



Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Требования и процедура аудита безопасности

Версия 1.2.1

Июль 2009

PCI DSS.RU

Содержание

Введение и обзор стандарта PCI DSS.....	3
Область применения PCI DSS	4
Область аудита соответствия требованиям PCI DSS.....	5
<i>Сегментация сети</i>	5
<i>Беспроводные сети</i>	5
<i>Привлечение третьих сторон</i>	6
<i>Выборочная оценка системных компонентов</i>	6
<i>Компенсирующие меры</i>	7
Инструкции по заполнению и требования к содержанию Отчета о соответствии.....	8
<i>Содержание и формат отчета</i>	8
<i>Проведение повторных проверок</i>	11
<i>Оценка соответствия PCI DSS – шаги создания отчета</i>	11
Детальные требования PCI DSS и процедуры проведения аудита	11
Построение и обслуживание защищенной сети	13
<i>Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт</i>	13
<i>Требование 2: Не использовать пароли и другие системные параметры, заданные производителем по умолчанию</i>	18
Защита данных о держателях карт	21
<i>Требование 3: Обеспечить безопасное хранение данных о держателях карт</i>	21
<i>Требование 4: Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования</i>	29
Управление уязвимостями.....	31
<i>Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение</i>	31
<i>Требование 6: Разрабатывать и поддерживать безопасные системы и приложения</i>	33
Внедрение строгих мер контроля доступа	40
<i>Требование 7: Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью</i>	40
<i>Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре</i>	42
<i>Требование 9: Ограничить физический доступ к данным платежных карт</i>	48
Регулярный мониторинг и тестирование сети	54
<i>Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт</i>	54
<i>Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности</i>	58
Разработка политики информационной безопасности	62
<i>Требование 12: Разработать и поддерживать политику информационной безопасности</i>	62
Приложение А: Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров).....	70
Приложение В: Компенсирующие меры	73
Приложение С: Компенсирующие меры – форма для заполнения	74
Приложение D: Оценка соответствия – торгово-сервисные предприятия	76
Приложение Е: Оценка соответствия – поставщики услуг	80
Приложение F: Определение области аудита и выборки.....	84
Информация о переводе.....	85

Введение и обзор стандарта PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан в целях упрощения внедрения и распространения мер по обеспечению безопасности данных о держателях карт. В основе данного стандарта лежат 12 требований, сгруппированных таким образом, чтобы упростить процедуру аудита безопасности. Данный стандарт предназначен для использования аудиторами при проверке торговых-сервисных предприятий и поставщиков услуг на соответствие его требованиям. Ниже приведен краткий обзор этих 12 требований. На следующих страницах приведены основные сведения по подготовке к аудиту соответствия требованиям PCI DSS, проведению аудита и написанию отчетных материалов. Детальное описание требований начинается со страницы 13.

Обзор PCI DSS

Построение и обслуживание защищенной сети

Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт.

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

Защита данных о держателях карт

Требование 3: Обеспечить безопасное хранение данных о держателях карт.

Требование 4: Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования.

Управление уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение.

Требование 6: Разрабатывать и поддерживать безопасные системы и приложения.

Внедрение строгих мер контроля доступа

Требование 7: Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью.

Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре.

Требование 9: Ограничить физический доступ к данным о держателях карт.

Регулярный мониторинг и тестирование сети

Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт.

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

Разработка политики информационной безопасности

Требование 12: Разработать и поддерживать политику информационной безопасности.

Область применения PCI DSS

Приведенная ниже таблица иллюстрирует наиболее часто используемые элементы данных о держателях карт и критичных аутентификационных данных; разрешено или запрещено их хранение; должен ли быть защищен каждый из этих элементов. Таблица не является исчерпывающей, она демонстрирует различные типы требований, предъявляемых к каждому элементу.

Требования PCI DSS применимы к системе, если в ней хранится, обрабатывается или передается номер карты (PAN). Если PAN не хранится, не обрабатывается и не передается, то требования PCI DSS не применяются.

	Элемент данных	Хранение разрешено	Требуется защита	Требование 3.4 PCI DSS
Данные о держателях карт	Номер платежной карты (PAN)	ДА	ДА	ДА
	Имя держателя карты (Cardholder Name) ¹	ДА	ДА ¹	НЕТ
	Сервисный код (Service Code) ¹	ДА	ДА ¹	НЕТ
	Дата истечения срока действия карты (Expiration Date) ¹	ДА	ДА ¹	НЕТ
Критичные аутентификационные данные ²	Вся магнитная полоса карты ³	НЕТ	Не определено	Не определено
	CAV2/CVC2/CVV2/CID	НЕТ	Не определено	Не определено
	PIN / PIN Block	НЕТ	Не определено	Не определено

¹Эти элементы данных должны быть защищены в случае, если хранятся совместно с PAN. Эта защита должна соответствовать требованиям PCI DSS по безопасности среды данных о держателях карт. Хотя PCI DSS не требует защиты таких данных, если не передается, не хранится и не обрабатывается PAN, их защита и раскрытие применяемых компанией методов обработки и хранения персональных данных клиентов может потребоваться согласно требованиям других законодательных актов (например, защита персональных данных, обеспечение конфиденциальности, предотвращение кражи идентификатора или обеспечение безопасности данных).

²критичные аутентификационные данные не должны храниться после авторизации (даже в зашифрованном виде).

³ полная магнитная полоса карты, её зашифрованное представление в чипе и другие виды представления

Область аудита соответствия требованиям PCI DSS

Требования PCI DSS предъявляются ко всем системным компонентам. Под «системным компонентом» понимается любое сетевое оборудование, сервер или приложение, которое включено в среду данных о держателях карт или соединено с ней. Среда данных о держателях карт – это часть вычислительной сети, которая обрабатывает данные о держателях карт и критичные аутентификационные данные. Сетевые компоненты включают в себя межсетевые экраны, коммутаторы, маршрутизаторы, беспроводные точки доступа, устройства сетевой безопасности и другие. Под серверами понимаются веб-сервера, сервера приложений, сервера баз данных, сервера аутентификации, почтовые сервера, прокси-сервера, сервера службы времени (NTP) и DNS-сервера. Приложения включают в себя все приобретенные или самостоятельно разработанные приложения, в том числе внутренние и внешние (Интернет-приложения).

