Приоритетный подход к достижению соответствия PCI DSS

Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS) детально описывает разделенные на 12 групп требования к обеспечению безопасности данных о держателях платежных карт, обрабатываемых, хранимых, либо передаваемых торгово-сервисными и иными компаниями. Благодаря своей всеобъемлющей природе стандарт содержит большое количество информации, описывающей различные методы обеспечения информационной безопасности. Количество информации настолько велико, что многим специалистам, по долгу службы занимающимся безопасностью карточных данных, не совсем очевидно, с чего же начинать свой путь к соответствию. По этой причине Совет по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC) предложил приоритетный подход, чтобы помочь понять, где следует снижать информационные риски в первую очередь. Ни один из этапов в отдельности не обеспечит всеобъемлющей безопасности, однако следование этому руководству поможет ускорить снижение рисков компрометации карточных данных.

Что такое приоритетный подход?

Приоритетный подход предполагает разделение деятельности по достижению соответствия PCI DSS на шесть этапов, что поможет торгово-сервисным и другим компаниям защититься от наиболее критичных рисков и угроз на пути к соответствию. Приоритетный подход несет следующие выгоды:

- Предлагает готовый план, который компания может использовать для обработки рисков в порядке уменьшения их приоритета;
- Предлагает прагматичный подход, нацеленный на достижение результата;
- Обеспечивает возможность финансового и операционного планирования;
- Предоставляет объективные и измеримые показатели прогресса;
- Способствует слаженности действий QSA-аудиторов.

Цели приоритетного подхода

ОСНОВАТЕЛИ PCI SSC

Приоритетный подход помогает последовательно реализовать мероприятия по приведению компании в соответствие PCI DSS в соответствии с уровнем рисков, связанных с хранением, обработкой и/или передачей данных о держателях карт. Расстановка приоритетов помогает планировать мероприятия по выполнению требований стандарта, снижающие риски компрометации карточных данных, а также помогает банкам-эквайерам объективно оценивать деятельность торгово-сервисных предприятий и поставщиков услуг по достижению соответствия. Концепция приоритетного подхода была разработана на основе анализа информации об утечках данных, обратной связи от QSA-аудиторов и комиссий по расследованию инцидентов, а также рекомендаций Консультационного Совета PCI SSC. Она не предлагается как замена всем другим подходам к достижению соответствия, равно как не является универсальной «волшебной таблеткой», подходящей для всех компаний.

Ответственность

Для достижения соответствия PCI DSS компания должна выполнить все требования стандарта, независимо от того, в каком порядке они выполняются и применяется ли при этом приоритетный подход. Настоящий документ никак не изменяет и не сокращает стандарт PCI DSS или какое-либо из его требований, Совет PCI SSC не несет ответственности за результаты применения изложенной здесь информации.

Этапы приоритетного подхода

Приоритетный подход включает в себя шесть этапов, главная цель каждого из которых в общем процессе достижения соответствия PCI DSS приведена в таблице:

Этап	Цель
1	**Удаление критичных аутентификационных данных и ограничение хранения данных о держателях карт.** Этот этап направлен на ключевой момент снижения рисков. Отсутствие в информационной инфраструктуре критичных аутентификационных данных и других данных о держателях карт значительно снижает негативные последствия её компрометации.
2	**Защита периметра, внутренних и беспроводных сетей.** Целью мероприятий этого этапа является защита наиболее уязвимых мест информационной инфраструктуры – активного сетевого оборудования и беспроводных точек доступа.
3	**Обеспечение безопасности платежных приложений.** Этот этап включает в себя меры по защите приложений, процессов и серверов. Уязвимости прикладного уровня предоставляют возможности для легкой компрометации данных о держателях карт.
4	**Управление и контроль доступа к системам.** Мероприятия, выполняемые в рамках этого этапа, позволяют отследить кто, когда и как получает доступ к сети и среде данных о держателях карт.
5	**Защита хранимых данных о держателях карт.** Тем компаниям, которым с точки зрения бизнеса необходимо хранение данных о держателях карт, следует внедрить механизмы защиты хранимых данных.
6	**Устранить оставшиеся несоответствия и убедиться в выполнении всех требований.** Наконец, следует выполнить все оставшиеся требования стандарта и завершить разработку сопутствующих политик и процедур, необходимых для защиты данных о держателях карт.

