторы — это ключевые компоненты архитектуры, которые используются для контроля входа в сеть и выхода из нее. Эти устройства являются программным обеспечением или аппаратными устройствами, блокирующими несанкционированный доступ к сети, и управляют входом в сеть и выходом из нее. Стандарты и процедуры конфигурации помогают убедиться, что в организации обеспечена и поддерживается надежная первая линия защиты данных.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.1 Формальный процесс утверждения и тестирования всех сетевых подключений и изменений в конфигурациях межсетевых экранов и маршрутизаторов	**1.1.1.a** Изучите документированные процедуры и убедитесь, что существует формальный процесс тестирования и утверждения всех: • Сетевых соединений и • Изменений в конфигурациях межсетевых экранов и маршрутизаторов.	Документированный и внедренный процесс согласования и тестирования всех подключений и изменений межсетевых экранов и маршрутизаторов поможет предотвратить возникновение проблем безопасности, вызванных неправильной конфигурацией сети, маршрутизатора или межсетевого экрана. Без официального согласования и тестирования изменений записи об изменениях могут не быть обновлены, что может привести к несоответствию между документированной и реальной конфигурацией сети.
	1.1.1.b Для выборки сетевых соединений опросите ответственных сотрудников и изучите записи, чтобы убедиться, что сетевые соединения были согласованы и протестированы.	
	1.1.1.c Сделайте выборку реальных изменений в конфигурации межсетевого экрана и маршрутизатора, сравните их с записями об изменениях и опросите ответственных сотрудников, чтобы убедиться, что изменения были согласованы и протестированы.	
1.1.2 Актуальная схема сети с указанием всех подключений к среде данных держателей карт из других сетей, включая все беспроводные сети	**1.1.2.a** Изучите схему (схемы) и конфигурации сети и проверьте наличие актуальной схемы сети, а также то, что в схеме отмечены все подключения к данным держателей карт, включая беспроводные сети.	Схемы сети описывают конфигурацию сети и расположение всех сетевых устройств. Без актуальной схемы сети устройства могут остаться незамеченными, к ним не будут применены средства контроля безопасности, предусмотренные в PCI DSS, и таким образом они станут уязвимыми к взлому.
	1.1.2.b Опросите ответственных сотрудников, чтобы проверить актуальность схемы сети.	
1.1.3 Актуальная схема, отображающая все потоки данных держателей карт в системах и сетях	**1.1.3** Изучите схему потоков данных и опросите сотрудников, чтобы убедиться, что схема: • Отображает все потоки ДДК во всех системах и сетях. • Поддерживается в актуальном состоянии и обновляется в случае внесения изменений в среду.	На схемах потоков данных держателей карт указано расположение всех данных держателей карт, которые хранятся, обрабатываются или передаются внутри сети. Схемы сети и схемы потоков данных держателей карт помогают организации получить представление об области среды и отслеживать ее показывая, как данные держателей карт проходят через сети и между отдельными системами и устройствами.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.4 Требования к межсетевому экранированию для каждого Интернет-соединения и между любой демилитаризованной зоной (DMZ) и внутренней сетью	**1.1.4.a** Проверьте стандарты конфигурации межсетевого экрана на наличие требований о необходимости межсетевого экранирования каждого Интернет-соединения, а также между демилитаризованной зоной (DMZ) и внутренней сетью.	Использование межсетевого экрана на каждом входящем и исходящем подключении, а также между любой демилитаризованной зоной и внутренней сетью позволяет организации отслеживать и контролировать доступ и свести к минимуму шансы злоумышленников на получение доступа к внутренней сети через незащищенное соединение.
	1.1.4.b Проверьте, выполнена ли текущая схема сети в соответствии со стандартами конфигурации межсетевых экранов.	
	1.1.4.c Изучите конфигурации сети для проверки наличия межсетевого экранирования каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью согласно документированным стандартам конфигурации и схемам сети.	
1.1.5 Описание групп, ролей и обязанностей по управлению сетевыми компонентами	**1.1.5.a** Убедитесь, что стандарты конфигурации межсетевых экранов и маршрутизаторов включают в себя описание ролей, групп и обязанностей по управлению сетевыми компонентами.	Описание ролей и распределение ответственности гарантирует осведомленность персонала о том, кто отвечает за безопасность всех компонентов сети, и осведомленность лиц, ответственных за управление компонентами, о своих обязанностях. Без официального назначения ролей и обязанностей устройства могут остаться без управления.
	1.1.5.b Опросите сотрудников, ответственных за управление компонентами сети, чтобы подтвердить, что роли и обязанности назначены в соответствии с документацией.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.6 Оформленное обоснование и согласование для использования сервисов, протоколов и портов, включая документацию, описывающую внедренные механизмы защиты небезопасных протоколов.	**1.1.6.a** Убедитесь, что в стандартах конфигурации межсетевых экранов и маршрутизаторов содержится список служб, протоколов и портов с обоснованием необходимости использования и согласованием каждого из них.	Компрометация часто происходит из-за наличия неиспользуемых и небезопасных служб и портов, поскольку они часто содержат известные уязвимости, и многие организации не устанавливают патчи для служб, протоколов и портов, которые они не используют (даже при наличии уязвимостей). Четкое определение и документальное оформление служб, протоколов и портов, необходимых для осуществления деятельности, позволяет организациям обеспечить отключение или удаление всех остальных служб, протоколов и портов. Выполнять согласование должны сотрудники, не зависящие от сотрудников, занимающихся администрированием устройств. Если небезопасные службы, протоколы или порты необходимы для ведения бизнеса, нужно четко понимать и принимать риск, связанный с их использованием, обосновать необходимость использования таких протоколов, а также задокументировать и внедрить механизмы защиты, которые позволят безопасно использовать эти протоколы. Если эти небезопасные службы, протоколы и порты не являются необходимыми для ведения бизнеса, их следует отключить или удалить. Для ознакомления с сервисами, протоколами или портами, считающимися небезопасными, см. промышленные стандарты и руководства (например, NIST, ENISA, OWASP и др.)
	1.1.6.b Выявите разрешенные небезопасные сервисы, протоколы и порты и проверьте документальное оформление механизмов защиты для каждой службы.	
	1.1.6.c Изучите конфигурацию межсетевых экранов и маршрутизаторов и убедитесь, что механизмы защиты документированы и внедрены для каждой небезопасной службы, протокола и порта.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.1.7 Требование пересмотра правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода	**1.1.7.a** Убедитесь, что в стандартах конфигурации межсетевых экранов и маршрутизаторов предусмотрено требование пересмотра правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода.	Такой пересмотр правил дает организации возможность каждые полгода удалять все ненужные, устаревшие или некорректные правила и гарантирует, что все правила разрешают доступ только авторизованным службам и портам, для которых существует документированное обоснование использования. Организациям, которые вносят много изменений в правила межсетевых экранов и маршрутизаторов, рекомендуется проводить пересмотр чаще, чтобы гарантировать, что правила все еще соответствуют нуждам бизнеса.
	1.1.7.b Проверьте документацию, относящуюся к пересмотру правил и опросите ответственных сотрудников, чтобы убедиться, что правила пересматриваются не реже одного раза в полгода.	
1.2 Настраивать ограничения соединений на межсетевых экранах и маршрутизаторах между недоверенными сетями и любыми системными компонентами, находящимися в среде данных держателей карт. ***Примечание:*** *Недоверенная сеть — это любая сеть, являющаяся внешней по отношению к сетям, принадлежащим проверяемой организации, и/или любая сеть, контролировать которую или управлять которой проверяемая организация не может.*	**1.2** Изучите конфигурацию межсетевых экранов и маршрутизаторов, убедитесь, что соединения между незащищенными сетями и системными компонентами, находящимися в среде данных держателей карт, ограничены.	Важно установить защиту сети между внутренней доверенной сетью и любыми недоверенными внешними сетями и (или) сетями, которые не контролируются или не управляются организацией. При несоблюдении данной меры организация будет подвержена риску несанкционированного доступа злоумышленников или вредоносного программного обеспечения к данным. Для того, чтобы межсетевой экран действительно выполнял свои функции, он должен быть соответствующим образом настроен для контроля и (или) ограничения входящего и исходящего трафика в сети организации.
1.2.1 Ограничивать входящий и исходящий трафик только соединениями, необходимыми для среды держателей карт, запрещать весь остальной трафик.	**1.2.1.a** Проверьте стандарты конфигураций межсетевого экрана и маршрутизатора и убедитесь, что в них определен входящий и исходящий трафик, необходимый для среды данных держателей карт.	Анализ всех входящих и исходящих соединений позволяет проверять и ограничивать трафик, основываясь на адресе источника и/или адресе назначения, тем самым предотвращая свободный доступ между защищенной и недоверенной средами. Это требование направлено на предотвращение доступа злоумышленников к сети организации
	1.2.1.b Проверьте конфигурации межсетевого экрана и маршрутизатора и убедитесь, что разрешен только входящий и исходящий трафик, необходимый для среды данных держателей карт.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	1.2.1.c Проверьте конфигурации межсетевого экрана и маршрутизатора и убедитесь, что весь прочий входящий и исходящий трафик явно запрещен, например, путем явного запрета «deny all» или неявного запрета по умолчанию после разрешающих правил.	через неавторизованные IP-адреса или использование служб, протоколов и портов несанкционированным образом (например, для отправки данных, которые они получили из сети организации, на недоверенный сервер). Установка запрета на весь входящий и исходящий трафик, кроме необходимого, помогает предотвратить возникновение неочевидных брешей в системе безопасности из-за несанкционированного и потенциально вредоносного входящего или исходящего трафика.
1.2.2 Обеспечивать безопасность и своевременную синхронизацию конфигурационных файлов маршрутизаторов.	**1.2.2.a** Убедитесь, что конфигурационные файлы маршрутизаторов защищены от несанкционированного доступа.	Хотя рабочие (или активные) конфигурационные файлы обычно включают текущие безопасные настройки, файлы стартовой конфигурации (используемых маршрутизаторами при перезапуске или загрузке) должны быть обновлены и иметь те же безопасные настройки для их применения при каждом перезапуске. Поскольку они выполняются только время от времени, о файлах стартовой конфигурации часто забывают и не обновляют их. Если маршрутизатор выполняет перезапуск и загружает стартовую конфигурацию, в которую не были внесены изменения настроек безопасности, аналогичные внесенным в рабочую конфигурацию, это приведет к наличию слабых правил, которыми могут воспользоваться злоумышленники для проникновения в сеть.
	1.2.2.b Убедитесь, что конфигурации маршрутизаторов синхронизированы, например, рабочая (или активная) конфигурация и стартовая конфигурация (используемая при загрузке устройств) совпадают.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.2.3 Устанавливать межсетевые экраны между каждой беспроводной сетью и средой данных держателей карт. Настраивать межсетевые экраны на блокирование любого трафика из беспроводной сети, либо разрешение только авторизованного трафика между беспроводной средой и средой данных держателей карт в том случае, если для такого трафика существует производственная необходимость.	**1.2.3.a** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что межсетевые экраны установлены между каждой беспроводной сетью и средой данных держателей карт.	Злоумышленники часто используют уязвимости беспроводных технологий для получения доступа к сети и данным держателей карт. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может просто и незаметно проникнуть в сеть. Если межсетевые экраны не запрещают доступ к среде данных держателей карт из беспроводной сети, злоумышленники, которые имеют несанкционированный доступ к беспроводной сети, могут без труда подключиться к среде данных держателей карт и получить доступ к карточным данным. Межсетевые экраны должны быть установлены между всеми беспроводными сетями и средой ДДК независимо от назначения среды, к которой подключена беспроводная сеть. Помимо прочего, это могут быть корпоративные сети, розничные магазины, гостевые сети, склады и т.д.
	1.2.3.b Убедитесь, что межсетевые экраны настроены на блокирование любого трафика из беспроводной сети, либо на разрешение только авторизованного трафика между беспроводной сетью и средой данных держателей карт в том случае, если для такого трафика существует производственная необходимость.	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3 Запрещать прямой публичный доступ между Интернетом и любыми системными компонентами в среде данных держателей карт.	**1.3** Проверьте конфигурацию межсетевых экранов и маршрутизаторов, включая, но не ограничиваясь, маршрутизатор на границе с Интернетом, маршрутизатор и межсетевой экран демилитаризованной зоны (DMZ), сегмент DMZ, пограничный маршрутизатор и внутренний сегмент сети данных держателей карт, чтобы убедиться в отсутствии прямого доступа из Интернета к системным компонентам внутреннего сегмента сети данных держателей карт.	Возможны случаи, когда по обоснованным причинам к системам в DMZ предоставляется доступ через недоверенные соединения (например, чтобы обеспечить публичный доступ к веб-серверу). Такие соединения никогда не должны предоставляться для систем, размещенных во внутренней сети. Назначение межсетевых экранов состоит в управлении и контроле всех соединений между общедоступными системами и внутренними системами, особенно теми, которые используются для хранения, обработки или передачи данных держателей карт. Если разрешен прямой доступ между общедоступными системами и средой данных держателей карт, значит межсетевой экран удалось обойти, и системные компоненты, которые используются для хранения данных держателей карт, становятся уязвимыми для злоумышленников.
1.3.1 Внедрить демилитаризованную зону (DMZ), чтобы ограничить входящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным службам, протоколам и портам.	**1.3.1** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что демилитаризованная зона (DMZ) внедрена, чтобы ограничить входящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным службам, протоколам и портам.	Демилитаризованная зона (DMZ) — это часть сети, которая управляет соединениями между Интернетом (или другими недоверенными сетями) и общедоступными службами (такими как веб-сервер). Такие функциональные возможности позволяют предотвратить доступ злоумышленников к внутренней сети организации из Интернета и использование служб, протоколов или портов несанкционированным образом.
1.3.2 Ограничивать входящие Интернет-соединения только адресами, находящимися в DMZ.	**1.3.2** Изучите конфигурации межсетевого экрана и маршрутизатора, чтобы убедиться, что входящие Интернет-соединения ограничены только IP-адресами, находящимися в демилитаризованной зоне (DMZ).	

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.3 Внедрить меры антиспуфинга (меры по противодействию подмене IP-адреса), позволяющие определить фальшивые IP-адреса источника и заблокировать им доступ в сеть. (Например, блокировать трафик из Интернета, содержащий адреса внутренних источников).	**1.3.3** Убедитесь, что в конфигурации межсетевых экранов и маршрутизаторов внедрены меры антиспуфинга, например, пакеты с внутренними адресами не могут попасть от источника из Интернета в демилитаризованную зону (DMZ).	Обычно, пакет содержит IP-адрес компьютера, который его отправил, чтобы остальные компьютеры сети знали, откуда пакет был отправлен. Злоумышленники будут часто стараться подменить (или сымитировать) отправляемый IP-адрес таким образом, чтобы система-получатель сочла, что пакет из доверенного источника. Фильтрация пакетов, поступающих в сеть, помимо прочего, позволяет убедиться, что пакеты не «подделаны», чтобы выглядеть так, как будто они поступают из внутренней сети организации.
1.3.4 Запрещать неавторизованный исходящий трафик из среды данных держателей карт в Интернет.	**1.3.4** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что весь исходящий трафик из среды держателей карт в Интернет явно авторизован.	Весь трафик, исходящий из среды данных держателей карт, должен быть проверен на соответствие установленным правилам. Необходимо проверить соединения, чтобы ограничить трафик только авторизованными соединениями (например, посредством ограничения адресов (портов) источника или назначения и (или) блокирования содержимого).
1.3.5 Разрешать только «established» (установленные) соединения в сети.	**1.3.5** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что межсетевые экраны разрешают только установленные соединения во внутреннюю сеть и блокируют любые входящие соединения, которые не связаны с предварительно установленной сессией.	Межсетевой экран, обслуживающий «состояние» (или статус) каждого соединения через межсетевой экран, знает, является ли очевидный ответ на предыдущее соединение действительным авторизованным ответом (поскольку он сохраняет статус каждого соединения) или это мошеннический трафик, который пытается обманом заставить межсетевой экран разрешить соединение.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.6 Размещать системные компоненты (например, базы данных), в которых хранятся данные держателей карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей.	**1.3.6** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что системные компоненты, в которых хранятся данные держателей карт, располагаются во внутренней сети, отделенной от демилитаризованной зоны (DMZ) и иных недоверенных сетей.	Если ДДК размещены в DMZ, задача получения доступа к этой информации для злоумышленника упрощается, поскольку ему нужно будет преодолеть меньшее количество уровней защиты. Размещение системных компонентов, в которых хранятся данные держателей карт, во внутренней сети, отделенной от демилитаризованной зоны и иных недоверенных сетей межсетевым экраном, не позволит неавторизованному сетевому трафику дойти до системного компонента. ***Примечание:*** *Это требование не распространяется на временное хранение данных держателей карт в энергозависимой памяти.*

Требования PCI DSS	Проверочные процедуры	Пояснение
1.3.7 Не раскрывать частные IP-адреса и данные о маршрутах третьим сторонам, не имеющим санкционированного доступа к такой информации. ***Примечание:*** *Методы сокрытия IP-адресации включают, но не ограничиваются:* • *преобразование сетевых адресов (NAT);* • *размещение серверов, содержащих данные держателей карт, 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 зарегистрированных адресов.*	**1.3.7.a** Изучите конфигурации межсетевых экранов и маршрутизаторов и убедитесь, что используются методы, обеспечивающие предотвращение раскрытия частных IP-адресов и данных о маршрутизации из внутренней сети в Интернет. **1.3.7.b** Опросите сотрудников и изучите документацию, чтобы убедиться, что любое раскрытие частных IP-адресов и данных о маршрутизации является санкционированным.	Запрет передачи внутренних или частных IP-адресов является действенным способом предотвращения получения злоумышленником информации об адресе внутренней сети и использования им этой информации для проникновения в сеть. Средства, используемые для соблюдения этого требования, зависят от используемой сетевой технологии. Например, меры, предпринимаемые для соблюдения данного требования, могут быть разными для сетей IPv4 и сетей IPv6.

Требования PCI DSS	Проверочные процедуры	Пояснение
1.4 Устанавливать персональные межсетевые экраны или эквивалентные механизмы на все мобильные устройства (включая корпоративные и/или принадлежащие сотрудникам), имеющие доступ в Интернет при нахождении вне корпоративной сети (например, ноутбуки, используемые сотрудниками), и также используемые для подключения к среде данных держателей карт (CDE). Конфигурации межсетевых экранов (или их аналогов) включают: • Определенные настройки конфигурации. • Запущенный и активный персональный межсетевой экран (или аналогичный функционал). • Запрет на изменения настроек персональных межсетевых экранов (или аналогичного функционала) пользователями мобильных устройств.	**1.4.a** Изучите политики и стандарты конфигурации и убедитесь, что: • Требуется установка персональных межсетевых экранов или эквивалентного функционала на все мобильные устройства (включая корпоративные и/или принадлежащие сотрудникам), имеющие доступ в Интернет при нахождении вне корпоративной сети (например, ноутбуки, используемые сотрудниками), и также используемые для подключения к среде данных держателей карт (CDE). • Установлены определенные настройки конфигурации для персональных межсетевых экранов (или аналогичного функционала). • Персональные межсетевые экраны (или аналогичный функционал) запущены и активны. • Настройки персональных межсетевых экранов (или аналогичного функционала) не могут быть изменены пользователями мобильных устройств.	Мобильные устройства с прямым доступом в Интернет вне зоны действия защиты межсетевого экрана организации более уязвимы к Интернет-угрозам. Использование функционала межсетевого экрана (например, программного или аппаратного персонального межсетевого экрана) помогает защитить устройства от Интернет-атак, которые могут использовать мобильное устройство для получения доступа к системам и данным организации после повторного подключения устройства к сети. Конкретные настройки конфигурации для персональных межсетевых экранов определяются организацией. ***Примечание:*** *Это требование применяется к компьютерам, принадлежащим сотрудникам или организации. Системы, которыми невозможно управлять с помощью корпоративных политик, создают уязвимости, которыми могут воспользоваться злоумышленники. Разрешение недоверенным системам подключаться к среде ДДК организации может привести к предоставлению доступа хакерам и другим злоумышленникам.*
	1.4.b Проведите выборочную проверку мобильных устройств организации и (или) устройств, принадлежащих сотрудникам, и убедитесь, что: • Персональные межсетевые экраны (или аналогичный функционал) установлены и настроены согласно определенным организацией настройкам конфигурации. • Персональный межсетевой экран (или аналогичный функционал) запущен и активен. • Запрещены изменения настроек персональных межсетевых экранов (или аналогичного функционала) пользователями мобильных устройств.	
1.5 Гарантировать, что политики безопасности и рабочие процедуры управления межсетевыми экранами документированы, используются и известны всем заинтересованным лицам.	**1.5** Проверьте документацию и опросите сотрудников для подтверждения того, что политики безопасности и рабочие процедуры управления межсетевыми экранами: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о политиках и процедурах безопасности и следовать им для обеспечения постоянного контроля над межсетевыми экранами и маршрутизаторами с целью предотвращения несанкционированного доступа к сети.

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

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

Требования PCI DSS	Проверочные процедуры	Пояснение
2.1 Всегда изменять значения параметров, заданные производителями по умолчанию, и отключать или удалять учетные записи по умолчанию **перед** установкой систем в сети. Это требование применимо ко ВСЕМ паролям по умолчанию, включая пароли, используемые операционными системами, программным обеспечением, реализующим функции защиты, приложениями и системными учетными записями, POS-терминалами, платежными приложениями, строками доступа в протоколах SNMP и т.д.	**2.1.a** Сделайте выборку системных компонентов и с помощью системного администратора попытайтесь осуществить вход в устройства и приложения, используя учетные записи и пароли, устанавливаемые производителем по умолчанию, чтобы убедиться, что ВСЕ установленные производителем пароли (включая пароли к операционным системам, программному обеспечению, реализующего функции защиты, приложениям и системным учетным записям, POS-терминалам (в точках продаж) и строки доступа SNMP) были изменены. (Используйте руководства производителей и Интернет-ресурсы, чтобы узнать аутентификационные данные (учетные записи/пароли), устанавливаемые производителем по умолчанию).	Злоумышленники (находящиеся внутри и вне организации) часто используют настройки, учетные записи и пароли, заданные производителями по умолчанию, для получения доступа к операционным системам, приложениям и устройствам, на которых они установлены. Поскольку эти стандартные настройки хорошо известны и часто публикуются в хакерских сообществах, их изменение сделает вашу систему менее уязвимой для злоумышленников. Даже если учетная запись по умолчанию не предназначена для использования, изменение пароля по умолчанию на надежный уникальный пароль и последующее отключение учетной записи не позволят злоумышленнику повторно включить ее и получить доступ с помощью пароля по умолчанию.
	2.1.b Для выборки системных компонентов убедитесь, что все ненужные учетные записи по умолчанию (включая учетные записи к операционным системам, программному обеспечению, реализующего функции защиты, приложениям, устройствам, POS-терминалам, а также строки доступа SNMP и т.д.) были удалены или отключены.	
	2.1.c Опросите сотрудников и изучите сопроводительную документацию для подтверждения того, что: • Все учетные данные по умолчанию, предоставленные производителем (включая пароли по умолчанию к операционным системам, программному обеспечению, реализующего функции защиты, приложениям и системным учетным записям, POS-терминалам, а также строки доступа SNMP и т.д.) изменяются перед подключением систем к сети. • Ненужные учетные записи, настроенные по умолчанию, (включая учетные записи к операционным системам, программному обеспечению, реализующего функции защиты, приложениям, устройствам, POS-терминалам, строки доступа SNMP и т.д.) удаляются или отключаются	

Требования PCI DSS	Проверочные процедуры	Пояснение
	перед подключением систем к сети.	
2.1.1 Для использования беспроводных сред, подключенных к среде данных держателей карт, или беспроводных сред, передающих данные держателей карт, во время установки изменять ВСЕ параметры, установленные по умолчанию производителями беспроводных сред, (включая, ключи шифрования, пароли и строки доступа SNMP беспроводных сред).	**2.1.1.a** Опросите ответственных сотрудников и изучите сопроводительную документацию для подтверждения того, что: • Все ключи шифрования, заданные по умолчанию, были заменены при установке. • Ключи шифрования заменяются новыми ключами шифрования каждый раз, когда сотрудник, имеющий доступ к таким ключам, покидает компанию или переводится на другую должность.	Если беспроводные сети реализованы без установки надежных настроек безопасности (включая замену настроек по умолчанию), снифер (анализатор пакетов беспроводных сетей) может прослушивать трафик, легко перехватывать данные и пароли, а также атаковать и входить в сеть. Кроме того, протокол обмена ключами для ранних версий шифрования Стандарта 802.11x (протокол WEP) был взломан и может сделать все шифрование бесполезным. Встроенное ПО устройств должно обновляться, чтобы поддерживать более надежные протоколы.
	2.1.1.b Опросите сотрудников и изучите политики и процедуры, чтобы убедиться, что: • Требуется замена строк доступа SNMP, заданных по умолчанию, при установке. • Требуется замена паролей/парольных фраз, заданных по умолчанию, при установке в точках доступа.	
	2.1.1.c Изучите документацию производителя и выполните вход в беспроводное устройство с помощью системного администратора, чтобы убедиться, что: • Строки доступа SNMP, заданные по умолчанию, не используются. • Заданные по умолчанию пароли/парольные фразы на точках доступа не используются.	
	2.1.1.d Изучите документацию производителя и настройки конфигурации беспроводной сети, чтобы убедиться, что системное ПО беспроводного устройства обновляется с целью обеспечения надежного шифрования для: • Выполнения аутентификации через беспроводные сети. • Выполнения передачи данных через беспроводные сети.	
	2.1.1.e Изучите документацию производителя и настройки конфигурации беспроводной сети, чтобы убедиться, что иные настройки безопасности, заданные производителем беспроводной сети, были изменены (если применимо).	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2 Разработать стандарты конфигурации для всех системных компонентов. Убедиться, что стандарты учитывают все известные уязвимости безопасности, а также положения общепринятых отраслевых стандартов безопасной конфигурации. К примерам источников общепринятых отраслевых стандартов безопасной конфигурации относятся, но не ограничиваются ими: • 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** Изучите стандарты конфигурации всех системных компонентов организации. Убедитесь, что стандарты конфигурации системы согласуются с требованиями отраслевых стандартов безопасной конфигурации.	У многих операционных систем, баз данных и корпоративных приложений существуют известные уязвимости, а также известные способы настройки данных систем для устранения этих уязвимостей системы безопасности. Чтобы помочь лицам, которые не являются экспертами в области безопасности, многие организации, специализирующиеся на защите информации, предоставляют рекомендации по повышению уровня безопасности и устранению уязвимостей. К примерам источников, в которых можно найти рекомендации по стандартам конфигурации относятся (но не ограничиваются ими): www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org, а также веб-сайты производителей. Стандарты системной конфигурации должны быть актуальными, чтобы гарантировать, что недавно обнаруженные уязвимости устраняются до установки системы в сети.
	2.2.b Изучите политики и опросите сотрудников для подтверждения того, что стандарты конфигурации обновляются по мере обнаружения новых уязвимостей безопасности, как определено в требовании 6.1.	
	2.2.c Изучите политики и опросите сотрудников для подтверждения того, что стандарты конфигурации применяются при настройке новых систем, и что перед установкой системы в сети выполняется проверка, что стандарты конфигурации применены.	
	2.2.d Проверьте стандарты системной конфигурации на наличие следующих процедур для всех типов системных компонентов: • Изменение всех параметров по умолчанию, заданных производителем, и удаление ненужных учетных записей по умолчанию. • Реализация на каждом сервере только одной основной функции для того, чтобы исключить совмещение на одном и том же сервере функций, требующих различных уровней безопасности. • Включение только необходимых служб, протоколов, демонов и т.д., требующихся для функционирования системы. • Настройка дополнительных параметров безопасности для любых необходимых служб, протоколов и демонов, которые признаны небезопасными. • Настройка параметров безопасности системы таким образом, чтобы исключить возможность некорректного использования системы. • Удаление из системы всего неиспользуемого функционала: сценариев, драйверов, дополнительных возможностей, подсистем, файловых систем и ненужных для работы веб-серверов.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2.1 Реализовывать на каждом сервере только одну основную функцию для того, чтобы исключить совмещение на одном и том же сервере функций, требующих различных уровней безопасности. (Например, веб-серверы, серверы баз данных и DNS-серверы должны быть развернуты на разных серверах.) ***Примечание:*** *Если используются технологии виртуализации, реализовать только одну основную функцию на одном виртуальном системном компоненте.*	**2.2.1.a** Сделайте выборку системных компонентов, проверьте системные конфигурации и убедитесь, что выполняется правило «одна основная функция - один сервер».	Если функции, для которых необходим разный уровень безопасности, расположены на одном сервере, уровень безопасности функций с более высокими требованиями к безопасности будет понижен. Кроме того, функции сервера с более низким уровнем безопасности могут создавать угрозы для безопасности других функций того же сервера. Рассматривая потребности в безопасности различных серверных функций как часть стандартов системной конфигурации и связанных с ними процессов, организации могут обеспечить, чтобы функции, требующие различных уровней безопасности, не сосуществовали на одном и том же сервере.
	2.2.1.b Если используются технологии виртуализации, изучите системные конфигурации и убедитесь, что выполняется правило «одна основная функция - один виртуальный системный компонент или устройство».	
2.2.2 Включать только необходимые службы, протоколы, демоны и т.д., требующиеся для функционирования системы.	**2.2.2.a** Сделайте выборку системных компонентов и проверьте включенные службы, демоны и протоколы, и убедитесь, что включены только необходимые службы и протоколы.	Как указано в требовании 1.1.6, существует много протоколов, которые необходимы для ведения бизнеса (или которые включены по умолчанию) и которые часто используются злоумышленниками для компрометации сети. Включение этого требования в стандарты конфигурации организации и связанные с этим процессы обеспечивает включение только необходимых служб и протоколов.
	2.2.2.b Выявите любые включенные незащищенные службы, демоны и протоколы, и опросите персонал для подтверждения того, что их использование обосновано согласно документированным стандартам конфигурации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2.3 Настраивать дополнительные параметры безопасности для любых необходимых служб, протоколов и демонов, которые признаны небезопасными.	**2.2.3** Изучите стандарты конфигурации и убедитесь, что механизмы защиты для каждой небезопасной службы, демона и протокола документированы и внедрены.	Включение механизмов защиты до развертывания новых серверов позволит предотвратить установку серверов в среду с небезопасной конфигурацией. Надлежащая защита всех небезопасных служб, протоколов и демонов затруднит злоумышленникам использование распространенных уязвимостей через сеть. Информацию относительно стойкой криптографии и безопасных протоколов см. в промышленных стандартах и рекомендациях (например, NIST SP 800-52 и SP 800-57, OWASP и пр.). ***Примечание:*** *Протокол SSL/ранняя версия TLS не считаются стойкой формой криптографии и не должны быть использованы в качестве средства контроля безопасности. Исключение составляют POS POI терминалы, для которых получено подтверждение того, что на них не оказывают влияния известные эксплойты и точки подключения, к которым они подключены, как указано в Приложении A2.*

Требования PCI DSS	Проверочные процедуры	Пояснение
2.2.4 Настраивать параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.	**2.2.4.a** Опросите системных администраторов и (или) администраторов по безопасности с целью проверки того, что им известны настройки основных параметров защиты системных компонентов.	Стандарты системной конфигурации и связанные с этим процессы должны предусматривать применение настроек и параметров безопасности с известными последствиями для каждого используемого типа системы. Для обеспечения безопасности системной конфигурации сотрудники, ответственные за настройку и (или) администрирование системных компонентов, должны быть осведомлены о конкретных параметрах безопасности и настройках, применимых к системе.
	2.2.4.b Изучите стандарты конфигурации и убедитесь, что они включают основные параметры безопасности.	
	2.2.4.c Сделайте выборку системных компонентов и убедитесь, что основные параметры безопасности установлены соответствующим образом и согласно стандартам конфигурации.	
2.2.5 Удалять из системы весь неиспользуемый функционал: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы и ненужные для работы веб-серверы.	**2.2.5.a** Сделайте выборку системных компонентов, изучите конфигурации и убедитесь, что неиспользуемый функционал (например, сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы и т.д.) удален.	Неиспользуемые функции могут предоставить злоумышленникам дополнительные возможности для получения доступа к системе. Удаление ненужного функционала позволит организации сконцентрироваться на защите только необходимых функций и снизить риск использования неизвестных функций злоумышленниками. Включение этого требования в стандарты и процессы укрепления сервера позволит устранить риски связанные с неиспользуемыми функциями (например, удаление/отключение FTP или веб-сервера, если сервер не будет выполнять свои функции).
	2.2.5.b. Изучите документацию и параметры безопасности и проверьте, что включенные функции документированы и поддерживают безопасную конфигурацию.	
	2.2.5.c. Изучите документацию и параметры безопасности и убедитесь, что в выборке системных компонентов присутствует только документированная функциональность.	
2.3 При использовании неконсольного административного доступа к системе шифровать канал с использованием стойких криптографических алгоритмов.	**2.3** Сделайте выборку системных компонентов и убедитесь, что канал неконсольного административного доступа зашифрован выполняя следующее:	Если при неконсольном (в т.ч. удаленном) администрировании не используется безопасная аутентификация и шифрование канала, существует возможность перехвата злоумышленником конфиденциальной информации и информации операционного уровня (например, имен и паролей администратора). Злоумышленник может использовать эту информацию для проникновения в сеть, получения прав администратора и кражи данных.
	2.3.a Пронаблюдайте за входом администратора в каждую систему и изучите системные конфигурации для того, чтобы подтвердить активизацию механизмов шифрования до запроса пароля администратора.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	2.3.b Проверьте сервисы и файлы параметров на системах и убедитесь, что Telnet и другие небезопасные протоколы удаленного доступа к системе не доступны для неконсольного доступа.	Протоколы, которые передают информацию в открытом виде (например, HTTP, Telnet и т.д.), не используют шифрование трафика или учетных данных, упрощая перехват этой информации злоумышленником.
	2.3.c Пронаблюдайте за входом администратора в каждую систему чтобы убедиться, что административный доступ к любому веб-интерфейсу управления зашифрован с использованием стойкой криптографии.	Под использованием «стойкой криптографии (стойких криптографических алгоритмов)» понимается использование признанных в отрасли протоколов с надлежащей стойкостью ключей и процессами управления ключами в рамках используемых технологий удаленного доступа. (см. определение термина «стойкая криптография» в документе «PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms» (Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS) и в промышленных стандартах и рекомендациях, таких как NIST SP 800-52 и SP 800-57, OWASP и пр.). ***Примечание:*** *Протокол SSL/ранняя версия TLS не считаются стойкой формой криптографии и не должны быть использованы в качестве средства контроля безопасности. Исключение составляют POS POI терминалы, для которых получено подтверждение того, что на них не оказывают влияния известные эксплойты и точки подключения, к которым они подключены, как указано в Приложении A2.*
	2.3.d Ознакомьтесь с документацией производителя и опросите сотрудников чтобы убедиться, что используются надежные криптографические алгоритмы в соответствии с последними отраслевыми стандартами и (или) рекомендациями поставщиков.	
2.4 Вести журнал учета системных компонентов, которые входят в область применения стандарта PCI DSS.	**2.4.a** Проверьте журнал учета систем, чтобы убедиться, что список программных и аппаратных компонентов ведется и содержит описание функции/применения для каждого из них.	Наличие актуального списка системных компонентов позволяет организации точно и эффективно определить область внедрения средств контроля PCI DSS. Без журнала учета есть риск того, что некоторые системные компоненты будут забыты или случайно исключены из стандартов конфигурации организации.
	2.4.b Опросите сотрудников для подтверждения того, что журнал учета поддерживается в актуальном состоянии.	

Требования PCI DSS	Проверочные процедуры	Пояснение
2.5 Гарантировать, что политики безопасности, процедуры управления учетными данными поставщиков по умолчанию и другие параметры безопасности документированы, используются и известны всем заинтересованным лицам.	**2.5** Проверьте документацию и опросите работников на предмет того, что политики безопасности, операционные процедуры управления параметрами по умолчанию, заданными производителями, и другими параметрами безопасности: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть ознакомлены и следовать политикам безопасности и повседневным операционным процедурам, чтобы гарантировать постоянный контроль над учетными данными поставщиков, настроенными по умолчанию, и другими параметрами безопасности для недопущения небезопасных конфигураций.
2.6 Поставщики услуг хостинга с общей средой должны обеспечивать безопасность данных держателей карт и сред, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным в *Приложении A1: Дополнительные требования стандарта PCI DSS в отношении поставщиков услуг совместного хостинга.*	**2.6** Выполните Проверочные процедуры **A.1.1- A.1.4**, описанные в *Приложении A1: Дополнительные требования стандарта PCI DSS в отношении поставщиков услуг совместного хостинга* для оценки соответствия таких поставщиков требованиям PCI DSS, чтобы проверить, что данные поставщики защищают размещенные у них среды и данные организаций (торгово-сервисных предприятий и поставщиков услуг).	Данное требование предназначено для хостинг-провайдеров, которые предоставляют общую среду размещения для нескольких клиентов на одном и том же сервере. Когда все данные находятся на одном и том же сервере и управление ими осуществляется из единой среды, отдельные клиенты обычно не управляют настройками этих совместно используемых серверов. Добавление клиентами небезопасных функций и скриптов влияет на защищенность сред других клиентов. Поэтому злоумышленник может, получив доступ к данным одного клиента, без труда получить доступ к данным всех остальных клиентов. См. подробные сведения о требованиях в Приложении A1.