Сегментация сети

Выделение среды обработки данных о держателях карт в отдельный сегмент не является требованием PCI DSS, но рекомендовано, как средство, позволяющее уменьшить:

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

В случае отсутствия адекватной сегментации (т.н. «плоская сеть»), под область действия PCI DSS попадает вся сеть. Сегментация сети может быть выполнена путем настройки межсетевых экранов, маршрутизаторов со списками контроля доступа или при помощи другой технологии, которая ограничивает доступ к определенному сегменту сети.

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

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

Аудитор должен удостовериться в корректности применения сегментации сети для сужения границ проведения оценки соответствия PCI DSS. Если подходить с точки зрения высокого уровня, адекватная сегментация сети изолирует системы, которые хранят, обрабатывают или передают данные о держателях карт от остальных систем. Адекватность реализации сегментации очень сильно зависит от конфигурации сети, используемых технологий и других мер, которые могут быть реализованы.

Приложение F: Обзор PCI DSS – Определение области аудита и выборки – содержит дополнительную информацию об эффективном определении границ области оценки.

Беспроводные сети

Если в компании используется беспроводная технология для хранения, обработки или передачи данных о держателях карт (например, для POS-транзакций) или беспроводная локальная сеть является частью среды обработки данных о держателях карт (например, в случае

некорректной сегментации), в силу вступают требования PCI DSS для беспроводных сетей (в частности, требования 1.2.3, 2.1.1 и 4.1.1). Компания должна тщательно проанализировать необходимость внедрения беспроводных технологий и оценить связанные с этим риски. Рекомендуется использовать беспроводные технологии только для некритичных сегментов сети.

Привлечение третьих сторон

При прохождении ежегодного аудита необходимо провести проверку всех системных компонентов, где хранится, обрабатывается или передается информация о держателях карт.

Поставщики услуг и торгово-сервисные предприятия могут воспользоваться услугами сторонних организаций по обработке, хранению и передаче данных о держателях карт; обслуживанию маршрутизаторов, межсетевых экранов, серверов, обеспечению физической безопасности. Однако это может оказать негативное влияние на безопасность данных о держателях карт.

Для тех организаций, которые используют услуги третьих сторон для хранения, обработки или передачи данных о держателях карт, Отчет о соответствии (Report on Compliance, ROC) должен содержать описание роли каждой третьей стороны, для четкого понимания того, какие требования предъявляются к организации, а какие – к поставщику услуг (третьей стороне). Поставщик услуг (третья сторона) может подтвердить соответствие требованиям двумя способами: 1) Предоставление доказательств пройденного аудита соответствия PCI DSS 2) Прохождение аудита соответствия PCI DSS совместно с каждым из своих клиентов. Подробности указаны в разделе «Для проверки организаций, имеющих статус MSP (Managed Service Providers)» части 3 «Инструкции и содержание отчета о соответствии».

Дополнительно торгово-сервисные предприятия и поставщики услуг должны контролировать статус соответствия PCI DSS всех сторонних организаций, которые имеют доступ к данным о держателях карт. *Подробности см. в требовании 12.8.*

Выборочная оценка системных компонентов

Аудитор, выполняющий проверки PCI DSS, может выбрать несколько бизнес-единиц и системных компонентов для проверок. Эта выборка должна включать в себя как бизнес-единицы, так и системные компоненты и быть достаточно обширной, чтобы аудитор мог удостовериться в выполнении всех требований.

Примеры бизнес-единиц: офисы компании, магазины, франчайзинговые предприятия и географически разнесенные офисные помещения. В каждой выбранной бизнес-единице необходимо проверить на соответствие какой-либо из системных компонентов. Например, операционные системы или приложения, доступные для проверок. В каждой структурной единице примером аудитору могут служить сервера под управлением Sun Solaris, на которых функционирует веб-сервер Apache, Windows-сервера, на которых функционирует СУБД Oracle, мейнфреймы, на которых функционируют платежные приложения, сервера передачи данных под управлением HP-UX и Linux-сервера с MySQL. Если все приложения работают на одной платформе, может проверяться множество различных приложений (см. Приложение F: *Определение области аудита и выборки*).

При выборе бизнес-единиц и системных компонентов для оценки проверяющий должен учесть следующее:

- Выборка может быть меньше при наличии стандартизированных процессов, согласно которым выполняются требования PCI DSS.

- В случае наличия более одного процесса (например, для разных системных компонентов), выборка должна быть достаточно большой, чтобы включать объекты, привязанные к каждому процессу.
- В случае отсутствия налаженных процессов, размер выборки должен быть достаточно большим, чтобы проверяющий мог убедиться, что каждая бизнес-единица корректно понимает и выполняет требования PCI DSS.

Подробнее см. Приложение F: Определение области аудита и выборки.

Компенсирующие меры

Все компенсирующие меры должны быть ежегодно документированы, проанализированы и утверждены аудитором и включены в Отчет о соответствии, в соответствии с *Приложением B: Компенсирующие меры* и *Приложением C: Компенсирующие меры – форма для заполнения*.

Для каждой компенсирующей меры в обязательном порядке должна быть заполнена таблица (Приложение C). Кроме того, результаты компенсирующих мер должны быть отражены в Отчете о соответствии в разделе соответствующего требования PCI DSS.

Подробности см. в Приложении B и C.

Инструкции по заполнению и требования к содержанию Отчета о соответствии

Этот документ следует использовать как шаблон Отчета о соответствии. Проверяемая организация должна выполнять требования каждой платежной системы по заполнению отчета для подтверждения статуса соответствия. За подробностями следует обращаться к соответствующей платежной системе.

Содержание и формат отчета

Следуйте этим инструкциям по содержанию при заполнении Отчета о соответствии.

1. Краткое описание

Включает в себя следующее:

- Описание бизнеса проверяемой компании, а именно:
 - задачи компании, связанные с работой с платежными картами, как, где и зачем они хранятся, обрабатываются или передаются.
Примечание: Это должно быть не выдержкой, скопированной с корпоративного сайта компании, а кратким описанием, показывающим, что аудитор понимает роль компании в платежной индустрии.
 - Как компания проводит платежи (сама, или с помощью других организаций).
 - Какие платежные сервисы предоставляет компания: транзакции в случае отсутствия карты (заказ по телефону или почте, электронная коммерция) или при ее наличии.
 - Перечень организаций, с которыми сотрудничает данная компания для обработки платежной информации.
- Схему сети (предоставленную проверяемой организацией или составленную аудитором) компании:
 - Входящие и исходящие соединения с сетью.
 - Критичные компоненты среды данных о держателях карт, такие как POS-терминалы, СУБД, веб-сервера.
 - Другие важные компоненты.