Привязка этапов к требованиям

В таблице приведена привязка каждого из 12 разделов стандарта и содержащихся в них требований соответствующему этапу приоритетного подхода.

Требование PCI DSS	Этап					
	1	2	3	4	5	6
Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт						
1.1 Должны быть разработаны стандарты конфигурации межсетевых экранов, которые должны включать в себя:						**6**
1.1.1 Формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурации межсетевого экрана.						**6**
1.1.2 Актуальную схему сети с указанием всех каналов доступа к данным о держателях карт, включая все беспроводные сети.	**1**					
1.1.3 Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании.		**2**				
1.1.4 Описание групп, ролей и ответственности за управление сетевыми устройствами.						**6**
1.1.5 Обоснованный документированный перечень всех разрешенных для использования сервисов, протоколов и портов, необходимых для работы бизнес-приложений, включающий документальное описание внедренных механизмов защиты небезопасных протоколов.		**2**				
1.1.6 Требование пересмотра настроек межсетевых экранов и маршрутизаторов не реже одного раза в полгода.						**6**
1.2 Должна быть создана конфигурация межсетевых экранов, которая контролирует все соединения между недоверенными сетями и всеми системными компонентами в среде данных о держателях карт. Примечание: недоверенной является любая сеть, которая не контролируется проверяемой организацией		**2**				
1.2.1 Входящий и исходящий трафик должен быть ограничен только необходимыми соединениями для среды данных о держателях карт.		**2**				

Требование PCI DSS	Этап					
	1	2	3	4	5	6
1.2.2 Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов межсетевых экранов.		2				
1.2.3 Необходима установка межсетевых экранов между любой беспроводной сетью и средой данных о держателях карт, такие межсетевые экраны должны быть настроены на блокирование любого трафика из беспроводной сети, либо его контроля в том случае, если такой трафик необходим для бизнес-приложений.		2				
1.3 Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды данных о держателях карт.		2				
1.3.1 Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только протоколами, необходимыми для среды данных о держателях карт.		2				
1.3.2 Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.		2				
1.3.3 Должны быть запрещены любые прямые маршруты входящего или исходящего трафика между сетью Интернет и средой данных о держателях карт.		2				
1.3.4 Необходимо запретить соединения с внутренними адресами от источника из Интернета к адресам, расположенным в DMZ.		2				
1.3.5 Необходимо ограничить исходящий трафик из среды данных о держателях карт в сеть Интернет таким образом, чтобы исходящий трафик имел доступ только к IP адресам, расположенным в DMZ.		2				
1.3.6 Необходимо включить динамическую пакетную фильтрацию с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений).		2				
1.3.7 Необходимо размещать базы данных во внутреннем сегменте сети, отделенном от DMZ.		2				
1.3.8 Должен быть реализован механизм трансляции IP-адресов для предотвращения раскрытия внутренних адресов. Для этого следует использовать такие технологии, как PAT и NAT.		2				
1.4 Должны быть установлены персональные межсетевые экраны на все мобильные и принадлежащие сотрудникам компьютеры, имеющие прямой доступ в Интернет и используемые также для доступа к локальной сети организации.		2				