Защита данных держателей карт

Требование 3: Защищать хранимые данные держателей карт

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

См. документ «PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms» (Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS) для определения термина «стойкая криптография» и других терминов PCI DSS.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.1 Огранивать хранение данных только необходимым минимумом. Разработать политики, процедуры и процессы хранения и уничтожения данных, которые включают, как минимум, следующие положения по хранению данных держателей карт: • Объем и сроки хранения данных должны быть ограничены в той мере, в которой это необходимо для выполнения законодательных, нормативных и/или коммерческих требований; • Определенные требования к хранению данных держателей карт; • Процессы безопасного удаления данных, хранение которых более не является необходимым; • Ежеквартальный процесс обнаружения и безопасного удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	**3.1.a** Изучите политики, процедуры и процессы хранения и уничтожения данных и убедитесь, что они включают следующие положения по хранению данных держателей карт: • Ограничение объема и сроков хранения данных в той мере, в которой это необходимо для выполнения законодательных, нормативных и/или коммерческих требований. • Определенные требования к хранению данных держателей карт; например, данные держателей карт необходимо хранить в течение срока X для выполнения Y требований). • Процессы безопасного удаления данных держателей карт, если их хранение более не является необходимым по юридическим, нормативным и коммерческим причинам. • Ежеквартальный процесс обнаружения и безопасного удаления ДДК, по которым превышены сроки хранения, установленные требованиями.	Формальная политика хранения данных определяет, какие данные необходимо хранить и где находятся эти данные, чтобы их можно было безопасно удалить, как только они станут не нужны. После авторизации разрешается хранить только номер карты (PAN) (в нечитаемом виде), дату истечения срока действия, имя держателя карты и сервисный код. Знание мест хранения данных держателей карт необходимо для их надлежащего хранения или удаления, как только они станут не нужны. Чтобы определить требования к хранению, необходимо понимать потребности бизнеса, а также знать нормативные положения, которые относятся к соответствующей отрасли и применяются к тому типу данных, которые хранятся.

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.1.b Опросите сотрудников и убедитесь, что: • Все места хранения данных держателей карт включены в процессы хранения и удаления данных. • Реализован ежеквартальный процесс обнаружения и безопасного удаления данных держателей карт, проводимый вручную или автоматически. • Этот ежеквартальный процесс реализуется вручную или автоматически во всех местах хранения данных держателей карт.	
	3.1.c Для выборки системных компонентов, хранящих данные держателей карт, необходимо: • Проверить файлы и системные записи и убедиться, что сроки хранения данных не превышают сроки, определенные политикой хранения данных. • Проверить механизм удаления и убедиться, что данные удаляются безопасным образом.	Обнаружение и удаление хранящихся данных с истекшим сроком хранения позволяет предотвратить хранение данных, которые больше не требуются. Данный процесс может проводиться автоматически, вручную или полуавтоматически. Например, можно проводить процедуру обнаружения и удаления данных по расписанию (автоматически или вручную) и (или) проверку мест хранения данных вручную. Внедрение методов безопасного удаления данных гарантирует, что данные невозможно будет восстановить, когда они больше не нужны. ***Важно! Если данные вам не нужны, не храните их!***

Требования PCI DSS	Проверочные процедуры	Пояснение
3.2 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). В случае получения критичных аутентификационных данных, следует сделать все данные невосстановимыми до завершения процесса авторизации. *Эмитентам и компаниям, которые оказывают услуги эмиссии, разрешается хранить критичные аутентификационные данные, если выполняются следующие условия:* • *Имеется производственная необходимость и* • *Данные хранятся безопасно.* К критичным аутентификационным данным относятся данные, перечисленные в требованиях 3.2.1 - 3.2.3.	**3.2.a** В отношении эмитентов и/или компаний, которые выполняют услуги эмиссии и хранят критичные аутентификационные данные, изучите политики и опросите сотрудников, чтобы убедиться, что существует задокументированное служебное обоснование для хранения критичных аутентификационных данных . **3.2.b** В отношении эмитентов и/или компаний, которые выполняют услуги эмиссии и хранят критичные аутентификационные данные, изучите центры обработки данных и системные конфигурации, чтобы убедиться, что критичные аутентификационные данные надежно защищены. **3.2.c** В отношении других организаций, если они получают критичные аутентификационные данные, ознакомьтесь с политиками и процедурами, и проверьте системные конфигурации, чтобы убедиться, что данные не сохраняются после авторизации. **3.2.d** В отношении других организаций, если они получают критичные аутентификационные данные, ознакомьтесь с процедурами и изучите процесс безопасного удаления данных, чтобы убедиться, что данные не подлежат восстановлению.	Критичные аутентификационные данные состоят из полных данных дорожки, проверочных параметров или значений карты, и данных ПИН-кода. Хранить критичные аутентификационные данные после авторизации запрещается! Эти данные представляют интерес для злоумышленников, поскольку позволяют им генерировать поддельные платежные карты и осуществлять мошеннические операции. Эмитенты платежных карт или компании, предоставляющие услуги эмиссии или поддерживающие этот процесс, часто создают и контролируют критичные аутентификационные данные в рамках процесса эмиссии. Компании, которые занимаются выпуском платежных карт или поддерживают этот процесс, могут хранить критичные аутентификационные данные ТОЛЬКО В ТОМ СЛУЧАЕ, если у них есть обоснованная потребность в хранении таких данных. Важно отметить, что все требования стандарта PCI DSS применяются к эмитентам, и единственное исключение для эмитентов и их процессинговых центров заключается в том, что они могут хранить критичные аутентификационные данные, если у них есть для этого обоснованная причина. Под обоснованной причиной понимается такая причина, в силу которой необходимо выполнять определенную функцию для эмитента, а не та, которая обосновывается удобством. Любые такие данные должны храниться безопасно, в соответствии с требованиями стандарта PCI DSS и требованиями платежных систем. Организациям, не осуществляющим эмиссию, запрещается сохранять критичные аутентификационные данные после аутентификации.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.2.1 Запрещается хранить полное содержимое любой дорожки (данные магнитной полосы на обороте карты, аналогичные данные с чипа или данные хранимые иным образом). Эти данные также называются «данные полной дорожки», «данные дорожки», «данные дорожки 1», «данные дорожки 2» и «данные магнитной полосы». ***Примечание:*** *В рабочем порядке может потребоваться сохранение следующих элементов данных с магнитной дорожки:* • *Имя держателя карты* • *Номер карты (PAN)* • *Дата истечения срока действия карты* • *Сервисный код.* *В целях минимизации риска храните только эти элементы данных, если это требуется в производственных целях.*	**3.2.1** Проверьте источники данных в выборке системных компонентов, включая, в том числе, перечисленные ниже, и убедитесь, что полные данные любой дорожки магнитной полосы, находящейся на обратной стороне карты (или ее аналог на чипе), не сохраняются после авторизации: • Входящие данные о транзакции. • Все журналы регистрации событий (журналы транзакций, журналы истории, журналы отладки, журналы ошибок). • Файлы истории. • Файлы трассировки. • Несколько схем баз данных. • Содержимое баз данных.	Если полные данные дорожки сохранены, злоумышленник, получивший доступ к этим данным, может использовать их для воспроизведения платежных карт и осуществления мошеннических транзакций.
3.2.2 Запрещается хранить проверочный код карты или проверочное значение (трех- или четырехзначное число, изображенное на лицевой или обратной стороне карты, и используемое в операциях без предъявления карты), после авторизации.	**3.2.2** Проверьте источники данных в выборке системных компонентов, включая, в том числе, перечисленные ниже, и убедитесь, что трех- или четырехзначный проверочный код или проверочное значение, изображенное на лицевой стороне карты или на месте для подписи (данные CVV2, CVC2, CID, CAV2), не сохраняются после авторизации: • Входящие данные о транзакции. • Все журналы регистрации событий (журналы транзакций, журналы истории, журналы отладки, журналы ошибок). • Файлы истории. • Файлы трассировки. • Несколько схем баз данных. • Содержимое баз данных.	Назначение кода проверки подлинности карты состоит в защите операций без предъявления карты (например, при заказе товаров через Интернет, по почте или по телефону (mail order/telephone order - MO/TO)), в которых покупатель и карта физически не присутствуют. В случае кражи этих данных, злоумышленник получит возможность совершения мошеннических операций через Интернет, по почте или телефону.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.2.3 Запрещается хранить персональный идентификационный номер (ПИН) или зашифрованный ПИН-блок после авторизации.	**3.2.3** Проверьте источники данных в выборке системных компонентов, включая, в том числе, перечисленные ниже, и убедитесь, что персональные идентификационные номера (ПИН) или зашифрованные ПИН-блоки не сохраняются после авторизации: • Входящие данные о транзакции. • Все журналы регистрации событий (журналы транзакций, журналы истории, журналы отладки, журналы ошибок). • Файлы истории. • Файлы трассировки. • Несколько схем баз данных. • Содержимое баз данных.	Данные значения должны быть известны только владельцу карты или банку, который выпустил карту. В случае кражи этих данных у злоумышленника появится возможность совершения мошеннических дебетовых операций с использованием ПИН-кода (например, для получения наличных через банкомат).
3.3 Маскировать основной номер держателя карты (PAN) при его отображении (максимально возможное количество цифр для отображения - первые шесть и последние четыре), чтобы только сотрудники с обоснованной служебной необходимостью могли видеть больше чем первые шесть и последние четыре цифры PAN. ***Примечание**: Это требование не заменяет собой иные более строгие требования к отображению данных держателей карт (например, юридические требования или требования платежных систем к чекам POS-терминалов).*	**3.3.a** Изучите письменные политики и процедуры маскирования основного номера держателя карты (PAN) при его отображении и убедитесь, что: • Список ролей, которым требуется доступ к полному PAN, документирован, и для каждой роли есть обоснованная служебная необходимость такого доступа. • PAN должен маскироваться при отображении, так что полный PAN виден только тем сотрудникам, у которых на это есть служебная необходимость. • Для всех остальных ролей, которым явным образом не разрешено видеть полный PAN, должен быть виден только маскированный PAN. **3.3.b** Проверьте системные конфигурации и убедитесь, что PAN отображается только для пользователей/ролей с задокументированной служебной необходимостью и маскируется для всех остальных запросов.	Отображение полного PAN на экранах компьютеров, чеках об оплате по платежным картам, факсах или в бумажных отчетах может привести к тому, что эти данные станут известны неавторизованным лицам и могут быть использованы в мошеннических целях. Отображение полного основного номера держателя карты только для тех лиц, у которых есть на то служебная необходимость, позволяет снизить риск несанкционированного доступа к данным этого номера. Принцип маскировки должен всегда обеспечивать отображение только минимального количества цифр номера, требуемого для выполнения необходимой служебной функции. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.3.c Проверьте, как отображаются PAN (например, на бумажных чеках или экране монитора) и убедитесь, что PAN маскируются при отображении данных держателя карты, и только сотрудники с обоснованной служебной необходимостью могут видеть весь PAN.	Например, если для выполнения какой-либо служебной функции необходимы только последние четыре цифры номера, маскируйте основной номер держателя карты так, чтобы сотрудник, выполняющий эту операцию, видел только последние четыре цифры. Также, если для выполнения функции требуется доступ к банковскому идентификационному номеру (БИН) для целей маршрутизации, при выполнении такой операции снимайте маскировку только с номера БИН (обычно первые шесть цифр). Это требование касается защиты основного номера держателя карты, *отображаемого* на экранах, бумажных чеках, распечатках и т.д., и его следует отличать от Требования 3.4, которое касается защиты полного номера держателя карты при его *хранении* в файлах, базах данных и т.д.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.4 Приводить PAN в нечитаемый вид во всех местах хранения (включая портативные цифровые носители, резервные носители данных и журналы событий), используя любой из следующих методов: • Однонаправленная хеш-функция, основанная на стойкой криптографии (хэш должен вычисляться от всего PAN). • Усечение (хеширование не может использоваться для замещения усеченного сегмента PAN). • Использование индексных токенов и шифровальных блокнотов (блокноты должны быть защищены). • Стойкие криптографические алгоритмы и связанные с ними процессы и процедуры - управления ключами. ***Примечание:*** *При наличии доступа одновременно к усеченному и хешированному PAN для злоумышленника не составит большого труда восстановить данные исходного PAN. Если усеченное и хешированное значение одного и того же PAN содержатся внутри среды какой-либо организации, необходимо ввести дополнительные средства контроля, чтобы не допустить сопоставления усеченных и хешированных значений для восстановления исходного PAN.*	**3.4.a** Изучите документацию о системе, используемую для защиты основного номера держателя карты, в том числе информацию о ее производителе, типе системы/процедуры, применяемых алгоритмах шифрования (если они используются), и убедитесь, что основной номер держателя карты приводится в нечитаемый вид с помощью одного из следующих методов: • Однонаправленная хеш-функция, основанная на стойкой криптографии. • Усечение. • Использование индексных токенов и шифровальных блокнотов (блокноты должны быть защищены). • Стойкая криптография совместно с процессами и процедурами управления ключами. **3.4.b** Изучите несколько таблиц или файлов из выборки хранилищ данных и убедитесь, что PAN представлен в нечитаемом виде (т. е. не хранится в открытом виде). **3.4.c** Изучите выборку съемных носителей (например, кассеты с резервными копиями данных) и убедитесь, что PAN представлен в нечитаемом виде. **3.4.d** Изучите выборку журналов регистрации событий, включая журналы регистрации платежных приложений, и убедитесь, что PAN из них удален или представлен в них в нечитаемом виде.	Все номера PAN, которые хранятся в основных хранилищах (базах данных, неструктурированных файлах, таких как текстовые файлы, таблицы и т.д.), а также во вспомогательных хранилищах (резервных копиях, журналах регистрации событий, журналах исключений и устранения неисправностей и т.д.), должны быть защищены. Для приведения данных держателей карт к нечитаемому виду можно использовать однонаправленные хеш-функции, основанные на стойкой криптографии. Использование хеширования целесообразно тогда, когда нет необходимости в восстановлении исходного номера (так как однонаправленная хеш-функция является необратимой). Желательно, но не обязательно добавлять случайное значение к данным держателей карт перед хешированием, чтобы снизить вероятность сравнения данных (и получения основного номера держателя карты) с таблицами предварительно подсчитанных значений хеша. Целью использования усечения является полное удаление части основного номера держателя карты таким образом, чтобы хранилась только его часть (не больше шести первых и четырех последних цифр). Индексный токен — это криптографический токен, который заменяет номер карты на основании заданного индекса для непредсказуемого значения. Одноразовый блокнот — это система, в которой закрытый ключ, сгенерированный случайным образом, используется только один раз для шифрования сообщения, которое затем расшифровывается с помощью соответствующего одноразового блокнота и ключа.

Требования PCI DSS	Проверочные процедуры	Пояснение
	3.4.e Если усеченное и хешированное значение одного и того же PAN содержатся внутри среды, изучите используемые средства контроля, чтобы убедиться, что хешированные и усеченные значения не могут быть сопоставлены для восстановления исходного PAN	Назначение стойкой криптографии (см. определение в документе «PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms» (Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS)) заключается в том, что шифрование основывается на использовании проверенных стандартизованных алгоритмов с высокой стойкостью ключей шифрования (а не собственных алгоритмов). Посредством сопоставления хешированных и усеченных версий PAN злоумышленник может без труда узнать оригинальный номер PAN. Средства контроля, которые используются для предотвращения сопоставления этих данных, помогут обеспечить нечитаемость исходного номера PAN.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.4.1 Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или столбцов базы данных), то управление логическим доступом должно осуществляться отдельно и независимо от механизмов аутентификации и контроля доступа операционной системы (например, не используются локальные базы данных учетных записей или основные учетные данные для входа в сеть). Ключи дешифрования не должны быть связаны с учетными записями пользователей. ***Примечание:*** *Это требование дополнительно применяется ко всем другим требованиям относительно типов шифрования и управления ключами в стандарте PCI DSS.*	**3.4.1.a** Если применяется шифрование на уровне диска, изучите конфигурацию и проследите за процессом аутентификации, чтобы убедиться, что логический доступ к зашифрованным файловым системам реализован при помощи механизма, независимого от собственных механизмов аутентификации операционной системы (например, не используются локальные базы данных учетных записей или основные учетные данные для входа в сеть). **3.4.1.b** Изучите процессы и опросите персонал, чтобы убедиться, что криптографические ключи хранятся безопасно (например, на съемном носителе, который защищен соответствующими процедурами контроля доступа). **3.4.1.c** Изучите конфигурации и процессы, чтобы убедиться, что данные держателей карт на съемных носителях хранятся только в зашифрованном виде. ***Примечание:*** *Если шифрование диска не используется для шифрования съемных носителей, данные на съемных носителях должны быть приведены в нечитаемый вид с использованием других методов.*	Назначение данного требования состоит в определении условий к использованию шифрования на уровне диска для приведения данных держателей карт в нечитаемый вид. При шифровании на уровне диска шифруется весь жесткий диск/раздел компьютера, а информация автоматически расшифровывается при запросе авторизованным пользователем. Многие решения для шифрования дисков перехватывают операции чтения/записи операционной системы и выполняют соответствующие криптографические преобразования, не требуя каких-либо дополнительных действий со стороны пользователя, за исключением ввода пароля или кодовой фразы в начале сеанса или при запуске системы. С учетом данных характеристик шифрования на уровне диска, чтобы соответствовать данному требованию, метод шифрования не должен: 1) Использовать то же имя пользователя, которое используется для аутентификации в операционной системе, или 2) Использовать ключ дешифрования, связанный или взятый из локальных баз данных учетных записей или общих учетных данных для входа в сеть. Полное шифрование диска помогает защитить данные в случае физической утраты диска и, следовательно, может быть полезно для портативных устройств, содержащих данные держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5 Задокументировать и внедрить процедуры для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования следующим образом: ***Примечание:*** *Это требование применяется к ключам шифрования данных держателей карт, а также для шифрования ключей, которые используются для защиты ключей шифрования данных. Такие ключи должны обладать таким же уровнем защиты, как и ключи для шифрования данных.*	**3.5** Проверьте политики и процедуры управления ключами на наличие процессов для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования, которые должны включать следующие минимальные требования: • Доступ к криптографическим ключам ограничен и разрешен наименьшему возможному числу сотрудников, ответственных за их использование и хранение. • Ключи шифрования ключей обладают таким же уровнем защиты, как и ключи шифрования данных. • Ключи шифрования ключей хранятся отдельно от ключей шифрования данных. • Ключи хранятся только в строго определенных защищенных хранилищах и строго определенном виде.	Криптографические ключи должны быть надежно защищены, поскольку лица, получившие к ним доступ, смогут расшифровать данные. Ключи для шифрования ключей (если они используются) должны обладать таким же уровнем защиты, как и ключи для шифрования данных, чтобы гарантировать надлежащую защиту ключей, которые используются для шифрования данных, и самих данных, которые шифруются с помощью этих ключей. Требование по защите ключей от раскрытия и неправильного использования применяется как к ключам для шифрования ключей, так и к ключам для шифрования данных. Поскольку один ключ для шифрования ключей может предоставить доступ ко многим ключам для шифрования данных, ключи для шифрования ключей должны быть надежно защищены.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5.1 ***Дополнительное требование только для сервис-провайдеров:*** Включить следующую информацию в описание криптографической архитектуры: • Подробную информацию обо всех алгоритмах, протоколах, и ключах, используемых для защиты данных держателей карт, включая уровень стойкости ключей и дату истечения их срока действия. • Описание сферы применения каждого ключа. • Описание любого модуля безопасности (HSM) и прочих защищенных криптографических устройств (SCD), используемых для управления ключами.	**3.5.1** Опросите ответственных сотрудников и изучите документацию, чтобы убедиться, что в наличии имеется документ, описывающий криптографическую архитектуру и включающий: • Подробную информацию обо всех алгоритмах, протоколах, и ключах, используемых для защиты данных держателей карт, включая уровень стойкости ключей и дату истечения их срока действия. • Описание сферы применения каждого ключа. • Описание любого модуля безопасности (HSM) и прочих защищенных криптографических устройств (SCD), используемых для управления ключами.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Поддержание в актуальном состоянии документации, описывающей архитектуру используемого криптографического решения, дает организации возможность понять, какие алгоритмы, протоколы и криптографические ключи, используются для защиты данных держателей карт так же, как и устройства, которые генерируют, используют и защищают ключи. Это позволяет организации быть в курсе новых угроз для используемой криптографической архитектуры, позволяя планировать обновления из-за меняющихся уровней стойкости различных алгоритмов/ключей. Ведение указанной документации, помимо прочего, позволяет организации выявить потерянные или отсутствующие ключи или устройства управления ключами, и обнаружить ранее не идентифицированные дополнения в своей архитектуре криптографического решения.
3.5.2 Ограничить доступ к криптографическим ключам. Разрешать доступ к таким ключам наименьшему возможному числу сотрудников, ответственных за криптографические ключи.	**3.5.2** Изучите списки доступа и убедитесь, что доступ к ключам предоставлен наименьшему возможному числу сотрудников, ответственных за хранение и использование таких ключей.	Необходимо максимально уменьшить количество лиц, имеющих доступ к ключам шифрования. Обычно это лица, отвечающие за хранение ключей. Это позволит снизить вероятность разглашения данных держателей карт неуполномоченным лицам.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.5.3 Хранить секретные и закрытые ключи для шифрования/дешифрования данных держателей карт, в одной (или нескольких) из следующих форм: • Зашифрованными с использованием ключа шифрования криптографических ключей, который имеет такой же уровень стойкости, как и криптографический ключ для шифрования данных, и хранящийся отдельно от этого ключа. • Внутри защищенного криптографического устройства (такого, как аппаратный модуль безопасности (HSM) или одобренное по PCI PTS устройство точки обслуживания). • В форме как минимум двух компонентов полноразмерного ключа или части разделяемого ключа (секрета) в соответствии с принятым в отрасли методом. ***Примечание:*** *Хранение публичных ключей в одной из этих форм не требуется.*	**3.5.3.a** Изучите процедуры, чтобы убедиться, что криптографические ключи для шифрования/дешифрования данных держателей карт хранятся исключительно в одной (или нескольких) из следующих форм: • Зашифрованными с использованием ключа шифрования криптографических ключей, который имеет такой же уровень стойкости, как и криптографический ключ для шифрования данных, и хранящийся отдельно от этого ключа. • Внутри защищенного криптографического устройства (такого, как аппаратный модуль безопасности (HSM) или одобренное по PCI PTS устройство точки обслуживания). • В форме компонентов ключа или части разделяемого ключа (секрета) в соответствии с принятым в отрасли методом.	Криптографические ключи должны храниться безопасно для предотвращения несанкционированного или ненужного доступа, который может привести к разглашению данных держателей карт. Это требование не подразумевает, что ключи для шифрования должны быть зашифрованы, но они должны быть защищены от раскрытия и неправильного использования в соответствии с требованием 3.5. В случае использования ключей для шифрования ключей, их хранение отдельно от ключей для шифрования данных (в физически и (или) логически отдельных местах) снижает риск несанкционированного доступа к тем и другим ключам.
	3.5.3.b Изучите конфигурации системы и места хранения ключей, чтобы убедиться, что криптографические ключи для шифрования/дешифрования данных держателей карт хранятся исключительно в одной (или нескольких) из следующих форм: • Они зашифрованы ключом для шифрования ключей. • Внутри защищенного криптографического устройства (такого, как аппаратный модуль безопасности (HSM) или одобренное по PCI PTS устройство точки обслуживания). • В форме компонентов ключа или части разделяемого ключа (секрета) в соответствии с принятым в отрасли методом.	
	3.5.3.c В каком бы варианте ключи для шифрования ключей ни использовались, изучите системные конфигурации и места хранения ключей и убедитесь в том, что: • Ключи шифрования ключей обладают таким же уровнем защиты, как и ключи шифрования данных. • 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.	**3.5.4** Изучите места хранения ключей и проследить за процессами, чтобы убедиться, что они хранятся в как можно меньшем количестве мест.	Хранение криптографических ключей в как можно меньшем количестве мест помогает организации отслеживать и осуществлять мониторинг всех мест хранения ключей и снижает вероятность разглашения ключей посторонним лицам.
3.6 Документировать в полной мере и применять все процессы и процедуры управления криптографическими ключами для шифрования данных держателей карт, а также: ***Примечание**: Существует множество стандартов по управлению ключами, которые доступны в различных источниках (например, стандарт Национального института стандартов и технологий США (NIST), с которым можно ознакомиться на сайте http://csrc.nist.gov).*	**3.6.a *Дополнительная проверочная процедура для сервис-провайдеров:*** Если сервис-провайдеры предоставляют клиентам ключи шифрования для передачи или хранения данных держателей карт, проверьте документацию, предоставляемую сервис-провайдерами клиентам, на наличие рекомендаций по условиям безопасной передачи, хранения и обновления ключей, в соответствии с требованиями 3.6.1-3.6.8, приведенными ниже. **3.6.b** Изучите процедуры и процессы управления ключами шифрования данных держателей карт и выполните следующее:	Способ управления криптографическими ключами представляет собой критичную часть непрерывного обеспечения безопасности посредством шифрования. Правильно организованный процесс управления ключами, вне зависимости от того, выполняется ли он вручную или автоматически в составе средства шифрования, должен соответствовать отраслевым стандартам и всем требованиям с 3.6.1 по 3.6.8. Предоставление потребителям рекомендаций по безопасной передаче, хранению и обновлению криптографических ключей, которые помогут предотвратить неправильное управление или раскрытие неавторизованным сторонам. Данное требование применяется к ключам, которые используются для шифрования данных держателей карт, и соответствующим ключам для шифрования ключей. ***Примечание:** Процедура проверки 3.6.a является дополнительной процедурой, которая применима только к сервис-провайдерам.*
3.6.1 Генерировать стойкие криптографические ключи	**3.6.1.a** Убедитесь, что процедуры управления ключами указывают, каким образом генерировать стойкие ключи. **3.6.1.b** Изучите метод создания ключей и убедитесь, что генерируются стойкие ключи.	Средство шифрования должно генерировать стойкие ключи согласно определению для термина «Создание криптографических ключей», в документе «PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms» (Глоссарий терминов, аббревиатур и сокращений PCI DSS и PA-DSS)). Использование стойких ключей шифрования значительно повышает уровень безопасности зашифрованных данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6.2 Безопасно распространять ключи шифрования	**3.6.2.a** Убедитесь, что процедуры управления ключами указывают, как безопасным образом распространять ключи.	Средство шифрования должно обеспечивать безопасное распространение ключей (то есть ключи не должны распределяться в открытом виде), и только среди ответственных за их хранение и использование сотрудников в соответствии с требованием 3.5.2.
	3.6.2.b Изучите метод распространения ключей и убедитесь, что ключи распространяются безопасно.	
3.6.3 Безопасно хранить ключи шифрования	**3.6.3.a** Убедитесь, что процедуры управления ключами указывают, как безопасным образом хранить ключи.	Средство шифрования должно обеспечивать безопасное хранение ключей (например, шифруя их при помощи ключа шифрования ключей). Хранение ключей без надлежащей защиты может привести к предоставлению доступа злоумышленникам, дешифрованию и разглашению данных держателей карт.
	3.6.3.b Изучите метод хранения ключей и убедитесь, что ключи хранятся безопасно.	
3.6.4 Предусмотреть процедуры замены криптографических ключей с истекшим криптопериодом (например, когда истек установленный срок и (или) после того, как с помощью данного ключа было создано определенное количество шифротекстов), как установлено соответствующим производителем приложений или владельцем ключа на основании отраслевых рекомендаций и руководств (например, специальная публикация NIST 800-57).	**3.6.4.a** Убедитесь, что процедуры управления ключами устанавливают криптопериод для каждого типа ключей, а также процесс их изменения по завершении установленного криптопериода (криптопериодов).	Криптопериод — это период времени, в течение которого криптографический ключ можно использовать по его назначению. При определении криптопериода необходимо учитывать, как минимум: стойкость используемого алгоритма, размер или длину ключа, риск компрометации ключа и критичность данных, зашифрованных с помощью ключа. Периодическая смена ключей шифрования, достигших конца криптопериода, является обязательной для минимизации рисков несанкционированного получения ключей шифрования и последующего дешифрования данных.
	3.6.4.b Опросите сотрудников и убедитесь, что ключи заменяются по завершении установленного криптопериода (криптопериодов).	

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6.5 Заменять ключи или удалять их (например, путем архивирования, уничтожения и (или) отзыва) по мере необходимости, при нарушении целостности (например, увольнение сотрудника, обладающего компонентой ключа в открытом виде), либо в случае, когда в отношении ключей существует подозрение в компрометации. ***Примечание:*** *Если существует необходимость сохранения изъятых из обращения или замененных криптографических ключей, они должны быть безопасно заархивированы (например, с использованием ключа шифрования ключей). Помещенные в архив криптографические ключи должны использоваться только в целях дешифрования/проверки.*	**3.6.5.a** Изучите процедуры управления ключами и убедитесь, что в них предусмотрены следующие процессы: • Изъятие либо замена ключей в случае нарушения целостности. • Замена ключей шифрования, которые были или могли быть скомпрометированы. • Проверка того, что удаленные или замененные ключи не используются для операций шифрования. **3.6.5.b** Опросите сотрудников и убедитесь в том, что внедрены следующие процессы: • Изъятие либо, при необходимости, замена ключей в случае нарушения целостности, включая увольнение сотрудника, обладающего информацией о ключе. • Замена ключей шифрования, которые были или могли быть скомпрометированы. • Проверка того, что удаленные или замененные ключи не используются для операций шифрования.	Ключи, которые больше не используются или в которых нет необходимости, а также ключи, относительно которых существуют подозрения в компрометации, должны быть изъяты и (или) уничтожены, чтобы исключить возможность их использования. Если требуется хранение таких ключей (например, для поддержки архивированных зашифрованных данных), то они должны быть надежно защищены. Средство шифрования должно обеспечивать возможность смены ключей, которые необходимо заменить или относительно которых существуют подозрения в компрометации.
3.6.6 Если процедуры управления ключами шифрования в открытом виде осуществляются вручную, данные процедуры должны координироваться с использованием принципа разделения знания и двойного контроля. ***Примечание:*** *Примеры процедур ручного управления ключами включают, в том числе: генерацию ключа, его передачу, загрузку, хранение и уничтожение.*	**3.6.6.a** Проверьте процедуры управления открытыми ключами вручную на наличие следующих условий: • Раздельное знание, при котором как минимум двое людей владели компонентами одного ключа, и каждый из них знал только свой компонент ключа; И • Двойной контроль, чтобы требовалось как минимум два человека для выполнения любых операций по управлению ключами и чтобы один из таких людей не обладал бы доступом к аутентификационным данным (например, паролям или ключам) другого. **3.6.6.b** Опросите сотрудников и (или) изучите процессы, чтобы убедиться, что процедуры ручного управления открытыми ключами предусматривают следующее: • Разделенное знание; и • Двойной контроль.	Разделенное знание и двойной контроль за ключами используются для исключения возможности того, что один человек получит доступ к целому ключу. Такой метод контроля обычно применяется для систем шифрования с ручным вводом ключа шифрования или в средствах шифрования, где управление ключами не реализовано. Разделенное знание — это метод, при использовании которого двое или более людей раздельно владеют компонентами одного ключа; каждый из этих людей знает только свой компонент ключа, а отдельные компоненты не дают знания всего ключа шифрования. Двойной контроль требует наличия двух или более людей для выполнения такой функции, при этом ни один из них не имеет доступа к учетным данным другого.

Требования PCI DSS	Проверочные процедуры	Пояснение
3.6.7 Исключить несанкционированную замену криптографического ключа.	**3.6.7.a** Убедитесь, что процедуры управления ключами определяют процессы для защиты от неавторизованной замены ключей.	Средство шифрования не должно допускать или принимать замену ключей, инициированную неавторизованными источниками или неожиданными процессами.
	3.6.7.b Опросите сотрудников и (или) проследите за процессами, чтобы убедиться в наличии защиты от неавторизованной замены ключей.	
3.6.8 Обеспечивать официальное подтверждение сотрудниками, ответственными за хранение и использование ключей, их согласия с ознакомлением и принятием таких обязанностей.	**3.6.8.a** Убедитесь, что процедуры управления ключами включают процессы признания (в письменном или электронном виде) сотрудниками, ответственными за хранение и использование ключей, того, что они понимают и принимают свои обязанности.	Этот процесс поможет гарантировать исполнение сотрудниками, ответственными за хранение и использование ключей, своей работы, а также понимание и согласие со своими обязанностями.
	3.6.8.b Изучите документацию или иные свидетельства того, что сотрудники, ответственные за хранение и использование ключей, подтвердили (в электронном виде или письменно), что понимают и принимают свои обязанности.	
3.7 Гарантировать, что политики безопасности и процедуры защиты данных держателей карт документированы, используются и известны всем заинтересованным лицам.	**3.7** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и рабочие процедуры защиты хранимых данных держателей карт: • задокументированы; • используются, • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур, обеспечивающих надежное хранение данных держателей карт на постоянной основе.

Требование 4: Шифровать данные держателей карт при их передаче в открытых общедоступных сетях

Критичная информация должна быть зашифрована при ее передаче через общедоступные сети, в которых злоумышленники могут получить к ней доступ. Неправильно сконфигурированные беспроводные сети и уязвимости, связанные с использованием устаревших протоколов шифрования и аутентификации, остаются легкими целями для злоумышленников, которые могут использовать их для получения привилегированного доступа к среде данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
4.1 Использовать стойкую криптографию и протоколы безопасности для защиты конфиденциальных данных держателей карт при их передаче в открытых общедоступных сетях, с учетом следующего: • Принимаются только доверенные ключи и сертификаты. • Используемый протокол поддерживает только безопасные версии и конфигурации. • Стойкость шифрования соответствует используемой методологии шифрования. *К примерам общедоступных сетей относятся, помимо прочего:* • *Интернет;* • *беспроводные технологии, включая протоколы 802.11 и Bluetooth;* • *технологии сотовой связи, например GSM, CDMA;* • *GPRS;* • *Спутниковые средства связи.*	**4.1.a** Выявите все места, где осуществляется прием или передача ДДК через открытые общедоступные сети. Проверьте документированные стандарты и сравнить их с системными конфигурациями, чтобы подтвердить, что везде используются протоколы безопасности и стойкое шифрование.	Критичные данные должны шифроваться при передаче по сетям общего пользования, потому что злоумышленник может перехватить и (или) изменить их маршрут при передаче. Безопасная передача данных держателей карт требует использования доверенных ключей/сертификатов, безопасного протокола передачи и шифрования достаточной стойкости для шифрования данных держателей карт. Не следует принимать запросы на подключение от систем, которые не поддерживают требуемую стойкость шифрования, и подключение к которым будет небезопасно. Обратите внимание на то, что некоторые версии протоколов (например, SSL, SSH v1.0 и ранняя версия TLS) содержат известные уязвимости, которые могут быть использованы злоумышленником для получения контроля над уязвимой системой. Независимо от того, какой протокол используется, убедитесь, что он настроен для использования только безопасных версий и конфигураций. Например, установлено использование только доверенных сертификатов и поддержка только стойкого шифрования (не поддерживая слабые, ненадежные протоколы или методы). Проверка того, что сертификат является доверенным (например, того факта, что срок его
	4.1.b Изучите документированные политики и процедуры и убедитесь, что они содержат следующие процессы, предусматривающие: • Прием только доверенных ключей и (или) сертификатов. • Поддержку используемых протоколов только безопасных версий и конфигураций (небезопасные версии или конфигурации не поддерживаются). • Применение шифрования достаточной стойкости согласно используемой методологии шифрования.	
	4.1.c Выберите и изучите выборку входящих и исходящих транзакций (например, путем изучения системных процессов или сетевого трафика), чтобы убедиться, что данные держателей карт передаются в зашифрованном виде с использованием стойкого алгоритма шифрования.	
	4.1.d Изучите ключи и сертификаты, и убедитесь, что принимаются только доверенные ключи и (или) сертификаты.	
	4.1.e Изучите системные конфигурации, и убедитесь, что в рамках протокола используются только безопасные конфигурации и не поддерживаются небезопасные версии и конфигурации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	4.1.f Изучите системные конфигурации и убедитесь, что для используемой методологии шифрования применяется шифрование достаточной стойкости. (См. рекомендации производителя и (или) лучшие практики).	действия не истек, и он получен из доверенного источника), помогает обеспечить целостность безопасного подключения.
	4.1.g При использовании протокола TLS следует изучить системные конфигурации и убедиться, что TLS используется при каждой передаче или получении данных держателей карт. Например, для браузерных решений: • «HTTPS» указан в качестве протокола URL и • Данные держателей карт запрашиваются только в том случае, если URL-адрес содержит «HTTPS».	Как правило, URL-адрес должен начинаться с «HTTPS», а в окне веб-браузера должен быть значок замка. Многие поставщики TLS-сертификатов также предоставляют хорошо заметную печать подтверждения проверки (иногда называемую «печать безопасности», «печать безопасного сайта» или «печать доверия»), по которой можно щелкнуть для просмотра информации о веб-сайте. Информацию по стойкому шифрованию и безопасным протоколам можно найти в промышленных стандартах и рекомендациях (например, NISP SP 800-52 и SP 800-57, OWASP и т.д.) ***Примечание:*** *Протокол SSL/ранняя версия TLS не считаются стойкой криптографией и не должны быть использованы в качестве средства контроля безопасности. Исключение составляют POS/POI терминалы, поскольку считается, что они не подвержены никаким известным инструментам эксплуатации уязвимости, и точки подключения, к которым они подключаются, как указано в Приложении A2.*

Требования PCI DSS	Проверочные процедуры	Пояснение
4.1.1 Убедиться, что при использовании беспроводных сетей, передающих данные держателей карт либо подключенных к среде данных держателей карт, используются передовые практические методы индустрии безопасности, чтобы реализовать стойкое шифрование при аутентификации и передаче данных.	**4.1.1** Определите все беспроводные сети, передающие данные держателей карт либо подключенные к информационной среде держателей карт. Изучите документированные стандарты и сравните их с настройками системных конфигураций, чтобы убедиться, что в отношении всех обнаруженных беспроводных сетей применяется следующее: • Применяются отраслевые рекомендации для обеспечения стойкого шифрования при аутентификации и передаче данных. • Протоколы со слабым шифрованием (например, WEP, SSL) не используются в качестве протокола безопасности при аутентификации и передаче данных.	Злоумышленники используют свободно распространяемые и широкодоступные средства для прослушивания беспроводного трафика. Использование стойкой криптографии может предотвратить раскрытие критичной информации, передаваемой по беспроводной сети. Стойкая криптография для аутентификации и передачи данных держателей карт помогает предотвратить доступ злоумышленников к беспроводным сетям или использование беспроводных сетей для получения доступа к другим внутренним сетям и данным.
4.2 Запретить пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (например, электронная почта, системы мгновенного обмена сообщениями, СМС-сообщения, чаты и т.д.).	**4.2.a** В случае использования пользовательских технологий передачи ДДК изучите процесс отправки основного номера держателя карты и изучите несколько исходящих передач данных, чтобы проверить, что основной номер держателя карты передается в нечитаемом виде или защищен посредством стойких криптографических механизмов при использовании пользовательских технологий передачи сообщений.	Сообщения, передаваемые по электронной почте, с помощью систем мгновенного обмена сообщениями, в чате или через SMS, могут быть перехвачены в процессе доставки, как во внутренней, так и во внешней общедоступной сети. Не следует использовать эти средства передачи сообщений для отправки основного номера держателя карты, если они не обеспечивают стойкого шифрования. В дополнение, если организация запрашивает PAN посредством технологий обмена мгновенными сообщениями, организация должна обеспечить применение средства или метода защиты PAN с использованием стойкой криптографии или приводить PAN в нечитаемый формат до передачи.
	4.2.b Изучите задокументированные политики и проверьте наличие политики, запрещающей отправку незашифрованного основного номера держателя карты при помощи пользовательских технологий передачи сообщений.	
4.3 Гарантировать, что политики безопасности и процедуры шифрования передач данных держателей карт документированы, используются и известны всем заинтересованным лицам.	**4.3** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и рабочие процедуры шифрования передач данных держателей карт: • задокументированы; • используются; • Известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур, обеспечивающих безопасную передачу данных держателей карт на постоянной основе.