2. Описание границ аудита и методов оценки

Следует описать область проведения аудита, согласно разделу «Границы проведения аудита» данного документа, включая:

- Среду, которой уделено внимание при проведении аудита (например, клиентские точки доступа к сети Интернет, внутренняя корпоративная сеть, системы обработки данных и т.п.).
- Если в компании используется сегментация сети для уменьшения области действия стандарта, следует кратко описать принципы сегментирования и аргументировать подтверждение аудитором эффективности сегментации.
- Документальное обоснование выбранных для оценки бизнес-единиц и системных компонентов, в том числе следует указать:
 - Общее количество компонентов.
 - Количество выбранных компонентов.
 - Обоснование причин выбора этих компонентов.
 - Обоснование достаточности количества выбранных компонентов для вынесения заключения о том, что рассмотренная выборка является репрезентативной с точки зрения выполнения требований стандарта.
 - Места, в которых хранятся или обрабатываются данные о держателях карт, которые были ИСКЛЮЧЕНЫ из области проведения аудита, и обоснование того, почему они были исключены.
- Дочерние организации, которым также необходимо удовлетворять требованиям PCI DSS, с указанием того, проверяются ли они отдельно или в составе текущего аудита.
- Интернациональные компании, которым также необходимо удовлетворять требованиям PCI DSS, с указанием того, проверяются ли они отдельно или в составе текущего аудита.
- Беспроводные сети или беспроводные платежные приложения (например, POS-терминалы), которые имеют сетевое соединение со средой данных о держателях карт, и используемые механизмы защиты.
- Используемую версию документа «PCI DSS: Требования и процедура аудита безопасности».
- Временные рамки проведения аудита.

3. Подробности о проверенной системе

В этом разделе в отчет должны быть включены следующие сведения:

- Диаграмма всех соединений с внешними сетями (LAN, WAN, Internet).
- Описание среды данных о держателях карт, например:
 - Схема передачи и обработки данных о держателях карт, в том числе авторизация, проведение транзакции, возврат платежей и т.п.
 - Перечень файлов и таблиц, в которых хранятся данные о держателях карт, а также инвентаризационный журнал, полученный от проверяемой компании или созданный аудитором. Для каждого хранилища данных этот журнал должен включать:

- Перечень всех хранимых элементов данных о держателях карт.
 - Информацию о способе защиты данных.
 - Информацию о ведении журналов доступа к данным.
- Перечень аппаратного и программного обеспечения, используемого в среде данных о держателях карт, с описанием выполняемых задач.
 - Перечень поставщиков услуг и других сторонних организаций, с которыми проверяемая компания совместно хранит или обрабатывает данные о держателях карт (Примечание: подробнее см. требование 12.8).
 - Перечень используемых платежных приложений и их версий, в том числе указание того, имеют ли платежные приложения сертификат PA-DSS. Даже если платежное приложение имеет сертификат соответствия PA-DSS, проверяющий должен убедиться, что они используются в соответствии с требованиями PCI DSS, а также согласно *Руководству по внедрению PA-DSS. Примечание: Использование платежных приложений, имеющих сертификат соответствия PA-DSS, не является требованием PCI DSS. Пожалуйста, уточните требования отдельных платежных систем к платежным приложениям.*
 - Перечень опрошенных лиц и их должности.
 - Перечень изученной документации.
 - Для аудита организаций, имеющих статус MSP (Managed Service Provider), проверяющий должен четко определить, какие требования предъявляются к MSP и отражены в данном отчете, а какие – клиентам MSP и должны быть отражены в отчете при проведении аудита у них. В том числе следует включить информацию о том, какие IP-адреса MSP просканированы как часть ежеквартального сканирования и за какие адреса ответственны клиенты MSP.

4. Контактная информация и дата создания отчета

Включает в себя:

- Контактную информацию торгового-сервисного предприятия или поставщика услуг и аудитора.
- Дату заполнения отчета.

5. Результаты ежеквартального сканирования

- В разделе «краткое описание» и комментариях к пункту 11.2 следует также указать результаты четырех последних результатов ежеквартального сканирования.

Примечание: наличие отчетов обо всех четырех ежеквартальных сканированиях не требуется для первоначального аудита PCI DSS, в случае если аудитор убедился, что:

- 1) последние результаты сканирования не выявили несоответствий;
- 2) в проверяемой организации существуют политики и документированные процедуры проведения ежеквартального сканирования;
- 3) любые уязвимости, выявленные в результате первоначального сканирования, были устранены, что указано в отчете о повторном сканировании.

Для всех последующих аудитов наличие отчетов обо всех четырех сканированиях в год обязательно.

- Просканированы должны быть все внешние (доступные из Интернета) IP-адреса, согласно документу *Процедуры сканирования PCI DSS*.

6. Наблюдения

- В Сводном отчете следует отразить все дополнительные наблюдения, которые могут не попадать под пункты Отчета о соответствии.
- Все проверяющие лица обязаны использовать подробный «Перечень требований PCI DSS» и руководствоваться «Процедурами проведения аудита» для предоставления детального отчета и подробного описания результатов проверки каждого требования.
- Проверяющий обязан проверить и документировать все компенсирующие меры, используемые в организации.

См. Секцию «Компенсирующие меры» и Приложения B и C.

Проведение повторных проверок

Если Отчет о соответствии содержит невыполненные требования или перечень проблем, устранение которых планируется в будущем, проверяемая организация считается несоответствующей требованиям PCI DSS и должна принять меры по устранению проблем перед повторным аудитом. После этого проверяющий должен убедиться, что проблемы устранены корректно и все требования PCI DSS выполнены. После повторного аудита проверяющий должен составить новый Отчет о соответствии, подтверждая, что вся платежная инфраструктура соответствует требованиям PCI DSS, и предоставить его в следующем порядке (см. ниже).