Требование PCI DSS	Этап					
	1	2	3	4	5	6
Требование 2: Не использовать пароли и другие системные параметры, заданные производителем по умолчанию						
2.1 Всегда следует менять установленные производителем настройки по умолчанию перед установкой системы в сетевую инфраструктуру (например, сменить установленные по умолчанию пароли, строки доступа SNMP, удалить ненужные для работы учетные записи).		**2**				
2.1.1 Для беспроводных устройств необходимо изменить установленные по умолчанию производителем параметры, такие как: ключи шифрования, пароли, строки доступа SNMP. Следует включить стойкие криптографические механизмы для шифрования данных и аутентификации.		**2**				
2.2 Должны быть разработаны стандарты конфигурации для всех системных компонентов. Стандарты должны учитывать все известные проблемы безопасности, а также положения общепринятых отраслевых стандартов в области безопасности.			**3**			
2.2.1 Каждый сервер должен выполнять одну основную функцию.			**3**			
2.2.2 Должны быть отключены все небезопасные и ненужные для работы сервисы и протоколы (те сервисы и протоколы, использование которых не требуется для выполнения устройством своей основной функции).			**3**			
2.2.3 Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.			**3**			
2.2.4 Из системы должна быть удалена вся ненужная функциональность: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.			**3**			
2.3 Следует всегда шифровать канал удаленного административного доступа к системе. Для этого необходимо использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов удаленного административного доступа.		**2**				
2.4 Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным в Приложении А: «Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)».			**3**			

Требование PCI DSS	Этап					
	1	2	3	4	5	6
Требование 3: Обеспечить безопасное хранение данных о держателях карт						
3.1 Хранение данных о держателях карт должно быть ограничено только необходимым минимумом. Должна быть разработана политика хранения и обращения с данными. Количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований параметрами; эти параметры должны быть отражены в политике хранения данных.	**1**					
3.2 Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). К критичным аутентификационным данным относятся данные, перечисленные в требованиях 3.2.1 – 3.2.3.	**1**					
3.2.1 Запрещается хранить полную дорожку магнитной полосы, находящейся на обратной стороне карты, на чипе, либо ином месте, («полная дорожка», «дорожка», «дорожка 1», «дорожка 2»). Для ведения бизнеса, может быть необходимо хранение следующих элементов данных магнитной полосы: - имя держателя карты, - номер платежной карты (PAN), - дата истечения срока действия карты, - сервисный код. Для минимизации рисков разрешается хранить только указанные элементы данных. Дополнительная информация приведена в «Глоссарии PCI DSS: Основные определения, аббревиатуры и сокращения».	**1**					
3.2.2 Запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с кредитной карты (трех- или четырехзначного числа, изображенного на лицевой или обратной стороне карты). Дополнительная информация приведена в «Глоссарии PCI DSS».	**1**					
3.2.3 Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.	**1**					

Требование PCI DSS	Этап					
	1	2	3	4	5	6
3.3 Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4). Это требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть весь PAN; также это требование не заменяет собой иные более строгие требования к отображению данных о держателях карт (например, на чеках POS-терминалов).					5	
3.4 Из всех данных о держателе карты как минимум PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий, а также данные, получаемые по беспроводным сетям). Для этого следует использовать любой из следующих методов: - стойкая однонаправленная хэш-функция; - укорачивание (truncation); - использование механизмов One-Time-Pad («одноразовые блокноты») и использование и хранение ссылок на данные вместо самих данных (index tokens); - стойкие криптографические алгоритмы, совместно с процессами и процедурами управления ключами. Из всей информации о держателе карты как минимум PAN должен быть преобразован в нечитаемый вид.					5	
3.4.1 Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или полей базы данных), то управление логическим доступом должно осуществляться независимо от механизмов разграничения доступа операционной системы (например, локальных учетных записей). Ключи шифрования не должны быть привязаны к учетным записям пользователей.					5	
3.5 Следует обеспечить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования:					5	
3.5.1 Доступ к ключам шифрования должен быть разрешен только нескольким ответственным за их хранение и использование сотрудникам.					5	
3.5.2 Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.					5	
3.6 Должны быть документированы все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе:					5	