Ведение программы по управлению уязвимостями

Требование 5: Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО или программы

Большинство видов вредоносного программного обеспечения, включая вирусы, черви, трояны, проникают в сеть через разрешенные в компании виды деятельности, включающие электронную почту сотрудников, использование Интернета, съемных носителей или мобильных устройств, использование которых приводит к системным уязвимостям. Антивирусное программное обеспечение должно быть установлено на всех системах подверженных воздействию вредоносного ПО, чтобы защитить их от текущих и возможных угроз со стороны вредоносного ПО. Дополнительные решения для защиты от вредоносного ПО могут использоваться в качестве дополнения к антивирусному ПО; однако такие дополнительные решения не заменяют антивирусное ПО.

Требования PCI DSS	Проверочные процедуры	Пояснение
5.1 Разворачивать антивирусное программное обеспечение на всех системах, подверженных воздействию вредоносного ПО (особенно на рабочих станциях и серверах).	**5.1** Для выборки системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО, убедитесь, что используется антивирусная защита в случае наличия применимой антивирусной технологии.	Существует большое количество атак, использующих широко распространенные уязвимости. Их часто называют «атаками нулевого дня» (такие атаки используют *ранее* неизвестные уязвимости) и они направлены против, казалось бы, полностью защищенных систем. Без наличия регулярно обновляемого антивирусного ПО сеть подвержена воздействию новых видов вредоносного ПО, которые могут ее атаковать, нарушить ее работу или привести к компрометации данных.
5.1.1 Гарантировать, что антивирусное программное обеспечение способно обнаруживать и удалять все известные виды вредоносного программного обеспечения, а также обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	**5.1.1** Изучите документацию поставщика и конфигурации антивирусов, чтобы убедиться в том, что антивирусные программы способны: • Обнаруживать все известные виды вредоносного программного обеспечения. • Удалять все известные виды вредоносного программного обеспечения. • Обеспечивать защиту от всех известных видов вредоносного программного обеспечения. *Примерами вредоносного ПО являются вирусы, трояны, черви, 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 для выявления и оценки рисков заражения вредоносным ПО систем, которые считаются не подверженными заражению вредоносным ПО, с целью подтверждения отсутствия необходимости в антивирусном ПО.	**5.1.2** Опросите сотрудников и убедитесь, что проводятся периодические проверки для выявления и оценки рисков заражения вредоносным ПО систем, которые считаются не подверженными заражению вредоносным ПО, чтобы убедиться, что необходимость в антивирусном ПО отсутствует.	Обычно мэйнфреймы, компьютеры среднего уровня (такие как AS/400, например) и подобные системы не подвержены заражению вредоносным ПО. Однако, тенденции в области вредоносного ПО могут быстро измениться, поэтому организациям важно знать о новых видах вредоносного ПО, которые могут быть опасны для их систем. Узнать, угрожают ли системам новые виды вредоносного ПО, можно, к примеру, путем мониторинга сообщений о безопасности от поставщиков ПО и новостных групп антивирусов. Тенденции использования вредоносных программ должны быть включены в процесс выявления новых уязвимостей в системе безопасности, а методы работы с такими новыми тенденциями должны быть внедрены в стандарты конфигураций и механизмы защиты в той мере, в которой это необходимо.
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** Изучите политики и процедуры, и убедитесь, что в них содержится требование поддерживать антивирусное ПО и антивирусные базы в актуальном состоянии.	Даже лучшие антивирусы имеют ограниченную эффективность при отсутствии последних обновлений безопасности, файлов сигнатур или механизмов защиты от вредоносного ПО. Журналы регистрации событий предоставляют возможность отслеживать активность вирусов и вредоносного ПО, и то, какие действия были предприняты для защиты от вредоносного ПО. Поэтому важно настроить решения для защиты от вредоносного ПО на создание журналов регистрации событий в соответствии с Требованием 10.
	5.2.b Изучите конфигурацию антивирусов, включая эталонный образ установочного дистрибутива антивирусного ПО и убедитесь, что антивирусные механизмы: • Настроены на выполнение автоматического обновления. • Настроены на выполнение периодического сканирования.	
	5.2.c Изучите выборку системных компонентов, включая все типы операционных систем, подверженных воздействию вредоносного ПО, и убедитесь, что: • Антивирусное ПО и сигнатурные базы поддерживаются в актуальном состоянии. • Выполняется периодическое сканирование.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	5.2.d Изучите конфигурацию антивирусов, включая эталонный образ установочного дистрибутива антивирусного ПО и выборку системных компонентов и убедитесь, что: • Включено создание журналов регистрации событий. • Журналы хранятся согласно требованию 10.7 стандарта PCI DSS.	
5.3 Гарантировать, что антивирусные механизмы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени. ***Примечание:*** *Антивирусы могут быть временно отключены только в случае оправданной технической необходимости, с разрешения руководства с учетом специфики конкретного случая. Если антивирусная защита должна быть отключена для определенной цели, необходимо получить официальное разрешение. Также может понадобиться принятие дополнительных мер безопасности на период времени, в течение которого антивирусная защита будет неактивна.*	**5.3.a** Изучите конфигурацию антивирусов, включая эталонный образ установочного дистрибутива антивирусного ПО и выборку системных компонентов и убедитесь, что антивирусное ПО запущено и работает. **5.3.b** Изучите конфигурацию антивирусов, включая эталонный образ установочного дистрибутива антивирусного ПО и выборку системных компонентов, чтобы убедиться, что антивирусное ПО не может быть отключено или изменено пользователями. **5.3.c** Опросите ответственных сотрудников и изучите процессы, чтобы проверить, что антивирусные программы не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени.	Антивирус, работающий постоянно и защищенный от изменений, обеспечит надежную защиту от вредоносного ПО. Использование политик по предотвращению изменений или отключения антивирусной защиты на всех системах позволит предотвратить использование уязвимостей систем вредоносным ПО. Также может понадобиться принятие дополнительных мер безопасности на период времени, в течение которого антивирусная защита будет неактивна (например, отключение незащищенной системы от Интернета на время отключения антивирусной защиты и выполнение полного сканирования после его повторного включения).
5.4 Гарантировать, что политики безопасности и процедуры защиты систем от вредоносного ПО задокументированы, используются и известны всем заинтересованным лицам.	**5.4** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и рабочие процедуры защиты систем от вредоносного ПО: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур, обеспечивающих защиту систем от вредоносного ПО на постоянной основе.

Требование 6: Разрабатывать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости безопасности для получения привилегированного доступа к системам. Большинство из таких уязвимостей устраняется путем установки исправлений безопасности, выпускаемых производителем, которые должны быть установлены организациями, управляющими системами. На все системы должны быть установлены все необходимые обновления программного обеспечения для защиты данных держателей карт от компрометации и раскрытия путем использования уязвимостей злоумышленниками и вредоносным ПО.

Примечание: *Необходимыми являются те обновления программного обеспечения, которые были оценены и протестированы на совместимость с текущими конфигурациями безопасности. В случае самостоятельной разработки приложений множества уязвимостей удастся избежать, в случае использования стандартных процессов разработки систем и приемов безопасного программирования.*

Требования PCI DSS	Проверочные процедуры	Пояснение
6.1 Наладить процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также ранжирования риска (например, «высокий», «средний» или «низкий») недавно обнаруженных уязвимостей. ***Примечание:*** *Ранжирование рисков должно выполняться на основании лучших отраслевых практик, а также с учетом возможных последствий. Например, критерии ранжирования уязвимостей могут основываться на уровне риска по шкале CVSS и (или) классификации производителя, и (или) типе поражаемых систем.*	**6.1.a** Изучите политики и процедуры и убедитесь, что они содержат следующие процессы, предусматривающие: • Выявление новых уязвимостей. • Ранжирование уязвимостей по уровню риска, в т. ч. идентификация всех уязвимостей с «высоким» и «критичным» уровнями риска. • Использование авторитетных внешних источников информации об уязвимостях. **6.1.b** Опросите ответственных сотрудников и изучите процессы, чтобы убедиться, что: • Выявляются новые уязвимости. • Уязвимостям присваивается уровень риска, а также выполняется идентификация всех уязвимостей с «высоким» и «критичным» уровнями. • Процессы выявления новых уязвимостей системы безопасности включают в себя использование для этого внешних источников информации.	Цель данного требования состоит в том, что организации должны своевременно узнавать о новых уязвимостях, которые могут оказать влияние на их среду. Источники информации об уязвимостях должны быть достоверными и включать в себя веб-сайты поставщиков, отраслевые новостные группы, почтовые рассылки или RSS-потоки. Как только организация выявляет уязвимость, которая может оказать негативное влияние на ее среду, необходимо оценить и ранжировать риск, который представляет эта уязвимость. У организации должен быть в наличии метод оценки уязвимостей и присвоения им уровня риска на постоянной основе. Для этого недостаточно провести сканирование авторизованным поставщиком услуг сканирования (ASV) или внутреннее сканирование на наличие уязвимостей; для этого необходим процесс активного мониторинга отраслевых источников информации об уязвимостях. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
Методы оценки уязвимостей и определения уровня риска разнятся в зависимости от среды организации и стратегии оценки рисков такой организации. При ранжировании рисков должна выполняться, как минимум, идентификация всех уязвимостей с высоким уровнем риска для среды. Уязвимости считаются критическими, если они представляют неотвратимую угрозу для среды, влияют на работу важнейших систем и (или) могут привести к компрометации данных, если не будут устранены. Примерами критически важных систем могут служить системы безопасности, общедоступные устройства и системы, базы данных и другие системы, осуществляющие хранение, обработку или передачу данных держателей карт.		Ранжирование рисков (например, «высокий», «средний» или «низкий») позволяет организациям быстрее выявлять, устанавливать приоритет и устранять проблемы с высоким риском, а также минимизировать вероятность использования злоумышленниками уязвимостей, которые представляют наиболее высокий риск для системы безопасности.
6.2 Гарантировать, что все компоненты систем и ПО защищены от известных уязвимостей при помощи установки патчей безопасности, выпускаемых производителем. Устанавливать критичные исправления безопасности в течение месяца с даты их выпуска. ***Примечание:*** *Какие из исправлений безопасности считаются критичными, должно быть установлено исходя из ранжирования рисков (см. Требование 6.1).*	**6.2.a** Проверьте политики и процедуры установки исправлений безопасности на наличие следующих процессов: • Установка критичных исправлений безопасности в течение месяца с даты их выпуска. • Установка всех необходимых исправлений безопасности в течение соответствующего срока с момента выпуска поставщиком (например, в течение трех месяцев).	Существует большое количество атак, использующих широко распространенные уязвимости. Их часто называют «атаками нулевого дня» (такие атаки используют ранее неизвестные уязвимости) и они направлены против, казалось бы, полностью защищенных систем. Без своевременного внедрения актуальных исправлений безопасности на критических системах злоумышленник может использовать эти уязвимости для проведения атак на систему и нарушения ее работы или для получения доступа к критичной информации.

Требования PCI DSS	Проверочные процедуры	Пояснение
	6.2.b Для выборки системных компонентов и связанного с ними программного обеспечения сравните список исправлений безопасности, установленных на каждой системе с самым актуальным списком исправлений безопасности от производителя, чтобы убедиться, что: • Установка критичных исправлений безопасности выполнена в течение месяца с даты их выпуска. • Все необходимые исправления безопасности устанавливаются в течение соответствующего срока с момента выпуска поставщиком (например, в течение трех месяцев).	Установка приоритетов исправлений для критичной инфраструктуры обеспечивает скорейшую защиту высокоприоритетных систем и устройств от уязвимостей после выхода исправлений. Необходимо определить приоритеты установки исправлений таким образом, чтобы критичные исправления безопасности устанавливались на критичные или подверженные риску системы в течение 30 дней, а исправления с меньшим уровнем риска - в течение 2-3 месяцев. Данное требование распространяется на применимые исправления для любого установленного ПО, включая платежные приложения (и те, что сертифицированы по стандарту PA-DSS и те, что не сертифицированы).
6.3 Разрабатывать внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс) безопасным образом с соблюдением следующих требований: • Обеспечение соответствия со стандартом PCI DSS (например, предусмотрены ли безопасная аутентификация и логирование). • Приложения должны быть основаны на отраслевых стандартах и/или лучших практиках. • Учет вопросов информационной безопасности в течение всего жизненного цикла разработки ПО. ***Примечание:*** *Требование относится к любому ПО собственной разработки и заказному ПО, разработанному третьим лицом.*	**6.3.a** Изучите документированные процессы разработки ПО и убедитесь, что они основаны на отраслевых стандартах и (или) лучших практиках. **6.3.b** Изучите документацию по разработке ПО и убедитесь, что она принимает во внимание информационную безопасность в течение всего цикла разработки. **6.3.c** Изучите документацию по разработке ПО и убедитесь, что разработка программных приложений учитывает требования стандарта PCI DSS. **6.3.d** Опросите разработчиков ПО для подтверждения того, что в ходе разработки ПО используются документированные процессы.	Если не уделять должного внимания безопасности на этапах разработки ПО (определения требований, проектирования, анализа и тестирования), в производственную среду непреднамеренно или сознательно могут быть внесены уязвимости. Понимание процессов обработки критичных данных приложениями – в том числе во время хранения, передачи и пребывания в памяти – поможет упростить определение методов защиты данных.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.3.1 Удалять учетные записи разработчиков, тестовые и (или) пользовательские учетные записи, идентификаторы пользователей и пароли перед переводом приложений в производственный режим или их доступностью клиентам.	**6.3.1** Изучите задокументированные процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться в том, что все тестовые и (или) пользовательские учетные записи приложения, идентификаторы пользователей и (или) пароли удаляются перед переводом приложений в производственный режим или их доступностью клиентам.	Учетные записи разработчиков, тестовые и (или) пользовательские учетные записи приложения, идентификаторы пользователей и пароли следует удалять из производственного кода до перевода приложения в производственный режим или доступностью клиентам, поскольку эти элементы могут использоваться для получения информации о функционировании приложения. Обладая этой информацией, злоумышленники могут получить доступ к приложению и данным держателей карт.
6.3.2 Проверять написанный программный код (автоматически или вручную) на наличие потенциальных уязвимостей до запуска в производственный режим или доступностью клиентам и убеждаться, что: • Изменения в коде проверяются другими сотрудниками, которые не являются авторами кода, а также сотрудниками, знакомыми с методиками code review и принципами безопасного программирования. • Код разработан в соответствии с принципами безопасного программирования. • Необходимые корректировки вносятся до выпуска ПО. • Результаты code review рассматриваются и согласовываются с руководством до выпуска ПО. *(Продолжение на следующей странице)*	**6.3.2.a** Изучите документированные процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что в отношении всех изменений разрабатываемого программного кода должен быть выполнен контроль кода (вручную или автоматически) следующим образом: • Изменения в коде проверяются другими сотрудниками, которые не являются авторами кода, а также сотрудниками, знакомыми с методиками code review и принципами безопасного программирования. • Code review кода обеспечивает его разработку в соответствии с основными принципами безопасного программирования (см. Требование 6.5 PCI DSS). • Необходимые корректировки вносятся до выпуска ПО. • Результаты code review рассматриваются и согласовываются с руководством до выпуска ПО.	Уязвимости в написанном коде обычно используются злоумышленниками для получения доступа к сети и компрометации данных держателей карт. Опытные специалисты, знакомые с методиками code review, должны участвовать в процессе рецензирования. Для обеспечения объективной и независимой оценки code review должны выполнять лица, которые не участвовали в написании проверяемого ими кода. Автоматизированные средства или процессы могут использоваться в сочетании с контролем кода вручную, но учтите, что при использовании автоматизированных средств контроля некоторые ошибки или уязвимости в коде бывает сложно или вообще невозможно обнаружить. Исправление ошибок в коде перед публикацией клиентам или переводом его в производственный режим позволяет предотвратить потенциальное использование кода злоумышленниками. Исправить ошибки в коде после установки или переводом его в производственный режим гораздо сложнее и дороже. Проведение формальной проверки и утверждение кода руководством до выпуска позволяет гарантировать, что код одобрен и разработан в соответствии с политиками и процедурами.

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *Данное требование к code review применимо ко всему написанному коду (как внутренним, так и общедоступным системам) в рамках жизненного цикла разработки системы.* *Code review могут проводиться компетентным внутренним персоналом или третьими сторонами. Дополнительные меры по защите от появляющихся угроз и уязвимостей должны применяться к публично доступным веб-приложениям после их внедрения согласно Требованию 6.6 стандарта PCI DSS.*	**6.3.2.b** Выберите несколько недавних изменений в приложениях и проверьте, что в отношении программного кода выполняется code review согласно требованию 6.3.2.a, представленному выше.	
6.4 Соблюдать процессы и процедуры управления изменениями системных компонентов. Эти процессы должны в себя включать следующее:	**6.4** Изучите политики и процедуры на предмет наличия в них следующих требований: • Среды разработки/тестирования и производственного функционирования должны быть отделены друг от друга, и при этом должны использоваться механизмы контроля доступа. • Существует разделение обязанностей между сотрудниками, занимающимися средами разработки/тестирования ПО, и сотрудниками, занимающимися средой производственного функционирования ПО. • Производственные данные (действующие основные номера держателей карт) не используются для тестирования и разработки. • Тестовые данные и счета должны быть удалены из системы перед переводом ее в производственный режим. • Процедуры контроля изменений, относящиеся к внедрению исправлений безопасности и изменений ПО должны быть задокументированы.	Без надлежащего документирования и выполнения процесса контроля за изменениями, механизмы защиты могут быть непреднамеренно или сознательно не использоваться или быть отключены, возможно появление ошибок обработки или внедрение вредоносного кода.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.1 Отделить среды разработки/тестирования от производственных сред, а также внедрить механизмы разграничения доступа.	**6.4.1.a** Изучите документацию сети и конфигурации сетевых устройств и убедитесь, что среды разработки/тестирования и производственные среды отделены друг от друга.	Из-за постоянной изменчивости сред разработки и тестирования, такие среды обычно менее защищены, чем производственные среды. Без надлежащего разделения между средами производственная среда и данные держателей карт могут быть скомпрометированы из-за менее строгой конфигурации защиты или возможных уязвимостей в среде тестирования или разработки.
	6.4.1.b Изучите настройки контроля доступа и убедитесь, что внедрены механизмы разграничения доступа к средам разработки/тестирования и производственным средам.	
6.4.2 Разделять обязанности между сотрудниками, выполняющими обязанности разработки/тестирования, и сотрудниками, работающими в производственной среде.	**6.4.2** Понаблюдайте за процессами и опросите персонал, ответственный за среды разработки/тестирования, и персонал, ответственный за производственные среды, чтобы убедиться в том, что обязанности в средах разработки/тестирования и обязанности в производственных средах разделены.	Уменьшение количества сотрудников с доступом к производственной среде и данным держателей карт гарантирует, что доступ предоставляется только тем сотрудникам, кому он в действительности нужен для выполнения должностных обязанностей. Цель данного требования состоит в отделении функции разработки и тестирования от производственных функций. Например, разработчик может использовать учетную запись с правами уровня администратора в среде разработки и иметь отдельную учетную запись с правами доступа на уровне пользователя в производственной среде.
6.4.3 Не использовать производственные данные (действующие основные номера держателей карт) для тестирования и разработки.	**6.4.3a** Изучите процессы проведения тестирования и опросите сотрудников, чтобы убедиться в наличии процедур контроля за тем, что производственные данные (действующие основные номера держателей карт) не используются для тестирования и разработки.	В средах разработки или тестирования обычно осуществляется менее жесткий контроль за обеспечением безопасности. Использование в таких средах производственных данных позволит злоумышленникам получить неавторизованный доступ к информации, используемой в производственной среде (например, к данным держателей карт).
	6.4.3.b Изучите выборку тестовых данных и убедитесь в том, что производственные данные (действующие основные номера держателей карт) не используются для тестирования и разработки.	

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.4 Удалять все тестовые данные и учетные записи из системы перед переводом такой системы в эксплуатацию / производственный режим.	**6.4.4.a** Понаблюдайте за процессами проведения тестирования и опросите персонал, чтобы убедиться в том, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	Тестовые данные и учетные записи следует удалять перед переводом системных компонентов в производственный режим (в эксплуатацию), поскольку эти элементы могут использоваться для получения информации о функционировании приложения или системы. Владение этой информацией может облегчить компрометацию системы и соответствующих данных держателей карт.
	6.4.4.b Изучите выборку данных и учетных записей из недавно установленных или обновленных производственных систем и убедитесь в том, что все тестовые данные и учетные записи удаляются из системы перед переводом ее в производственный режим.	
6.4.5 Включить в процедуры контроля изменений следующее:	**6.4.5.a** Изучите документированные процедуры контроля изменений и убедитесь, что в них предусмотрены следующие процедуры: • Документирование влияния изменения на систему. • Документированное согласование изменений уполномоченными сторонами. • Функциональное тестирование с целью проверки отсутствия негативного влияния на безопасность системы. • Процедуры отмены изменений.	Без надлежащего управления, влияние изменений системы (обновления ПО или аппаратного обеспечения и установки исправлений безопасности) может быть оценено недостаточно полно и тем самым привести к непредусмотренным последствиям.
	6.4.5.b Сделайте выборку системных компонентов и опросите ответственных сотрудников для определения недавних изменений. Отследите эти изменения с помощью соответствующей документации по контролю изменений. Для каждого изменения нужно выполнить следующие проверки:	
6.4.5.1 Документирование влияния изменения на систему.	**6.4.5.1** Убедитесь, что влияние изменения задокументировано по каждому из выбранных изменений.	Последствия изменений должны документироваться, чтобы все вовлеченные стороны могли надлежащим образом запланировать все изменения в обработке данных.
6.4.5.2 Документированное согласование изменений уполномоченными сторонами.	**6.4.5.2** Убедитесь, что для каждого выбранного изменения есть документированное согласование от уполномоченных лиц.	Согласование от уполномоченных лиц указывает на то, что изменение является законным и санкционированным организацией.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.5.3 Проведение функционального тестирования с целью проверки отсутствия негативного влияния на безопасность системы.	**6.4.5.3.a** Проверьте, что в отношении каждого выбранного изменения проведено функциональное тестирование с целью проверки отсутствия негативного влияния на безопасность системы.	Следует выполнять тщательное тестирование для проверки того, что внедрение изменения не оказывает негативного влияния на уровень безопасности среды. Тестирование должно подтвердить, что все существующие механизмы защиты в наличии, заменяются механизмами защиты с аналогичным уровнем стойкости или усиливаются после внесения изменений в среду.
	6.4.5.3.b Для изменений программного кода убедитесь, что все обновления протестированы на соответствие требованию 6.5 PCI DSS перед их запуском в производственный режим.	
6.4.5.4 Процедуры отмены изменения.	**6.4.5.4** Убедитесь, что предусмотрены процедуры отмены для каждого изменения.	Для каждого изменения должна существовать документированная процедура отмены, которая позволит вернуть систему в первоначальное состояние в случае сбоя или неблагоприятного воздействия изменения на приложение или систему.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.4.6 По завершении значимого изменения, в отношении всех новых или измененных систем и сетей должны выполняться все соответствующие требования стандарта PCI DSS и выполняться обновление документации при необходимости.	**6.4.6** Для выборки значимых изменений, изучите записи об изменениях, опросите сотрудников и понаблюдайте за измененными системами/сетями, чтобы убедиться, что все применимые требования стандарта PCI DSS были применены и документация обновлена как часть изменений.	Наличие процессов анализа значимых изменений помогает гарантировать применение всех соответствующих стандарту PCI DSS мер защиты для любых систем или сетей, добавленных или измененных в рамках области проверяемой среды. Встраивание данной проверки в процессы управления изменениями способствует поддержанию в актуальном состоянии перечня устройств и стандартов конфигураций, а также применения защитных мер там, где это требуется. Процедура управления изменениями должна включать свидетельства, подтверждающие реализацию требований PCI DSS или их итеративное выполнение. Примеры требований стандарта PCI DSS, на которые могут повлиять изменения, включают, но не ограничиваются: • Сетевая схема обновлена и отражает изменения. • Системы настроены согласно стандартам конфигурации, с изменением всех паролей по умолчанию и отключением ненужных сервисов. • Системы защищены необходимыми механизмами (например, мониторинг целостности файлов (FIM), антивирус, исправления безопасности, ведение журналов аудита). • Подтверждение того, что критичные аутентификационные данные (SAD) не хранятся и, что все хранилища данных держателей карт задокументированы и включены в политики и процедуры хранения данных. • Новые системы включены в ежеквартальное сканирование на наличие уязвимостей.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5 Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом: • Не реже раза в год обучать разработчиков актуальным методикам безопасного программирования, включая обучение тому, как избежать распространенных программных уязвимостей. • Разрабатывать приложения в соответствии с основными принципами безопасного программирования. ***Примечание:*** *Уязвимости, перечисленные в Требованиях 6.5.1 — 6.5.10, соответствовали отраслевым рекомендациям на момент публикации данной версии стандарта PCI DSS. В случае обновления лучших мировых практик управления уязвимостями (таких как руководства OWASP, SANS CWE Top 25, CERT Secure Coding и т.д.), следует использовать их актуальную версию в отношении указанных требований.*	**6.5.a** Изучите политики и процедуры разработки ПО и убедитесь, что разработчики обязаны как минимум ежегодно проходить обучение актуальным методикам безопасного программирования в соответствии с известными отраслевыми рекомендациями и руководствами. **6.5.b** Изучите документацию об обучении и убедитесь, что разработчики не реже раза в год проходят обучение актуальным методикам безопасного программирования, в том числе тому, как избежать распространенных программных уязвимостей. **6.5.c** Убедитесь, что предусмотрены процедуры защиты приложений, по меньшей мере, от следующих уязвимостей:	Уровень приложений подвержен высокому риску и может являться целью как внутренних, так и внешних угроз. Требования 6.5.1 — 6.5.10 представляют собой минимально необходимые меры безопасности, и организации должны внедрять те методики безопасного программирования, которые применимы к определенным технологиям в их среде. Разработчики приложений должны проходить надлежащее обучение определению и устранению проблем, связанных с этими и другими распространенными уязвимостями программного кода. Осведомленность персонала о правилах безопасного программирования позволит свести к минимуму количество уязвимостей, связанных с низким качеством кода. Обучение разработчиков может осуществляться как самой организацией, так и третьими лицами и должно касаться используемой технологии. Общепризнанные отраслевые методики безопасного программирования меняются со временем, поэтому методики программирования и обучения разработчиков в организации также должны обновляться для соответствия новым угрозам (например, атакам memory scraping). Уязвимости, указанные в требованиях 6.5.1 — 6.5.10, представляют собой лишь минимальный список. Соответствие тенденциям в области уязвимостей и внедрение соответствующих мер безопасности в свои методики безопасного программирования является задачей организации.

Требования PCI DSS	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 особенности, SQL-инъекции. Также примите во внимание риски внедрения OS Command, LDAP и XPath, а также иные уязвимости, связанные с внедрением кода.	**6.5.1** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению внедрения кода, в том числе: • Проверяется, что введенная пользователями информация не может изменить существующие команды и запросы. • Используются параметризованные запросы.	Внедрения кода, в особенности внедрения SQL-кода, являются распространенным способом взлома приложений. Внедрение происходит, когда предоставленные пользователем данные передаются интерпретатору вместе с командой или запросом. Злоумышленнику удается обмануть интерпретатор, запустить вредоносные команды и изменить данные, что позволяет ему атаковать компоненты внутри сети через приложение, инициировать такие атаки, как переполнение буфера, получить доступ к конфиденциальной информации или информации о функциональности серверного приложения. Необходимо проверять информацию перед отправкой в приложение (например, посредством проверки всех буквенных символов, сочетания буквенных и цифровых символов и т.д.).
6.5.2 Переполнение буфера	**6.5.2** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению переполнения буфера, в том числе: • Проверяются границы буфера. • Усекаются 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 пространства буферной памяти в пространство исполняемой памяти. Когда это происходит, злоумышленник получает возможность внедрить в конец буфера вредоносный код и затем поместить этот вредоносный код в пространство исполняемой памяти посредством переполнения буфера. Затем вредоносный код выполняется, что позволяет злоумышленнику получить удаленный доступ к приложению и (или) зараженной системе.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.3 Небезопасное криптографическое хранилище.	**6.5.3** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании учитывается небезопасность криптографического хранилища следующим образом: • Обеспечивается защита от криптографических уязвимостей. • Используются стойкие криптографические алгоритмы и ключи.	Приложения, которые не используют для хранения данных стойкие криптографические функции надлежащим образом, подвергаются повышенному риску компрометации и утечки данных держателей карт и (или) аутентификационных данных. Если злоумышленник сможет использовать уязвимости криптографических процессов, он получит доступ к зашифрованным данным.
6.5.4 Небезопасная передача данных.	**6.5.4** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению небезопасных коммуникаций, обеспечивающие надлежащую аутентификацию и шифрование всех критичных коммуникаций.	Приложения, которые не шифруют надлежащим образом сетевой трафик с применением стойкой криптографии, подвергаются повышенному риску компрометации и утечки данных держателей карт. Если злоумышленник сможет использовать уязвимости, связанные со слабыми криптографическими процессами, он сможет получить контроль над приложением или даже доступ к зашифрованным данным в открытом виде.
6.5.5 Некорректная обработка ошибок.	**6.5.5** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению некорректной обработки ошибок путем использования методик, исключающих утечку информации через сообщения об ошибках (например, отображая общие, а не конкретные сведения об ошибке).	Вследствие некорректной обработки ошибок в приложении может происходить непреднамеренная утечка информации о конфигурации и внутренних процессах функционирования или разглашение информации о правах доступа. Злоумышленники используют этот недостаток для кражи критичных данных или для компрометации системы. Если злоумышленник сможет вызвать появление ошибок, которые приложение не сможет правильно обработать, существует возможность получения злоумышленником подробной информации о системе, возникновения ситуации отказа в обслуживании, нарушения работы системы безопасности или сбоя сервера. Например, сообщение «введен неправильный пароль» говорит злоумышленнику о том, что использовалось верное имя пользователя и теперь необходимо сфокусировать свои усилия только на подборе пароля. Следует использовать сообщения об ошибках более общего характера, например: «данные не могут быть подтверждены».

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.6 Все уязвимости с высокой степенью риска, найденные в процессе обнаружения уязвимостей (в соответствии с требованием 6.1 стандарта PCI DSS).	**6.5.6** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению уязвимостей с высокой степенью риска, которые могут повлиять на работу приложения (в соответствии с требованием 6.1 стандарта PCI DSS).	Все уязвимости, которым была присвоена высокая степень риска (в соответствии с требованием стандарта 6.1) и которые могут повлиять на работу приложения, должны быть выявлены и устранены во время разработки приложения.
Примечание: *Требования 6.5.7 — 6.5.10, приведенные ниже, распространяются на веб-приложения и интерфейсы приложений (внешние или внутренние):*		Веб-приложениям, как внутренним, так и внешним (общедоступным), свойственны уникальные риски безопасности в связи с их архитектурой, а также относительная простота и распространенность взлома.
6.5.7 Межсайтовый скриптинг (XSS).	**6.5.7** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению межсайтового скриптинга (XSS), в том числе: • Проверка всех параметров перед их включением в код. • Использование контекстно-зависимого изолирования.	Межсайтовый скриптинг (XSS) происходит, когда приложение отправляет предоставленные пользователем данные в веб-браузер без предварительной проверки или шифрования этого содержимого. Межсайтовый скриптинг позволяет злоумышленникам выполнять сценарии в браузере жертвы для кражи сеансов пользователя, изменения вида веб-сайтов, возможного внедрения червей и т.д.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.8 Ненадлежащее управление доступом (например, защита от небезопасных прямых ссылок на объекты, отсутствие ограничения доступа по URL, защита от обхода директорий и отсутствия ограничения прав доступа пользователя к функциям).	**6.5.8** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению ошибок в контроле доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий), в том числе: • Надлежащая аутентификация пользователей. • Проверка введенных данных. • Отсутствие доступа пользователей к прямым ссылкам на внутренние объекты. • Пользовательские интерфейсы, ограничивающие доступ к неразрешенным функциям.	Проблемы, связанные с контролем доступа, возникают, когда разработчик предоставляет ссылку на внутренний объект, такой как файл, каталог, запись в базе данных или ключ, в виде URL-адреса или параметра формы. Злоумышленники могут использовать эти ссылки для доступа к другим объектам без авторизации. Необходимо обеспечить надлежащий контроль доступа на уровне представления и бизнес-логики для всех URL-адресов. Часто единственным способом защиты критичной функциональности является предотвращение отображения ссылок или URL-адресов несанкционированным пользователям. Злоумышленники могут использовать эти уязвимости для выполнения неавторизованных операций посредством прямого доступа к URL-адресам. Злоумышленник может вычислить и разобраться в структуре директорий веб-сайта (обход директорий), чтобы получить неавторизованный доступ к данным или информации о функционировании сайта для дальнейшей эксплуатации. Если пользовательские интерфейсы не ограничивают доступ к запрещенным функциям, это может позволить злоумышленникам получить доступ к привилегированным учетным данным или данным держателей карт. Доступ к прямым ссылкам на критичные ресурсы должен быть разрешен только авторизованным пользователям. Ограничение доступа к ресурсам данных поможет предотвратить передачу данных держателей карт на неавторизованные ресурсы.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.5.9 Подделка межсайтовых запросов (CSRF)	**6.5.9** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по предотвращению подделки межсайтовых запросов и обеспечению того, чтобы приложения не полагались на учетные данные для проверки подлинности и токены, автоматически отправляемые браузерами.	В случае подделки межсайтовых запросов (CSRF) браузер жертвы, через который был выполнен вход в веб-приложение, отправляет предварительно аутентифицированный запрос в это уязвимое веб-приложение, что позволяет злоумышленнику совершить любые действия, которые может совершить жертва (например, обновление сведений о счете, совершение покупок или даже вход в приложение).
6.5.10 Противодействие взлому механизмов аутентификации и управления сеансами.	**6.5.10** Изучите политики и процедуры разработки ПО и опросите ответственных сотрудников, чтобы убедиться, что при программировании предпринимаются меры по противодействию взлому механизмов аутентификации и управления сеансами, в том числе: • Сеансовые токены (например, cookies) помечаются как «безопасные». • Отсутствие идентификатора сеанса в URL-адресе. • Внедрение соответствующих ограничений по длительности сеанса и ротации идентификаторов после успешного входа.	Безопасная аутентификация и управление сессией не позволят злоумышленнику скомпрометировать подлинные учетные данные, ключи или сеансовые токены, с помощью которых можно выдать себя за авторизованного пользователя.