Оценка соответствия PCI DSS – шаги создания отчета

1. Заполнение Отчета о соответствии, согласно требованиям приведенного выше раздела «Инструкции по заполнению и содержание Отчета о соответствии».
2. Проверка результатов проведения ASV-сканирования уполномоченной организацией (ASV – *Approved Scanning Vendor*), а также запрос подтверждения его проведения у уполномоченной организации.
3. Заполнение Свидетельства о соответствии (Attestation of Compliance). См. Приложения D и E.
4. Направление Отчета о соответствии, результатов ASV-сканирования и Свидетельства о соответствии вместе со всей требуемой документацией банку-эквайеру (для торгово-сервисных предприятий), или платежной системе, или другой уполномоченной организации (для поставщиков услуг).

Детальные требования PCI DSS и процедуры проведения аудита

В нижеприведенной таблице поля означают следующее:

- **Требование PCI DSS** – требование стандарта по достижению соответствия PCI DSS.
- **Процедура проведения проверки** – действия, которые должен выполнить аудитор для проверки выполнения требований PCI DSS.
- **Выполнено** – краткое описание выполненных требований, в том числе с помощью компенсирующих мер.
- **Не выполнено** – краткое описание требований, не выполненных на должном уровне. Примечание: отчет с отметками в этом столбце не должен направляться в платежные системы или банк-эквайер, если специально не запрошен. См. Приложение D и E.
- **Дата устранения недостатков/Комментарии** – возможная дата выполнения требования (вопрос о включении в отчет решается аудитором), а также все дополнительные комментарии.

Построение и обслуживание защищенной сети

Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт

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

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

Все системы должны быть защищены от неавторизованного доступа из сети Интернет, будь то системы электронной коммерции, удаленный доступ сотрудников, доступ к корпоративной почте или выделенные соединения. Зачастую кажущиеся малозначимыми каналы связи с внешней средой могут представлять собой незащищенные пути доступа к ключевым системам. Межсетевые экраны – основные механизмы обеспечения безопасности любой компьютерной сети.

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
1.1 Должны быть разработаны стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя:	1.1 Изучить стандарты конфигурации межсетевых экранов и маршрутизаторов, а также иную документацию для проверки того, что стандарты включают в себя все необходимые требования. Выполнить следующие действия:			
1.1.1 Формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурации межсетевого экрана.	1.1.1 Проверить, что существует формальный процесс утверждения всех сетевых соединений, а также изменений в конфигурациях межсетевых экранов и маршрутизаторов.			
1.1.2 Актуальную схему сети с указанием всех каналов доступа к данным о держателях карт, включая все беспроводные сети.	1.1.2.a Проверить наличие схемы сети (например, отражающей потоки данных о держателях карт через корпоративную сеть). Проверить, что в схеме отмечены все подключения к среде данных о держателях карт, в том числе беспроводные. 1.1.2.b Проверить актуальность схемы сети.			
1.1.3 Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании.	1.1.3 Проверить, что стандарты конфигурации включают требование о необходимости межсетевого экранирования каждого Интернет-соединения, а также между DMZ и внутренней сетью. Проверить, что конфигурации межсетевых экранов не противоречат схеме сети.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
1.1.4 Описание групп, ролей и ответственности за управление сетевыми устройствами.	1.1.4 Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат описание ролей, групп и ответственности за управление сетевыми компонентами.			
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.	1.1.5.a Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат документированный перечень сервисов, протоколов и портов, необходимых для бизнеса (например, HTTP, SSL, SSH, VPN).			
	1.1.5.b Выявить разрешенные небезопасные сервисы, протоколы и порты, проверить их необходимость, а также то, что механизмы защиты документированы и внедрены, путем изучения стандартов конфигурации межсетевых экранов и маршрутизаторов и настроек каждого сервиса. В качестве примера небезопасного протокола может служить протокол FTP, который передает аутентификационные данные в открытом виде.			
1.1.6 Требование пересмотра настроек межсетевых экранов и маршрутизаторов не реже одного раза в полгода.	1.1.6.a Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов требуют пересмотра правил для межсетевых экранов и маршрутизаторов как минимум раз в полгода.			
	1.1.6.b Получить и проверить документацию, подтверждающую, что наборы правил пересматриваются как минимум раз в полгода.			
1.2 Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в среде данных о держателях карт.	1.2 Изучить конфигурации межсетевых экранов и маршрутизаторов, проверить, что ограничены соединения между недоверенными сетями и системными компонентами, находящимися в среде данных о держателях карт, а именно:			
<i>Примечание: недоверенной является любая сеть, которая не контролируется проверяемой организацией</i>				
1.2.1 Входящий и исходящий трафик должен быть ограничен только необходимыми соединениями для среды данных	1.2.1.a Проверить, что входящий и исходящий трафик ограничен только необходимыми для среды данных о держателях карт соединениями и что ограничения документированы.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
о держателях карт.	1.2.1.b Проверить, что весь иной входящий и исходящий трафик явно запрещен.			
1.2.2 Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов маршрутизаторов.	1.2.2 Проверить, что конфигурационные файлы маршрутизаторов синхронизированы, например, рабочие конфигурационные файлы и конфигурационные файлы, используемые при перезагрузке маршрутизатора, имеют одинаковую безопасную конфигурацию.			
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 контроль в том случае, если такой трафик необходим для бизнес-приложений.	1.2.3 Проверить, что между любой беспроводной сетью и системами, хранящими данные о держателях карт, установлены межсетевые экраны, запрещающие или контролирующие (в случае производственной необходимости) весь трафик из беспроводной сети в среду данных о держателях карт.			
1.3 Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды данных о держателях карт.	1.3 Проверить конфигурацию межсетевых экранов и маршрутизаторов, как описано ниже, чтобы убедиться в отсутствии прямого доступа из сети Интернет к системным компонентам, включая маршрутизатор между DMZ и внутренней сетью, сервисы в DMZ, обрабатывающие данные о держателях карт, внутренний сегмент сети, в котором циркулируют данные о держателях карт.			
1.3.1 Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только протоколами, необходимыми для среды данных о держателях карт.	1.3.1 Проверить, что DMZ применяется для ограничения входящего и исходящего трафика только теми протоколами, которые необходимы для среды данных о держателях карт.			
1.3.2 Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.	1.3.2 Проверить, что входящие Интернет-соединения ограничены только адресами, находящимися в DMZ.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
1.3.3 Должны быть запрещены любые прямые маршруты входящего или исходящего трафика между сетью Интернет и средой данных о держателях карт.	1.3.3 Проверить, что отсутствуют прямые входящие и исходящие маршруты между сетью Интернет и средой данных о держателях карт.			
1.3.4 Необходимо запретить соединения с внутренними адресами от источника из сети Интернет к адресам, расположенным в DMZ.	1.3.4 Проверить, что пакеты с внутренними адресами не могут достигнуть DMZ от источника из сети Интернет.			
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.	1.3.5 Проверить, что исходящий трафик из среды данных о держателях карт имеет доступ только к IP-адресам, расположенным в DMZ.			
1.3.6 Необходимо включить динамическую пакетную фильтрацию с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений).	1.3.6 Проверить, что межсетевые экраны применяют динамическую пакетную фильтрацию с запоминанием состояния. [Должны быть разрешены прохождения пакетов только для установленных соединений и только в пределах предварительно установленной сессии (запустить сканирование всех TCP-портов путем отправки запросов SYN RST и SYS ACK – ответ будет означать, что пакеты разрешены за пределами предварительно установленной сессии)].			
1.3.7 Необходимо размещать базы данных во внутреннем сегменте сети, отделенном от DMZ.	1.3.7 Проверить, что базы данных расположены во внутренней сети, отделенной от DMZ.			
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.	1.3.8 Для нескольких межсетевых экранов и маршрутизаторов проверить работоспособность механизма трансляции адресов для предотвращения раскрытия внутренних адресов.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
1.4 Должны быть установлены персональные межсетевые экраны на все мобильные и принадлежащие сотрудникам компьютеры, имеющие прямой доступ в сеть Интернет и используемые также для доступа к локальной сети организации.	1.4.a Проверить, что на все мобильные и принадлежащие сотрудникам компьютеры, имеющие прямой доступ в сеть Интернет и используемые для доступа к локальной сети организации, установлены персональные межсетевые экраны.			
	1.4.b Проверить, что настройки персонального межсетевого экрана выполнены в соответствии со стандартами организации и не могут быть изменены пользователем.			