Требование PCI DSS	Этап					
	1	2	3	4	5	6
3.6.1 Генерация стойких ключей.					5	
3.6.2 Безопасное распространение ключей.					5	
3.6.3 Безопасное хранение ключей.					5	
3.6.4 Периодическая смена ключей: - насколько часто этого требуют применяемые приложения, предпочтительно автоматически; - не реже одного раза в год.					5	
3.6.5 Уничтожение старых (просроченных) ключей, а также ключей, относительно которых существуют подозрения в их компрометации.					5	
3.6.6 Раздельное владение частями ключей с принципом контроля двумя лицами.					5	
3.6.7 Защита от неавторизованной смены ключа.					5	
3.6.8 Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с письменным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности.					5	
Требование 4. Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования						
4.1 Для защиты критичных данных о держателях карт во время передачи их через общедоступные сети, следует использовать стойкие криптографические алгоритмы и протоколы, такие как SSL/TLS и IPSEC. Примерами общедоступных сетей, на которые распространяются требования PCI DSS, являются: - Интернет; - Беспроводные технологии; - GSM; - GPRS.		2				

Требование PCI DSS	Этап					
	1	2	3	4	5	6
4.1.1 При использовании беспроводных сетей, передающих данные о держателях карт, либо подключенных к среде данных о держателях карт, следует использовать передовые практические методы (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных. - Для вновь устанавливаемых беспроводных сетей запрещается использование протокола WEP с 31 марта 2009 года; - Для существующих беспроводных сетей запрещается использование протокола WEP с 30 июня 2010 года.		**2**				
4.2 Никогда не следует пересылать незашифрованный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты).		**2**				
Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение						
5.1 Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).		**2**				
5.1.1 Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного ПО.		**2**				
5.2 Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий.		**2**				
Требование 6: Разрабатывать и поддерживать безопасные системы и приложения						
6.1 На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем. Обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем. Примечание: Организация может применять подход к распределению приоритетов при установке обновлений, основанный на оценке рисков. Для более критичных приложений срок установки обновлений не должен превышать одного месяца, для менее критичных - три месяца			**3**			

Требование PCI DSS	Этап					
	1	2	3	4	5	6
6.2 Должен быть внедрен процесс выявления новых уязвимостей (например, подписка на бесплатную рассылку сообщений о новых уязвимостях). Стандарты конфигурации системных компонентов (требование 2.2 PCI DSS) должны обновляться для учета вновь обнаруженных уязвимостей.			3			
6.3 Приложения должны разрабатываться в соответствии с требованиями PCI DSS (например, безопасная аутентификация и регистрация событий). Разработка приложений должна быть основана на передовых практических методиках и принимать во внимание информационную безопасность в течение всего цикла разработки, в том числе:			3			
6.3.1 Все обновления безопасности и изменения в конфигурации должны быть протестированы перед внедрением, тестирование должно включать в себя:			3			
6.3.1.1 Проверку всех входных данных (чтобы исключить XSS, инъекции, исполнение вредоносного файла, и т. д.).			3			
6.3.1.2 Проверку корректной обработки ошибок.			3			
6.3.1.3 Проверку использования защищенного криптографического хранилища для критичной информации			3			
6.3.1.4 Проверку безопасности передачи данных			3			
6.3.1.5 Проверку корректности разграничения доступа, основанного на ролях			3			
6.3.2 Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга.			3			
6.3.3 Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть разделены.			3			
6.3.4 Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.			3			
6.3.5 Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.			3			

Требование PCI DSS	Этап					
	1	2	3	4	5	6
6.3.6 Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчикам или переводом его в производственный режим.			3			
6.3.7 Программный код приложений должен быть исследован на наличие потенциальных уязвимостей перед передачей готовых приложений заказчикам или переводом их в производственный режим. Примечание: это требование применимо ко всем разрабатываемым приложениям (как внутренним, так и общедоступным) как элемент обеспечения безопасности цикла разработки, регламентируемого требованием 6.3. PCI DSS. Оценка программного кода может проводиться как компетентным персоналом, так и третьими сторонами. Веб-приложения также являются объектом применения дополнительных мер по защите; если они находятся в публичном доступе, следует учесть угрозы и уязвимости, в соответствии с требованием 6.6 PCI DSS.			3			
6.4 Должны быть разработаны и внедрены процедуры управления изменениями, включающие в себя:						6
6.4.1 Документирование влияния изменения на систему						6
6.4.2 Согласование изменения с руководством						6
6.4.3 Тестирование производственной функциональности						6
6.4.4 Процедуру отмены изменения						6
6.5 Разработка веб-приложений должна проходить в соответствии с руководствами по безопасному программированию, например, такими как руководства от проекта OWASP. Программный код приложений должен быть исследован на наличие потенциальных уязвимостей, в частности, таких как:			3			
6.5.1 Атаки типа XSS.			3			
6.5.2 Инъекции, в особенности, SQL-инъекции. Также следует учесть LDAP и Xpath инъекции.			3			