Требования PCI DSS	Проверочные процедуры	Пояснение
6.6 Изучать на постоянной основе новые угрозы и уязвимости общедоступных веб-приложений и гарантировать, что эти приложения защищаются от известных атак при помощи следующих методов: • Проверка общедоступных веб-приложений на наличие уязвимостей с использованием методов, средств ручного или автоматического анализа защищенности не реже одного раза в год, а также после внесения любых изменений. ***Примечание:*** *Данный анализ защищенности отличается от сканирования на наличие уязвимостей, выполняемого согласно Требованию 11.2.* • Установка перед общедоступными веб-приложениями технического средства для постоянной проверки всего трафика (например, межсетевой экран уровня приложений) с целью обнаружения и предупреждения веб-атак.	**6.6** Для *общедоступных* веб-приложений убедитесь, что выполняется одно из следующих требований: • Изучите документированные процессы и отчеты о результатах анализа защищенности приложений и опросите сотрудников, чтобы убедиться, что анализ (с использованием средств или методов ручного, или автоматического анализа защищенности приложений) общедоступных веб-приложений проходит следующим образом: – Как минимум ежегодно – После каждого изменения – Организацией, специализирующейся на безопасности приложений – С включением в анализ как минимум проверки всех уязвимостей, перечисленных в Требовании 6.5 – С проверкой устранения всех уязвимостей – С повторной проверкой приложения после устранения уязвимостей • Изучите настройки системной конфигурации и опросите ответственных сотрудников, чтобы убедиться, что установлено автоматизированное техническое средство (например, межсетевой экран уровня приложений) для обнаружения и предупреждения веб-атак, отвечающее следующим требованиям: – Такое решение располагается перед общедоступными веб-приложениями для обнаружения и предупреждения веб-атак – Такое решение работает в активном режиме и выполняется его постоянное обновление – Создаются журналы регистрации событий – Такое решение настроено на блокирование веб-атак или создание предупреждений о них	Общедоступные веб-приложения являются основной целью для злоумышленников и некорректно написанные веб-приложения могут упростить злоумышленникам получение доступа к критичным данным и системам. Целью требования проверки приложений или установки межсетевого экрана прикладного уровня является снижение количества компрометаций веб-приложений вследствие высокой уязвимости программного кода или ненадлежащего контроля приложений. • Средства и методы ручной или автоматизированной оценки защищенности приложений используются для анализа и (или) проверки приложений на наличие уязвимостей. • Межсетевые экраны прикладного уровня используются для фильтрации и блокировки ненужного трафика на уровне приложений. При использовании совместно с межсетевым экраном сетевого уровня правильно сконфигурированный межсетевой экран прикладного уровня позволяет предотвратить атаки уровня приложений, если приложения настроены ненадлежащим образом или имеются уязвимости в коде. Такая цель может быть достигнута при одновременном использовании технологий и процедур. Такие решения должны иметь механизмы, способствующие своевременному реагированию на предупреждения от системы, чтобы отвечать данному требованию по недопущению атак. ***Примечание:*** *Организацией, которая специализируется на безопасности приложений, может быть сторонняя компания или внутреннее подразделение, сотрудники которого специализируются на безопасности приложений и независимы от группы разработчиков.*

Требования PCI DSS	Проверочные процедуры	Пояснение
6.7 Гарантировать, что политики безопасности и процедуры разработки для обеспечения безопасности систем и приложений документированы, используются и известны всем заинтересованным лицам.	**6.7** Ознакомьтесь с документацией и опросите сотрудников для подтверждения того, что политики безопасности и процедуры разработки и обеспечения безопасности систем и приложений: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения безопасной разработки и защиты систем и приложений от уязвимостей на постоянной основе.

Внедрение строгих мер контроля доступа

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

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

«Принцип служебной необходимости» — права доступа предоставляются только к тем данным, которые необходимы для выполнения должностных обязанностей.

Требования PCI DSS	Проверочные процедуры	Пояснение
7.1 Ограничивать доступ к системным компонентам и данным держателей карт только для тех лиц, которым такой доступ требуется в соответствии с их должностными обязанностями.	**7.1** Изучите задокументированную политику контроля доступа и убедитесь, что она отражает требования 7.1.1 — 7.1.4 следующим образом: • Определяет права доступа и назначает привилегии для каждой роли. • Предоставляет доступ пользователям только к тем данным, которые необходимы им для выполнения их должностных обязанностей. • Назначает права доступа на основании классификации должностей и должностных обязанностей. • Выполняет согласование всех прав доступа уполномоченными сторонами (в письменной или электронной форме) с описанием конкретных утвержденных привилегий.	Чем больше людей имеют доступ к данным держателей карт, тем выше риск использования злоумышленниками пользовательских учетных записей. Предоставление доступа лишь тем сотрудникам, которым он необходим для выполнения должностных обязанностей, позволит организации предотвратить ненадлежащее обращение с данными держателей карт, связанное с отсутствием опыта или злым умыслом.
7.1.1 Определить права доступа для каждой роли, включая: • Системные компоненты и информационные ресурсы, доступ к которым необходим каждой роли для выполнения должностных обязанностей. • Необходимый уровень привилегий (например, пользователь, администратор и т.д.) для доступа к ресурсам.	**7.1.1** Сделайте выборку ролей и убедитесь, что права доступа для каждой роли определены и включают: • Системные компоненты и информационные ресурсы, доступ к которым необходим каждой роли для выполнения должностных обязанностей • Определение привилегий, необходимых для каждой роли для выполнения должностных обязанностей.	Для предоставления доступа к данным держателей карт только тем лицам, которым он необходим, сначала нужно определить права доступа для каждой роли (например, системного администратора, сотрудника колл-центра, продавца), системы, устройства и данные, доступ к которым необходим для каждой роли, и уровень привилегий, необходимых для каждой должности для эффективного выполнения должностных обязанностей. После определения должностей и необходимых прав доступа, лицам могут быть назначены соответствующие права доступа.

Требования PCI DSS	Проверочные процедуры	Пояснение
7.1.2 Предоставлять привилегированным идентификаторам пользователей только те привилегии, которые необходимы этим идентификаторам для выполнения должностных обязанностей.	**7.1.2.a** Опросите сотрудников, ответственных за назначение прав доступа, для подтверждения того, что доступ к привилегированным идентификаторам пользователей: • Назначен только тем ролям, которым действительно необходим привилегированный доступ. • Ограничен привилегиями с минимальным набором прав, необходимым для выполнения должностных обязанностей.	При назначении привилегированных идентификаторов важно предоставлять лицам только те права, которые необходимы им для выполнения должностных обязанностей («минимально необходимые полномочия»). Например, администратор баз данных или администратор резервного копирования не должны иметь те же полномочия, что и системный администратор.
	7.1.2.b Сделайте выборку идентификаторов пользователей с привилегированным доступом и опросите руководство для подтверждения того, что назначенные полномочия: • Необходимы для выполнения должностных обязанностей. • Ограничены привилегиями с минимальным набором прав, необходимым для выполнения должностных обязанностей.	Назначение минимальных привилегий помогает предотвратить ошибочное или случайное изменение конфигурации приложения или настроек безопасности со стороны пользователей, не обладающих достаточными знаниями о приложении. Обеспечение минимальных прав доступа также поможет свести к минимуму ущерб в случае, если неавторизованное лицо получит доступ к идентификатору пользователя.
7.1.3 Назначать права доступа на основании классификации должностей и должностных обязанностей.	**7.1.3** Сделайте выборку идентификаторов пользователей и опросите руководство, чтобы убедиться, что привилегии назначены на основании классификации должностей и должностных обязанностей сотрудников.	После определения прав доступа для каждой роли (согласно требованию 7.1.1 стандарта PCI DSS) сотрудникам можно легко назначить права доступа на основании классификации должностей и их должностных обязанностей, используя для этого уже созданные роли.
7.1.4 Требовать формального утверждения доступа уполномоченными сторонами с указанием требуемых привилегий.	**7.1.4** Сделайте выборку идентификаторов пользователей и сравните их с формальными утверждениями, чтобы убедиться, что: • Имеется формальное утверждение назначенных привилегий. • Утверждение выполнено уполномоченными сторонами. • Указанные привилегия соответствуют роли, присвоенной сотруднику.	Формальное утверждение (например, в письменном или электронном виде) гарантирует, что сотрудники, получившие права доступа и привилегии, известны и утверждены руководством, а доступ им необходим для выполнения их должностных обязанностей.

Требования PCI DSS	Проверочные процедуры	Пояснение
7.2 Установить систему(-ы) контроля доступа к системным компонентам, которая ограничивает доступ в соответствии со служебной необходимостью пользователя и которая настроена запрещать все, что явным образом не разрешено. Система (-ы) контроля доступа должна включать следующее:	**7.2** Изучите системные настройки и документацию производителя, чтобы убедиться, что система (-ы) контроля доступа включает в себя следующее:	Без механизма ограничения доступа по принципу служебной необходимости пользователь может получить доступ к данным держателей карт, не зная об этом. Система контроля доступа автоматизирует процесс ограничения доступа и назначения привилегий. Кроме того, параметр по умолчанию «запрещено все, что явно не разрешено» («deny all») гарантирует, что ни один сотрудник не получит прав доступа, до тех пор пока не будет создано правило, в соответствии с которым будут предоставлены эти права. Организация может иметь одну или более системы контроля доступа для управления доступом пользователей. ***Примечание:*** *Некоторые механизмы контроля доступа применяют правило "разрешить все" по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.*
7.2.1 Покрытие (контроль за) всех системных компонентов.	**7.2.1** Подтвердите, что система (-ы) контроля доступа внедрена на всех системных компонентах.	
7.2.2 Назначение привилегий на основании классификации должностей и должностных обязанностей.	**7.2.2** Подтвердите, что назначение привилегий пользователям основано на классификации должностей и должностных обязанностей.	
7.2.3 По умолчанию должен быть запрещен любой доступ (установлен параметр «запрещено все, что явно не разрешено» («deny all»)).	**7.2.3** Подтвердите, что по умолчанию запрещен любой доступ (установлен параметр «запрещено все, что явно не разрешено» («deny all»)).	
7.3 Гарантировать, что политики безопасности и процедуры ограничения доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**7.3** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и рабочие процедуры ограничения доступа к данным держателей карт: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о следующих политиках безопасности и процедурах работы для обеспечения контроля доступа и предоставления доступа только к необходимым данным и минимально необходимым привилегиям на постоянной основе.

Требование 8: Определять и подтверждать доступ к системным компонентам

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

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

Примечание: *Данные требования применимы ко всем учетным записям, включая учетные записи на терминалах оплаты, имеющие административные полномочия, и ко всем учетным записям, которые используются для просмотра или доступа к данным держателей карт или системам, содержащим данные держателей карт. К таким записям относятся учетные записи поставщиков и других третьих лиц (например, для поддержки или техобслуживания). Данные требования не распространяются на учетные записи, используемые клиентами (например, держателями карт).*

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1 Определить и внедрить политики и процедуры управления идентификацией пользователей (не-клиентов и администраторов) на всех системных компонентах, регламентирующих следующие требования:	**8.1.a** Изучите процедуры и подтвердите, что они регламентируют процессы для выполнения каждого из нижеуказанных требований 8.1.1-8.1.8.	Используя уникальные идентификаторы для каждого пользователя — вместо использования одного идентификатора для нескольких сотрудников — организация сможет гарантировать то, что каждый сотрудник будет нести индивидуальную ответственность за свои действия, и эффективно отслеживать все действия, выполняемые каждым сотрудником. Это поможет ускорить разрешение и предотвращение инцидентов, связанных с некорректным или неправомерным использованием данных.
	8.1.b Убедитесь в том, что процедуры управления идентификацией пользователей реализуются с выполнением следующих условий:	
8.1.1 Присваивать каждому пользователю уникальный идентификатор перед предоставлением ему доступа к системным компонентам или данным держателей карт.	**8.1.1** Опросите административный персонал и подтвердите, что каждому пользователю назначен уникальный идентификатор для доступа к системным компонентам или данным держателей карт.	
8.1.2 Контролировать добавление, удаление и изменение идентификаторов пользователей, аутентификационных данных и иных объектов идентификации.	**8.1.2** Сделайте выборку привилегированных и обычных идентификаторов пользователей, изучите связанные с ними авторизационные мероприятия и проверьте настройки системы, чтобы убедиться, что каждый привилегированный и каждый обычный идентификатор используются только в рамках тех привилегий, которые указаны в согласовании.	Для обеспечения гарантии того, что получившие доступ к системам пользователи действительны и правомочны, любые добавления, удаления и изменения пользовательских идентификаторов и других учетных данных для проверки подлинности должны строго контролироваться.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1.3 Немедленно отзывать доступ у учетных записей уволенных сотрудников.	**8.1.3.a** Сделайте выборку учетных записей сотрудников уволенных за прошедшие шесть месяцев и проанализируйте списки доступа (как локального, так и удаленного), чтобы убедиться в том, что их идентификаторы заблокированы или удалены из списков доступа.	Если сотрудник уволился из компании и все еще имеет доступ к сети через свою учетную запись, существует риск несанкционированного или злонамеренного доступа к данным держателей карт через старую и (или) неиспользуемую учетную запись со стороны бывшего сотрудника или злоумышленника. Для предотвращения несанкционированного доступа пользовательские учетные данные и другие средства аутентификации должны быть отозваны немедленно (как можно скорее) после ухода сотрудника.
	8.1.3.b Убедитесь, что все физические средства аутентификации (например, смарт-карты, токены и т.д.) были возвращены или деактивированы.	
8.1.4 Удалять/блокировать неактивные учетные записи не реже одного раза в 90 дней.	**8.1.4** Изучите учетные записи пользователей и убедитесь в том, что неактивные более 90 дней учетные записи удаляются или блокируются.	Редко используемые учетные записи часто подвергаются атакам в связи с меньшей вероятностью того, что изменения (например, смена пароля) будут замечены. Следовательно, такие учетные записи легче взломать и использовать для доступа к данным держателей карт.
8.1.5 Управлять идентификаторами, используемыми третьими лицами для удаленного доступа, поддержки и обслуживания системных компонентов, следующим образом: • Включать только на необходимый промежуток времени и отключать, когда они не используются. • Проводить мониторинг во время их использования.	**8.1.5.a** Опросите сотрудников и изучите процессы управления учетными записями, используемыми третьими лицами для доступа, поддержки и обслуживания системных компонентов, чтобы убедиться в том, что учетные записи, используемые третьими лицами для удаленного доступа: • Отключаются, когда они не используются. • Включаются только когда они нужны третьим лицам и отключаются, когда они не используются.	Предоставление поставщикам круглосуточного доступа в сеть организации семь дней в неделю для поддержки систем увеличивает вероятность несанкционированного доступа, осуществляемого пользователями из среды поставщика или злоумышленником, который обнаружит и сможет использовать внешнюю, постоянно доступную для подключений точку входа в сеть. Включение доступа только на необходимый промежуток времени и отключение его, когда в нем нет необходимости, помогает предотвратить ненадлежащее использование таких подключений. Мониторинг доступа поставщиков позволяет убедиться в том, что поставщики получают доступ только к необходимым системам и только в соответствующий промежуток времени.
	8.1.5.b Опросите сотрудников и изучите процессы, чтобы убедиться, что во время проведения работ выполняется контроль за учетными записями, используемыми третьими лицами дистанционно.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.1.6 Ограничивать попытки получить доступ путем блокировки идентификатора пользователя после шести неудачных попыток входа в учетную запись подряд.	**8.1.6.a** Сделайте выборку системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что учетная запись пользователя блокируется после шести неудачных попыток входа подряд. **8.1.6.b Дополнительная проверочная процедура для сервис-провайдеров:** Изучите внутренние процессы и клиентскую/пользовательскую документацию и понаблюдайте за внедренными процессами, чтобы убедиться в том, что неклиентская учетная запись временно блокируется после не более чем шести неудачных попыток входа.	Без реализованного механизма блокировки учетных записей злоумышленник может непрерывно пытаться подобрать пароль или вручную, или с использованием автоматизированных средств (программ взлома паролей) до достижения успеха и получения доступа к пользовательской учетной записи. ***Примечание:*** *Процедура проверки 8.1.6.b является дополнительной процедурой, которая применима только к сервис-провайдерам.*
8.1.7 Устанавливать время блокировки учетной записи равным 30 минутам, либо до момента, пока администратор не снимет блокировку.	**8.1.7** Сделайте выборку системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что учетная запись пользователя блокируется не менее чем на 30 минут, либо до момента, пока администратор не снимет блокировку.	Если учетная запись пользователя блокируется в результате непрекращающихся попыток подбора пароля, защитные меры в виде задержки активации заблокированных учетных записей помогут остановить злоумышленника от непрерывного подбора пароля (он будет вынужден остановиться, по крайней мере, на 30 минут до автоматической разблокировки 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 работы пользователя находится в режиме ожидания свыше 15 минут, требовать от пользователей пройти повторную аутентификацию, чтобы возобновить работу терминала или сессии.	**8.1.8** Сделайте выборку системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что сеанс работы пользователя или система блокируется не позднее чем через 15 минут простоя.	Когда пользователи отлучаются от работающих компьютеров, имеющих доступ к критичным компонентам сети или данным держателей карт, эти компьютеры могут использоваться кем-нибудь в их отсутствие, что приведет к несанкционированному доступу к учетной записи и (или) ненадлежащему ее использованию. Повторная проверка подлинности может быть применена на системном уровне для защиты всех сеансов, запущенных на компьютере или на уровне приложений.
8.2 Помимо назначения уникального идентификатора, для обеспечения надлежащего управления аутентификацией пользователей (для не-клиентов и администраторов) на уровне всех системных компонентов применять хотя бы один из следующих методов аутентификации всех пользователей: • То, что вам известно (например, пароль или парольная фраза) • То, что у вас есть (например, электронный или аппаратный ключ, или смарт-карта) • То, чем вы обладаете (например, биометрические параметры).	**8.2** Проверьте, что для аутентификации пользователей применяются уникальный идентификатор и дополнительные механизмы аутентификации (например, пароль или парольная фраза) для доступа к информационной среде держателей карт. Для этого: • Изучите документацию, описывающую метод (методы) аутентификации; • Для каждого типа метода аутентификации и каждого типа системного компонента проверьте, что метод аутентификации работает в соответствии с документацией.	Данные методы аутентификации при использовании совместно с уникальными идентификаторами помогают защитить идентификаторы пользователей от компрометации, поскольку злоумышленнику нужно знать и уникальный идентификатор, и пароль (или другой элемент аутентификации). Учтите, что цифровой сертификат является подходящим вариантом для аутентификации по типу «то, что у вас есть», если он уникален для каждого конкретного пользователя. Поскольку одним из первых действий, которые злоумышленник предпринимает для получения доступа к системе, является использование простых или отсутствующих паролей, важно внедрить и использовать надежные процессы управления аутентификацией пользователей.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.1 Использование стойкой криптографии для шифрования учетных данных для проверки подлинности (например, паролей/парольных фраз) при их передаче и хранении во всех системных компонентах.	**8.2.1.a** Изучите документацию поставщика и настройки системной конфигурации, чтобы убедиться, что пароли защищены стойкой криптографией во время передачи и хранения.	Многие сетевые устройства и приложения передают незашифрованные пароли по сети и (или) хранят пароли без применения шифрования. Злоумышленник может перехватить незашифрованные пароли при их передаче, используя анализатор пакетов, или получить прямой доступ к незашифрованным паролям в файлах, в которых они хранятся, и использовать эти данные для получения несанкционированного доступа. ***Примечание:*** *Тестовые процедуры 8.2.1.d и 8.2.1.e являются дополнительными и применимы только к сервис-провайдерам.*
	8.2.1.b Сделайте выборку системных компонентов, изучите файлы паролей и убедитесь в том, что пароли являются нечитаемыми при хранении.	
	8.2.1.c Сделайте выборку системных компонентов, изучите процессы передачи данных и убедитесь в том, что пароли не читаемы при передаче.	
	8.2.1.d ***Дополнительная проверочная процедура для сервис-провайдеров:*** изучите файлы паролей и убедитесь в том, что клиентские пароли не читаемы при хранении.	
	8.2.1.e Дополнительная проверочная процедура для сервис-провайдеров: изучите процедуры передачи данных и убедитесь в том, что клиентские пароли не являются нечитаемыми при передаче.	
8.2.2 Проверка личности пользователя перед изменением любых аутентификационных данных (например, сбросом пароля, предоставлением новых токенов или генерацией новых ключей)	**8.2.2** Изучите процедуры аутентификации и процедуры изменения учетных данных для проверки подлинности и убедитесь в том, что при запросе сброса учетных данных для проверки подлинности по телефону, электронной почте, с использованием веб-приложения или иным удаленным способом, личность пользователя удостоверяется перед выполнением запроса.	Многие злоумышленники используют социальную инженерию — например, звонят в службу поддержки для изменения пароля и действуют как легитимный пользователь, чтобы затем получить возможность использовать идентификатор пользователя. Рекомендуется использовать секретный вопрос, ответ на который может дать только реальный пользователь, для помощи администраторам в идентификации и проверки подлинности пользователя перед сбросом или изменением учетных данных.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.2.3 Обеспечение соответствия паролей/парольных фраз следующим требованиям: • Минимальная длина пароля должна составлять семь символов. • Пароль должен состоять из цифр и букв. Как вариант, пароли/парольные фразы должны иметь сложность и стойкость, сравнимые с указанными выше параметрами.	**8.2.3 a** Сделайте выборку системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что пароли/парольные фразы должны соответствовать следующим требованиям к сложности и стойкости: • Минимальная длина пароля должна составлять семь символов. • Пароль должен состоять из цифр и букв. **8.2.3.b** ***Дополнительная проверочная процедура для сервис-провайдеров:*** Изучите внутренние процессы и клиентскую/пользовательскую документацию и убедитесь в том, что пароли/парольные фразы сотрудников должны соответствовать следующим требованиям к сложности и стойкости: • Минимальная длина пароля должна составлять семь символов. • Пароль должен состоять из цифр и букв.	Надежные пароли/парольные фразы являются первой линией обороны в сети, поскольку злоумышленник обычно сначала пытается найти учетные записи со слабыми или отсутствующими паролями. Злоумышленнику относительно просто найти слабозащищенные учетные записи и проникнуть в сеть под видом настоящего пользователя, если используются короткие или легко угадываемые пароли. В соответствии с данным требованием пароли/парольные фразы должны насчитывать не менее семи символов и содержать и цифры, и буквы. В случае, если данное требование не может быть выполнено в силу технических ограничений, организации могут использовать альтернативные решения, но руководствуясь принципом «эквивалентной надежности». Информацию относительно вариантности и равнозначности надежности паролей (так же называемой «энтропией») для паролей/парольных фраз различного формата см. в промышленных стандартах (например, актуальной версии NIST SP 800-63). ***Примечание:*** *Процедура проверки 8.2.3.b является дополнительной процедурой, которая применима только к сервис-провайдерам.*
8.2.4 Смена паролей/парольных фраз не реже одного раза в 90 дней.	**8.2.4.a** Сделайте выборку системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что от пользователя требуется менять пароли/парольные фразы минимум один раз в 90 дней.	Пароли/парольные фразы, не изменяемые в течение длительного времени, дают злоумышленникам больше возможностей для их взлома. ***Примечание:*** *Процедура проверки 8.2.4.b является дополнительной процедурой, которая применима только к сервис-провайдерам.*

Требования PCI DSS	Проверочные процедуры	Пояснение
	8.2.4.b ***Дополнительная проверочная процедура для сервис-провайдеров:*** Изучите внутренние процессы и клиентскую/пользовательскую документацию и убедитесь в том, что: • Требуется периодическое изменение паролей/парольных фраз пользователей (не клиентов); и • Пользователи (не-клиенты) получают инструкции о том, когда и при каких обстоятельствах пароль/парольная фраза должен/должна быть изменен/изменена.	
8.2.5 Запрет смены пользователем пароля/парольной фразы на какие-либо из четырех последних паролей/парольных фраз данного пользователя, использованных ранее.	**8.2.5.a** Сделайте выборку нескольких системных компонентов, проверьте настройки системной конфигурации и убедитесь в том, что новый пароль/парольная фраза должен/должна отличаться от четырех использованных ранее паролей/парольных фраз.	Если история паролей не ведется, эффективность смены паролей снижается, так как предыдущие пароли могут быть использованы повторно снова и снова. Запрет повторного использования паролей в течение определенного периода времени снижает вероятность того, что угаданные или подобранные пароли будут использованы в будущем. ***Примечание:*** *Процедура проверки 8.2.5.b является дополнительной процедурой, которая применима только к сервис-провайдерам.*
	8.2.5.b ***Дополнительная проверочная процедура для сервис-провайдеров:*** Изучите внутренние процессы и клиентскую/пользовательскую документацию и убедитесь в том, что новый пароль пользователя (не клиента) должен отличаться от четырех предыдущих паролей, использованных ранее.	
8.2.6 Установка уникального первоначального пароля/парольной фразы для каждого пользователя и требование их немедленной смены при первом входе пользователя в систему.	**8.2.6** Изучите парольные процедуры и убедитесь в том, что для первого входа в систему новому пользователю устанавливается, а для существующих пользователей предустанавливается уникальный первоначальный пароль, который изменяется при первом входе в систему.	Если для каждого нового пользователя устанавливается один и тот же пароль, то внутренний пользователь, бывший сотрудник или злоумышленник могут знать или легко обнаружить этот пароль и использовать его для получения доступа к учетным записям.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.3 Обеспечение безопасности всех индивидуальных неконсольных административных доступов и всех удаленных доступов к среде данных держателей карт с использованием многофакторной аутентификации. ***Примечание:*** *Многофакторная аутентификация требует, чтобы для аутентификации использовались как минимум два из трех методов аутентификации (описание методов аутентификации см. в Требовании 8.2). Использование одного метода дважды (например, использование двух различных паролей) не считается многофакторной аутентификацией.*		Многофакторная аутентификация требует, как минимум, двух отдельных форм аутентификации (как описано в Требовании 8.2) до получения доступа. Многофакторная аутентификация дает дополнительную гарантию, что пользователь, пытающийся получить доступ тот, за кого себя выдает. При многофакторной аутентификации злоумышленнику придется взломать, как минимум, два аутентификационных механизма, что повышает сложность взлома и, как следствие, снижает риски. Многофакторная аутентификация не требуется и на системном уровне, и на уровне приложений для определенного системного компонента. Многофакторная аутентификация может быть выполнена или при аутентификации в конкретную сеть, или же на системном компоненте. Примеры технологий многофакторной аутентификации включают, но не ограничиваются: удаленная аутентификация и сервис внешнего подключения (RADIUS) с токенами; Система управления доступом для контроллера доступа к терминалу (TACACS) с токенами; и прочие технологии, которые обеспечивают многофакторную аутентификацию.

Требования PCI DSS	Проверочные процедуры	Пояснение
8.3.1 Предусмотреть многофакторную аутентификацию для всех случаев неконсольного доступа в среду данных держателей карт для сотрудников с правами администратора.	**8.3.1.a** Изучите системные конфигурации серверов и/или систем и убедитесь, что многофакторная аутентификация требуется для любого административного неконсольного доступа к среде данных держателей карт.	Данное требование применяется ко всем сотрудникам с административным доступом к среде данных держателей карт. Требование применимо только к сотрудникам с административным доступом и только для неконсольного доступа к среде данных держателей карт; оно неприменимо к учетным записям приложений или системным учетным записям, осуществляющим автоматизированные функции. Если организация не использует сегментацию для отделения среды данных держателей карт от остальной сети, администратор может использовать многофакторную аутентификацию либо для входа в среду данных держателей карт, либо для входа в систему. Если среда данных держателей карт отделена от остальной сети организации, администратору потребуется использовать многофакторную аутентификацию для доступа в среду держателей карт из сетей вне среды держателей карт. Многофакторная аутентификация может быть внедрена на уровне сети или на уровне системы/приложения; не обязательно на обоих уровнях. Если администратор использует многофакторную аутентификацию для доступа в сеть среды данных держателей карт, то ему необязательно использовать многофакторную аутентификацию для доступа в определенную систему или приложение внутри самой среды держателей карт.
	8.3.1.b Изучите, каким образом администраторы получают доступ к среде данных держателей карт и убедитесь, что используются как минимум два из трех методов аутентификации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.3.2 Предусмотреть многофакторную аутентификацию для всех случаев удаленного сетевого доступа (пользователей и администраторов, включая доступ любых третьих лиц для поддержки или техобслуживания), исходящего извне сети организации.	**8.3.2.a** Изучите системные конфигурации серверов и систем удаленного доступа и убедитесь, что многофакторная аутентификация требуется для: • Любого удаленного доступа сотрудников (пользователей и администраторов); и • Любого удаленного доступа третьих лиц/поставщиков (включая доступ к приложениям и системным компонентам в целях поддержки или техобслуживания).	Данное требование применяется ко всем сотрудникам (включая обычных пользователей, администраторов и поставщиков, осуществляющих поддержку или техобслуживание), которые имеют удаленный доступ к сети, если такой удаленный доступ может привести к доступу к среде держателей карт. Если удаленный доступ осуществляется к сети, которая сегментирована таким образом, что удаленные пользователи не могут получить доступ к среде данных держателей карт, многофакторная аутентификация для удаленного доступа к такой сети не является обязательной. Однако многофакторная аутентификация требуется для удаленного доступа к сетям из которых можно получить доступ к среде данных держателей карт и рекомендована для всего удаленного доступа в сеть организации.
	8.3.2.b Изучите, каким образом выборка сотрудников (например, пользователей и администраторов) получает удаленный доступ к сети и убедитесь, что минимум два из трех методов аутентификации используются.	
8.4 Задокументировать и довести до всех пользователей процедуры и политики аутентификации, включающие: • Руководство по выбору надежных учетных данных для проверки подлинности • Руководство пользователей по защите учетных данных для проверки подлинности • Указание не использовать ранее использованные пароли • Указание сменить пароли, если есть подозрение на компрометацию.	**8.4.a** Изучите процедуры и опросите сотрудников для подтверждения того, что процедуры и политики аутентификации доведены до всех пользователей.	Информирование всех пользователей о политиках и процедурах в отношении паролей и аутентификации помогает пользователям понять эти процедуры и следовать этим политикам. Например, рекомендации по выбору стойких паролей могут включать советы по выбору трудноугадываемых паролей, которые не содержат словарных слов или информацию о пользователе (например, имя пользователя, имена членов семьи, дата рождения и т.д.). Рекомендации по защите учетных данных для проверки подлинности могут быть следующими: не записывать пароли и не сохранять их в незащищенных файлах, а также предупреждать пользователей о злоумышленниках, которые могут попытаться использовать их пароли (например, они могут позвонить сотруднику с просьбой сообщить пароль для решения некой проблемы). *(Продолжение на следующей странице)*
	8.4.b Изучите процедуры и политики аутентификации для пользователей и убедитесь, что они включают: • Руководство по выбору надежных учетных данных для проверки подлинности • Руководство пользователей по защите учетных данных для проверки подлинности. • Указание пользователям не использовать ранее использованные пароли • Указание сменить пароли, если есть подозрение на компрометацию.	
	8.4.c Опросите ряд пользователей, чтобы убедиться в том, что им известны положения политик и процедур аутентификации.	

Требования PCI DSS	Проверочные процедуры	Пояснение
		Информирование пользователей о необходимости сменить пароли, если есть вероятность, что пароль больше не является надежным, может предотвратить использование злоумышленниками реального пароля для получения несанкционированного доступа.
8.5 Не использовать групповые, общие и стандартные идентификаторы и пароли, а также прочие методы аутентификации и гарантировать, что: • Стандартные идентификаторы пользователей заблокированы или удалены. • Общие идентификаторы пользователей для системного администрирования и иных критичных функций не существуют. • Общие и стандартные идентификаторы пользователей не используются для администрирования каких-либо системных компонентов.	**8.5.a** Сделайте выборку системных компонентов, изучите списки идентификаторов пользователей и убедитесь в следующем: • Стандартные идентификаторы пользователей заблокированы или удалены. • Общие идентификаторы пользователей для системного администрирования и выполнения иных критичных функций не существуют. • Общие и стандартные идентификаторы пользователей не используются для администрирования каких-либо системных компонентов.	При использовании несколькими пользователями одних и тех же учетных данных для аутентификации (например, учетной записи и пароля) становится невозможным проследить за доступом в систему и действиями того или иного пользователя. Это, в свою очередь, не позволит организации устанавливать ответственность за действия конкретного пользователя, или фактически регистрировать события, связанные с этими действиями, поскольку эти действия могут быть совершены любым членом группы, которой известны учетные данные для аутентификации.
	8.5.b Изучите политику и процедуры аутентификации и убедитесь, что они запрещают использование групповых и общих идентификаторов, паролей и прочих подобных средств аутентификации.	
	8.5.c Опросите системных администраторов и убедитесь в том, что пользователям не выдаются групповые и общие идентификаторы и (или) пароли и прочие подобные средства аутентификации, даже если таковые запрашиваются.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.5.1 ***Дополнительное требование только для сервис-провайдеров:*** Сервис-провайдеры с удаленным доступом к оборудованию клиента (например, для поддержки POS-систем или серверов) должны использовать уникальные учетные данные для аутентификации (такие как пароль/парольная фраза) в отношении каждого клиента. ***Примечание:*** *Это требование не применяется к поставщикам услуг совместного хостинга, которые получают доступ к собственной среде внешнего размещения, в которой располагаются многие среды заказчика.*	**8.5.1** ***Дополнительная проверочная процедура для сервис-провайдеров:*** Изучите политики и процедуры аутентификации и опросите сотрудников, чтобы убедиться, что различные учетные данные для аутентификации используются каждым клиентом для получения доступа.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Чтобы не допустить компрометацию ряда клиентов при использовании одного набора учетных данных, поставщики с удаленным доступом к учетным записям в клиентской среде должны использовать разные учетные данные для аутентификации для каждого клиента. Технологии, такие как многофакторные механизмы, позволяющие получить учетные данные для каждого подключения (например, одноразовый пароль), должны также соответствовать данному требованию.
8.6 В случае использования других механизмов аутентификации (например, физических или логических токенов безопасности, смарт-карт, сертификатов т.д.), назначение эти механизмов должно происходить следующим образом: • Механизмы аутентификации должны назначаться для каждой учетной записи отдельно и не должны применяться в отношении нескольких учетных записей. • Необходимо использовать физические и/или логические механизмы контроля, чтобы только определенный пользователь мог использовать такие механизмы для получения доступа.	**8.6.a** Изучите политики и процедуры аутентификации, чтобы убедиться, что процедуры использования механизмов аутентификации (например, физических токенов безопасности, смарт-карт и сертификатов) определены и включают следующие требования: • Механизмы аутентификации должны назначаться для каждой учетной записи отдельно и не должны применяться в отношении нескольких учетных записей. • Необходимо использовать физические и (или) логические механизмы контроля, чтобы только авторизованный пользователь мог использовать такие механизмы для получения доступа.	Если механизмы пользовательской аутентификации (например, токены, смарт-карты и сертификаты) могут использоваться несколькими учетными записями, то определить пользователя, использующего этот механизм аутентификации, может быть невозможно. Наличие физических и (или) логических механизмов контроля (например, ПИН-код, биометрические данные или пароль), уникальных для каждого пользователя, не позволит неавторизованным пользователям получить доступ с помощью общего механизма аутентификации.
	8.6.b Опросите сотрудников службы безопасности и убедитесь, что механизмы аутентификации назначаются для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу.	
	8.6.c Изучите настройки системной конфигурации и, при необходимости, физические механизмы контроля, чтобы убедиться, что такие механизмы внедрены, чтобы гарантировать, что только авторизованный пользователь может использовать такие механизмы для получения доступа.	

Требования PCI DSS	Проверочные процедуры	Пояснение
8.7 Выполнять ограничение доступа к любой базе данных, содержащей данные держателей карт (включая доступ со стороны приложений, администраторов и любых других пользователей), следующим образом: • Все доступы, запросы и операции с базами данных должны осуществляться только программными методами. • Только администраторам баз данных разрешено направлять запросы и запрашивать прямой доступ к базам данных. • Использование идентификаторов приложений разрешено только приложениям (а не отдельным пользователям или иным процессам, не относящимся к приложениям).	**8.7.a** Проанализируйте настройки конфигураций баз данных и приложений, проверьте, что все пользователи проходят аутентификацию перед предоставлением доступа.	Если аутентификация пользователя для доступа к базам данных и приложениям не выполняется, увеличивается риск неавторизованного или злонамеренного доступа. Кроме того, события, связанные с таким доступом, не могут быть зарегистрированы, поскольку пользователь не аутентифицируется и, следовательно, неизвестен системе. Доступ к базам данных должен предоставляться только программными методами (например, с использованием хранимых процедур), а не посредством прямого доступа к базе данных конечными пользователями (за исключением администраторов баз данных, которым может потребоваться прямой доступ к базе данных для выполнения своих административных обязанностей).
	8.7.b Изучите настройки баз данных и приложений и убедитесь, что доступ пользователя к базе данных, поиск пользователя по базе данных и операции пользователя с базой данных выполняются только программными методами (например, через хранимые процедуры).	
	8.7.c Убедитесь, что настройки контроля доступа к базам данных и настройки приложений для доступа к базам данных разрешают запросы и прямой доступ к базам данных только для администраторов баз данных.	
	8.7.d Изучите настройки контроля доступа к базам данных, настройки и идентификаторы приложений для доступа к базам данных и убедитесь в том, что идентификаторы приложений могут использоваться только приложениями (но не пользователями или иными процессами).	
8.8 Гарантировать, что политики безопасности и рабочие процедуры идентификации и аутентификация документированы, используются и известны всем заинтересованным лицам.	**8.8** Проверьте документацию и опросите сотрудников для подтверждения того, что политики безопасности и рабочие процедуры идентификации и аутентификации: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур по управлению идентификацией и авторизацией на постоянной основе.