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

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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).</p>	<p>2.1 Сделать выборку системных компонентов, критичных серверов и беспроводных точек доступа. Попытаться осуществить вход на каждое устройство из выборки, используя аутентификационные данные по умолчанию, чтобы проверить, что установленные производителем аутентификационные данные были изменены (Следует использовать руководства пользователя и Интернет-ресурсы, чтобы узнать устанавливаемые по умолчанию производителем аутентификационные данные).</p>			
<p>2.1.1 Для беспроводных сетей, подключенных к среде данных о держателях карт либо передающих данные о держателях карт, необходимо изменить установленные по умолчанию производителем параметры, такие как ключи шифрования, пароли, строки доступа SNMP. Следует включить стойкие криптографические механизмы для шифрования данных при передаче и аутентификации.</p>	<p>2.1.1 Проверить следующие настройки для беспроводных устройств, чтобы убедиться в стойкости применяемых криптографических механизмов:</p> <ul style="list-style-type: none"> ▪ ключи шифрования по умолчанию были изменены и изменяются каждый раз, когда кто-либо, знающий ключи, уходит из компании либо переходит на другую должность; ▪ строки доступа SNMP по умолчанию были изменены; ▪ пароли/парольные фразы точек доступа по умолчанию были изменены; ▪ программное обеспечение устройств обновлено до актуальной версии и поддерживает стойкие криптографические алгоритмы для передачи данных и аутентификации (WPA/WPA2); ▪ иные настройки безопасности, установленные производителем по умолчанию. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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.	2.2.a Изучить стандарты конфигурации всех системных компонентов. Проверить, что стандарты конфигурации учитывают положения общепринятых отраслевых стандартов (SANS, NIST, CIS).			
	2.2.b Проверить, что стандарты конфигураций учитывают требования 2.2.1 - 2.2.4.			
	2.2.c Убедиться, что стандарты конфигураций применяются при настройке новых систем.			
2.2.1 Каждый сервер должен выполнять одну основную функцию.	2.2.1 Для нескольких системных компонентов проверить, что выполняется правило "один сервер - одна основная функция". Например, веб-сервер, сервер СУБД и DNS-сервер следует размещать на разных компьютерах.			
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).	2.2.2 Для выборки из нескольких системных компонентов проверить включенные сервисы и протоколы. Проверить, что ненужные или небезопасные сервисы и протоколы выключены или их использование обосновано и документировано.			
2.2.3 Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.	2.2.3.a Опросить системных администраторов и администраторов безопасности с целью проверки того, что им известны настройки основных параметров безопасности системных компонентов.			
	2.2.3.b Проверить, что основные параметры безопасности включены в стандарты конфигурации системных компонентов.			
	2.2.3.c Для нескольких системных компонентов проверить, что основные параметры безопасности установлены соответствующим образом.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>2.2.4 Из системы должна быть удалена вся ненужная функциональность: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.</p>	<p>2.2.4 Для нескольких системных компонентов проверить, что ненужная функциональность выключена. Проверить, что включенные функции документированы и безопасно настроены.</p>			
<p>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.</p>	<p>2.3 Для нескольких системных компонентов проверить, что для защиты удаленного административного доступа применяются криптографические механизмы:</p> <ul style="list-style-type: none"> ▪ Изучить записи журнала каждой системы для того, чтобы подтвердить активизацию механизмов шифрования до запроса пароля администратора. ▪ Проверить, что для использования не доступны Telnet и другие протоколы удаленного доступа к системе. ▪ Проверить, что для веб-ориентированных систем удаленного административного доступа применяются стойкие криптографические механизмы. 			
<p>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)».</p>	<p>2.4 Выполнить проверочные процедуры А.1.1 - А.1.4., описанные в Приложении А: «Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)» по обеспечению безопасности сред и данных, принадлежащих каждой из обслуживаемых сторон (торгово-сервисные предприятия и поставщики услуг).</p>			

Защита данных о держателях карт

Требование 3: Обеспечить безопасное хранение данных о держателях карт

Методы защиты данных, такие как шифрование, обрезка, маскирование и хеширование являются критическими компонентами защиты данных о держателях карт. Если взломщик обойдет остальные средства управления безопасностью сети и получит доступ к зашифрованным данным, не зная ключа шифрования, то эти данные останутся для него нечитаемыми и практически бесполезными. Иные способы защиты хранимых данных должны рассматриваться как средства уменьшения риска. Методы минимизации риска включают в себя запрет сохранения данных о держателях карт, кроме случаев крайней необходимости, хранение обрезанного PAN, если не требуется хранение полного PAN, и избежание пересылки PAN по электронной почте в открытом виде.