Требование PCI DSS	Этап					
	1	2	3	4	5	6
6.5.3 Исполнение вредоносных файлов.			**3**			
6.5.4 Небезопасные прямые ссылки.			**3**			
6.5.5 Подделка межсайтовых запросов (CSRF).			**3**			
6.5.6 Утечка данных и некорректная обработка ошибок.			**3**			
6.5.7 Обход системы аутентификации и управления сессиями.			**3**			
6.5.8 Небезопасное криптографическое хранилище.			**3**			
6.5.9 Небезопасная передача данных.			**3**			
6.5.10 Ошибки в контроле доступа по URL			**3**			
6.6 Следует обеспечить защиту веб-ориентированных приложений от известных атак одним из следующих методов: - Проверить приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности. - Установить межсетевой экран прикладного уровня перед веб-ориентированными приложениями.			**3**			
Требование 7: Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью						
7.1 Доступом к вычислительным ресурсам и информации о держателях карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями. Ограничения доступа должны включать в себя:				**4**		
7.1.1 Доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей.				**4**		

Требование PCI DSS	Этап					
	1	2	3	4	5	6
7.1.2 Назначение привилегий пользователям должно быть основано на их должностных обязанностях.				4		
7.1.3 Подписание руководством заявки о предоставлении прав доступа.				4		
7.1.4 Внедрение автоматизированной системы контроля доступа				4		
7.2 Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания и применяющий принцип «запрещено всё, что явно не разрешено». Механизм контроля доступа должен включать следующее:				4		
7.2.1 Покрытие всех системных компонентов.				4		
7.2.2 Назначение привилегий пользователям должно быть основано на их должностных обязанностях.				4		
7.2.3 По-умолчанию должен быть запрещен любой доступ.				4		
Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре						
8.1 Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.				4		
8.2 Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей: - пароль. - двухфакторная аутентификация (ключи, смарт-карты, биометрические параметры, открытые ключи).				4		
8.3 Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети должен быть реализован механизм двухфакторной аутентификации. Для этого следует использовать такие технологии, как RADIUS и TACACS с ключами или VPN (SSL/TLS или IPSEC) с индивидуальными сертификатами.				4		

Требование PCI DSS	Этап					
	1	2	3	4	5	6
8.4 Все пароли должны храниться и передаваться только в зашифрованном виде.				4		
8.5 Должен быть установлен контроль над выполнением процедур аутентификации и управления паролями учетных записей сотрудников и администраторов, включающий в себя:				4		
8.5.1 Контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации.				4		
8.5.2 Проверку подлинности пользователя перед сменой пароля.				4		
8.5.3 Установку уникального первоначального пароля для каждого пользователя и его немедленное изменение при первом входе пользователя.				4		
8.5.4 Немедленный отзыв доступа при увольнении пользователя.				4		
8.5.5 Удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней.				4		
8.5.6 Включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ.				4		
8.5.7 Доведение правил и процедур использования и хранения пароля до всех пользователей, имеющих доступ к данным о держателях карт.				4		
8.5.8 Запрет использования групповых, разделяемых и стандартных учетных записей и паролей.				4		
8.5.9 Изменение пароля пользователя не реже одного раза в 90 дней.				4		
8.5.10 Требование использования в пароле не менее семи символов.				4		
8.5.11 Требование использования в пароле как цифр, так и букв.				4		
8.5.12 Запрет при смене пароля выбора в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей.				4		