Требование 9: Ограничить физический доступ к данным держателей карт

Любой физический доступ к данным или системам, содержащим данные держателей карт, предоставляет возможность получить доступ к устройствам и данным, а также украсть системы или печатные материалы. Такой доступ должен быть соответствующим образом ограничен. В контексте Требования 9 под «сотрудниками организации на объекте» понимаются работники, занятые полный и неполный рабочий день, временные работники, подрядчики и консультанты, физически присутствующие на территории организации. Под «посетителем» понимается производитель, гость или любой сотрудник организации, работник сферы обслуживания, или любой другой человек, которому требуется попасть на территорию организации на короткий период, обычно не дольше чем на день. Под «носителем данных» понимаются все бумажные и электронные носители данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.1 Использовать надлежащие средства контроля доступа в помещение, чтобы ограничивать и отслеживать физический доступ к системам в среде данных держателей карт.	**9.1** Проверьте наличие средств контроля физического доступа в каждый вычислительный центр, дата-центр и иные помещения, в которых располагаются системы, которые хранят, обрабатывают или передают данные держателей карт: • Убедитесь, что доступ контролируется при помощи устройств считывания бейджей или иных устройств, в том числе бейджей для авторизации и механических замков с ключом. • Проследите за попытками системного администратора выполнить консольный вход в случайно выбранные системы в среде данных держателей карт, и убедитесь в том, что такой вход заблокирован, чтобы не допустить несанкционированный доступ.	Без физических механизмов контроля доступа (например, бейджей и контроля над входом в помещения) посторонние могут без труда получить доступ к помещениям с целью кражи, отключения, порчи и уничтожения критичных систем и данных держателей карт. Блокировка экрана входа в консоль не позволит посторонним получить доступ к критичной информации, внести изменения в конфигурацию систем, внести уязвимости в сеть или уничтожить записи.
9.1.1 Использовать камеры видеонаблюдения или механизмы контроля и управления доступом (или и то и другое) для контроля физического доступа в критичные помещения. Проводить анализ данных, собранных механизмами контроля доступа, и сопоставление их с другими фактами доступа в такие помещения. Хранить такие данные не менее трех месяцев, если иной срок не предписан законодательством.	**9.1.1.a** Убедитесь в том, что камеры видеонаблюдения или иные механизмы контроля доступа (или и то и другое) применяются для мониторинга доступа к критичным помещениям/выхода из критичных помещений.	В ходе расследования фактов проникновения в критичные помещения, такие средства контроля помогают выявить лиц, которые имеют физический доступ к критичным помещениям, а также установить, когда они вошли и вышли. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
Примечание: *Под «критичным помещением» понимается любой центр обработки данных, серверное помещение или любое помещение, в котором находятся системы, хранящие, обрабатывающие или передающие данные держателей карт. К таким помещениям не относятся общедоступные помещения, где располагаются только POS-терминалы (например, кассовая зона в розничном магазине).*	**9.1.1.b** Убедитесь, что видеокамеры и механизмы контроля и управления доступом (или и то и другое) защищены от взлома и отключения.	Злоумышленники, желающие получить физический доступ к критичным помещениям, часто пытаются отключить или обойти механизмы слежения. Для защиты таких устройств от взлома можно разместить видеокамеры за пределами досягаемости и (или) установить наблюдение за попытками взлома. Механизмы контроля доступа также могут находиться под наблюдением или быть оснащены физическими средствами защиты от повреждения или отключения злоумышленниками.
	9.1.1.c Убедитесь, что данные с камер видеонаблюдения и/или иных механизмов контроля доступа просматриваются и хранятся не менее трех месяцев.	Критичными являются такие помещения, как комнаты с серверами корпоративных баз данных, внутренние помещения, где хранятся данные держателей карт, и хранилища с большим объемом данных держателей карт. Каждая организация должна составить список критичных помещений и убедиться в наличии надлежащих физических механизмов наблюдения.
9.1.2 Внедрить механизмы физического и/или логического контроля для ограничения доступа к общедоступным сетевым разъемам. *Например, сетевые разъемы, расположенные в общедоступных местах и местах, доступных посетителям, можно включать только, если доступ к сети явно разрешен. Также можно внедрить процессы, исключающие наличие посетителей без сопровождения в помещениях с работающими сетевыми разъемами.*	**9.1.2** Опросите ответственных сотрудников и проверьте помещения с общедоступными сетевыми разъемами, чтобы убедиться в наличии механизмов физического и (или) логического контроля для ограничения доступа к сетевым разъемам, расположенным в общедоступных местах.	Ограничение доступа к сетевым разъемам (или портам) поможет предотвратить подключение злоумышленника к сетевым разъемам и получение доступа к внутренним сетевым ресурсам. Независимо от типа используемых механизмов контроля (физических, логических или их комбинации) они должны обеспечивать достаточную защиту от несанкционированного доступа к сети со стороны лиц или устройств.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.1.3 Ограничивать доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи.	**9.1.3** Убедитесь, что доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи ограничен надлежащим образом.	Без защиты доступа к беспроводным компонентам и устройствам злоумышленники могут использовать неконтролируемые беспроводные устройства организации для получения доступа к сетевым ресурсам или даже подключать собственные устройства к беспроводной сети для получения несанкционированного доступа. Кроме того, благодаря защите сетевого и коммуникационного оборудования злоумышленники не смогут перехватить сетевой трафик или физически подключить свои собственные устройства к проводным сетевым ресурсам.
9.2 Разработать процедуры, позволяющие легко различать сотрудников организации на объекте и посетителей, и включающие: • Идентификацию сотрудников организации на объекте и посетителей (например, путем выдачи бейджей). • Внесение изменений в права доступа. • Процедуры отзыва или отключения средств идентификации уволенных сотрудников организации или просроченных средств идентификации посетителей (например, бейджей).	**9.2.a** Проанализируйте документированные процессы и убедитесь в наличии процедур идентификации и различения сотрудников и посетителей на объекте. Проверьте, что среди процедур есть процедуры, предусматривающие: • Идентификацию сотрудников организации на объекте и посетителей (например, путем выдачи бейджей), • Изменение требований к доступу, и • Процедуры отзыва или отключения средств идентификации уволенных сотрудников организации или просроченных средств идентификации посетителей (например, бейджей).	Идентификация авторизованных посетителей организована таким образом, чтобы их можно было легко отличать от сотрудников объекта, и позволяет исключить предоставление доступа посторонним посетителям к местам хранения данных держателей карт.
	9.2.b Изучите методы идентификации (такие, как использование бейджей) и процессы идентификации и различения сотрудников и посетителей и убедитесь, что: • Посетители четко идентифицированы, и • Можно легко отличить сотрудников организации от посетителей.	
	9.2.c Убедитесь, что доступом к системе идентификации (например, к системе выдачи бейджей) обладает только уполномоченный персонал.	

Требования PCI DSS	Проверочные процедуры	Пояснение
9.3 Контролировать физический доступ сотрудников к критичным помещениям следующим образом: • Доступ должен быть разрешен на основании должностных обязанностей. • Доступ сотрудника моментально отзывается после увольнения, а также ими возвращаются и отключаются все устройства физического доступа (например, ключи, карты доступа и т.д.).	**9.3.a** Сделайте выборку сотрудников с физическим доступом к критичным помещениям, опросите ответственных сотрудников и изучите списки контроля доступа, чтобы убедиться, что: • Доступ к критическим помещениям санкционирован. • Доступ необходим для выполнения должностных обязанностей.	Контроль физического доступа к критичным помещениям позволяет гарантировать, что доступ предоставляется только авторизованным сотрудникам, которым он необходим для выполнения должностных обязанностей. При увольнении сотрудника из организации все средства физического доступа должны быть немедленно (как можно скорее) возвращены или отключены, чтобы сотрудник не смог получить физический доступ к критичным помещениям после увольнения.
	9.3.b Проследите за входом сотрудников в критичные помещения и убедитесь, что все сотрудники проходят авторизацию перед получением доступа.	
	9.3.c Сделайте выборку недавно уволенных сотрудников с физическим доступом и изучите списки контроля доступа, чтобы убедиться, что у них нет физического доступа к критичным помещениям.	
9.4 Внедрить процедуры идентификации и авторизации посетителей. Процедуры должны быть следующими:	**9.4** Проверьте наличие авторизации и механизмов контроля доступа посетителей.	Контроль над посетителями снижает риск получения доступа в помещения организации (и, потенциально, к данным держателей карт) посторонними и злоумышленниками. Контроль над посетителями осуществляется для того, чтобы они идентифицировались именно как посетители, а сотрудники могли отслеживать их перемещения и действия; и чтобы продолжительность их нахождения на территории организации была ограничена допустимым временем посещения. Возврат бейджей посетителей после истечения срока действия или завершения посещения не даст злоумышленникам воспользоваться ранее авторизованным пропуском для получения физического доступа в здание после завершения визита. Журнал регистрации посетителей является недорогим и несложным в ведении средством идентификации физического доступа в здание или помещение и потенциального доступа к данным держателей карт.
9.4.1 Перед входом в помещения, где обрабатываются или хранятся данные держателей карт, посетителям должно выдаваться разрешение. Во время пребывания в таких помещениях, посетителей должны постоянно сопровождать.	**9.4.1.a** Изучите процедуры и опросите сотрудников, чтобы убедиться, что до получения доступа в помещения, где обрабатываются или хранятся ДДК, посетители получают разрешение и посетителей постоянно сопровождают во время пребывания в этих помещениях.	
	9.4.1.b Понаблюдайте за использованием бейджей посетителей или других средств идентификации и убедитесь в том, что бейдж не дает возможность получить доступ в помещения, где хранятся данные держателей карт, без сопровождения персонала организации.	
9.4.2 Выполнять идентификацию посетителей и выдачу им бейджей или иных средств идентификации с ограниченным сроком действия, позволяющих отличить посетителя от сотрудника организации.	**9.4.2.a** Осмотрите бейджи персонала и посетителей и убедитесь в использовании бейджей или других средств идентификации посетителей и в том, что посетителей легко отличить от сотрудников организации.	
	9.4.2.b Проверьте, что бейдж или другое средство идентификации посетителя имеет ограниченный срок действия.	

Требования PCI DSS	Проверочные процедуры	Пояснение
9.4.3 Требовать от посетителей возвращать выданный бейдж или средство идентификации при выходе с объекта или по истечении срока его действия.	**9.4.3** Ознакомьтесь с процессом ухода посетителей с объекта, и убедитесь, что от посетителей требуется возврат бейджа или другого средства идентификации при уходе либо окончании срока действия.	
9.4.4 Обеспечить ведение журнала регистрации посетителей на входе в офисные помещения и на входе в вычислительные центры и центры обработки данных, в которых хранятся или передаются данные держателей карт. Фиксировать в журнале учета посетителей: имя посетителя, название организации, которую представляет посетитель, и имя сотрудника организации, разрешившего доступ посетителю. Храните журнал не менее трех месяцев, если иное не предусмотрено законодательством.	**9.4.4.a** Убедитесь, что ведется журнал регистрации посетителей на входе в офисные помещения и на входе в вычислительные центры и центры обработки данных, в которых хранятся или передаются данные держателей карт.	
	9.4.4.b Убедитесь, что журнал содержит: • имя посетителя; • название организации, которую он представляет; • имя сотрудника организации, разрешившего доступ посетителю.	
	9.4.4.c Убедитесь в том, что журнал хранится не менее трех месяцев.	
9.5 Обеспечивать физическую безопасность всех видов носителей.	**9.5** Убедитесь, что процедуры физической защиты данных держателей карт включают меры по защите всех видов носителей (включая, в том числе: компьютеры, съемные электронные носители, бумажные чеки, бумажные отчеты и факсы).	Механизмы обеспечения физической безопасности носителей предназначены для предотвращения несанкционированного доступа к данным держателей карт на носителях любого типа. Если данные держателей карт не защищены должным образом на съемных и портативных носителях, распечатаны или оставлены без присмотра у какого-либо сотрудника на столе, существует вероятность их несанкционированного просмотра, копирования или сканирования.
9.5.1 Хранить носители с резервными копиями данных в безопасных местах (желательно вне объекта), таких как альтернативное или резервное место, или же воспользоваться услугами организаций, обеспечивающих безопасное хранение. Проверять безопасность мест хранения не реже одного раза в год.	**9.5.1** Проверьте, что физическая безопасность места хранения носителей проверяется не реже одного раза в год, чтобы убедиться, что это место безопасно.	В случае хранения резервных копий, содержащих данные держателей карт, в незащищенных помещениях есть риск утери таких резервных копий, их кражи или копирования со злым умыслом. Периодическая проверка хранилища позволяет организации вовремя устранять обнаруженные проблемы с безопасностью, сводя к минимуму потенциальный риск.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.6 Обеспечить строгий контроль за передачей всех видов носителей информации внутри организации и вне ее, в том числе следующее:	**9.6** Убедитесь в наличии политики, определяющей порядок передачи носителей информации, а также распространение всех видов носителей информации, включая те, что передаются отдельным лицам.	Процедуры и процессы помогают защитить данные держателей карт на носителях, которые передаются сотрудникам организации или сторонним пользователям. В отсутствие таких процедур существует риск потери или кражи данных либо их использования в мошеннических целях.
9.6.1 Выполнять классификацию носителей данных, чтобы можно было определить уровень критичности хранимых данных.	**9.6.1** Убедитесь, что классификация носителей информации выполнена таким образом, чтобы можно было определить уровень критичности хранимых данных.	Важно, чтобы носитель был промаркирован таким образом, чтобы его статус был легко идентифицируемым. Носитель, который не маркирован как конфиденциальный, может быть не защищен должным образом, вследствие чего он может быть потерян или украден. ***Примечание:*** *Это не означает, что необходимо прикреплять к носителям маркировку «конфиденциально»; цель требования состоит в идентификации носителей, содержащих критичные данные, для их защиты.*
9.6.2 Выполнять пересылку носителей данных исключительно с доверенным курьером или иным способом, который может быть точно отслежен.	**9.6.2.a** Опросите сотрудников и изучите записи, чтобы убедиться в том, что вынос любого носителя за пределы предприятия регистрируется, а пересылка носителей осуществляется только с доверенным курьером или иным способом, который может быть тщательно проконтролирован и отслежен.	Если носитель отправляется способом, не предусматривающим отслеживание (например, обычной почтой), то он может быть утерян или украден. Использование услуг курьерской службы для доставки всех носителей, которые содержат данные держателей карт, позволяет организации использовать систему отслеживания, чтобы вести учет местонахождения посылок.
	9.6.2.b Изучите выборку недавних записей в журнале перемещения всех носителей за пределы охраняемой территории за несколько последних дней и убедитесь, что сведения о перемещении носителей документируются.	
9.6.3 Гарантировать, что любой вынос носителей за пределы контролируемой территории (включая передачу носителя частным лицам) согласуется руководством.	**9.6.3** Изучите выборку недавних записей в журнале перемещения всех носителей за пределы контролируемой территории за несколько последних дней. Изучите журналы и опросите ответственных сотрудников, чтобы убедиться, что любой вынос носителей за пределы контролируемой территории (включая передачу носителя частным лицам) надлежащим образом согласуется руководством.	Без наличия четкого регламента, согласно которому руководство должно согласовывать любой вынос носителей за пределы контролируемой территории, невозможно обеспечить отслеживание и надлежащую защиту носителей, а их местонахождение будет неизвестно, что приведет к потере или краже носителей.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.7 Обеспечивать строгий контроль хранения носителей данных и управление доступом к ним.	**9.7** Изучите политику хранения носителей и работы с ними, и убедитесь в том, что она регламентирует регулярную инвентаризацию носителей.	Без использования методов инвентаризации и контроля за хранением факт кражи или утери носителя может оставаться незамеченным в течение неопределенного периода времени. Если инвентаризация носителей не выполняется, то факт кражи или утери носителя может оставаться незамеченным в течение длительного периода времени.
9.7.1 Поддерживать в актуальном состоянии журналы инвентаризации всех носителей и проводить инвентаризации не реже одного раза в год.	**9.7.1** Изучите журналы инвентаризации носителей и убедитесь, что такие журналы ведутся, а инвентаризация носителей проводится не реже одного раза в год.	
9.8 Уничтожать носители данных, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства:	**9.8** Изучите политику регулярного уничтожения носителей и убедитесь в том, что она распространяется на все носители, и содержит следующие требования: • Печатные копии документов должны измельчаться, сжигаться или преобразовываться в целлюлозную массу способом, исключающим их восстановление. • Контейнеры для материалов, приготовленных для уничтожения, должны быть защищены. • Уничтожение данных держателей карт на электронном носителе должно быть необратимым и должно осуществляться с помощью программы безопасного удаления данных (в соответствии с отраслевыми стандартами безопасного удаления) или путем физического уничтожения носителя.	Если уничтожение информации, содержащейся на жестких дисках компьютеров, портативных накопителях, CD- и DVD-дисках или на бумаге, не выполняется надлежащим образом, злоумышленники могут извлечь эту информацию с утилизированных носителей и получить доступ к данным держателей карт. Например, злоумышленники могут использовать прием, известный под названием «dumpster diving» (исследование содержимого мусорных контейнеров), при котором они просматривают мусорные корзины и используют найденную информацию для проведения атак. Защита контейнеров для материалов, приготовленных для уничтожения, позволяет предотвратить получение критичной информации при сборе материалов. Например, контейнеры с материалами, подлежащие измельчению, могут быть оборудованы замком для предотвращения доступа к их содержимому. Для безопасного уничтожения электронных носителей можно использовать такие методы, как безопасное стирание, размагничивание или физическое разрушение носителя (например, измельчение жесткого диска).
9.8.1 Измельчать, сжигать или преобразовывать бумажные носители в целлюлозную массу, чтобы данные держателей карт не могли быть восстановлены. Защитить контейнеры для материалов, приготовленных для уничтожения.	**9.8.1.a** Опросите сотрудников и изучите процедуры, чтобы убедиться, что печатные копии документов измельчаются, сжигаются или преобразуются в целлюлозную массу способом, исключающим их восстановление.	
	9.8.1.b Изучите контейнеры для материалов, приготовленных для уничтожения, и убедитесь, что они надежно защищены.	
9.8.2 Делать данные держателей карт на электронном носителе невосстанавливаемыми так, чтобы исключалась возможность их восстановления.	**9.8.2** Убедитесь, что данные держателей карт на электронном носителе сделаны невосстанавливаемыми (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 Обеспечивать защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой, от подделки и подмены следующим образом. ***Примечание:*** *Данные требования распространяются на устройства считывания данных карты в ходе транзакций с предъявлением карты (путем проведения карты через устройство или вставки карты в устройство) в точке продаж. Данное требование не распространяется на компоненты ручного кнопочного ввода (например, компьютерные клавиатуры и клавиатуры POS-терминала).*	**9.9** Изучите документированные политики и процедуры и проверьте наличие следующих требований: • Ведение списка устройств. • Периодическую проверку устройств на случай взлома или подмены. • Сотрудники должны наблюдать за подозрительными лицами и сообщать о взломе или подмене устройств.	Злоумышленники часто пытаются украсть данные держателей карт путем кражи и/или подмены считывающих устройств и терминалов. Например, они пытаются украсть устройства, чтобы понять, как их взломать и часто пытаются заменить настоящие устройства на поддельные, присылающие им информацию о платежной карте каждый раз, когда вставляется карта. Злоумышленники также пытаются установить снаружи устройств так называемые «скиммеры», предназначенные для перехвата данных о платежной карте еще перед ее вставкой в устройство (например, прикрепляя дополнительный картридер сверху настоящего, чтобы данные о платежной карте считывались дважды - сначала поддельным, а затем настоящим компонентом устройства). Таким образом, «скиммеры» считывают информацию с платежной карты, не прерывая финансовую операцию. Данное требование является рекомендуемым, но не обязательным, для компонентов ручного ввода (например, компьютерных клавиатур и клавиатур кассовых терминалов). Дополнительные рекомендации по предотвращению скимминга можно найти на сайте PCI SSC.
9.9.1 Составить и регулярно обновлять списки устройств. Список должен включать следующую информацию: • Марка и модель устройства • Местонахождение устройства (например, адрес объекта, в котором находится устройство) • Серийный номер устройства или другой уникальный идентификатор.	**9.9.1.a** Изучите список устройств и убедитесь, что он содержит: • Марку и модель устройства • Местонахождение устройства (например, адрес объекта, в котором находится устройство) • Серийный номер устройства или другой уникальный идентификатор. **9.9.1.b** Сделайте выборку устройств из списка, проверьте местонахождение устройств и убедитесь, что список является точным и актуальным.	Составление и регулярное обновление списка устройств помогает организации отслеживать предполагаемое местонахождение устройства и быстро обнаружить пропажу. Составление списка устройств может выполняться автоматически (например, с помощью системы управления устройствами) или вручную (например, ведение электронных или бумажных записей). Сведения о местонахождении устройства в процессе перемещения могут включать имя сотрудника, за которым это устройство закреплено.

Требования PCI DSS	Проверочные процедуры	Пояснение
	9.9.1.c Опросите сотрудников и убедитесь, что список обновляется при каждом добавлении, перемещении, списании устройств и т.д.	
9.9.2 Регулярно выполнять проверку поверхности устройств для обнаружения признаков взлома (например, прикрепленных к устройствам «скиммеров») или подмены (например, путем проверки серийного номера или иных характеристик устройств, чтобы убедиться, что устройство не было заменено на мошенническое). ***Примечание:*** *Признаком того, что устройство было взломано или заменено на мошенническое, может служить наличие подозрительных насадок или кабелей, подключенных к устройству, отсутствующие или измененные защитные наклейки (пломбы), поврежденный или перекрашенный корпус, изменение серийного номера или иных внешних обозначений.*	**9.9.2.a** Проверьте документированные процедуры чтобы убедиться, что процессы определены и включают: • Процедуры осмотра устройств. • Частоту осмотра. **9.9.2.b** Опросите ответственных сотрудников и изучите процедуры осмотра, чтобы убедиться, что: • Сотрудники знают о процедурах осмотра устройств. • Все устройства регулярно осматриваются на предмет взлома и подмены.	Регулярный осмотр устройств позволит организациям быстрее обнаружить взлом или подмену устройства и, следовательно, снизить потенциальный вред от поддельных устройств. Вид осмотра зависит от устройства (например, можно использовать фотографию изначально безопасного устройства для сравнения текущего вида устройства с оригинальным и обнаружения изменений). Также можно использовать защитный маркер (например, видимый в ультрафиолетовом излучении) для маркировки поверхностей и отверстий устройства, чтобы любой взлом или подмену можно было легко заметить. Злоумышленники часто заменяют наружный корпус устройства, чтобы скрыть следы взлома, и указанные выше методы помогут обнаружить такую замену. Поставщики устройств также часто предоставляют рекомендации по защите и инструкции, которые помогут определить, было ли устройство взломано. Частота осмотра зависит от таких факторов, как местонахождение устройства и наличие наблюдения за устройством. Например, устройства, оставленные сотрудниками организации без присмотра в общедоступном месте, требуют более частых осмотров, чем устройства, расположенные в безопасном месте и находящиеся под присмотром. Тип и частота осмотра определяется ТСП согласно процессу ежегодной оценки рисков.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.9.3 Обучать сотрудников распознаванию признаков взлома или подмены устройств. Обучение должно включать следующую информацию: • Следует установить личность третьих лиц, представляющихся ремонтным или обслуживающим персоналом, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами. • Не следует устанавливать, заменять или возвращать устройства без проверки. • Следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство). • Сотрудники должны сообщать о подозрительном поведении, признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности).	**9.9.3.a** Изучите обучающие материалы для сотрудников в точках продаж и убедитесь, что они содержат следующую информацию: • Следует установить личность третьих лиц, представляющихся ремонтным или обслуживающим персоналом, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами. • Не следует устанавливать, заменять или возвращать устройства без проверки. • Следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство). • Сотрудники должны сообщать о подозрительном поведении, признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности). **9.9.3.b** Опросите нескольких сотрудников в местах установки кассовых терминалов и убедитесь, что они прошли обучение и знают, что: • Следует установить личность третьих лиц, представляющихся ремонтным или обслуживающим персоналом, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами • Не следует устанавливать, заменять или возвращать устройства без проверки • Следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство) • Сотрудники должны сообщать о подозрительном поведении, признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности).	Злоумышленники часто выдают себя за авторизованный обслуживающий персонал для получения доступа к устройствам кассовых терминалов. Следует проверять всех третьих лиц, запрашивающих доступ к устройствам перед предоставлением им доступа, например, посовещавшись с руководством или позвонив в компанию, обслуживающую POS-терминалы (например, поставщику или эквайреру) для проверки. Злоумышленники часто пытаются обмануть сотрудников, одевшись соответствующим образом (например, носят с собой чемоданчик с инструментами и одеваются в служебную униформу) и также могут быть осведомлены о местонахождении устройств, поэтому важно, чтобы сотрудники всегда соблюдали установленные процедуры. Еще один излюбленный трюк злоумышленников - отправка почтой «нового» 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 сотрудники должны всегда удостоверять у руководителя и поставщика, что оно настоящее и получено из доверенного источника.

Требования PCI DSS	Проверочные процедуры	Пояснение
9.10 Гарантировать, что политики безопасности и процедуры ограничения физического доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**9.10** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и рабочие процедуры ограничения физического доступа к данным держателей карт: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур по ограничению физического доступа к данным держателей карт и среде данных держателей карт на постоянной основе.

Регулярный мониторинг и тестирование сети

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

Наличие механизмов ведения записей о событиях, а также возможность проследить действия пользователей, важны для обнаружения, предотвращения и минимизации последствий компрометации данных. Необходимо наличие журналов во всех средах, что позволяет отслеживать действия, предпринимаемые в нештатных ситуациях, выполнять оповещение о нештатных ситуациях и проводить анализ нештатных ситуаций. Определение причин компрометации данных затруднено (а подчас и невозможно) в отсутствие журналов записей о событиях в системе.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.1 Внедрить журнал регистрации событий, связывающий любой доступ к системным компонентам с конкретным пользователем.	**10.1** Путем наблюдения и опроса системного администратора убедитесь, что: • Внедрен и используется журнал регистрации событий в системных компонентах. • Доступ к системным компонентам соотносится с конкретными пользователями.	Важно иметь процесс или систему, которые связывают доступ пользователей с компонентами системы, к которым он осуществлен. Данная система будет генерировать журналы регистрации событий и позволит отслеживать подозрительную деятельность определенного пользователя.
10.2 Выполнять автоматизированную регистрацию событий всех системных компонентов для восстановления следующих событий:	**10.2** Путем опроса ответственных сотрудников, изучения журналов регистрации событий и настроек журналов регистрации осуществите следующие проверки:	Генерация журналов регистрации событий подозрительной деятельности позволяет предупреждать системного администратора, отправлять данные другим устройствам мониторинга (например, системам обнаружения вторжений), а также отслеживать хронологию событий для расследования инцидентов безопасности. Регистрация следующих событий позволяет организации выявить и отследить потенциально вредоносную активность.
10.2.1 Регистрировать все факты доступа пользователя к данным держателей карт	**10.2.1** Убедитесь, что все факты доступа пользователя к данным держателей карт регистрируются.	Злоумышленники могут получить информацию об учетной записи пользователя с доступом к системам в среде данных держателей карт или создать новую неавторизованную учетную запись для получения доступа к данным держателей карт. Регистрация всех событий доступа к данным держателей карт позволяет выявить, какие учетные записи могут быть скомпрометированы или неправильно использованы.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.2.2 Регистрировать все действия пользователя с неограниченными правами доступа (root) и пользователя с административными привилегиями	**10.2.2** Убедитесь, что все действия пользователя с неограниченными правами доступа (root) и пользователя с административными привилегиями регистрируются.	Учетные записи с расширенными правами доступа, такими как «administrator» или «root», могут влиять на безопасность или функционирование системы. Если не регистрировать события, организация не сможет отслеживать проблемы, связанные с ошибками администрирования или ненадлежащим использованием прав доступа.
10.2.3 Регистрировать доступ ко всем записям о событиях в системе	**10.2.3** Убедитесь в том, что факты доступа к записям о событиях в системе регистрируются.	Злоумышленники часто пытаются изменить записи в журнале, чтобы скрыть свои действия. Регистрация событий доступа позволяет организации определять несоответствия или факт подмены записей в журнале. Доступ к журналам изменений, добавлений и удалений может помочь отследить несанкционированные действия сотрудников.
10.2.4 Регистрировать все неуспешные попытки логического доступа	**10.2.4** Убедитесь в том, что неуспешные попытки логического доступа регистрируются.	Злоумышленники часто предпринимают многочисленные попытки доступа к целевым системам. Несколько неуспешных попыток входа в систему могут свидетельствовать о том, что неавторизованный пользователь пытается войти в систему путем подбора паролей.
10.2.5 Регистрировать факты использования и изменения механизмов идентификации и аутентификации включая, помимо прочего, факты создания новых учетных записей, расширения привилегий — а также все изменения, добавления, удаления учетных записей пользователя с неограниченными правами доступа (root) или пользователя с административными привилегиями.	**10.2.5.a** Убедитесь в том, что использование механизмов идентификации и аутентификации регистрируется.	Без знания того, кто входил в систему на момент возникновения инцидента, невозможно выявить учетные записи, которые могли быть использованы. Кроме того, злоумышленники могут также предпринимать попытки обхода механизмов аутентификации или выполнить ряд действий под видом законного пользователя.
	10.2.5.b Убедитесь в том, что любое расширение привилегий регистрируется.	
	10.2.5.c Убедитесь в том, что любые изменения, добавления или удаления учетных записей с неограниченными правами доступа (root) или с правами пользователя с административными привилегиями регистрируются.	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.2.6 Регистрировать запуски, остановки или приостановки ведения журналов регистрации событий.	**10.2.6** Убедитесь, что ведется регистрация следующих событий: • Запуска журнала регистрации событий • Остановки или приостановки ведения журналов регистрации событий.	Выключение (или приостановка ведения) журналов регистрации событий перед выполнением подозрительных действий является распространенной практикой среди злоумышленников, которые стремятся избежать обнаружения. Инициализация журналов регистрации событий может свидетельствовать о том, что функции журнала были отключены пользователем в целях сокрытия действий.
10.2.7 Регистрировать факты создания и удаления объектов системного уровня.	**10.2.7** Убедитесь, что факты создания и удаления объектов системного уровня регистрируются.	Вредоносное программное обеспечение часто создает или заменяет объекты системного уровня на целевой системе, чтобы получить контроль над определенной функцией или операцией в этой системе. Регистрация создания или удаления объектов системного уровня, таких как таблицы баз данных или хранимые процедуры, упростит процесс установления легитимности таких изменений.
10.3 Регистрировать как минимум следующие параметры в журналах регистрации событий в отношении каждого события каждого системного компонента:	**10.3** Посредством опроса и изучения журналов регистрации событий выполните следующие действия для каждого регистрируемого события (из требования 10.2):	Записывая указанные элементы для контролируемых событий, перечисленных в требовании 10.2, можно быстро идентифицировать потенциальную компрометацию и иметь достаточно сведений о том, кто, что, когда, где и как сделал.
10.3.1 Идентификатор пользователя.	**10.3.1** Убедитесь в том, что идентификатор пользователя включен в записи журнала.	
10.3.2 Тип события.	**10.3.2** Убедитесь в том, что тип события включен в записи журнала.	
10.3.3 Дата и время.	**10.3.3** Убедитесь, что дата и время включены в записи журнала.	
10.3.4 Каким было событие - успешным или неуспешным.	**10.3.4** Убедитесь, что в журнал записывается, каким было событие - успешным или неуспешным.	
10.3.5 Источник события.	**10.3.5** Убедитесь в том, что источник события включен в записи журнала.	
10.3.6 Идентификатор или название данных, системного компонента или ресурса, затронутых событием.	**10.3.6** Убедитесь в том, что идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие, включены в записи журнала.	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.4 Синхронизировать все системные часы и системное время на критичных системах и обеспечивать выполнение следующих требований для получения, распространения и хранения данных о времени. ***Примечание:*** *Примером технологии синхронизации времени является Протокол синхронизации времени (Network Time Protocol).*	**10.4** Изучите конфигурационные стандарты и процессы и убедитесь, что для синхронизации часов используется технология синхронизации времени (и поддерживается актуальность ее использования), удовлетворяющая требованиям 6.1 и 6.2 стандарта PCI DSS.	Технология синхронизации времени используется для синхронизации часов на нескольких системах. Если часы синхронизированы некорректно, бывает сложно или даже невозможно сравнить файлы журналов из различных систем и установить точную последовательность событий (что имеет большое значение при расследовании каких-либо нарушений). Для групп, расследующих инциденты, точность и согласование времени на всех системах и время совершения каждого действия является критичным для установления способов компрометации систем.
10.4.1 Устанавливать точное и согласованное время на критичных системах.	**10.4.1.a** Изучите процесс получения, распространения и хранения точного времени в организации, и убедитесь, что: • Только назначенные центральные серверы времени получают информацию о времени из внешних источников, и данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC). • Если назначенных серверов времени несколько, между ними выполняется синхронизация времени для отображения корректного времени. • Системы получают информацию о времени только от назначенных центральных серверов времени.	

Требования PCI DSS	Проверочные процедуры	Пояснение
	10.4.1.b Сделайте выборку системных компонентов и изучите системные параметры времени, чтобы убедиться, что: • Только назначенные центральные серверы времени получают информацию о времени из внешних источников, и данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC). • Если назначенных серверов времени несколько, между ними выполняется синхронизация времени для отображения корректного времени. • Системы получают информацию о времени только от назначенных центральных серверов времени.	
10.4.2 Защищать данные о времени.	**10.4.2.a** Изучите конфигурации систем и настройки синхронизации времени и убедитесь, что доступ к данным о времени разрешен только персоналу, имеющему служебную необходимость.	
	10.4.2.b Изучите конфигурацию систем, настройки, журналы и процессы синхронизации времени и убедитесь, что любые изменения в настройках времени на критичных системах отслеживаются, контролируются и регистрируются.	
10.4.3 Получать настройки времени из общепризнанных отраслевых источников.	**10.4.3** Изучите конфигурацию систем и убедитесь, что серверы времени принимают обновления времени от специализированных, общепризнанных отраслевых внешних источников (чтобы предотвратить смену времени злоумышленником). Такие обновления могут быть дополнительно зашифрованы при помощи симметричного ключа. Также могут быть созданы списки учета доступа, в которых могут быть указаны IP-адреса клиентских машин, которые будут получать обновления времени (чтобы предотвратить неавторизованное использование внутренних серверов времени).	

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

Требования PCI DSS	Проверочные процедуры	Пояснение
10.5.5 Использовать ПО для мониторинга контроля целостности файлов или обнаружения изменений в журналах регистрации событий, чтобы существующие данные журналов нельзя было изменить без генерации оповещения (исключение составляет добавление новых данных, которое не должно вызывать генерацию оповещения).	**10.5.5** Изучите системные настройки, отслеживаемые файлы и результаты мониторинга и убедитесь в использовании ПО для мониторинга контроля целостности файлов или обнаружения изменений в журналах регистрации событий.	Системы мониторинга целостности файлов или системы защиты от несанкционированных изменений выполняют проверку на внесение изменений в критичные файлы и генерируют предупреждения при обнаружении изменений. В целях мониторинга целостности файлов система выполняет мониторинг файлов, которые обычно не меняются, но изменение которых может свидетельствовать о компрометации.
10.6 Просматривать журналы регистрации событий и события безопасности всех системных компонентов с целью обнаружения аномалий или подозрительной активности. ***Примечание:*** *Для обеспечения соответствия данному требованию могут использоваться средства сбора и парсинга журналов регистрации событий, а также средства оповещения.*	**10.6** Выполните следующее:	Большое количество компрометаций существует в течение нескольких дней или даже месяцев до обнаружения. Регулярная проверка журналов регистрации событий сотрудниками или автоматизированными средствами позволяет обнаруживать и активно реагировать на несанкционированный доступ к среде данных держателей карт. Просмотр журналов не обязательно выполнять вручную. Использование средств сбора и анализа журналов событий, а также средств оповещения поможет облегчить проверку благодаря идентификации событий, которые требуют проверки.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.6.1 Проверяйте не реже одного раза в день: • Все события безопасности • Журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и/или критичных аутентификационных данных • Журналы всех критичных системных компонентов • Журналы всех серверов и системных компонентов, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.).	**10.6.1.a** Изучите политики и процедуры безопасности, чтобы убедиться, что процедурами не реже одного раза в день в ручную или с использованием автоматизированных средств предусмотрена проверка следующего: • Всех событий безопасности • Журналов всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и/или критичных аутентификационных данных • Журналов всех критичных системных компонентов • Журналов всех серверов и системных компонентов, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.)	Ежедневная проверка журналов регистрации событий позволяет минимизировать время обнаружения и снизить риск компрометации. Ежедневная проверка событий безопасности (например, уведомлений или предупреждений о подозрительной или аномальной активности), журналов критичных системных компонентов и журналов систем, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения и предотвращения вторжений, систем мониторинга целостности файлов) необходима для обнаружения потенциальных проблем. Учтите, что значение термина «событие безопасности» зависит от организации и может включать ограничения по типу технологий, местонахождении и функции устройства. Организациям также рекомендуется определить так называемый «нормальный» трафик в целях идентификации аномального поведения.
	10.6.1.b Понаблюдайте за процессами и опросите сотрудников для подтверждения того, что не реже раза в день проверяются: • Все события безопасности • Журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и/или критичных аутентификационных данных • Журналы всех критичных системных компонентов • Журналы всех серверов и системных компонентов, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.).	
10.6.2 Периодически просматривайте журналы других системных компонентов на основании политик и стратегии управления рисками, определяемой в рамках ежегодной оценки рисков.	**10.6.2.a** Проверьте политики и процедуры безопасности на наличие процедур проведения периодической проверки журналов всех остальных системных компонентов (вручную или автоматически) на основании политик и стратегии управления рисками.	Следует периодически проверять журналы всех остальных системных компонентов для обнаружения признаков потенциальных проблем или попыток получить доступ к критичным системам через другие, менее критичные системы. Частота проведения проверки определяется организацией в рамках ежегодной оценки рисков.