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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.</p>	<p>3.1 Изучить политики и процедуры хранения и уничтожения данных и выполнить следующее:</p> <ul style="list-style-type: none"> ▪ Проверить, что политики и процедуры содержат требования бизнеса и законодательства к хранению данных, включая специфические требования к хранению данных о держателях карт. ▪ Проверить, что политики и процедуры содержат оговорки о необходимости уничтожения данных, если их хранение более не требуется по требованиям бизнеса, законодательства и иным регулирующим требованиям. ▪ Проверить, что действие политик и процедур распространяется на все места хранения данных о держателях карт. ▪ Проверить, что политики и процедуры предусматривают автоматические методы уничтожения данных о держателях карт, сроки хранения которых превысили необходимые согласно требованиям бизнеса либо требованиям по пересмотру и оценке необходимости дальнейшего хранения данных о держателях карт не реже одного раза в квартал. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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.</p>	<p>3.2 В случае, если критичные аутентификационные данные принимаются и уничтожаются, необходимо проверить процессы их уничтожения и убедиться, что данные невозможны восстановить. Для каждого вида критичных аутентификационных данных выполнить следующие шаги:</p>			
<p>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»).</p> <p><i>Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы:</i></p> <ul style="list-style-type: none"> ▪ имя держателя карты, ▪ номер платежной карты (PAN), ▪ дата истечения срока действия карты, ▪ сервисный код. <p><i>Для минимизации рисков разрешается хранить только указанные элементы данных.</i></p> <p><i>Дополнительная информация приведена в «Глоссарии PCI DSS: Основные определения, аббревиатуры и сокращения».</i></p>	<p>3.2.1 Для нескольких системных компонентов проверить следующие элементы и убедиться, что полная дорожка магнитной полосы, находящейся на обратной стороне карты, не сохраняется ни при каких обстоятельствах:</p> <ul style="list-style-type: none"> ▪ входящие данные о транзакции; ▪ все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); ▪ файлы истории; ▪ файлы трассировки; ▪ несколько схем баз данных; ▪ содержимое баз данных. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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».</p>	<p>3.2.2 Для нескольких системных компонентов проверить следующие элементы и убедиться, что трех- или четырехзначное проверочное значение (CVC2, CVC2, CID, CAV2) не сохраняется ни при каких обстоятельствах:</p> <ul style="list-style-type: none"> ▪ входящие данные о транзакции; ▪ все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); ▪ файлы истории; ▪ файлы трассировки; ▪ несколько схем баз данных; ▪ содержимое баз данных. 			
<p>3.2.3 Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.</p>	<p>3.2.3 Для нескольких системных компонентов проверить следующие элементы и убедиться, что персональный идентификационный номер (PIN), а также зашифрованный PIN-блок не сохраняется ни при каких обстоятельствах:</p> <ul style="list-style-type: none"> ▪ входящие данные о транзакции; ▪ все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок); ▪ файлы истории; ▪ файлы трассировки; ▪ несколько схем баз данных; ▪ содержимое баз данных. 			
<p>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).</p>	<p>3.3 Изучить политики и проверить правила отображения PAN. Проверить, что PAN маскируется при его отображении (например, на бумаге или экране монитора), кроме случаев, когда для работы сотрудников необходимо видеть весь PAN.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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:</p> <ul style="list-style-type: none"> ▪ 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 	<p>3.4.a Изучить документацию о системе, используемой для защиты PAN, в том числе информацию о её производителе, типе системы, применяемых алгоритмах шифрования (если они используются). Проверить, что PAN представлен в нечитаемом виде при помощи одного из следующих методов:</p> <ul style="list-style-type: none"> ▪ 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. 			
	<p>3.4.b Изучить несколько таблиц или файлов из нескольких хранилищ данных и убедиться, что PAN представлен в нечитаемом виде.</p>			
	<p>3.4.c Изучить несколько съемных носителей (например, кассеты с резервными копиями данных) и убедиться, что PAN представлен в нечитаемом виде.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>управления ключами.</p> <p>Из всей информации о держателе карты как минимум PAN должен быть преобразован в нечитаемый вид.</p> <ul style="list-style-type: none"> ▪ Если, по каким-то причинам, компания не может преобразовать PAN в нечитаемый вид, то следует применять компенсирующие меры. О компенсирующих мерах подробно написано в Приложении В: «Компенсирующие меры». ▪ Термин «стойкие криптографические алгоритмы» определен в «Глоссарии PCI DSS: Основные определения, аббревиатуры и сокращения» 	<p>3.4.d Изучить несколько журналов регистрации событий и убедиться, что из них убран PAN либо PAN представлен в нечитаемом виде.</p>			
<p>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.</p>	<p>3.4.1.a Если применяется шифрование на уровне диска, проверить, что логический доступ к файловой системе реализован при помощи механизма, независимого от механизмов разграничения доступа операционной системы.</p>			
	<p>3.4.1.b Проверить, что криптографические ключи хранятся безопасно (например, на съемном носителе, который защищен соответствующими процедурами контроля доступа).</p>			
	<p>3.4.1.c Проверить, что данные о держателях карт на съемных носителях хранятся только в зашифрованном виде.</p> <p><i>Примечание: Часто шифрование на уровне всего диска не зашифровывает информацию на съемных носителях, поэтому может потребоваться шифровать данные на съемных носителях отдельно.</i></p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
3.5 Следует обеспечить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования:	3.5 Проверить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования следующим образом:			
3.5.1 Доступ к ключам шифрования должен быть разрешен только нескольким ответственным за их хранение и использование сотрудникам.	3.5.1 Изучить списки доступа и убедиться, что доступ к ключам предоставлен только ограниченному кругу сотрудников.			
3.5.2 Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.	3.5.2 Изучить системные конфигурационные файлы, убедиться, что ключи хранятся в зашифрованном виде и ключи шифрования ключей хранятся отдельно от ключей шифрования данных.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
3.6 Должны быть документированы все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе:	3.6.a Проверить наличие процедур управления ключами шифрования данных о держателях карт. <i>Примечание: Существует множество различных источников, из которых можно почерпнуть информацию о стандартах в управлении ключами (например, стандарт национального института стандартов и технологий США (NIST), с которым можно ознакомиться на сайте http://csrc.nist.gov).</i>			
	3.6.b Убедиться, что поставщики услуг при предоставлении клиентам ключей шифрования для передачи данных о держателях карт также предоставляют документацию по условиям их безопасного хранения и обработки.			
	3.6.c Изучить процедуры управления ключами и выполнить следующие проверки:			
3.6.1 Генерация стойких ключей.	3.6.1 Убедиться, что процедуры управления ключами обеспечивают генерацию стойких ключей.			
3.6.2 Безопасное распространение ключей.	3.6.2 Убедиться, что процедуры управления ключами обеспечивают безопасное распространение ключей.			
3.6.3 Безопасное хранение ключей.	3.6.3 Убедиться, что процедуры управления ключами обеспечивают безопасное хранение ключей.			
3.6.4 Периодическая смена ключей: <ul style="list-style-type: none"> ▪ насколько часто этого требуют применяемые приложения, предпочтительно автоматически; ▪ не реже одного раза в год. 	3.6.4 Убедиться, что процедуры управления ключами обеспечивают периодическое изменение ключей не реже одного раза в год.			
3.6.5 Уничтожение старых (просроченных) ключей, а также ключей, относительно которых существуют подозрения в их компрометации.	3.6.5.a Убедиться, что процедуры управления ключами обеспечивают изъятие из обращения старых ключей (архивацию, уничтожение, отзыв).			
	3.6.5.b Убедиться, что процедуры управления ключами обеспечивают изменение скомпрометированных ключей, а также ключей, относительно которых существуют подозрения в их компрометации.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
3.6.6 Раздельное владение частями ключей с принципом контроля двумя лицами.	3.6.6 Убедиться, что процедуры управления ключами обеспечивают раздельное владение частями ключей (например, таким образом, чтобы для расшифровки данных требовался составной ключ, компоненты которого хранятся у 2-3 сотрудников).			
3.6.7 Защита от неавторизованной смены ключа.	3.6.7 Убедиться, что процедуры управления ключами обеспечивают защиту от неавторизованного изменения ключа.			
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.	3.6.8 Убедиться, что процедуры управления ключами обеспечивают письменное согласие сотрудников, ответственных за хранение и использование ключей, с ознакомлением и принятием таких обязанностей и ответственности.			