Требование PCI DSS	Этап					
	1	2	3	4	5	6
8.5.13 Блокировку учетной записи после шести неудачных попыток ввода пароля.				4		
8.5.14 Установку периода блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором.				4		
8.5.15 Блокировку рабочей сессии пользователя через 15 минут простоя с требованием ввода пароля для разблокировки терминала.				4		
8.5.16 Аутентификацию всех вариантов доступа к любой базе данных, содержащей данные о держателях карт, в том числе доступ со стороны приложений, администраторов и любых других пользователей.				4		
Требование 9: Ограничить физический доступ к данным платежных карт						
9.1 Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные о держателях карт.					5	
9.1.1 Следует использовать камеры видеонаблюдения, чтобы следить за критичными местами. Данные, собранные камерами видеонаблюдения, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством. Примечание: критичными являются места, относящиеся к любому дата-центру, серверной комнате или иному помещению, в котором расположены системы, хранящие, обрабатывающие или передающие данные о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов					5	
9.1.2 Доступ к сетевым разъемам, расположенным в общедоступных местах, должен быть ограничен.					5	
9.1.3 Доступ к беспроводным точкам доступа, шлюзам и портативным устройствам должен быть ограничен.					5	

Требование PCI DSS	Этап					
	1	2	3	4	5	6
9.2 Должны быть внедрены процедуры, позволяющие легко различать сотрудников и посетителей, особенно в помещениях, где циркулируют данные о держателях карт. Примечание: Под термином «сотрудники» в данном случае понимаются постоянные и временные сотрудники, а также консультанты, работающие на объекте. Под термином «посетители» понимаются поставщики, гости сотрудников, сервисный персонал и иные люди, кратковременно находящиеся на объекте, обычно не более одного дня.					5	
9.3 Следует ввести процедуру прохода посетителей на объект, обеспечивающую:					5	
9.3.1 Авторизацию посетителя, перед входом в помещения, где циркулируют данные о держателях карт.					5	
9.3.2 Выдачу посетителю материального идентификатора (например, бейджа или электронного ключа), имеющего ограничение срока действия, при входе на объект.					5	
9.3.3 Возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении срока его действия.					5	
9.4 Следует вести журнал учета посетителей и использовать его для анализа посещений. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством.					5	
9.5 Носители с резервными копиями данных следует хранить в безопасных местах, желательно вне объекта, таких как запасной центр обработки данных, или же воспользовавшись услугами компаний, обеспечивающих безопасное хранение.					5	
9.6 Должна быть обеспечена физическая безопасность всех бумажных и электронных средств, содержащих данные о держателях карт.					5	
9.7 Должен быть обеспечен строгий контроль над перемещением носителей информации, содержащих данные о держателях карт, включающий:					5	
9.7.1 Классификацию носителей информации, их маркировку, как содержащих конфиденциальную информацию.					5	
9.7.2 Пересылку носителей только с доверенным курьером, или иным способом, который может быть тщательно проконтролирован.					5	

Требование PCI DSS	Этап					
	1	2	3	4	5	6
9.8 Должна быть внедрена процедура разрешения руководством выноса за пределы охраняемой территории носителей, содержащих данные о держателях карт.					5	
9.9 Должен быть обеспечен строгий контроль хранения носителей, содержащих данные о держателях карт, и доступом к ним.					5	
9.9.1 Должны поддерживаться в актуальном состоянии журналы инвентаризации всех носителей данных о держателях карт; инвентаризация носителей должна проводиться не реже одного раза в год.					5	
9.10 Носители, содержащие данные о держателях карт, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, должны быть уничтожены следующими способами:	1					
9.10.1 Измельчение, сжигание или растворение бумажного носителя.	1					
9.10.2 Уничтожение данных о держателях карт на электронном носителе, исключающее возможность их восстановления.	1					
Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт						
10.1 Должен быть разработан процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам.				4		
10.2 Для каждого системного компонента должен быть включен механизм протоколирования следующих событий:				4		
10.2.1 Любой доступ пользователя к данным о держателях карт.				4		
10.2.2 Любые действия, совершенные с использованием административных полномочий.				4		
10.2.3 Любой доступ к записям о событиях в системе.				4		
10.2.4 Неуспешные попытки логического доступа.				4		