Требования PCI DSS	Проверочные процедуры	Пояснение
	10.6.2.b Изучите документацию по оценке рисков и опросите сотрудников, чтобы убедиться, что проверка выполняется в соответствии с политиками и стратегией управления рисками, принятыми в организации.	
10.6.3 Проводить изучение исключений и аномалий, выявленных ходе проверки.	**10.6.3.a** Проверьте политики безопасности и процедуры на наличие процедур изучения исключений и аномалий, обнаруженных во время проверки.	Если исключения и аномалии, обнаруженные во время проверки журналов, не будут изучены, организация может не узнать о несанкционированной и потенциально вредоносной активности внутри своей сети.
	10.6.3.b Понаблюдайте за процессами и опросите сотрудников для подтверждения того, что проводится изучение исключений и аномалий.	
10.7 Хранить журналы регистрации событий не менее одного года, и в оперативном доступе не менее трех месяцев (например, они могут находиться в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии).	**10.7.a** Изучите политики и процедуры и убедитесь, что они включают: • Политики хранения журналов регистрации событий. • Процедуры хранения журналов регистрации событий в течение не менее одного года, в том числе в оперативном доступе не менее трех месяцев.	Хранение журналов по крайней мере в течение года связано с тем фактом, что на обнаружение компрометации требуется время, а журналы отражают достаточную хронологию событий при расследовании инцидентов и дают возможность более точного определения продолжительности существования потенциальной компрометации и систем, подверженных ее воздействию. Располагая журналами за три месяца, организация может быстро выявить нарушения и снизить их влияние. Хранение журналов на неподключенных к сети системах может затруднить получение к ним оперативного доступа и привести к увеличению времени, необходимого для восстановления данных журнала, выполнения анализа и выявления систем или данных, подвергшихся влиянию нарушения.
	10.7.b Опросите сотрудников и изучите журналы регистрации событий, чтобы убедиться, что журналы регистрации событий хранятся как минимум один год.	
	10.7.c Опросите сотрудников и изучите процессы, чтобы убедиться, что журналы регистрации событий за последние три месяца находятся в оперативном доступе.	

Требования PCI DSS	Проверочные процедуры	Пояснение
10.8 ***Дополнительное требование только для сервис-провайдеров:*** Внедрить процедуру своевременного выявления отказов и уведомления об отказах критических систем контроля безопасности, включающих отказы: • Межсетевых экранов • Систем обнаружения и предотвращения вторжений (IDS/IPS) • Мониторинга целостности файлов (FIM) • Антивируса • Средств физического контроля доступа • Средств логического контроля доступа • Механизмов ведения журналов аудита • Средств контроля сегментации (если применимо)	**10.8.a** Изучите документированные политики и процедуры, чтобы убедиться, что в них предусмотрены процессы для своевременного выявления отказов и уведомления об отказах критических систем контроля безопасности, включающих отказы: • Межсетевых экранов • Систем обнаружения и предотвращения вторжений (IDS/IPS) • Мониторинга целостности файлов (FIM) • Антивируса • Средств физического контроля доступа • Средств логического контроля доступа • Механизмов ведения журналов аудита • Средств контроля сегментации (если применимо) **10.8.b** Изучите процедуры выявления и оповещения и опросите персонал, чтобы убедиться, что процедуры внедрены для всех механизмов обеспечения безопасности и, что отказ какого-либо механизма обеспечения безопасности приводит к генерации оповещений.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Без формальных процедур выявления и оповещения при отказе механизма обеспечения безопасности, отказы могут оставаться не выявленными продолжительный период, тем самым, давая злоумышленникам достаточно времени для взлома системы и кражи критичных данных из среды данных держателей карт. Определенные типы отказов могут варьироваться в зависимости от функции устройства и используемой технологии. Типичные отказы включают остановку работы системы, реализующей функций безопасности, или ее некорректное функционирование: например, удаление межсетевым экраном всех его правил или его отключение.

Требования PCI DSS	Проверочные процедуры	Пояснение
10.8.1 ***Дополнительное требование только для сервис-провайдеров:*** Выполнять своевременное реагирование на любые отказы критичных средств контроля безопасности. Процедуры для реагирования на отказы механизмов обеспечения безопасности должны включать: • Восстановление функций систем безопасности • Идентификацию и регистрацию длительности (даты и времени от начала до конца) отказа систем безопасности • Идентификацию и регистрацию причины (причин) отказа, включая основную причину, и регистрацию исправлений, требуемых для устранения основной причины • Выявление и устранение любых проблем безопасности, возникающих в ходе отказа • Выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты • Осуществление контроля для предотвращения повторного возникновения причины отказа • Возобновление мониторинга контроля безопасности	**10.8.1.a** Изучите документированные политики и процедуры и опросите персонал, чтобы убедиться, что процедуры для реагирования на отказы механизмов обеспечения безопасности определены и внедрены, и включают: • Восстановление функций систем безопасности • Идентификацию и регистрацию длительности (даты и времени от начала до конца) отказа систем безопасности • Идентификацию и регистрацию причины (причин) отказа, включая основную причину, и регистрацию исправлений, требуемых для устранения основной причины • Выявление и устранение любых проблем безопасности, возникающих в ходе отказа • Выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты • Осуществление контроля для предотвращения повторного возникновения причины отказа • Возобновление мониторинга контроля безопасности **10.8.1.b** Изучите документацию, чтобы убедиться, что отказы механизмов обеспечения безопасности задокументированы и включают: • Причину (причины) отказа, включая основную причину • Длительность (даты и времени от начала до конца) отказа систем безопасности • Данные о восстановительных мероприятиях требуемых для устранения основной причины	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Если на оповещение об отказе критичных механизмов обеспечения безопасности не следует быстрого и эффективного реагирования, злоумышленники могут использовать это время для внедрения вредоносного программного обеспечения, получить контроль над системой или украсть данные из среды организации. Документированные доказательства (к примеру, записи в рамках системы управления проблемами) должны подтвердить, что процессы и процедуры реагирования на отказ системы безопасности находятся в рабочем состоянии. В дополнение сотрудники должны знать свои зоны ответственности в случае отказа. Действия и реагирование на отказы должны быть отслежены и задокументированы.
10.9 Гарантировать, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт документированы, используются и известны всем заинтересованным лицам.	**10.9** Проверьте документацию и опросите сотрудников, чтобы убедиться, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о политиках безопасности и повседневных процедурах мониторинга любого доступа к сетевым ресурсам и данным держателей карт на постоянной основе, и соблюдать их.

Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности

Уязвимости непрерывно обнаруживаются злоумышленниками и исследователями, а также появляются вместе с новым программным обеспечением. Системные компоненты, процессы и написанное на заказ программное обеспечение следует периодически тестировать, чтобы убедиться, что их защищенность поддерживается на должном уровне в условиях меняющейся среды.

Требования PCI DSS	Проверочные процедуры	Пояснение
11.1 Внедрить процессы для проведения ежеквартальной проверки наличия беспроводных точек доступа (802.11) и для обнаружения всех авторизованных и неавторизованных беспроводных точек доступа. ***Примечание:*** *Методы, которые могут применяться, включают, но не ограничиваются: сканирование беспроводной сети, физическое/логическое обследование компонентов системы и инфраструктуры, контроль сетевого доступа (NAC) или беспроводные IDS/IPS.* *Какие бы методы ни использовались, они должны применяться в достаточном объеме для обнаружения и идентификации как авторизованных, так и неавторизованных устройств.*	**11.1.a** Изучите политики и процедуры и убедитесь, что существуют ежеквартальные процессы для обнаружения авторизованных и неавторизованных беспроводных точек доступа. **11.1.b** Убедитесь, что методика пригодна для обнаружения и идентификации несанкционированных беспроводных точек доступа, включающих в себя, как минимум, следующее: • Карты WLAN, установленные в системные компоненты. • Переносные 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 беспроводное сканирование, изучите результаты недавних сканирований беспроводных сетей и убедитесь, что: • Авторизованные и неавторизованные беспроводные точки доступа были обнаружены. • Сканирование всех системных компонентов и объектов проводится, по крайней мере, ежеквартально.	Злоумышленники часто используют беспроводные технологии и (или) уязвимости в них для получения доступа к сети и данным держателей карт. Если беспроводное устройство или сеть установлены без ведома организации, злоумышленник может без труда и незаметно проникнуть в сеть. Неавторизованные беспроводные устройства могут быть скрыты или подключены к компьютеру, другому компоненту системы или непосредственно к сетевому порту или сетевому устройству, такому как маршрутизатор или коммутатор. Любое такое неавторизованное устройство может выполнять роль неавторизованной точки доступа в среду. Зная, какие беспроводные устройства авторизованы, администраторы могут быстро обнаружить неавторизованные беспроводные устройства и отреагировать на это, что позволит снизить уязвимость среды держателей карт перед действиями злоумышленников. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
	11.1.d Если внедрен автоматизированный мониторинг (например, система обнаружения вторжений (IDS) или система предотвращения вторжений (IPS) для беспроводных сетей, контроль сетевого доступа (NAC) и т.п.), убедитесь, что конфигурация будет генерировать оповещения для уведомления сотрудников.	Вследствие того, что беспроводную точку доступа подключить к сети не составляет большого труда, а также вследствие сложности определения присутствия такой точки и выявления риска, связанного с неавторизованными беспроводными устройствами, эти процессы следует выполнять даже при наличии политики, запрещающей использование беспроводных технологий. Размер и сложность определенной среды обуславливает необходимость использования соответствующих инструментов и процессов для предотвращения установки в среде неавторизованных беспроводных точек доступа. ***Например:*** *В случае одного автономного розничного киоска в торговом центре, где все коммуникационные компоненты содержатся в устойчивом от взлома корпусе, выполнение подробного физического осмотра киоска может быть достаточно для того, чтобы быть уверенным в том, что к киоску не подключены беспроводные точки доступа. Однако в среде с несколькими узлами (например, в большом розничном магазине, колл-центре, серверной комнате или центре обработки данных) проведение подробного физического осмотра затруднительно. В этом случае для выполнения требования можно использовать несколько методов, например, физический осмотр системы и анализ беспроводной связи.*
11.1.1 Вести список авторизованных беспроводных точек доступа с указанием обоснования их необходимости.	**11.1.1** Изучите документацию и убедитесь, что ведется список авторизованных беспроводных точек доступа с указанием обоснования необходимости.	
11.1.2 Внедрить процедуры реагирования в случае, если обнаружены неавторизованные беспроводные точки доступа.	**11.1.2.a** Изучите политику реагирования на инциденты (требование 12.10) и убедитесь, что в ней указаны обязательные действия при обнаружении неавторизованной беспроводной точки доступа.	
	11.1.2.b Опросите ответственных сотрудников и (или) изучите результаты недавних сканирований и меры, предпринятые в связи с ними, и убедитесь, что при обнаружении неавторизованных беспроводных точек доступа предпринимаются соответствующие меры.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.2 Выполнять внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений в сеть (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов). ***Примечание:*** *Можно объединить несколько отчетов о результатах сканирования для подтверждения того, что все системы были просканированы, а все найденные уязвимости - устранены. Может потребоваться дополнительная документация для подтверждения того, что неустраненные уязвимости находятся в процессе устранения.* *Для первоначального подтверждения соответствия PCI DSS успешное прохождение четырех ежеквартальных сканирований необязательно, если аудитор подтверждает, что: 1) последнее сканирование было пройдено успешно, 2) организация имеет оформленные политики и процедуры требующие проведения ежеквартального сканирования, 3) уязвимости, описанные в отчетах сканирования, были устранены и это подтверждено повторным сканированием (сканированиями). Для всех последующих лет после первоначального подтверждения соответствия PCI DSS успешное прохождение всех четырех ежеквартальных сканирований обязательно.*	**11.2** Изучите отчеты о результатах сканирования и сопутствующую документацию и убедитесь, что внешнее и внутреннее сканирование сети на наличие уязвимостей проводится следующим образом:	Сканирование на наличие уязвимостей выполняется с использованием автоматизированных средств. Эти средства проверяют внутренние и внешние сетевые устройства и серверы, и предназначены для того, чтобы выявлять потенциальные уязвимости, которые могут быть обнаружены и использованы злоумышленниками. Существует три типа сканирований на наличие уязвимостей, требуемых стандартом PCI DSS: • Ежеквартальное внутреннее сканирование на наличие уязвимостей, проводимое квалифицированными специалистами (статус авторизованного поставщика услуг сканирования (ASV) по требованиям стандарта PCI SSC необязателен) • Ежеквартальное внешнее сканирование на наличие уязвимостей, которое должны выполнять специалисты компании, имеющей статус авторизованного поставщика услуг сканирования (ASV) • Внутреннее и внешнее сканирование после значительного изменения в сети После обнаружения уязвимостей организации устраняют их и проводят повторное сканирование до устранения всех уязвимостей. Своевременное выявление и устранение уязвимостей снижает вероятность использования злоумышленником уязвимости и получения доступа к компонентам системы или данным держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
11.2.1 Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей. Устранять уязвимости и проводить повторные сканирования, пока не будут устранены все уязвимости, представляющие «высокий» уровень риска согласно принятой в компании методике ранжирования уязвимостей (согласно Требованию 6.1). Сканирования должны выполняться квалифицированными специалистами.	**11.2.1.a** Изучите отчеты о результатах сканирования и убедитесь, что четыре последних внутренних сканирования производились ежеквартально в течение последних 12 месяцев.	Установленный процесс выявления уязвимостей во внутренних системах требует ежеквартального сканирования уязвимостей. Уязвимости, которые представляют большой риск для среды (например, те, которые имеют статус «высокий» согласно требованию 6.1), должны быть устранены в первую очередь.
	11.2.1.b Изучите отчеты о результатах сканирований и убедитесь, что процесс сканирования предусматривает повторные сканирования до тех пор, пока все уязвимости «высокого» уровня риска, определенные в требовании 6.1 стандарта PCI DSS, не будут устранены.	
	11.2.1.c Опросите сотрудников и убедитесь, что сканирование проводилось квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	Внутреннее сканирование на наличие уязвимостей должны выполнять квалифицированные сотрудники, которые являются независимыми относительно сканируемого компонента системы (например, администратор межсетевого экрана не должен быть ответственным за сканирование межсетевого экрана), либо организация может воспользоваться услугами другой организации, которая занимается сканированием на наличие уязвимостей.
11.2.2 Проводить ежеквартальное внешнее сканирование на наличие уязвимостей посредством авторизованного поставщика услуг сканирования (ASV), сертифицированного Советом по стандартам безопасности индустрии платежных карт (PCI SSC). Проводите повторные сканирования до достижения удовлетворительного результата. ***Примечание:*** *Ежеквартальное внешнее сканирование на наличие уязвимостей должно выполняться сторонней организацией, имеющей статус ASV, и одобренной Советом PCI SSC.* *Для получения информации об обязанностях клиентов по проведению сканирования, подготовке к сканированию и т.д. см. «Руководство по программе ASV», опубликованное на веб-сайте Совета PCI SSC.*	**11.2.2.a** Изучите результаты четырех последних внешних сканирований на наличие уязвимостей и убедитесь, что четыре последних внешних ежеквартальных сканирования проводились в течение последних 12 месяцев.	Поскольку внешние сети подвержены более высокому риску компрометации, ежеквартальное сканирование на наличие уязвимостей в таких сетях должны выполняться компанией, имеющей статус PCI SSC Approved Scanning Vendor (ASV). Надежная программа сканирования обеспечивает выполнение своевременного сканирования и устранение уязвимостей.
	11.2.2.b Изучите результаты каждого ежеквартального сканирования и убедитесь, что они отвечают критериям успешности сканирования согласно "Руководству по программе ASV" (например, отсутствуют уязвимости с оценкой 4.0 или выше по шкале CVSS и нет узлов, сканирование которых было автоматически прервано).	
	11.2.2.c Изучите отчеты о результатах сканирования и убедитесь, что сканирование производилось организацией, имеющей статус Авторизованного поставщика услуг сканирования (ASV) Совета по стандартам безопасности индустрии платежных карт (PCI SSC).	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.2.3 Проводить внутреннее и внешнее сканирования и, при необходимости, повторное сканирование после любого значительного изменения в сети. Сканирования должны выполняться квалифицированными специалистами.	**11.2.3.a** Изучите и сопоставьте документацию по контролю изменений в сети и отчеты о результатах сканирования и убедитесь, что выполнятся сканирование системных компонентов, подверженных значительным изменениям.	Определение значительного изменения сильно зависит от конфигурации данной среды. Если обновление или модификация могут обеспечить доступ к данным держателей карт или повлиять на безопасность среды данных держателей карт, то оно считается значительным. Сканирование среды после любых значительных изменений гарантирует, что изменения внедрены надлежащим образом, и безопасность среды не нарушена в результате этих изменений. Необходимо просканировать все системные компоненты, затронутые изменением.
	11.2.3.b Изучите отчеты о сканировании и убедитесь, что процедура сканирования предусматривает повторные сканирования до тех пор, пока: • Для внешнего сканирования - не будут устранены все уязвимости уровня 4.0 или выше согласно шкале CVSS. • Для внутреннего сканирования - не будут устранены все уязвимости с «высоким» риском, согласно Требованию 6.1 стандарта PCI DSS.	
	11.2.3.c Убедитесь, что сканирование проводилось квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или Авторизованного поставщика услуг сканирования (ASV) не требуется).	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3 Внедрить методологию проведения тестирования на проникновение, которая: • Основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115) • Покрывает весь периметр среды данных держателей карт и критичных систем • Предусматривает тестирование внутри и снаружи сети • Предусматривает тестирование механизмов сегментации и уменьшения области действия Стандарта PCI DSS • Определяет необходимость включения в состав тестов на проникновение на уровне приложений, как минимум, проверок на наличие уязвимостей, перечисленных в Требовании 6.5 • Определяет необходимость включения в состав тестов на проникновение на сетевом уровне компонентов, поддерживающих сетевые функции, а также операционных систем • Предусматривает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев • Регламентирует хранение результатов тестов на проникновение и результатов действий, выполненных для устранения уязвимостей.	**11.3** Изучите методологию проведения тестов на проникновение и опросите ответственных сотрудников, чтобы убедиться, что методология: • Основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115) • Покрывает весь периметр среды данных держателей карт и критичных систем • Предусматривает тестирование внутри и снаружи сети • Предусматривает тестирование механизмов сегментации и уменьшения области действия Стандарта PCI DSS • Определяет необходимость включения в состав тестов на проникновение на уровне приложений, как минимум, проверок на наличие уязвимостей, перечисленных в Требовании 6.5 • Определяет необходимость включения в состав тестов на проникновение на сетевом уровне компонентов, поддерживающих сетевые функции, а также операционных систем • Предусматривает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев • Регламентирует хранение результатов тестов на проникновение и результатов действий, выполненных для устранения уязвимостей.	Тест на проникновение выполняется для моделирования атаки с целью выявления того, насколько глубоко в среду может проникнуть злоумышленник. Это позволяет организации оценить степень риска и разработать стратегию защиты от атак. Отличие теста на проникновение от сканирования на наличие уязвимостей заключается в том, что тест на проникновение является активным процессом, который может включать использование обнаруженных уязвимостей. Сканирование на наличие уязвимостей может быть одним из первых шагов, который выполняет специалист по тестированию на проникновение для определения стратегии тестирования, но этот шаг не единственный. Даже если сканирование на наличие уязвимостей не обнаруживает известных уязвимостей, специалист, проводящий тестирование на проникновение, получает достаточно информации о системе, чтобы выявить потенциальные проблемы. Тесты на проникновение обычно выполняются вручную. Хотя можно использовать автоматизированные средства, проверяющий должен знать систему для проникновения в среду. Часто проверяющий использует несколько уязвимостей вместе, чтобы обойти несколько уровней защиты. Например, если проверяющий находит способ получить доступ к серверу приложений, он использует взломанный сервер для проведения атаки на ресурсы, доступ к которым имеет сервер. Таким образом, проверяющий имитирует методы, которыми пользуются злоумышленники, для выявления проблемных областей в среде. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
		Процедуры тестирования на проникновение различаются в зависимости от организации, а тип, глубина и сложность тестирования будут зависеть от конкретной среды и оценки рисков организации.
11.3.1 Проводить *внешний* тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети в среду, установки веб-сервера в среду).	**11.3.1.a** Изучите область работ и результаты последнего внешнего теста на проникновение и убедитесь в том, что тест на проникновение осуществляется: • В соответствии с определенной методологией. • Как минимум ежегодно. • После любых значительных изменений в среде.	Проведение тестов на проникновение на регулярной основе и после значительных изменений в среде — это мера проактивной защиты, позволяющая уменьшить вероятность доступа злоумышленников к среде данных держателей карт. Определение значительного обновления или модификации сильно зависит от конфигурации среды. Если обновление или модификация могут обеспечить доступ к данным держателей карт или повлиять на безопасность среды данных держателей карт, то оно считается значительным. Проведение тестов на проникновение после обновления или модификации сети гарантирует, что существующие механизмы продолжают быть эффективны после обновления или модификации.
	11.3.1.b Убедитесь, что тест проводился квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.3.2 Проводить *внутренний* тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети в среду, установки веб-сервера в среду).	**11.3.2.a** Изучите объем работы и результаты последнего внутреннего теста на проникновение и убедитесь в том, что тест на проникновение осуществляется. • В соответствии с определенной методологией. • Как минимум ежегодно. • После любых значительных изменений в среде.	
	11.3.2.b Убедитесь, что тест проводился квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.3.3 Устранять эксплуатируемые уязвимости, обнаруженные во время теста на проникновение, и проводить повторное тестирование для проверки их устранения.	**11.3.3** Изучите результаты теста на проникновение и убедитесь в том, что выявленные уязвимости были устранены и это подтверждено повторным тестом.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.3.4 В случае использования сегментации для изолирования среды данных держателей карт от других сетей, проводить тестирование на проникновение не реже одного раза в год и после любого изменения механизмов/методов сегментации для проверки функционирования и эффективности методов сегментации и изолирования всех систем, размещенных вне среды данных держателей карт, от систем, входящих в среду данных держателей карт.	**11.3.4.a** Изучите механизмы сегментации и методологию тестирования на проникновение, чтобы убедиться, что процедуры тестирования на проникновение включают тестирование всех методов сегментации для проверки их функционирования и эффективности, и изолирования всех систем, размещенных вне среды держателей карт, от систем, входящих в среду держателей карт.	Тест на проникновение — это важный инструмент для проверки эффективности методов сегментации, используемых для изолирования среды данных держателей карт от других сетей. Тест на проникновение необходимо сконцентрировать на механизмах сегментации, используемых как извне сети организации, так и изнутри сети, но вне среды данных держателей карт для подтверждения невозможности получения доступа к среде данных держателей карт в обход механизмов сегментации. Например, проверить и (или) просканировать сеть на наличие открытых портов для подтверждения невозможности соединения между проверенными и непроверенными сетями.
	11.3.4.b Изучите результаты последнего теста на проникновение и убедитесь в том, что: • Тест на проникновение для проверки механизмов сегментации выполняется не реже одного раза в год и после любого изменения средств/методов сегментации. • Тест на проникновение включает в себя все используемые средства/методы сегментации. • Тест на проникновение подтверждает, что средства/методы сегментации осуществимы и эффективны, и позволяют изолировать все системы, не входящие в среду данных держателей карт, от систем, входящих в среду данных держателей карт.	
	11.3.4.c Убедитесь, что тест проводился квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.3.4.1 ***Дополнительное требование только для сервис-провайдеров:*** В случае применения сегментации, подтверждать область применения стандарта PCI DSS выполнением тест на проникновение в отношении механизмов сегментации не реже одного раза в полгода и при любых изменениях механизмов/методов сегментации.	**11.3.4.1.a** Изучите результаты последнего теста на проникновение и убедитесь в том, что: • Тест на проникновение выполняется для проверки механизмов сегментации не реже одного раза в год и после любого изменения средств/методов сегментации. • Тест на проникновение включает в себя все используемые средства/методы сегментации. • Тест на проникновение подтверждает, что средства/методы сегментации осуществимы и эффективны, и позволяют изолировать все системы, не входящие в среду данных держателей карт, от систем включенных в среду данных держателей карт.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Для сервис-провайдеров подтверждение области применения стандарта PCI DSS должно выполняться настолько часто, насколько это возможно для того, чтобы убедиться, что область применения стандарта PCI DSS остается актуальной и совпадает с изменяющимися бизнес-целями.

Требования PCI DSS	Проверочные процедуры	Пояснение
	11.3.4.1.b Убедитесь, что тест проводился квалифицированными сотрудниками организации либо квалифицированной третьей стороной, а также убедитесь в их организационной независимости (если это возможно); при этом наличие статуса QSA или Авторизованного поставщика услуг сканирования (ASV) не требуется).	
11.4 Использовать механизмы обнаружения и/или предотвращения вторжений для обнаружения и/или предотвращения вторжения в сеть. Осуществлять мониторинг сетевого трафика по периметру среды данных держателей карт и в критичных точках внутри среды данных держателей карт, и оповещать сотрудников о подозрительных действиях. Поддерживать системы обнаружения и предотвращения вторжений и их сигнатуры в актуальном состоянии.	**11.4.a** Изучите системные конфигурации и схемы сети и убедитесь в том, что методы мониторинга всего трафика (например, системы обнаружения и (или) предотвращения вторжений) используются: • По периметру среды данных держателей карт и • В критичных точках внутри среды данных держателей карт.	Методы обнаружения и (или) предотвращения вторжений (например, система обнаружения вторжений (IDS)/система предотвращения вторжений (IPS)) сравнивают поступающий в сеть трафик с известными сигнатурами и (или) поведением (инструментарий злоумышленников, трояны и другое вредоносное программное обеспечение и т.д.), отправляют предупреждения и (или) блокируют попытку проведения атаки. Не используя превентивные меры для обнаружения несанкционированной деятельности, можно не заметить атаки на компьютерные ресурсы (или их ненадлежащее использование) в момент выполнения. Необходимо вести мониторинг предупреждений, генерируемых данными средствами, для своевременного блокирования предпринятых вторжений.
	11.4.b Изучите системные конфигурации и опросите ответственных сотрудников для подтверждения того, что средства обнаружения и (или) предотвращения вторжений оповещают сотрудников о подозрительных действиях.	
	11.4.c Изучите конфигурации систем обнаружения вторжений (IDS)/предотвращения вторжений (IPS) и документацию поставщиков, чтобы убедиться в том, что средства обнаружения и (или) предотвращения вторжений настроены, поддерживаются и обновляются в соответствии с рекомендациями производителя для обеспечения оптимальной защиты.	

Требования PCI DSS	Проверочные процедуры	Пояснение
11.5 Внедрить механизм обнаружения изменений (например, мониторинг целостности файлов) таким образом, чтобы оповещать сотрудников о неавторизованных модификациях (включая изменения, добавления и удаления) критичных системных файлов, файлов конфигурации и файлов данных; сконфигурировать ПО таким образом, чтобы проводить сравнение критичных файлов не реже одного раза в неделю. ***Примечание:*** *В контексте обнаружения изменений, критичные файлы — это файлы, изменение которых происходит редко, но факт изменения которых может служить признаком компрометации системы или риска компрометации системы. Механизмы обнаружения изменений (такие как средства мониторинга целостности файлов) обычно содержат предустановленный перечень критичных файлов в используемой операционной системе. Другие критичные файлы, такие, как файлы для клиентских приложений, должны быть определены организацией самостоятельно (т.е. ТСП или сервис-провайдером).*	**11.5.a** Убедитесь в использовании механизма обнаружения изменений путем изучения системных настроек и отслеживаемых файлов, а также проверки результатов мониторинга. Примеры файлов, подлежащих мониторингу: • Исполняемые файлы системы • Исполняемые файлы приложения • Файлы конфигурации и файлы параметров • Централизованно хранимые файлы, исторические или архивированные фалы, журналы и файлы регистрации событий • Дополнительные критичные файлы, определяемые организацией (например, путем оценки рисков или иными способами).	Решения для обнаружения изменений, например, системы мониторинга целостности файлов выполняют проверку на внесение изменений и добавлений в критичные файлы и их удаление, и генерируют предупреждения при обнаружении изменений. Если решение внедрено ненадлежащим образом и создаваемые им отчеты не проверяются, то злоумышленник может изменить или удалить содержимое конфигурационных файлов, программ операционной системы или исполняемые файлы приложений. Незамеченные несанкционированные изменения могут снизить эффективность работы механизмов контроля безопасности и/или привести к краже данных держателей карт без заметного влияния на процессы обработки.
	11.5.b Убедитесь, что механизм настроен на оповещение сотрудников организации о несанкционированных изменениях критичных файлов (включая изменения, добавления и удаления) и сравнение критичных файлов проводится не реже одного раза в неделю.	
11.5.1 Внедрить процесс реагирования на любое срабатывание решения для обнаружения изменений.	**11.5.1** Опросите сотрудников и убедитесь, что все предупреждения обработаны и расследованы.	
11.6 Гарантировать, что политики безопасности и процедуры мониторинга и проверки безопасности документированы, используются и известны всем заинтересованным лицам.	**11.6** Проверьте документацию и опросите сотрудников для подтверждения того, что политики безопасности и процедуры мониторинга и проверки безопасности: • задокументированы; • используются; • известны всем вовлеченным лицам.	Сотрудники должны быть осведомлены о и соблюдать требования политик безопасности и рабочих процедур мониторинга и проверки безопасности на постоянной основе.

Поддержание политики информационной безопасности

Требование 12: Разработать и поддерживать политику обеспечения информационной безопасности для всех сотрудников организации

Строгая политика безопасности задает характер безопасности для всей организации и информирует персонал организации о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите. В контексте требования 12 под термином «сотрудники» понимаются постоянные сотрудники (на полной и неполной ставке), временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте организации или так или иначе имеющие доступ к среде данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.1 Разработать, опубликовать, поддерживать в актуальном состоянии и распространять политику информационной безопасности.	**12.1** Изучите политику информационной безопасности и убедитесь в том, что она опубликована и распространена среди всех пользователей (включая поставщиков и бизнес-партнеров).	Политика информационной безопасности компании помогает разработать стратегический план по реализации мер защиты наиболее ценных ресурсов. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите.
12.1.1 Пересматривать политику безопасности не реже раза в год и обновлять ее в случае изменения среды организации.	**12.1.1** Убедитесь в том, что политика безопасности пересматривается не реже раза в год и обновляется в случае изменения бизнес-целей или рисков среды организации.	Угрозы для безопасности и методы защиты быстро развиваются. Без обновления политики безопасности с учетом этих изменений не будут приняты актуальные меры защиты против новых угроз.
12.2 Внедрить процесс оценки рисков, который: • Осуществляется не реже, чем раз в год и после значительного изменения среды (например, покупки, слияния, перемещения и т.д.). • Выявляет критичные активы, угрозы и уязвимости, и • Завершается официальным оформленным анализом рисков. *Примеры методик - оценки рисков включают в том числе: OCTAVE, ISO 27005 и NIST SP 800-30.*	**12.2.a** Убедитесь, что ежегодным официальным процессом оценки рисков предусмотрено: • Выявление критичных активов, угроз и уязвимостей, и • Официальное оформление анализов рисков по итогам **12.2.b** Изучите документацию по оценке рисков и убедитесь, что процесс оценки рисков выполняется как минимум раз в год и после выполнения значительных изменений в среде.	Оценка рисков позволяет выявить угрозы и связанные с ними уязвимости, которые могут негативно отразиться на ведении дел. Примерами различных видов риска, которые следует брать во внимание, являются киберпреступления, веб-атаки, вредоносное ПО для POS-терминалов. Ресурсы можно эффективно распределить для внедрения механизмов контроля, которые помогут снизить вероятность воздействия угроз. Проведение оценки рисков, по крайней мере, раз в год и после значительных изменений позволяет организации учитывать структурные изменения и реагировать на новые угрозы, тенденции и технологии.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3 Разработать политики эксплуатации критичных технологий и определите надлежащее применение для этих технологий. ***Примечание:*** *К примерам критичных технологий относятся в том числе: технологии удаленного доступа, беспроводные технологии, использование ноутбуков, планшетов, съемных электронных носителей информации, электронной почты и Интернет.* Гарантировать, что политики эксплуатации критичных технологий предусматривают:	**12.3** Изучите правила эксплуатации критичных технологий и опросите ответственных сотрудников, чтобы убедиться, что следующие политики внедрены и выполняются:	Политики использования для сотрудников могут либо запрещать использование определенных устройств и иных технологий, либо содержать инструкции для сотрудников по их надлежащему использованию и внедрению. Если политики использования отсутствуют, есть вероятность нарушения сотрудниками политик компании, в результате чего злоумышленники могут получить доступ к критичным системам и данным держателей карт.
12.3.1 Явное согласование уполномоченными лицами.	**12.3.1** Убедитесь, что правила эксплуатации включают процессы явного согласования используемых технологий уполномоченными лицами.	Без согласования руководством необходимости внедрения этих технологий, сотрудники могут непреднамеренно внедрить решение в соответствии с потребностями бизнеса, при этом создав брешь в системе безопасности и подвергнуть критичные системы и данные риску потери или кражи злоумышленниками.
12.3.2 Обязательная аутентификация для использования технологии.	**12.3.2** Убедитесь в том, что политики эксплуатации включают процессы аутентификации по идентификатору и паролю, либо иному средству аутентификации (например, токену) перед использованием любых технологий.	Если технология реализована без надлежащей аутентификации (через идентификаторы пользователей и пароли, токены, VPN и т.д.), злоумышленник может воспользоваться этой незащищенной технологией для получения доступа к критичным системам и данным держателей карт.
12.3.3 Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.	**12.3.3** Убедитесь в том, что политики эксплуатации включают: • Список всех используемых критичных устройств. • Список сотрудников, имеющих доступ к таким устройствам.	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве «черного хода». Сотрудники также могут обойти защиту и установить свои устройства. Тщательная инвентаризация и маркировка устройств позволит быстро идентифицировать несанкционированно установленные устройства.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3.4 Способ точного и быстрого определения владельца, контактных данных и назначения устройства (например, маркировка, кодирование и/или инвентаризация устройств).	**12.3.4** Убедитесь в том, что политики эксплуатации регламентируют способ точного и оперативного определения владельца, контактных данных и назначения (например, маркировка, кодирование и (или) инвентаризация устройств).	Злоумышленники могут преодолеть физическую защиту и разместить свои собственные устройства в сети в качестве «черного хода». Сотрудники также могут обойти защиту и установить свои устройства. Тщательная инвентаризация и маркировка устройств позволит быстро идентифицировать несанкционированно установленные устройства. Рекомендуется разработать официальную процедуру именования устройств и вести учет всех устройств с помощью механизмов инвентаризации. Можно применять логическую маркировку с использованием такой информации, как коды, которые помогают соотнести устройство с владельцем, контактной информацией и назначением.
12.3.5 Допустимые способы использования технологий.	**12.3.5** Убедитесь, что политики эксплуатации регламентируют допустимые способы использования технологий.	Определяя допустимые сценарии использования и размещение разрешенных устройств и технологий, компания может улучшить управление и контроль над появлением брешей в конфигурациях и операционных механизмах, чтобы исключить возможность появления «черных ходов», которыми могут воспользоваться злоумышленники для получения доступа к критичным системам и данным держателей карт.
12.3.6 Допустимые точки размещения технологий в сети.	**12.3.6** Убедитесь, что политики эксплуатации регламентируют допустимые точки размещения устройств в сети.	
12.3.7 Перечень одобренных компанией продуктов.	**12.3.7** Убедитесь, что политики эксплуатации включают перечень одобренных компанией продуктов.	
12.3.8 Автоматическое отключение сессий удаленного доступа после определенного периода простоя.	**12.3.8.a** Убедитесь, что политики эксплуатации регламентируют автоматическое отключение сеансов удаленного доступа после определенного периода простоя.	Технологии удаленного доступа часто могут играть роль «черных ходов», которые злоумышленники используют для доступа к критичным ресурсам и данным держателей карт. Отключение технологий удаленного доступа, когда они не используются (например, тех, что используются для поддержки систем поставщиками POS-терминалов, другими поставщиками или партнерами по бизнесу), позволит ограничить доступ к сети и минимизировать риски для безопасности сетей.
	12.3.8.b Изучите конфигурации технологий удаленного доступа и убедитесь, что сеансы удаленного доступа автоматически отключаются после определенного периода простоя.	
12.3.9 Включение механизмов удаленного доступа для производителей и деловых партнеров только в случае необходимости с немедленным выключением механизмов после использования.	**12.3.9** Убедитесь, что политики эксплуатации регламентируют включение механизмов удаленного доступа для производителей и деловых партнеров только в случае необходимости с немедленным выключением механизмов после использования.	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.3.10 Запретить копирование, перемещение и хранение данных держателей карт на локальных жестких дисках и съемных электронных носителях сотрудникам, имеющим доступ к данным держателей карт через технологии удаленного доступа, если они явно не уполномочены для выполнения этих действий в рамках определенной служебной необходимости. При наличии подтвержденной служебной необходимости политиками использования должна требоваться защита данных в соответствии со всеми применимыми требованиями стандарта PCI DSS.	**12.3.10.a** Убедитесь, что политики эксплуатации запрещают копирование, перемещение и хранение данных держателей карт на локальных дисках и иных съемных электронных носителях при удаленном доступе к данным. **12.3.10.b** Убедитесь, что политики эксплуатации предписывают авторизованным сотрудникам обеспечивать защиту данных держателей карт в соответствии с требованиями стандарта PCI DSS.	Для обеспечения осведомленности сотрудников о запрете хранения и копирования данных держателей карт на свои персональные компьютеры или другие носители информации политика компании должна явно запрещать действия такого рода, за исключением сотрудников, которым на выполнение такого действия дано специальное разрешение. Хранение или копирование данных держателей карт на локальный жесткий диск или другой носитель должно осуществляться в соответствии со всеми действующими требованиями стандарта PCI DSS.
12.4 Гарантировать, что политикой и процедурами обеспечения безопасности дано четкое определение обязанностей сотрудников по обеспечению информационной безопасности.	**12.4.a** Убедитесь, что политики информационной безопасности явно определяют обязанности по обеспечению защиты для всех сотрудников. **12.4.b** Опросите некоторых ответственных сотрудников и убедитесь, что они понимают политику информационной безопасности.	Без явно определенных ролей и обязанностей по обеспечению информационной безопасности взаимодействие между сотрудниками будет неэффективным, что может привести к небезопасному внедрению технологий или использованию устаревших или незащищенных технологий.
12.4.1 ***Дополнительное требование только для сервис-провайдеров:*** Высшему руководству следует установить ответственность по защите данных держателей карт и программы соответствия стандарту PCI DSS, которая должна включать: • Полную подотчетность за обеспечение соответствия стандарту PCI DSS. • Определение устава программы соответствия стандарту PCI DSS и отчетности перед высшим руководством.	**12.4.1.a** Изучите документацию, чтобы убедиться, что высшее руководство установило полную подотчетность за обеспечение соответствия организации стандарту PCI DSS.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Назначение высшим руководством ответственности за соответствие стандарту PCI DSS обеспечивает прозрачность программы соответствия стандарту PCI DSS на руководящем уровне и дает возможность задавать соответствующие вопросы для определения эффективности программы и ее влияния на стратегические приоритеты. Полная ответственность за программу соответствия стандарту PCI DSS может быть возложена на определенных сотрудников и/или структурные подразделения внутри организации.