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

Критичная информация должна передаваться через общедоступные сети, где её легко перехватить, изменить или перенаправить, только в зашифрованном виде. Неправильно сконфигурированные беспроводные сети и уязвимости, связанные с использованием устаревших механизмов шифрования, могут быть легкими целями для злоумышленника и способствовать получению несанкционированного доступа к среде данных о держателях карт.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>4.1 Для защиты данных о держателях карт во время передачи их через общедоступные сети следует использовать стойкие криптографические алгоритмы и протоколы, такие как SSL/TLS и IPSEC.</p> <p><i>Примерами общедоступных сетей, на которые распространяются требования PCI DSS, являются:</i></p> <ul style="list-style-type: none"> ▪ Интернет; ▪ Беспроводные технологии; ▪ GSM; ▪ GPRS. 	<p>4.1.a Проверить использование шифрования (например, SSL/TLS или IPSEC) в случае передачи данных о держателях карт через общедоступные сети.</p> <ul style="list-style-type: none"> ▪ Проверить, что используются криптостойкие алгоритмы шифрования ▪ Для SSL: <ul style="list-style-type: none"> – Проверить, что сервер поддерживает наиболее актуальную версию; – Проверить, что строка URL содержит HTTPS; – Проверить, что данные о держателях карт не передаются, когда URL не содержит HTTPS. ▪ Выбрать несколько входящих транзакций и проверить, что данные о держателях карт передаются в зашифрованном виде. ▪ Проверить, что принимаются только доверенные SSL/TLS ключи и сертификаты. ▪ Проверить, что для шифрования данных применяются стойкие алгоритмы (учесть рекомендации производителя и наиболее прогрессивные методы). 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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.</p> <ul style="list-style-type: none"> ▪ 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. 	<p>4.1.1 Для беспроводных сетей, передающих данные о держателях карт либо подключенных к среде данных о держателях карт, проверить, используются ли передовые практические методы и стандарты (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных.</p>			
<p>4.2 Никогда не следует пересылать незашифрованный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты).</p>	<p>4.2.a Проверить, что стойкие криптографические механизмы защиты применяются в случае, когда данные о держателях карт передаются при помощи технологий передачи сообщений.</p> <p>4.2.b Проверить наличие политики, запрещающей отправку незашифрованного PAN при помощи технологий передачи сообщений.</p>			

Управление уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение

Большинство видов вредоносного программного обеспечения проникают в сеть через электронную почту сотрудников, сеть Интернет, съемные носители или мобильные устройства в результате использования системных уязвимостей. Антивирусное программное обеспечение должно быть установлено на всех подверженных воздействию вирусов системах, чтобы защитить их от вредоносного кода.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
5.1 Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).	5.1 Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, проверить, что используется антивирусная защита (если подходящая антивирусная технология существует).			
5.1.1 Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	5.1.1 Для нескольких системных компонентов проверить, что антивирусное программное обеспечение обеспечивает защиту от всех известных форм вредоносного программного обеспечения, включая шпионские и рекламные программы.			
5.2 Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий.	5.2 Проверить, что антивирусные механизмы актуальны, постоянно включены и способны вести журналы протоколирования событий, а именно:			
	5.2.a Изучить политику и убедиться, что она регламентирует регулярное обновление антивирусного программного обеспечения и антивирусных баз.			
	5.2.b Убедиться, что в установочном образе используемых систем включено автоматическое обновление и регулярное сканирование.			
	5.2.c Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, проверить, что автоматическое обновление антивирусного программного обеспечения и периодические проверки включены.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	5.2.d Для нескольких системных компонентов проверить, что включено протоколирование событий антивирусного программного обеспечения и журналы протоколирования сохраняются в соответствии с требованием 10.7 PCI DSS.			