Требование PCI DSS	Этап					
	1	2	3	4	5	6
10.2.5 Использование механизмов идентификации и аутентификации.				4		
10.2.6 Инициализация журналов протоколирования событий.				4		
10.2.7 Создание и удаление объектов системного уровня.				4		
10.3 Для каждого события каждого системного компонента должны быть записаны следующие параметры:				4		
10.3.1 Идентификатор пользователя.				4		
10.3.2 Тип события.				4		
10.3.3 Дата и время.				4		
10.3.4 Успешным или неуспешным было событие.				4		
10.3.5 Источник события.				4		
10.3.6 Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.				4		
10.4 Все системные часы на критичных системах должны быть синхронизированы.				4		
10.5 Журналы протоколирования событий должны быть защищены от изменений.						6
10.5.1 Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.						6
10.5.2 Журналы протоколирования событий должны быть защищены от неавторизованного изменения.						6

Требование PCI DSS	Этап					
	1	2	3	4	5	6
10.5.3 Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования, или отдельный носитель, где их изменение было бы затруднено.						6
10.5.4 Копии журналов протоколирования активности событий доступных извне технологий (беспроводных сетей, межсетевых экранов, DNS, почтовых систем) должны сохраняться на сервер протоколирования, находящийся внутри локальной сети.						6
10.5.5 Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала).						6
10.6 Следует просматривать журналы протоколирования событий не реже одного раза в день. Следует анализировать журналы систем обнаружения вторжений (IDS) и серверов, осуществляющих аутентификацию, авторизацию и учет (например, RADIUS). Примечание: Для обеспечения соответствия Требованию 10.6 могут быть использованы средства сбора и анализа журналов регистрации событий, а также средства оповещения.				4		
10.7 Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев.				4		
Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности						
11.1 Следует ежеквартально проверять наличие беспроводных точек доступа, используя анализатор беспроводных сетей либо беспроводные IDS/IPS для обнаружения всех включенных беспроводных устройств.						6
11.2 Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значимых изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления системных компонентов). Примечание: ежеквартальное сканирование должно производиться сторонней сертифицированной компанией. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании.		2				

Требование PCI DSS	Этап					
	1	2	3	4	5	6
11.3 Следует проводить внешний и внутренний тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера). Эти тесты на проникновение должны включать:						6
11.3.1 Тесты на проникновение сетевого уровня.						6
11.3.2 Тесты на проникновение уровня приложений.						6
11.4 Следует использовать системы обнаружения вторжений, а также системы предотвращения вторжений для контроля всего сетевого трафика и оповещения персонала о подозрительных действиях. Системы обнаружения и предотвращения вторжений должны быть актуальными.		2				
11.5 Следует использовать приложения контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов и файлов данных; проверка целостности критичных файлов должна проводиться не реже одного раза в неделю. Примечание: Обычно контролируется целостность файлов, которые изменяются нечасто, но изменение которых может служить признаком компрометации или попытки компрометации системы. Средства контроля целостности обычно содержат предустановленный перечень файлов, подлежащих контролю, в зависимости от используемой операционной системы. Другие критичные файлы, такие как файлы специализированных приложений, должны быть определены самой компанией.				4		
Требование 12: Разработать и поддерживать политику информационной безопасности						
12.1 Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика информационной безопасности.						6
12.1.1 Политика информационной безопасности должна учитывать все требования настоящего стандарта.	1	2	3	4	5	6