Требования PCI DSS	Проверочные процедуры	Пояснение
	12.4.1.b Изучите устав компании в отношении стандарта PCI DSS, чтобы убедиться, что он излагает условия, на основании которых организована программа соответствия стандарту PCI DSS и ее подотчетность высшему руководству.	В состав высшего руководства могут входить позиции С-уровня, совет директоров, или аналогичные должности. Специальные должности будут зависеть от конкретной организационной структуры. Уровень детализации отчетов, предоставляемой высшему руководству, должен соответствовать конкретной организации и целевой аудитории.
12.5 Назначить определенному сотруднику или группе сотрудников следующие обязанности в области управления информационной безопасностью:	**12.5** Изучите политики и процедуры информационной безопасности и убедитесь, что: • Ответственность за информационную безопасность официально возложена на руководителя службы безопасности (Chief Security Officer) или другого члена руководства, компетентного в вопросах обеспечения информационной безопасности. • Следующие обязанности по обеспечению информационной безопасности назначены явно и официально:	Каждое лицо или группа лиц, которые отвечают за управление информационной безопасностью, должны понимать свои обязанности и связанные с ними задачи, которые доводятся до их сведения посредством соответствующей политики. Без такой ответственности недочеты в процессах могут открыть доступ к критичным ресурсам или данным держателей карт. Организации также должны учитывать планы перехода и/или преемственности для ключевых сотрудников, чтобы избежать возможных пробелов при делегировании обязанностей за обеспечение защиты. Это может привести к тому, что обязанности не будут вовремя назначены и, следовательно, не будут выполняться.
12.5.1 Обязанности разрабатывать, документировать и распространять политики и процедуры обеспечения безопасности.	**12.5.1** Убедитесь, что официально назначены ответственные за создание, документирование и доведение до сотрудников политик и процедур защиты.	
12.5.2 Обязанности контролировать и анализировать оповещения безопасности и информацию, а также информировать соответствующий персонал.	**12.5.2** Убедитесь, что официально назначены ответственные за мониторинг, анализ и доведение до сведения соответствующих сотрудников (специалистов по информационной безопасности и представителей бизнес-подразделений) информации о событиях информационной безопасности.	
12.5.3 Обязанности разрабатывать, оформлять и распространять процедуры реагирования на инциденты и передачи сообщений о них в соответствующие отделы для обеспечения своевременной эффективной обработки всех ситуаций.	**12.5.3** Убедитесь, что официально назначены ответственные за создание, документирование и доведение до сотрудников политик и процедур реагирования на инциденты и сообщения о них.	
12.5.4 Обязанности по администрированию учетных записей пользователей, включая их добавление, удаление и изменение.	**12.5.4** Убедитесь, что официально назначены ответственные за администрирование (добавление, удаление и изменение) учетных записей пользователей и управление аутентификацией.	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.5.5 Обязанности отслеживать и контролировать любой доступ к данным.	**12.5.5** Убедитесь, что официально назначены ответственные за мониторинг и контроль доступа к данным.	
12.6 Внедрить официальную программу повышения осведомленности сотрудников о безопасности, целью которой является информирование сотрудников о политиках и процедурах обеспечения безопасности данных держателей карт.	**12.6.a** Изучите программу повышения осведомленности сотрудников по вопросам безопасности и убедитесь, что она информирует сотрудников о политиках и процедурах безопасности данных о держателях карт.	Если сотрудники не осведомлены о своих обязанностях по обеспечению информационной безопасности, реализованные меры и процессы защиты могут потерять свою эффективность вследствие непреднамеренных ошибок или умышленных действий таких сотрудников.
	12.6.b Изучите процедуры программы повышения осведомленности персонала по вопросам информационной безопасности и выполните следующие проверки:	
12.6.1 Проводить обучение сотрудников при приеме на работу, а также не реже одного раза в год. ***Примечание:*** *Методики могут варьироваться в зависимости от ролей сотрудников и их уровня доступа к данным держателей карт.*	**12.6.1.a** Убедитесь в том, что в программе повышения осведомленности персонала используются различные методы доведения информации до персонала (например, плакаты, письма, заметки, веб-системы для обучения, специальные кампании).	Если программа повышения осведомленности персонала по вопросам информационной безопасности не будет включать в себя периодические напоминания, сотрудники могут забыть или пренебречь основными процессами и процедурами обеспечения безопасности, что приведет к уязвимости критичных ресурсов и данных держателей карт.
	12.6.1.b Убедитесь в том, что персонал организации проходит обучение по вопросам информационной безопасности при приеме на работу, а также не реже одного раза в год.	
	12.6.1.c Опросите нескольких сотрудников и убедитесь, что они прошли обучение по вопросам информационной безопасности и понимают важность обеспечения безопасности данных держателей карт.	
12.6.2 Требовать, чтобы персонал организации не реже одного раза в год подтверждал свое знание и понимание политик и процедур обеспечения информационной безопасности организации.	**12.6.2** Убедитесь, что программа повышения осведомленности сотрудников по вопросам информационной безопасности содержит требование о ежегодном подтверждении сотрудниками (в печатной или в электронной форме) прочтения и понимания корпоративной политики в отношении информационной безопасности.	Наличие подписи сотрудника (от руки или в электронном виде) гарантирует, что он действительно прочитал и понял все принципы и процедуры обеспечения безопасности, а также то, что он обязуется действовать в соответствии с этими документами.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.7 Проверять кандидатов (будущих сотрудников) при приеме на работу для минимизации риска внутренних атак. (Примером кадровых проверок является изучение послужного списка, записей правоохранительных органов, кредитной истории, проверки рекомендаций). ***Примечание:*** *Для кандидатов на определенные должности (например, кассир в магазине), которые имеют доступ только к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.*	**12.7** Опросите руководителей управления по работе с персоналом и убедитесь в том, что при приеме на работу новых сотрудников, которым будет предоставляться доступ к данным держателей карт или информационной среде держателей карт, осуществляются кадровые проверки (с учетом особенностей местного законодательства).	Тщательное изучение биографии будущих сотрудников, которые будут иметь доступ к данным держателей карт, уменьшает риск несанкционированного использования основных номеров держателей банковских карт и других данных держателей карт сотрудниками с сомнительным или криминальным прошлым.
12.8 Внедрить и поддерживать политики и процедуры взаимодействия с сервис-провайдерами, которые имеют доступ к данным держателей карт или которые могут повлиять на безопасность данных держателей карт, следующим образом:	**12.8** Путем наблюдения за процессами, изучения политик, процедур и сопутствующей документации убедитесь в наличии следующих процессов взаимодействия с поставщиками услуг, которые имеют доступ к данным держателей карт или могут повлиять на безопасность данных держателей карт:	Если ТСП или сервис-провайдер передают данные держателей карт другому сервис-провайдеру, то необходимо выполнить определенные требования, чтобы обеспечить защиту таких данных со стороны сервис-провайдера. Некоторые примеры различных типов сервис-провайдеров включают хранилища резервных копий на магнитной ленте, поставщики управляемых услуг, такие как компании веб-хостинга или поставщики услуг безопасности, организации, которые получают данные с целью моделирования мошеннических операций и пр.
12.8.1 Вести список сервис-провайдеров с перечислением оказываемых ими услуг.	**12.8.1** Убедитесь, что список сервис-провайдеров ведется и в нем перечисляются оказываемые ими услуги.	Ведение списка сервис-провайдеров помогает оценить потенциальные риски, существующие за пределами организации.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.8.2 Составить и использовать письменное соглашение, включающее положения о том, что сервис-провайдеры ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, а также за безопасность среды данных держателей карт, на которую они могут повлиять. ***Примечание:*** *Точная формулировка положения зависит от договора между двумя сторонами, сведений о предоставляемой услуге и обязанностей каждой из сторон по договору. Формулировка положения не обязательно должна копировать формулировку, указанную в данном требовании.*	**12.8.2** Изучите письменные соглашения и убедитесь, что они содержат положения о том, что сервис-провайдеры ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, а также за безопасность среды данных держателей карт клиентов, на которую они могут повлиять.	Сервис-провайдеры должны поддерживать надлежащий уровень безопасности данных держателей карт, которые они получают от своих клиентов. Объем, за который сервис-провайдер несет ответственность в отношении безопасности данных держателей карт, зависит от конкретных услуг, которые он оказывает и договоренностей с проверяемой организацией. В сочетании с требованием 12.9 данное требование о составлении письменного соглашения между организацией и сервис-провайдером нацелено на обеспечение понимания сторонами своих обязанностей по стандарту PCI DSS. Например, соглашение может включать соответствующие требования PCI DSS, которые необходимо соблюдать при предоставлении услуги.
12.8.3 Гарантировать, что установленная процедура привлечения сервис-провайдера существует и включает в себя комплексную проверку благонадежности (due diligence) сервис-провайдера до подписания договора с ним.	**12.8.3** Убедитесь, что политики и процедуры документированы, соблюдаются и включают необходимость выполнения комплексной проверки благонадежности сервис-провайдера до подписания договора с ним.	Данный процесс гарантирует, что возможность привлечения сервис-провайдера тщательно изучается внутри организации и включает в себя анализ рисков до установления деловых отношений с этим сервис-провайдером. Конкретные процессы и цели комплексной проверки благонадежности будут зависеть от организации. Примерами факторов, учитываемых при проверке, могут служить отчетность сервис-провайдера, процедуры уведомления об уязвимостях и реагирования на инциденты, сведения о разделении обязанностей по соблюдению требований PCI DSS между сторонами, подтверждение сервис-провайдером соответствия требованиям PCI DSS и предоставление доказательств этого и т.д.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.8.4 Внедрить и поддерживать программу проверки статуса соответствия сервис-провайдера требованиям PCI DSS по меньшей мере один раз в год.	**12.8.4** Убедитесь, что организация внедрила и поддерживает программу проверки статуса соответствия сервис-провайдера требованиям PCI DSS по меньшей мере один раз в год.	Когда вы знаете статус соответствия своих сервис-провайдеров требованиям стандарта PCI DSS, вы можете быть уверены в том, что они соответствуют тем же требованиям, что и ваша организация. Если сервис-провайдер предоставляет широкий спектр услуг, данное требование применяется только к услугам, которые предоставляются клиенту, и только такие услуги клиент должен включать в область оценки на соответствие стандарту PCI DSS. Конкретная информация, которая должна храниться организацией, зависит от действующих соглашений с сервис-провайдерами, вида услуг и т.д. Цель данного требования - обеспечить понимание организацией требований PCI DSS, которые согласились выполнять сервис-провайдеры.
12.8.5 Поддерживать актуальной информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый сервис-провайдер, а за какие несет ответственность сама организация.	**12.8.5** Убедитесь, что организация поддерживает актуальной информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый сервис-провайдер, а за какие несет ответственность сама организация.	
12.9 ***Дополнительное требование только для сервис-провайдеров:*** Сервис-провайдеры должны подтверждать в письменной форме тот факт, что они несут ответственность за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, в той или иной форме, или тот факт, что они несут ответственность за безопасность среды данных держателей карт клиента. ***Примечание:*** *Точная формулировка положения зависит от договора между двумя сторонами, сведений о предоставляемой услуге и обязанностей каждой из сторон по договору. Формулировка положения не обязательно должна копировать формулировку, указанную в данном требовании.*	**12.9** ***Дополнительная проверочная процедура для сервис-провайдеров:*** Изучите политики и процедуры сервис-провайдеров, а также шаблоны письменных соглашений и убедитесь, что сервис-провайдеры письменно обязуются клиентам соблюдать все соответствующие требования PCI DSS к сервис-провайдерам, которые хранят, обрабатывают или передают от имени клиента, в той или иной форме, или так или иначе несут ответственность за безопасность среды данных держателей карт клиента.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* В сочетании с требованием 12.8.2 данное требование нацелено на обеспечение понимания сервис-провайдерами и их клиентами своих обязанностей по стандарту PCI DSS. Сервис-провайдеры должны поддерживать надлежащий уровень безопасности данных держателей карт, которые они получают от своих клиентов. Внутренние политики и процедуры сервис-провайдера, относящиеся к процессу работы с клиентом и любые шаблоны, используемые для письменных соглашений между сторонами, должны включать в себя положение об обязательстве сервис-провайдера соблюдать все применимые требования PCI DSS. Способ, которым сервис-провайдер будет предоставлять свое письменное обязательство должен быть согласован между ним и его клиентами.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.10 Внедрить план реагирования на инциденты. Быть готовым немедленно отреагировать на взлом системы.	**12.10** Ознакомьтесь с планом и процедурами реагирования на инциденты и убедитесь, что организация готова немедленно отреагировать на взлом системы следующим образом:	При отсутствии детального плана реагирования на инциденты безопасности, его распределения, чтения и понимания ответственными сторонами, замешательство и отсутствие унифицированного подхода к реагированию могут увеличить время вынужденного простоя для бизнеса, привести к появлению в средствах массовой информации нежелательной информации, а также к возникновению дополнительных юридических обязательств.
12.10.1 Разработать план реагирования на инциденты, применяемый в случае взлома системы. Убедитесь, что в план включено как минимум следующее: • Роли, обязанности сотрудников, контактные данные и схемы оповещения в случае компрометации, включая, как минимум оповещение платежных систем. • Процедуры реагирования на определенные инциденты. • Процедуры восстановления и обеспечения непрерывности бизнеса. • Процессы резервного копирования данных. • Анализ требований законодательства об оповещении о фактах компрометации. • Покрытие всех критичных системных компонентов. • Ссылки на процедуры или цитаты из процедур реагирования на инциденты платежных систем.	**12.10.1.a** Убедитесь, что план реагирования на инциденты, включает в себя: • Роли, обязанности сотрудников и схемы оповещения в случае компрометации, включая, как минимум оповещение платежных систем. • Процедуры реагирования на определенные инциденты. • Процедуры восстановления и обеспечения непрерывности бизнеса. • Процессы резервного копирования данных. • Анализ требований законодательства об оповещении о фактах компрометации (например, требований Закона Калифорнии №1386, который регламентирует уведомление пострадавших клиентов в случае компрометации или подозрения на компрометацию данных любого предприятия, в базе данных которого есть жители Калифорнии). • Покрытие всех критичных системных компонентов. • Ссылки на процедуры или цитаты из процедур реагирования на инциденты платежных систем.	План реагирования на инциденты должен быть подробным и содержать все ключевые элементы, которые позволят компании эффективно реагировать на обнаруженные инциденты, подвергающие риску данные держателей карт.
	12.10.1.b Опросите сотрудников и проверьте документацию по нескольким ранее зарегистрированным инцидентам или оповещениям безопасности, чтобы убедиться, что документированный план реагирования на инциденты и процедуры были выполнены.	

Требования PCI DSS	Проверочные процедуры	Пояснение
12.10.2 Анализировать и тестировать план не реже одного раза в год, включая все элементы, приведенные в Требовании 12.10.1.	**12.10.2** Опросите сотрудников и проверьте документацию тестирования, чтобы убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год, и тестирование включает все элементы, приведенные в Требовании 12.10.1.	Без надлежащего тестирования можно пропустить ключевые этапы реагирования на инциденты, что может увеличить зону влияния инцидента.
12.10.3 Назначить соответствующих сотрудников, которые должны быть доступны в режиме 24/7 и реагировать на оповещения в режиме 24/7.	**12.10.3** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедитесь в наличии сотрудников, ответственных за круглосуточное и ежедневное реагирование на инциденты, мониторинг свидетельств любой несанкционированной деятельности, обнаружение несанкционированных беспроводных точек доступа, критичных предупреждений систем обнаружения вторжений (IDS) и (или) сообщений о несанкционированных изменениях в критичных системных файлах или файлах данных.	Без обученной и подготовленной группы реагирования на инциденты, сети может быть нанесен серьезный ущерб, а критичные данные и системы могут быть повреждены вследствие ненадлежащего обращения с целевыми системами. Это может помешать расследованию, проводимому после обнаружения инцидента.
12.10.4 Обеспечить надлежащее обучение сотрудников, ответственных за реагирование на нарушения безопасности.	**12.10.4** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедиться в том, что сотрудники, ответственные за реагирование на нарушения безопасности, проходят периодическое обучение.	
12.10.5 Включить в план процедуры реагирования на оповещения систем мониторинга безопасности, включая, без ограничения, системы обнаружения и предупреждения вторжений, межсетевые экраны, а также системы мониторинга целостности файлов.	**12.10.5** Путем наблюдения и изучения процессов убедитесь в том, что план реагирования на инциденты включает в себя процедуры контроля и реагирования на оповещения систем мониторинга безопасности.	Данные системы мониторинга предназначены для того, чтобы отслеживать потенциальный риск в отношении данных, и необходимы для быстрого реагирования в целях предотвращения инцидентов. Такие системы должны быть включены в процессы реагирования на инциденты.
12.10.6 Разработать процесс изменения и улучшения плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	**12.10.6** Путем наблюдения, изучения политик и опроса ответственных сотрудников убедитесь в том, что налажен процесс изменения и улучшения плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	Внесение «полученного опыта» в план реагирования на инциденты после возникновения инцидента помогает поддерживать актуальность плана и быстро реагировать на новые угрозы и тенденции в области безопасности.

Требования PCI DSS	Проверочные процедуры	Пояснение
12.11 ***Дополнительное требование только для сервис-провайдеров:*** Выполнять проверки как минимум ежеквартально, чтобы убедиться в том, что сотрудники соблюдают политики безопасности и установленные регламенты. Проверкам должны подвергаться следующие процессы: • Ежедневная проверка журналов • Проверки массива правил межсетевого экрана • Применение стандартов конфигурации к новым системам • Реагирование на оповещения систем безопасности • Процессы управления изменениями	**12.11.a** Изучите политики и процедуры, чтобы убедиться в том, что в них предусмотрено требование к сотрудникам соблюдать политики безопасности и установленные регламенты, а следующие процессы подвергаются проверкам: • Ежедневная проверка журналов • Проверки массива правил межсетевого экрана • Применение стандартов конфигурации к новым системам • Реагирование на оповещения систем безопасности • Процессы управления изменениями **12.11.b** Опросите ответственных сотрудников и изучите записи о проверках, чтобы убедиться в том, что проверки проводятся как минимум ежеквартально.	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Регулярное подтверждение следования политикам и процедурам безопасности дает уверенность в том, необходимые меры безопасности применяются и работают как следует. Цель этих проверок не в повторном выполнении других требований PCI DSS, а в подтверждении того, что процедуры выполняются как ожидается.
12.11.1 ***Дополнительное требование только для сервис-провайдеров:*** Предусмотреть, чтобы в документы по ежеквартальным проверкам было включено следующее: • Документирование результатов проверок • Изучение и утверждение результатов сотрудниками, ответственными за соблюдение требований стандарта PCI DSS	**12.11.1** Изучите документацию о ежеквартальных проверках, чтобы убедиться, что она включает: • Документирование результатов проверок • Изучение и утверждение результатов сотрудниками, ответственными за соблюдение требований стандарта PCI DSS	***Примечание:*** *Данное требование применимо только тогда, когда проверяемая организация является сервис-провайдером.* Цель этих независимых проверок состоит в подтверждении того, что деятельность по защите выполняется на регулярной основе. Эти проверки могут также быть использованы для проверки того, что необходимые свидетельства их выполнения поддерживаются в актуальном состоянии (например, журналы событий, отчеты о сканировании на уязвимости, пересмотры правил межсетевых экранов, и т.д.) для помощи организации в подготовке к последующей оценке соответствия стандарту PCI DSS.

Приложение A: Дополнительные требования стандарта PCI DSS

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

- Приложение A1: Дополнительные требования стандарта PCI DSS в отношении поставщиков услуг совместного хостинга
- Приложение A2: Дополнительные требования стандарта PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS для подключений POS/POI терминалов, требующих наличие карты
- Приложение A3: Дополнительные проверки для определенных организаций (DESV)

Пояснения и применимость приведены в каждом разделе.

Приложение A1: Дополнительные требования стандарта PCI DSS в отношении поставщиков услуг совместного хостинга

Согласно требованиям 12.8 и 12.9 все сервис-провайдеры, имеющие доступ к данным держателей карт (включая поставщиков услуг совместного хостинга), должны выполнять требования PCI DSS. В дополнение к этому, требование 2.6 говорит о том, что поставщики услуг совместного хостинга должны обеспечивать безопасность данных держателей карт и сред, принадлежащих каждой из обслуживаемых сторон. Таким образом, поставщики услуг совместного хостинга должны дополнительно выполнять требования, перечисленные в этом приложении.

Требования PCI DSS	Проверочные процедуры	Пояснение
A1 Защищать среду и данные каждой организации (т.е. ТСП, сервис-провайдера или иной организации) согласно требованиям с A.1.1 по A.1.4 следующим образом: Поставщик услуг хостинга должен выполнять все эти и остальные соответствующие требования стандарта PCI DSS. ***Примечание:*** *Даже если поставщик услуг хостинга соответствует этим требованиям, это не значит, что каждая организация, которая пользуется его услугами, соответствует требованиям стандарта PCI DSS. Каждая организация должна соответствовать требованиям стандарта PCI DSS и подтверждать свое соответствие применимым для нее способом.*	**A.1** Чтобы убедиться, что поставщик услуг совместного хостинга обеспечивает должный уровень защиты среды и данных организаций (ТСП и сервис-провайдеров), выберите несколько серверов (под управлением Windows и Unix/Linux) в репрезентативной выборке ТСП и сервис-провайдеров и проведите проверки, перечисленные в пунктах с A.1.1 по A.1.4:	*Приложение A* к стандарту PCI DSS предназначено для поставщиков услуг совместного хостинга, которые желают предоставлять своим клиентам (ТСП и/или сервис-провайдерам) среду размещения данных, которая соответствует требованиям стандарта PCI DSS.

Требования PCI DSS	Проверочные процедуры	Пояснение
A.1.1 Гарантировать, что каждая организация выполняет только процедуры, согласно которым у нее имеется доступ исключительно к своей среде данных держателей карт.	**A.1.1** Если поставщик услуг совместного хостинга позволяет организациям (например, ТСП или сервис-провайдерам) запускать собственные приложения, убедитесь, что эти приложения выполняются под уникальным идентификатором такой организации. Например: • Ни одна организация в системе не может использовать идентификатор пользователя общего веб-сервера. • Все CGI-скрипты, используемые организацией, должны быть созданы и выполняться под уникальным идентификатором пользователя.	Если ТСП или сервис-провайдеру разрешается выполнять свои собственные приложения на совместно используемом сервере, то они должны выполняться под идентификатором такого ТСП или сервис-провайдера, а не под идентификатором привилегированного пользователя.
A1.2 Ограничивать доступ и привилегии каждой организации только ее собственной средой данных держателей карт.	**A.1.2.a** Убедитесь, что ни один идентификатор пользователя для процессов приложения не является идентификатором привилегированного пользователя (пользователя с неограниченными правами доступа/с правами администратора).	Чтобы гарантировать, что доступ и полномочия предоставляются так, что каждые ТСП или сервис-провайдер имеют доступ только к собственной среде, необходимо принять во внимание, следующее: 1. Привилегии идентификатора пользователя веб-сервера ТСП или сервис-провайдера; 2. Разрешения на чтение, запись и исполнение файлов; 3. Разрешения на запись в системные двоичные файлы; 4. Разрешения на доступ к файлам журналов ТСП или сервис-провайдера; 5. Меры защиты системных ресурсов от монополизации одним ТСП или одним сервис-провайдером.
	A1.2.b Убедитесь, что каждая организация (ТСП, сервис-провайдер) имеет права чтения, записи и выполнения только для тех файлов и директорий, которыми она обладает, или для требуемых файлов системы (доступ к которым ограничен разрешениями файловой системы, списками контроля доступа, средствами chroot, jailshell и т.д.). **Обратите внимание!** Файлы организации не должны быть доступны группе пользователей.	
	A.1.2.c Убедитесь, что у пользователей организации нет доступа с правом записи к совместно используемым системным двоичным файлам.	
	A.1.2.d Убедитесь, что просмотр журналов регистрации событий доступен только владельцу.	
	A.1.2.e Чтобы гарантировать, что одна организация не может монополизировать ресурсы сервера для эксплуатации уязвимостей (например, ошибок, единовременного потребления ресурсов и условий перезапуска, результатом которых может стать переполнение буфера), следует убедиться, что на использование таких ресурсов системы установлены ограничения: • Дисковое пространство • Пропускная способность • Память • ЦП	

Требования PCI DSS	Проверочные процедуры	Пояснение
A1.3 Гарантировать, что выполняется регистрация действий и событий каждой среды данных держателей карт организации с сохранением уникальных данных по каждой организации и что такая регистрация соответствует Требованию 10 стандарта PCI DSS.	**A.1.3** Убедитесь, что поставщик услуг совместного хостинга обеспечивает ведение журналов регистрации событий для каждой среды ТСП и сервис-провайдера: • Ведется регистрация событий в отношении распространенных сторонних приложений. • Включена регистрация событий по умолчанию. • Журналы доступны для просмотра организации, которая ими владеет. • Месторасположение журналов сообщено организации, владеющей журналами.	Журналы должны быть доступны в общей среде размещения данных так, чтобы ТСП и сервис-провайдеры имели доступ и могли просматривать журналы регистрации событий, относящиеся только к собственной среде данных держателей карт.
A1.4 Предусмотреть процессы, позволяющие провести своевременную экспертизу в случае компрометации любых ТСП или сервис-провайдеров, размещенных на хостинге.	**A.1.4** Убедитесь в наличии у поставщика услуг совместного хостинга политик, которые требуют своевременно проводить экспертизу соответствующих серверов в случае компрометации.	Поставщики услуг совместного хостинга должны иметь процессы для быстрого реагирования в случае компрометации, если требуется расследование инцидентов, вплоть до такого уровня детализации, чтобы можно было получить подробные сведения о конкретном ТСП или сервис-провайдере.

Приложение A2: Дополнительные требования стандарта PCI DSS для организаций, использующих протокол SSL/раннюю версию TLS для подключений POS/POI терминалов, требующих наличие карты

Организации, использующие протокол SSL и раннюю версию TLS для подключений POS/POI терминалов, требующих наличие карты, должны как можно скорее рассмотреть переход на надежный криптографический протокол. Кроме того, протокол SSL и ранняя версия TLS не должны внедряться в среды, где эти протоколы отсутствуют. На момент публикации стандарта, известные уязвимости сложно использовать в платежных терминалах POS POI. Тем не менее, в любой момент могут возникнуть новые уязвимости, и от организации зависит, защищена ли она от современных уязвимостей и может ли определить насколько она подвержена или не подвержена воздействию известных уязвимостей.

Непосредственно затронутые требования стандарта PCI DSS:

Требование 2.2.3	Настраивать дополнительные параметры безопасности для любых необходимых служб, протоколов и демонов, которые признаны небезопасными.
Требование 2.3	При использовании неконсольного административного доступа к системе шифровать канал с использованием стойких криптографических алгоритмов.
Требование 4.1	Использовать стойкую криптографию и протоколы безопасности для защиты конфиденциальных данных держателей карт при их передаче в открытых общедоступных сетях.

Для выполнения этих требований протокол SSL и ранняя версия TLS не должны быть использованы в качестве механизма обеспечения безопасности, за исключением случаев использования подключений POS/POI терминалов, как указано в настоящем Приложении. Для помощи организациям, которые работают над переходом с протокола SSL и ранней версии TLS на POS/POI терминалах, включены следующие положения:

- Новые POS/POI терминалы не должны использовать протоколы SSL и раннюю версию TLS в качестве механизмов обеспечения безопасности.
- Все сервис-провайдеры POS/POI терминалов должны обеспечить безопасное предоставление услуг.
- Сервис-провайдеры, поддерживающие существующие POS/POI терминалы, использующие протоколы SSL и/или раннюю версию TLS должны иметь официальный План снижения риска и миграции.
- POS/POI терминалы в средах, требующих присутствия карт, которые могут быть верифицированы как устойчивые по отношению к любым известным уязвимостям для протокола SSL и ранней версии TLS, **а также оконечные точки терминации SSL/TLS, к которым они подключены**, могут продолжать использовать эти протоколы, как механизмы обеспечения безопасности.

Данное Приложение применимо к организациям, использующим протокол SSL/раннюю версию TLS в качестве механизмов обеспечения безопасности POS/POI терминалов, включая сервис-провайдеров, которые обеспечивают подключения к POS/POI терминалов.

Требования PCI DSS	Проверочные процедуры	Пояснение
A2.1 В случае использования терминалами POS/POI (в ТСП или месте приема карт) протокола SSL и/или ранней версии TLS, организация должна подтвердить, что устройства не подвержены никаким известным уязвимостям этим протоколов. ***Примечание:*** *Предполагается, что данное требование применяется в отношении организации с POS/POI терминалом, например ТСП. Данное требование не применяется в отношении сервис-провайдера, который выполняет функцию точки соединения для POS/POI терминалов. Требования A2.2 и A2.3 применяются к сервис-провайдерам POS/POI терминалов.*	**A2.1** *В отношении терминалов POS/POI, использующих протокол SSL и/или раннюю версию TLS*, подтвердите, что у организации имеется документация (например, документация производителя, информация о конфигурации системы/сети, и т.д.), которая подтверждает, что устройства не подвержены никаким известным уязвимостям в отношении протокола SSL и/или ранней версии TLS.	POS/POI терминалы, используемые в средах, требующих присутствия карт, могут продолжать использовать протокол SSL и/или раннюю версию TLS, если они могут подтвердить, что POS/POI терминалы Не подвержены известным уязвимостям. Тем не менее, протокол SSL является устаревшей технологией и в будущем может быть подвержен дополнительным уязвимостям; потому настоятельно рекомендуется перевести POS/POI терминалы на надежный протокол в кратчайшие сроки. Если протокол SSL/ранняя версия TLS не требуются для среды, то использование и откат до этих версий необходимо отключить. Для получения дополнительной информации изучите документ «Дополнения к Стандарту» Совета по стандартам безопасности индустрии платежных карт (PCI SSC), касающийся протокола SSL/ранней версии TLS. ***Примечание:*** *Допущения для POS/POI терминалов, которые, на текущий момент, устойчивы к известным уязвимостям, основываются на текущих известных рисках. При появлении новых уязвимостей, к которым POS/POI терминалы уязвимы, POS/POI терминалы необходимо будет незамедлительно обновить.*

Требования PCI DSS	Проверочные процедуры	Пояснение
A2.2 ***Требование только для сервис-провайдеров*****:** Все сервис-провайдеры, имеющие точки подключения к POS/POI терминалам, указанным в Требовании A2.1 и использующим протоколы SSL и/или раннюю версию TLS, должны иметь официальный План снижения риска и миграции.	**A2.2** Изучите официальный План снижения риска и миграции и убедитесь, что он включает в себя: • Описание применения, включая то, какие данные передаются, типы и количество систем, которые используют и/или поддерживают протокол SSL и раннюю версию TLS, тип среды; • Результаты оценки рисков и используемые средства снижения рисков; • Описание процедур контроля новых уязвимостей, связанных с протоколом SSL/ранней версии TLS; • Описание процессов управления изменениями, обеспечивающих контроль за отсутствием протокола SSL и ранних версий TLS в новых средах; • Краткое описание плана по миграции, предусматривающего замену протокола SSL и ранних версий TLS в будущем.	Точки подключений POS/POI терминалов, включая, но не ограничиваясь сервис-провайдерами, такими как эквайреры или процессинговые компании эквайреров, могут продолжать использовать протокол SSL/раннюю версию TLS, если сервис-провайдер может подтвердить, что он имеет механизмы контроля, которые способны снизить риск поддержки таких подключений для среды сервис-провайдера. План снижения риска и миграции – это документ, подготовленный организацией, который детально описывает планы организации по переходу на безопасный протокол, а также описывает действующие меры, используемые организацией для снижения рисков, связанных с протоколом SSL/ранней версией TLS, до того момента, как миграция будет завершена. Сервис-провайдеры должны сообщить всем клиентам, использующим протокол SSL/раннюю версию TLS, о рисках, связанных с их использованием, а также о необходимости перейти на безопасный протокол. Для получения дополнительной информации изучите документ «Дополнения к Стандарту» Совета по стандартам безопасности индустрии платежных карт (PCI SSC), касающийся SSL/ранней версии TLS.
A2.3 ***Требование только для сервис-провайдеров*****:** Все сервис-провайдеры должны обеспечить безопасное предоставление услуг.	**A2.3** Изучите системные конфигурации и сопутствующую документацию, чтобы убедиться, что сервис-провайдер предоставляет безопасный протокол для своего сервиса.	Сервис-провайдеры, поддерживающие протокол SSL/раннюю версию TLS для POS/POI терминалов, должны также поддерживать безопасный протокол подключения. Для получения дополнительной информации изучите документ «Дополнения к Стандарту» Совета по стандартам безопасности индустрии платежных карт (PCI SSC), касающийся SSL/ранней версии TLS.

Приложение A3: Дополнительные проверки для определенных организаций (DESV)

Данное приложение применяется в отношении организаций, которых платежные системы или эквайрер отдельно определили, как организации, требующие проведения дополнительных проверок на соблюдение существующих требований стандарта PCI DSS. Примеры организаций, к которым **может быть** применено данное Приложение, включают:

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

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

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

***A3.1** Внедрить программу соответствия стандарту PCI DSS.*

***A3.2** Задокументировать и подтвердить область применения PCI DSS.*

***A3.3** Подтвердить, что стандарт PCI DSS включен в традиционные бизнес-процессы.*

***A3.4** Контролировать и управлять логическим доступом в среду данных держателей карт.*

***A3.5** Выявлять и реагировать на подозрительные события.*

***Примечание:** Некоторые требования имеют определенные временные рамки (к примеру, выполнять не реже одного раза в квартал или каждые полгода), в пределах которых должны выполняться определенные процедуры. При первой проверке согласно данному документу, не требуется, чтобы процедура была реализована в каждый такой указанный временной период в течение предыдущего года, если аудитор сможет подтвердить, что:*

1) *Процедура была выполнена в соответствии с применимым требованием в пределах недавнего времени (т.е. самого ближайшего прошлого квартала или полугодия) и*
2) *Организация задокументировала политики и процедуры для продолжения реализации деятельности в установленные сроки.*

В последующие годы после первого аудита, процедура должна быть выполнена в каждый установленный срок, под требования которого она подпадает (к примеру, ежеквартальная процедура должна быть выполнена в каждый из четырех кварталов предыдущего года).