Требование PCI DSS	Этап					
	1	2	3	4	5	6
12.1.2 Политика информационной безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков.						6
12.1.3 Политика информационной безопасности должна пересматриваться не реже одного раза в год и обновляться в случае изменения инфраструктуры.						6
12.2 Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов протоколирования событий).						6
12.3 Должны быть разработаны правила эксплуатации для критичных технологий, с которыми непосредственно работают сотрудники (таких как системы удаленного доступа, беспроводные технологии, съемные носители информации, мобильные компьютеры, карманные компьютеры, электронная почта и Интернет), чтобы определить корректный порядок использования этих устройств сотрудниками. Эти правила должны включать следующее:						6
12.3.1 Процедуру явного одобрения руководством.						6
12.3.2 Аутентификацию перед использованием устройства.						6
12.3.3 Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.						6
12.3.4 Маркировку устройств с указанием владельца, контактной информации и назначения.						6
12.3.5 Допустимые варианты использования устройств.						6
12.3.6 Допустимые точки размещения устройств в сети.						6
12.3.7 Перечень одобренных компанией устройств.						6

Требование PCI DSS	Этап					
	1	2	3	4	5	6
12.3.8 Автоматическое отключение сессий удаленного доступа после определенного периода простоя.						6
12.3.9 Включение механизмов удаленного доступа для службы поддержки (производителям) только в случае необходимости такого доступа, с немедленным выключением механизмов после использования.						6
12.3.10 Запрет хранения данных о держателях карт на локальных дисках, дискетах и иных съемных носителях при удаленном доступе к данным, а также запрет использования функций копирования-вставки данных и вывода данных на принтер во время сеанса удаленного доступа.						6
12.4 Политика и процедуры безопасности должны однозначно определять обязанности всех сотрудников и партнеров, относящиеся к информационной безопасности.						6
12.5 Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:						6
12.5.1 Разработка, документирование и распространение политики и процедур безопасности.						6
12.5.2 Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных.						6
12.5.3 Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.						6
12.5.4 Администрирование учетных записей пользователей, включая их добавление, удаление и изменение.						6
12.5.5 Мониторинг и контроль любого доступа к данным.						6
12.6 Должна быть внедрена официальная программа повышения осведомленности сотрудников о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт.						6
12.6.1 Обучение сотрудников должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год.						6

Требование PCI DSS	Этап					
	1	2	3	4	5	6
12.6.2 Сотрудники должны не реже одного раза в год подтверждать своё знание и понимание политики и процедур информационной безопасности компании.						6
12.7 Следует тщательно проверять кандидатов при приеме на работу (будущих сотрудников), для минимизации риска внутренних атак. (Определение термина "сотрудник" приведено в пункте 9.2) Для таких сотрудников, как кассиры в магазине, которые имеют доступ к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.						6
12.8 В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними, включающие:		2				
12.8.1 Поддержку перечня поставщиков услуг.		2				
12.8.2 Поддержку письменного соглашения о том, что поставщики услуг ответственны за безопасность переданных им данных о держателях карт.		2				
12.8.3 Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним.		2				
12.8.4 Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS.		2				
12.9 Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы.						6
12.9.1 Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум: - роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных 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; - ссылки или включение процедур реагирования на инциденты международных платежных систем.						6

Требование PCI DSS	Этап					
	1	2	3	4	5	6
12.9.2 План должен тестироваться не реже одного раза в год.						6
12.9.3 Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7.						6
12.9.4 Персонал, ответственный за реагирование на нарушения безопасности, должен быть обучен соответствующим образом.						6
12.9.5 План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов.						6
12.9.6 Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.						6
Приложение A: Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)						
A.1 Обеспечить защиту данных каждого клиента, согласно требованиям с A.1.1 по A.1.4: Хостинг-провайдер должен удовлетворять всем этим требованиям, помимо требований PCI DSS Примечание: не смотря на то, что хостинг-провайдер будет соответствовать требованиям PCI DSS, каждый его клиент должен, тем не менее, проходить собственный аудит.			3			
A.1.1 Ограничить доступ приложений каждого клиента только к своей среде данных о держателях карт.			3			
A.1.2 Ограничить доступ клиента только к своей среде данных о держателях карт.			3			
A.1.3 Убедиться, что протоколирование действий и событий включено для каждого клиента, и соответствует требованию 10 стандарта.			3			
A.1.4 Убедиться в наличии процессов, позволяющих провести расследование инцидентов каждого клиента.			3			