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

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.1 Внедрить программу соответствия стандарту PCI DSS.		
A3.1.1 Высшему руководству следует установить ответственность по защите данных держателей карт и программы соответствия стандарту PCI DSS, которая должна включать: • Полную подотчетность за обеспечение соответствия стандарту PCI DSS • Определение устава программы соответствия стандарту PCI DSS • Не реже одного раза в год предоставлять отчет высшему руководству и совету директоров относительно вопросов и инициатив по программе соответствия стандарту PCI DSS, включая процедуры исправлений недочетов ***Ссылка на PCI DSS:*** *Требование 12*	**A3.1.1.a** Изучите документацию, чтобы убедиться, что высшее руководство установило полную подотчетность за обеспечение соответствия организации стандарту PCI DSS. **A3.1.1.b** Изучите устав компании в отношении стандарта PCI DSS, чтобы убедиться, что он излагает условия, на основании которых организована программа соответствия стандарту PCI DSS. **A3.1.1.c** Изучите протоколы совещаний и/или презентаций высшего руководства и совета директоров, чтобы убедиться, что инициативы по программе соответствия стандарту PCI DSS и процедурам исправлений недочетов доводятся до их сведения, как минимум, раз в год.	Назначение высшим руководством ответственности за соответствие стандарту PCI DSS обеспечивает прозрачность программы соответствия стандарту PCI DSS на руководящем уровне и дает возможность задавать соответствующие вопросы для определения эффективности программы и ее влияния на стратегические приоритеты. Полная ответственность за программу соответствия стандарту PCI DSS может быть возложена на определенных сотрудников и/или структурные подразделения внутри организации.
A3.1.2 Официальная программа соответствия PCI DSS должна включать: • Определение процедур для поддержания и мониторинга полного соответствия стандарту PCI DSS, включая традиционные бизнес-процессы • Процессы проведения ежегодной оценки соответствия Стандарту PCI DSS • Процедуры непрерывной оценки требований стандарта PCI DSS (к примеру, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием) • Анализ последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения ***Ссылка на PCI DSS:*** *Требования 1-12*	**A3.1.2.a** Проверьте политики и процедуры информационной безопасности и убедитесь, что они содержат следующие процессы, предусматривающие: • Поддержание и мониторинг полного соответствия стандарту PCI DSS, включая традиционные бизнес-процессы • Ежегодное проведение оценки на соответствие стандарту PCI DSS • Процедуры непрерывной оценки требований стандарта PCI DSS • Анализ последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения	Официальная программа соответствия позволяет организации отслеживать степень исправности ее механизмов и мер защиты, предупреждать случаи отказа механизмов, и эффективно обмениваться данными о действиях и статусе соответствия по всей организации. Программа соответствия стандарту PCI DSS может быть отдельной программой или частью программы соответствия и/или управления; должна включать четко определенную методологию, которая демонстрировала бы последовательную и эффективную оценку. К примерам таких методологий относятся: Методология PDCA (или Цикл Деминга «Plan-Do-Check-Act»), ISO 27001, COBIT, DMAIC, и Six Sigma. *(Продолжение на следующей странице)*

Требования PCI DSS	Проверочные процедуры	Пояснение
	A3.1.2.b Опросите сотрудников и изучите процедуры обеспечения соответствия, чтобы убедиться, что такие процедуры реализованы с целью обеспечить: • Поддержание и мониторинг полного соответствия стандарту PCI DSS, включая традиционные бизнес-процессы • Ежегодное проведение оценки на соответствие стандарту PCI DSS • Процедуры непрерывной оценки требований стандарта PCI DSS • Анализ последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения	Поддержание и мониторинг соответствия организации требованиям PCI DSS включает в себя определение перечня действий, которые должны выполняться ежедневно, еженедельно, ежемесячно, ежеквартально или ежегодно, и обеспечение выполнения этих действий соответствующим образом (например, с использованием самооценки уровня безопасности или методологии PDCA). К примерам стратегических бизнес-решений, которые следует проанализировать на предмет потенциального влияния требований PCI DSS, могут относиться слияния и поглощения, покупки новых технологий или новые каналы приема платежей.
A3.1.3 Четко определить задачи и области ответственности в отношение соответствия стандарту PCI DSS, и официально возложить ответственность на одного или более сотрудников, и включать, как минимум, следующее: • Управление процедурами PCI DSS относительно традиционных бизнес-процессов • Управление ежегодными оценками соответствия стандарту PCI DSS • Управление непрерывной оценкой требований стандарта PCI DSS (к примеру, ежедневно, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием) • Управление анализом последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения ***Ссылка на PCI DSS:*** *Требование 12*	**A3.1.3.a** Изучите политики и процедуры информационной безопасности и опросить сотрудников, чтобы убедиться, что задачи и области ответственности четко определены и обязанности распределены так, чтобы они включали, как минимум, следующее: • Управление процедурами PCI DSS относительно традиционных бизнес-процессов • Управление ежегодными оценками соответствия стандарту PCI DSS • Управление непрерывной оценкой требований стандарта PCI DSS (к примеру, ежедневно, еженедельно, ежеквартально и пр., насколько это применимо в соответствии с требованием) • Управление анализом последствий для деятельности с целью определения потенциального влияния стандарта PCI DSS на стратегические бизнес-решения **A3.1.3.b** Опросите ответственных сотрудников и убедитесь, что они осведомлены об обязанностях и выполняют возложенные на них обязанности по соблюдению соответствия стандарту PCI DSS.	Официальное определение конкретных ролей и ответственности за соблюдение соответствия стандарту PCI DSS помогает обеспечить подотчетность и мониторинг текущей деятельности, ведущейся в отношении соблюдения соответствия стандарту PCI DSS. Данные роли могут быть назначены одному сотруднику или нескольким, учитывая разные направления. Роли должны назначаться сотрудникам, имеющим полномочия принимать решения, основанные на анализе рисков, и на ком лежит ответственность за определенную функцию. Обязанности должны быть официально определены и ответственные должны суметь продемонстрировать понимание своей зоны ответственности и подотчетности.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.1.4 Обеспечить обучение сотрудников по действующему стандарту PCI DSS и/или по вопросам информационной безопасности, как минимум, раз в год, для сотрудников, несущих ответственность за соответствие стандарту PCI DSS (указанных в пункте A3.1.3) ***Ссылка на PCI DSS:*** *Требование 12*	**A3.1.4.a** Изучите политики и процедуры информационной безопасности, чтобы убедиться, что обучение по стандарту PCI DSS и/или вопросам информационной безопасности требуются не реже одного раза в год для каждой роли, в обязанности которой входит обеспечение соответствия стандарту PCI DSS.	Сотрудники, в обязанности которых входит соответствие стандарту PCI DSS, нуждаются в специальных знаниях, превышающих те, что обычно предоставляются на общих тренингах по безопасности. Сотрудники, в обязанности которых входит обеспечение соответствия стандарту PCI DSS, должны проходить специальные тренинги, которые, в дополнение к общим знаниям по информационной безопасности, фокусируются на специальных вопросах, навыках, процедурах или методиках безопасности, которые должны соблюдаться указанными сотрудниками, для должного исполнения своих обязанностей. Тренинги могут проводиться третьей стороной – к примеру, SANS или PCI SSC (Ознакомление с PCI, PCIP, и ISA), платежными системами и эквайрерами – или же могут быть внутренними. Обучающие материалы должны разрабатываться для каждой роли и быть актуальными, содержать информацию обо всех последних угрозах безопасности и/или версии PCI DSS. Для получения дополнительной информации о разработке обучающих материалов для конкретных ролей см. документ «Дополнения к Стандарту» Совета по стандартам безопасности индустрии платежных карт (PCI SSC), касающийся «Лучших практик по внедрению программы повышения осведомленности в области безопасности» (Best Practices for Implementing a Security Awareness Program).
	A3.1.4.b Опросите сотрудников и изучите сертификаты о прохождении курсов или прочие записи, чтобы убедиться, что сотрудники, в обязанности которых входит обеспечение соответствия стандарту PCI DSS проходят обучение по стандарту PCI DSS и/или вопросам информационной безопасности не реже одного раза в год.	

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2 Документировать и подтверждать область применения PCI DSS		
A3.2.1 Документировать и подтверждать правильность области применения PCI DSS не реже раза в квартал и при значительных изменениях в среде. Минимум, который должен входить в ежеквартальную проверку области применения стандарта: • Определение всех сетей и системных компонентов, входящих в область применения стандарта • Определение всех сетей, не входящих в область применения стандарта, и подтверждение того, что они не входят в области действия, включая описание используемых механизмов сегментации • Идентификация всех подключенных организаций (например, сторонних организаций, имеющих доступ к среде данных держателей карт) ***Ссылка на PCI DSS:*** *Область действия требований Стандарта PCI DSS*	**A3.2.1.a** Изучите документированные результаты проверки области применения стандарта и опросите сотрудников, чтобы убедиться, что проверки выполняются: • Не реже одного раза в квартал • При значительных изменениях в среде ДДК. **A3.2.1.b** Изучите документированные результаты ежеквартальной проверки области действия стандарта, чтобы убедиться, что выполняется: • Определение всех сетей и системных компонентов, входящих в область применения стандарта • Определение всех сетей, не входящих в область применения стандарта, и подтверждение того, что они не входят в области действия, включая описание используемых механизмов сегментации • Идентификация всех подключенных организаций, например, сторонних организаций, имеющих доступ к среде данных держателей карт	Подтверждение области применения стандарта PCI DSS должно выполняться настолько часто, насколько это возможно для того, чтобы убедиться, что область применения стандарта PCI DSS остается актуальной и совпадает с изменяющимися бизнес-целями.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.2 Определять влияние всех изменений в системах или сетях, включая введение новых систем и новых сетевых соединений, на область применения PCI DSS. Процедуры должны включать: • Выполнение официальной проверки влияния PCI DSS • Определение требований PCI DSS, применимых к системе или сети • Соответствующее обновление области применения PCI DSS • Документально подтвержденные подписью ответственного сотрудника результаты проверки влияния (как указано в пункте A3.1.3) ***Ссылка на PCI DSS:*** *Область действия стандарта PCI DSS, Требования 1-12*	**A3.2.2** Изучите документацию по изменениям и опросите сотрудников, чтобы убедиться, что по каждому изменению в системе или сети: • Была выполнена официальная проверка влияния PCI DSS • Определены требования PCI DSS, применимые к изменениям в системе или сети • Обновлена область применения PCI DSS в соответствии с изменением • Подпись ответственного сотрудника (как описано в требовании A3.1.3) была получена и задокументирована	Изменения в системах или сетях могут иметь значительное влияние на область применения PCI DSS. К примеру, изменения правил межсетевого экрана может привести к включению в область применения стандарта всех сегментов сети, или в среду ДДК могут быть добавлены новые системы, которые потребуют соответствующей защиты. Процедуры определения влияния изменений в системах или сетях на область применения PCI DSS, могут выполняться как часть отдельной программы соответствия стандарту PCI DSS или же быть частью общей программы соответствия и/или управления организации.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.2.1 По завершению изменения проверять все соответствующие требования стандарта PCI DSS по всем новым или измененным системам и сетям, и обновляйте документацию соответствующим образом. Примеры требований PCI DSS, которые должны быть подтверждены, включают, но не ограничиваются: ▪ Сетевая схема обновлена и отражает изменения. ▪ Системы настроены согласно стандартам конфигурации, с изменением всех паролей по умолчанию и отключением ненужных сервисов. ▪ Системы защищены необходимыми механизмами (например, мониторинг целостности файлов (FIM), антивирус, патчи безопасности, ведение журналов аудита). ▪ Подтверждение того, что критичные аутентификационные данные (SAD) не хранятся и, что все хранилища данных держателей карт задокументированы и включены в политики и процедуры хранения данных. ▪ Новые системы включены в ежеквартальное сканирование на наличие уязвимостей. ***Ссылка на PCI DSS:*** *Область действия стандарта PCI DSS, Требования 1-12*	**A3.2.2.1** Для выборки изменений систем и сети, изучите записи об изменениях, опросите сотрудников и понаблюдайте за измененными системами/сетями, чтобы убедиться, что все применимые требования стандарта PCI DSS были применены и документация обновлена как часть изменений.	Важно иметь процедуры для анализа всех изменений, чтобы гарантировать применение всех соответствующих стандарту PCI DSS мер защиты для любых систем или сетей, добавленных или измененных в рамках области проверяемой среды. Встраивание данной проверки в процедуры управления изменениями способствует поддержанию в актуальном состоянии перечня устройств и стандартов конфигураций, а также применения защитных мер там, где это требуется. Процедура управления изменениями должна включать свидетельства, подтверждающие реализацию требований PCI DSS или их итеративное выполнение.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.3 При изменении в организационной структуре (к примеру, слияние или приобретение компаний, смена или переназначение сотрудников, несущих ответственность за защитные меры) необходимо обеспечить официальную (внутреннюю) проверку влияния на область применения PCI DSS и применимость защитных мер. ***Ссылка на PCI DSS:*** *Требование 12*	**A3.2.3** Изучите политики и процедуры, чтобы убедиться, что изменение организационной структуры ведет к официальной проверке влияния на область применения PCI DSS и применимости защитных мер.	Структура и система управления организации определяют требования и протокол для эффективной и безопасной деятельности. Изменения этой структуры может оказать негативное влияние на существующие механизмы и инфраструктуру вследствие перераспределения или удаления ресурсов, которые поддерживали защитные меры PCI DSS, или же обретения новых обязанностей, для которых не применяются защитные меры. Потому важно пересматривать области применения и защитные меры PCI DSS при выполнении изменений, чтобы обеспечить реализацию защитных мер и их использование.
A3.2.4 В случае применения сегментации, подтверждать область применения стандарта PCI DSS выполнением тест на проникновение в отношении механизмов сегментации не реже одного раза в полгода и при любых изменениях механизмов/методов сегментации. ***Ссылка на PCI DSS:*** *Требование 11*	**A3.2.4** Изучите результаты последнего теста на проникновение и убедитесь в том, что: • Тест на проникновение выполняется для проверки механизмов сегментации не реже одного раза в год и после любого изменения средств/методов сегментации. • Тест на проникновение включает в себя все используемые средства/методы сегментации. • Тест на проникновение подтверждает, что средства/методы сегментации осуществимы и эффективны, и позволяют изолировать все системы, не входящие в объем проверки, от систем включенных в CDE.	В случае использования сегментации для отделения сетей входящих в область применения стандарта от сетей вне этой области, данные механизмы сегментации должны быть проверены посредством теста на проникновение с целью подтвердить, что они работают надлежащим образом и эффективны. Техники проведения теста на проникновение должны быть разработаны на основе существующей методологии, как описано в Требовании 11 стандарта PCI DSS. Дополнительную информацию по эффективному проведению теста на проникновение можно найти в документе «Дополнения к Стандарту» Совета по стандартам безопасности индустрии платежных карт (PCI SSC), касающемся «Руководства по тестированию на проникновение» (Penetration Testing Guidance).

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.5 Внедрить методологию обнаружения данных для подтверждения области применения PCI DSS и определения всех источников и местоположения PAN, представленных в открытом виде, не реже раза в квартал и при значительных изменениях в среде данных держателей карт или процессах. Методология обнаружения данных должна учитывать возможности того, что PAN, представленные в открытом виде, могут храниться в системах и сетях за пределами ранее определенной среды данных держателей карт. ***Ссылка на PCI DSS:*** *Область действия требований Стандарта PCI DSS*	**A3.2.5.a** Изучите документированную методологию обнаружения данных, чтобы убедиться в следующем: • Методология обнаружения данных включает процедуры для обнаружения всех источников и местоположения PAN, представленных в открытом виде. • Методология обнаружения учитывает возможности того, что PAN, представленные в открытом виде, могут храниться в системах и сетях за пределами ранее определенной среды данных держателей карт. **A3.2.5.b** Изучите последние результаты проведенных работ по обнаружению данных и опросите ответственных сотрудников, чтобы убедиться, что обнаружение данных выполняется не реже раза в квартал и при значительных изменениях в среде данных держателей карт или процессах.	Стандарт PCI DSS требует, чтобы проверяемые организации, в рамках оценки, идентифицировал и документировали наличие всех PAN, представленных в открытом виде, в своей среде. Внедрение методологии обнаружения данных, которая определяет все источники и местоположение PAN и позволяет обнаруживать PAN за пределами ранее определенной среды данных держателей карт, или же в неожиданных местах внутри определенной среды данных держателей карт (например, журналах регистрации ошибок или файл дампа памяти) помогает убедиться, что неизвестные ранее местоположения PAN, представленных в открытом виде, выявлены и должным образом защищены. Процесс обнаружения данных может быть выполнен с помощью разнообразных методов, включающих, но не ограничивающихся: (1) коммерческие программы обнаружения данных; (2) программа обнаружения данных, разработанная самой организацией; (3) ручной поиск. Вне зависимости от того, какой метод используется, целью работы является выявление всех источников и местоположений PAN, представленных в открытом виде (не только в рамках среды данных держателей карт).
A3.2.5.1 Обеспечить эффективность методов, используемых для обнаружения данных – т.е. методы должны позволять обнаруживать PAN, представленные в открытом виде, во всех типах системных компонентов (например, в каждой операционной системе или платформе) и используемых файловых форматах. Эффективность методов обнаружения данных должна подтверждаться не реже одного раза в год.	**A3.2.5.1.a** Опросите сотрудников и изучите документацию для подтверждения, что: ▪ В организации внедрена и используется процедура тестирования эффективности методов обнаружения данных. ▪ Процедура включает подтверждение того, что методы в состоянии выявить PAN, представленные в открытом виде, во всех типах системных компонентов и используемых файловых форматах.	Процедура проверки эффективности методов обнаружения данных, обеспечивает завершенность и точность выявления данных держателей карт. Для полноты проверки в процедуру обнаружения данных должны, как минимум, быть включены выборки системных компонентов, как из систем в области оценки, так и вне ее. Полноту можно проверить, поместив тестовые PAN в выборку используемых системных компонентов и файлов, и далее подтвердив, что метод обнаружения данных обнаружил тестовые PAN.

Требования PCI DSS	Проверочные процедуры	Пояснение
Ссылка на PCI DSS: *Область действия требований Стандарта PCI DSS*	**A3.2.5.1.b** Изучите результаты недавних проверок на эффективность, чтобы убедиться, что эффективность методов, применяемых для обнаружения данных подтверждается не реже одного раза в год.	
A3.2.5.2 Внедрить процедуры реагирования на события обнаружения PAN, представленных в открытом виде, вне среды данных держателей карт. Процедуры должны включать: ▪ Процедуры, определяющие порядок действий при обнаружении PAN, представленных в открытом виде, вне среды данных держателей карт, включая их извлечение, безопасное удаление и/или перенос в среду данных держателей карт. ▪ Процедуры для определения того, как данные оказались вне среды данных держателей карт. ▪ Процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые привели к тому, что данные оказались вне среды данных держателей карт. ▪ Процедуры по определению источника данных. ▪ Процедуры для определения того, не хранятся ли данные дорожек вместе с PAN.	**A3.2.5.2.a** Изучите документированные процедуры реагирования, чтобы убедиться, что процедуры реагирования на события обнаружения PAN, представленных в открытом виде, вне среды данных держателей карт определены и включают: ▪ Процедуры, определяющие порядок действий при обнаружении PAN, представленных в открытом виде, вне среды данных держателей карт, включая их извлечение, безопасное удаление и/или перенос в среду данных держателей карт. ▪ Процедуры для определения того, как данные оказались вне среды данных держателей карт. ▪ Процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые привели к тому, что данные оказались вне среды данных держателей карт. ▪ Процедуры по определению источника данных; ▪ Процедуры для определения того, не хранятся ли данные дорожек вместе с PAN.	Наличие документированных процедур реагирования, которым необходимо следовать в случае выявлении PAN, представленных в открытом виде, вне среды данных держателей карт, помогает определить нужные действия по устранению и предупреждению будущих утечек. К примеру, если PAN обнаружен вне среды данных держателей карт, необходимо выполнить анализ на: (1) определение того, был ли номер сохранен отдельно или же совместно с другими данными (или это была часть полной дорожки); (2) определение источника данных и (3) определение проблем в существующих мерах защиты, которые стали причиной нахождения данных вне среды данных держателей карт.
	A3.2.5.2.b Опросите сотрудников и изучите документацию по процедурам реагирования, чтобы убедиться, что мероприятия по устранению последствий при выявлении PAN, представленных в открытом виде, вне среды данных держателей карт выполняются.	

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.2.6 Внедрить механизмы обнаружения и предотвращения утечки PAN, представленных в открытом виде, из среды данных держателей карт через неавторизованные каналы, средства или механизмы, включая генерацию журналов событий и оповещений. ***Ссылка на PCI DSS:*** *Область действия требований Стандарта PCI DSS*	**A3.2.6.a** Изучите документацию и проследите за внедренными механизмами, чтобы убедиться, что механизмы: • Внедрены и активно работают. • Настроены на обнаружение и предотвращение утечки PAN, представленных в открытом виде, из среды данных держателей карт через неавторизованные каналы, средства или механизмы. • Генерируют журналы событий и оповещения относительно утечки PAN, представленных в открытом виде, из среды данных держателей карт через неавторизованный канал, средство или механизм.	Механизмами для обнаружения и предотвращения неавторизованной потери PAN, представленных в открытом виде, могут быть соответствующие инструменты (такие как решения по Предотвращению утечек (DLP)) и/или ручные процессы или механизмы. Механизмы должны обеспечивать обнаружение PAN в открытом виде в следующих местах, включая: электронные письма, загрузки на съемные носители и вывод на принтер. Использование данных механизмов позволяет организации выявлять и предотвращать ситуации, которые могут привести к потери данных.
	A3.2.6.b Изучите журналы аудита и предупреждения и опросите ответственных сотрудников, чтобы убедиться, что оповещения анализируются.	
A3.2.6.1 Внедрить процедуры реагирования, которые будут выполняться при выявлении попытки удалить PAN, представленных в открытом виде, из среды данных держателей карт через неавторизованный канал, средство или механизм. Процедуры реагирования должны включать: ▪ процедуры своевременного расследования предупреждений ответственными сотрудниками; ▪ процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые потребуются для предотвращения потери данных.	**A3.2.6.1** Изучите документацию по процедурам реагирования, чтобы убедиться, что процедуры реагирования на попытки удалить PAN, представленные в открытом виде, из среды данных держателей карт через неавторизованный канал, средство или механизм включают: ▪ процедуры своевременного расследования предупреждений ответственными сотрудниками; ▪ процедуры для устранения утечки данных или проблем в существующих мерах защиты, которые потребуются для предотвращения потери данных.	Попытки удалить PAN, представленные в открытом виде, из среды данных держателей карт через неавторизованный канал, средство или механизм могут указывать на кражу данных или на действия авторизованного сотрудника, который не знает или просто не следует должным методам. Своевременное расследование подобных случаев может выявить те зоны, где требуется исправление и дает ценную информацию, которая помогает понять, откуда исходит угроза.
	A3.2.6.1.b Опросите сотрудников и изучите записи о предпринятых действиях при выявлении утечки PAN, представленных в открытом виде, из среды данных держателей карт через неавторизованный канал, средство или механизм и убедитесь, что меры по устранению были предприняты.	

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3 Подтвердите, что стандарт PCI DSS включен в традиционные бизнес-процессы		
A3.3.1 Внедрить процесс для незамедлительного выявления и предупреждения отказов критических механизмов обеспечения безопасности. Примеры критических механизмов защиты включают, но не ограничиваются: • Межсетевые экраны • Системы обнаружения и предотвращения вторжений (IDS/IPS) • Мониторинг целостности файлов (FIM) • Антивирус • Средства физического контроля доступа • Средства логического контроля доступа • Механизмы ведения журналов аудита • Средства контроля сегментации (если применимо) ***Ссылка на PCI DSS:*** *Требования 1-12*	**A3.3.1.a** Изучите документированные политики и процедуры, чтобы убедиться в наличии процедур своевременного выявления и регистрации всех отказов механизмов защиты. **A3.3.1.b** Изучите процедуры выявления и оповещения и опросите персонал, чтобы убедиться, что процедуры внедрены для всех механизмов обеспечения безопасности и, что отказ какого-либо механизма обеспечения безопасности приводит к генерации оповещений.	Без официальных процедур мгновенного выявления и оповещения при отказе механизма защиты, отказы могут оставаться невыявленными продолжительный период, тем самым, давая злоумышленникам достаточно времени для взлома системы и кражи критичных данных из среды данных держателей карт.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3.1.1 Выполнять своевременное реагирование на любые отказы критичных средств контроля безопасности. Процедуры для реагирования на отказы механизмов обеспечения безопасности должны включать: ▪ Восстановление функций систем безопасности ▪ Идентификацию и регистрацию длительности (даты и времени от начала до конца) отказа систем безопасности ▪ Идентификацию и регистрацию причины (причин) отказа, включая основную причину, и регистрацию исправлений, требуемых для устранения основной причины ▪ Выявление и устранение любых проблем безопасности, возникающих в ходе отказа ▪ Выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты ▪ Осуществление контроля для предотвращения повторного возникновения причины отказа ▪ Возобновление мониторинга контроля безопасности ***Ссылка на PCI DSS:*** *Требования 1-12*	**A3.3.1.1.a** Изучите документированные политики и процедуры и опросите персонал, чтобы убедиться, что процедуры для реагирования на отказы механизмов обеспечения безопасности определены и внедрены, и включают: ▪ Восстановление функций систем безопасности ▪ Идентификацию и регистрацию длительности (даты и времени от начала до конца) отказа систем безопасности ▪ Идентификацию и регистрацию причины (причин) отказа, включая основную причину, и регистрацию исправлений, требуемых для устранения основной причины ▪ Выявление и устранение любых проблем безопасности, возникающих в ходе отказа ▪ Выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты ▪ Осуществление контроля для предотвращения повторного возникновения причины отказа ▪ Возобновление мониторинга контроля безопасности **A3.3.1.1.b** Изучите документацию, чтобы убедиться, что отказы механизмов обеспечения безопасности задокументированы и включают: ▪ Причина (причины) отказа, включая основную причину ▪ Длительность (даты и времени от начала до конца) отказа систем безопасности ▪ Данные о восстановительных мероприятиях требуемых для устранения основной причины	Документированные доказательства (к примеру, записи в рамках системы управления проблемами) должны подтвердить, что процессы и процедуры реагирования на отказ системы безопасности находятся в рабочем состоянии. В дополнение сотрудники должны знать свои зоны ответственности в случае отказа. Действия и реагирование на отказы должны быть отслежены и задокументированы.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3.2 Оценивать аппаратные и программные технологии не реже одного раза в год для подтверждения продолжения их соответствия требованиям PCI DSS (например, оценка технологий, которые более не поддерживаются поставщиком и/или не отвечают требованиям безопасности организации). Процесс оценки включает план по выведению из эксплуатации технологий, которые уже не отвечают требованиям PCI DSS, и включая замену технологии, если применимо. ***Ссылка на PCI DSS:*** *Требования 2, 6*	**A3.3.2.a** Изучите документированные политики и процедуры и опросите персонал, чтобы убедиться, что процедуры оценки аппаратных и программных технологий для подтверждения продолжения их соответствия требованиям PCI DSS определены и внедрены.	Аппаратные и программные технологии постоянно развиваются и организации должны быть в курсе изменений в технологиях, которые они используют, также как и развивающихся угроз для этих технологий. Организации так же должны быть в курсе сделанных производителем изменений в их продукте или в схеме поддержки, чтобы понимать насколько эти изменения могут повлиять на применение организацией технологии. Регулярные оценки технологий, которые оказывают влияние на механизмы безопасности PCI DSS, могут помочь в приобретении, использовании и стратегиях развертывания, и обеспечить эффективность механизмов, которые зависят от этих технологий.
	A3.3.2.b Изучите результаты последних оценок, чтобы убедиться, что оценки выполняются не реже одного раза в год.	
	A3.3.2.c Подтвердите, что относительно любых технологий, признанных уже не отвечающими требованиям PCI DSS, имеется в наличии план по выведению из эксплуатации таких технологий.	

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.3.3 Выполнять проверки, как минимум, раз в квартал, чтобы подтвердить, что традиционные бизнес-процессы соблюдаются. Проверки должны выполняться сотрудниками, назначенными на программу соответствия стандарту PCI DSS (как указано в A3.1.3) и включать следующее: • Подтверждение, что реализуются все традиционные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1) • Подтверждение, что сотрудники следуют политикам безопасности и операционным процедурам (к примеру, ежедневный анализ журналов событий, пересмотр правил межсетевого экранирования, разработка стандартов конфигураций для новых систем и т.д.) • Документирование того, как были выполнены оценки, включая то, как было подтверждено наличие всех традиционных бизнес-процессов • Собрание всех документальных свидетельств, которые требуются для ежегодного аудита PCI DSS • Оценка и визирование результатов сотрудниками, ответственными за программу соответствия стандарту PCI DSS (как указано в A3.1.3) • Сохранение записей и документации, которые охватывают все традиционные бизнес-процессы в течение, как минимум, 12 месяцев ***Ссылка на PCI DSS:*** *Требования 1-12*	**A3.3.3.a** Проверьте политики и процедуры и убедитесь, что определены процедуры оценки и подтверждения традиционных бизнес-процессов. Проверьте, что процедуры: • Подтверждают, что реализуются все традиционные бизнес-процессы (например, A3.2.2, A3.2.6 и A3.3.1) • Подтверждают, что сотрудники следуют политикам безопасности и операционным процедурам (к примеру, ежедневный анализ журналов событий, пересмотр правил межсетевого экранирования, разработка стандартов конфигураций для новых систем и т.д.) • Документируют то, как были выполнены оценки, включая то, как было подтверждено наличие всех традиционных бизнес-процессов • Собирают все документальные свидетельства, которые требуется для ежегодного аудита PCI DSS • Оценивают и визируют результаты сотрудниками, ответственными за программу соответствия стандарту PCI DSS • Сохраняют записи и документацию, которые охватывают все традиционные бизнес-процессы в течение, как минимум, 12 месяцев **A3.3.3.b** Опросите ответственных сотрудников и изучите записи о проверках, чтобы убедиться в том, что: • Оценки выполнены сотрудниками, назначенными на программу соответствия стандарту PCI DSS. • Оценки выполняются не реже одного раза в квартал.	Внедрение механизмов безопасности стандарта PCI DSS в традиционные бизнес-процессы является эффективным методом, гарантирующим, что безопасность является частью обычной коммерческой деятельности на постоянной основе. Потому важно, чтобы выполнялись независимые проверки для подтверждения того, что механизмы традиционных бизнес-процессов активны и работают надлежащим образом. Целью этих независимых проверок является оценка свидетельств, подтверждающих, что традиционные бизнес-процессы выполняются. Эти проверки могут также быть использованы для проверки того, что необходимые свидетельства их выполнения поддерживаются в актуальном состоянии (например, журналы событий, отчеты о сканировании на уязвимости, пересмотры правил межсетевых экранов, и т.д.) для помощи организации в подготовке к последующей оценке соответствия стандарту PCI DSS.

Требования PCI DSS	Проверочные процедуры	Пояснение
A3.4 Контролировать и управлять логическим доступом в среду данных держателей карт		
A3.4.1 Проверять учетные записи пользователей и привилегии доступа к системным компонентам области оценки не реже одного раза в полгода, чтобы убедиться, что пользовательские аккаунты и доступ остается соответствующим должностным обязанностям и авторизованным. ***Ссылка на PCI DSS:*** *Требование 7*	**A3.4.1** Опросите ответственных сотрудников и изучите сопроводительную документацию для подтверждения того, что: • Учетные записи пользователей и привилегии доступа к системным компонентам области оценки оцениваются не реже одного раза в полгода. • Оценки подтверждают, что доступ остается соответствующим должностным обязанностям и весь доступ авторизован.	Потребности в доступе со временем меняются, вместе с изменением должностных функций сотрудников или их уходом из компании, а также с изменением сферы деятельности. Руководство должно регулярно проверять, переоценивать и, по необходимости, обновлять доступ пользователей, чтобы отражать изменения в составе сотрудников, включая третьи лица, и должностные обязанности пользователей.
A3.5 Выявлять и реагировать на подозрительные события		
A3.5.1 Внедрить методологию своевременного обнаружения шаблонов атак и нежелательного поведения в системах (к примеру, использование скоординированных ручных проверок и/или централизованных или автоматических средств корреляции событий), которая должна включать, как минимум, следующее: • Идентификацию аномалий или подозрительной активности, при их возникновении • Гарантию своевременного оповещения ответственных сотрудников при выявлении подозрительной активности или аномалий • Реагирование на уведомления в соответствии с задокументированными процедурами реагирования ***Ссылка на PCI DSS:*** *Требования 10, 12*	**A3.5.1.a** Изучите документацию и опросите сотрудников, чтобы убедиться, что методология своевременного обнаружения шаблонов атак и нежелательного поведения в системах определена, внедрена и включает следующее: • Идентификацию аномалий или подозрительной активности, при их возникновении • Своевременное оповещение ответственных сотрудников • Реагирование на уведомления в соответствии с задокументированными процедурами реагирования **A3.5.1.b** Изучите процедуры реагирования на инциденты и опросите ответственных сотрудников, чтобы убедиться, что: • Дежурные сотрудники своевременно получают уведомления. • Реагирование на уведомления проходит согласно установленной процедуре.	Возможность выявлять шаблоны атак и нежелательное поведение в системах является критичной с точки зрения предотвращения, выявления или минимизации последствий компрометации данных. Наличие журналов регистрации во всех средах делает возможным отслеживать действия, предпринимаемые в нештатных ситуациях, выполнять оповещение о и проводить анализ нештатных ситуаций. Определить причины компрометации очень сложно, если не невозможно, без процесса анализа сообщений и уведомлений критичных системных компонентов и систем, выполняющих защитные функции (таких как межсетевые экраны, IDS/IPS, мониторинг целостности файлов (FIM)). Таким образом, журналы регистрации со всех критичных системных компонентов и систем, выполняющим защитные функции, должны собираться, коррелироваться и поддерживаться. Этот процесс может включать использование программных продуктов и сервисов с целью выполнения анализа событий в реальном времени, оповещения и отчетности (например, SIEM (Security information and event management), мониторинг целостности файлов (FIM) или обнаружение изменений).

Приложение B: Компенсационные меры

Компенсационные меры можно рассматривать в отношении большинства требований стандарта PCI DSS, когда организация не может выполнить требование в явном виде и в указанной форме из-за обоснованных технических или документированных коммерческих ограничений, но в достаточной степени снизила риск, связанный с требованием, путем внедрения компенсационных или других мер.

Компенсационные меры должны удовлетворять следующим требованиям:

1. Удовлетворять цели и строгости первоначального требования PCI DSS.
2. Обеспечивать ту же степень защищенности, что и изначальное требование PCI DSS, чтобы снизить риск так же эффективно, как и изначальное требование (см. Столбец «Пояснение» для определения цели каждого требования PCI DSS).
3. Обеспечивать определенную избыточность по сравнению с другими требованиями PCI DSS. (Недостаточно просто удовлетворять всем остальным требованиям PCI DSS — это не является компенсационной мерой).

   При анализе избыточности следует учитывать следующее:

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

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

   b) Существующие требования PCI DSS МОЖНО рассматривать как компенсационные меры, если они требуются в отношении иных объектов, но не требуются в отношении рассматриваемых объектов.

   c) Существующие требования PCI DSS в сочетании с другими защитными мерами могут использоваться как компенсационные меры. Например, если организация не может реализовать хранение данных держателей карт в нечитаемом виде в соответствии с Требованием 3.4 (например, путем шифрования), компенсационной мерой может считаться использование устройства или набора устройств, приложений и мер, направленных на: 1) внутреннюю сегментацию сети; 2) фильтрацию по IP- или MAC-адресам и 3) использование одноразовых паролей.

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

Аудитор должен тщательно оценивать компенсационные меры при каждой ежегодной оценке соответствия организации требованиям PCI DSS. Аудитор должен подтвердить, что каждая компенсационная мера адекватно учитывает риск, для нейтрализации которого предназначено исходное требование PCI DSS, согласно п. 1–4 выше. Для поддержания соответствия, должны применяться процессы и меры, которые обеспечат работу компенсационных мер после завершения оценки.

Приложение C: Компенсационные Меры - Форма для заполнения

Используйте эту таблицу для описания компенсационной меры для любого требования, в котором используется компенсационная мера для соответствия требованию PCI DSS. Обратите внимание, что компенсационные меры должны быть отражены в Отчете о соответствии в соответствующем разделе требования PCI DSS.

Примечание: *Только организации, которые выполнили анализ рисков и имеют обоснованные технические или документированные коммерческие ограничения, могут рассматривать использование компенсационных мер для достижения соответствия.*

Номер и определение требования:

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	
2. Цель	Определите цель исходного требования; укажите цель, которая достигнута с помощью компенсационных мер.	
3. Определение риска	Опишите любой дополнительный риск, связанный с невыполнением исходного требования.	
4. Определение компенсационных мер	Опишите компенсационные меры и объясните, как с их помощью достигаются цели исходного требования и снижается повышенный риск (при его наличии).	
5. Проверка компенсационных мер	Опишите, как компенсационные меры были проверены и протестированы.	
6. Соблюдение	Опишите, как контролируется процесс соблюдения компенсационной меры.	

«Компенсационные меры - Форма для заполнения» – пример заполнения

Используйте эту таблицу для описания компенсационных мер для требований, имеющих статус "Выполнено" благодаря использованию компенсационных мер.

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

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	*Компания XYZ использует Unix-серверы без LDAP-авторизации. Таким образом, на каждый из них требуется заходить под учетной записью суперпользователя ("root"). Организация не может управлять входом "root" и следить за использованием этой учетной записи каждым пользователем.*
2. Цель	Определите цель исходного требования; укажите цель, которая достигнута с помощью компенсационных мер.	*Использование уникального идентификатора преследует две цели. Во-первых, с точки зрения безопасности недопустимо использовать общие учетные записи. Во-вторых, в таком случае невозможно определить, какой администратор ответственен за определенные действия.*
3. Определение риска	Опишите любой дополнительный риск, связанный с невыполнением исходного требования.	*Дополнительный риск связан с тем, что не всем пользователям назначен уникальный идентификатор и их действия не могут быть отслежены.*
4. Определение компенсационных мер	Опишите компенсационные меры и объясните, как с их помощью достигаются цели исходного требования и снижается повышенный риск (при его наличии).	*Компания XYZ собирается требовать от всех пользователей входить на серверы с использованием их обычных пользовательских учетных записей, а затем использовать команду «sudo», чтобы запускать команды администрирования. Это позволяет пользователю под учетной записью с правами суперпользователя ("root") запускать предустановленные команды, которые записываются командой 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	Опишите, как компенсационные меры были проверены и протестированы.	*Компания XYZ продемонстрировала аудиторам, что команда «sudo» надлежащим образом сконфигурирована с использованием файлов «sudoers» и в ней предусмотрено выполнение определенных команд только определенными пользователями, а также то, что все действия тех пользователей, которые используют эту команду, записываются с целью определения того, что пользователь выполняет действия с правами суперпользователя ("root").*
6. Соблюдение	Опишите, как контролируется процесс соблюдения компенсационной меры.	*В компании XYZ задокументированы процессы и процедуры, которые обеспечивают неизменность конфигурации «sudo» (невозможность ее изменить или удалить) и невозможность выполнять команды пользователя "root" без отслеживания и регистрации событий.*

Приложение D: Сегментация и выборочная оценка помещений организации /системных компонентов