Требование 6: Разрабатывать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости в безопасности для получения привилегированного доступа к системе. Большинство из таких уязвимостей закрывается путем установки обновлений безопасности, выпускаемых производителем. На все системы должны быть установлены самые свежие подходящие обновления программного обеспечения для защиты от эксплуатации уязвимостей внутренними и внешними злоумышленниками, а также вирусами.

Примечание: Подходящими являются те обновления, которые протестированы на совместимость с текущей конфигурацией безопасности. В случае самостоятельной разработки приложений, множество уязвимостей удастся избежать, используя стандартные процессы разработки систем и приемы безопасного написания программного обеспечения.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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. <i>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.</i></p>	<p>6.1.a Для нескольких системных компонентов и программного обеспечения проверить, установлены ли актуальные обновления безопасности, выпущенные производителем.</p> <p>6.1.b Изучить политики, убедиться, что они регламентируют установку всех критичных обновлений безопасности в течение одного месяца.</p>			
<p>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.</p>	<p>6.2.a Опросить ответственных лиц, убедиться, что в компании внедрены процессы выявления новых уязвимостей.</p> <p>6.2.b Убедиться в наличии процесса выявления новых уязвимостей, в том числе использования для этого внешних источников информации и обновления стандартов конфигурации системных компонентов (требование 2.2 PCI DSS).</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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:	6.3.a Изучить документацию по разработке программного обеспечения и убедиться, что процесс разработки программного обеспечения основан на передовых практических методиках, принимает во внимание информационную безопасность в течение всего цикла разработки и учитывает требования стандарта PCI DSS. 6.3.b Путем изучения документации, опроса разработчиков программного обеспечения, а также иных наблюдений, проверить следующее:			
6.3.1 Все обновления безопасности и изменения в конфигурации должны быть протестированы перед внедрением; тестирование должно включать в себя:	6.3.1 Убедиться в том, что все изменения (в том числе установка обновлений) тестируются перед внедрением; тестирование должно включать в себя:			
6.3.1.1 Проверку всех входных данных (чтобы исключить XSS, инъекции, исполнение вредоносного файла, и т. д.).	6.3.1.1 Проверку всех входных данных (чтобы исключить XSS, инъекции, исполнение вредоносного файла, и т. д.).			
6.3.1.2 Проверку корректной обработки ошибок.	6.3.1.2 Проверку корректной обработки ошибок.			
6.3.1.3 Проверку использования защищенного криптографического хранилища для критичной информации.	6.3.1.3 Проверку использования защищенного криптографического хранилища для критичной информации.			
6.3.1.4 Проверку безопасности передачи данных	6.3.1.4 Проверку безопасности передачи данных			
6.3.1.5 Проверку корректности разграничения доступа, основанного на ролях	6.3.1.5 Проверку корректности разграничения доступа, основанного на ролях			
6.3.2 Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга.	6.3.2 Убедиться в том, что среды разработки, тестирования и производственного функционирования программного обеспечения отделены друг от друга, и при этом внедрены механизмы разграничения доступа.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
6.3.3 Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть разделены.	6.3.3 Убедиться в том, что обязанности по разработке, тестированию и производственному функционированию программного обеспечения разделены.			
6.3.4 Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.	6.3.4 Убедиться в том, что производственные данные (действующие PAN) не используются для тестирования и разработки.			
6.3.5 Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.	6.3.5 Убедиться в том, что все тестовые данные и платежные счета удаляются из системы перед переводом ее в производственный режим.			
6.3.6 Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчиком или переводом его в производственный режим.	6.3.6 Убедиться в том, что все индивидуальные учетные записи, имена пользователей и пароли удаляются перед передачей программного обеспечения заказчиком или переводом его в производственный режим.			
6.3.7 Программный код приложений должен быть исследован на наличие потенциальных уязвимостей перед передачей готовых приложений заказчиком или переводом их в производственный режим. <i>Примечание: это требование применимо ко всем разрабатываемым приложениям (как внутренним, так и общедоступным) как элемент обеспечения безопасности цикла</i>	6.3.7.a Изучить политики и убедиться, что они регламентируют необходимость анализа изменений программного кода всех внутренних приложений (автоматически, либо вручную) следующим образом: <ul style="list-style-type: none"> ▪ изменения программного кода анализируются сотрудниками, не принимавшими участие в его написании и знакомыми с методами безопасного программирования; ▪ все необходимые корректировки вносятся до выпуска программного обеспечения; ▪ результаты анализа программного кода утверждаются руководством до выпуска программного обеспечения. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>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.</i></p>	<p>6.3.7.b Изучить политики и убедиться, что они регламентируют необходимость анализа изменений программного кода всех веб-приложений (автоматически, либо вручную) следующим образом:</p> <ul style="list-style-type: none"> ▪ изменения программного кода анализируются сотрудниками, не принимавшими участие в его написании и знакомыми с методами безопасного программирования; ▪ все необходимые корректировки вносятся до выпуска программного обеспечения; ▪ результаты анализа программного кода утверждаются руководством до выпуска ПО. 			
	<p>6.3.7.c Для нескольких недавних изменений приложений проверить, что программный код был проанализирован согласно требованиям 6.3.7.a и 6.3.7.b.</p>			
<p>6.4 Должны быть разработаны и внедрены процедуры управления изменениями, включающие в себя:</p>	<p>6.4.a Изучить процедуры управления изменениями, относящиеся к установке обновлений безопасности и изменению программного обеспечения, убедиться, что выполняются требования 6.4.1-6.4.4.</p>			
	<p>6.4.b Для нескольких системных компонентов и нескольких изменений/обновлений изучить записи процедур управления изменениями. Для каждого изменения выполнить следующие проверки:</p>			
<p>6.4.1 Документирование влияния изменения на систему</p>	<p>6.4.1 Убедиться, что влияние изменения на систему документировано.</p>			
<p>6.4.2 Согласование изменения с руководством</p>	<p>6.4.2 Убедиться, что изменение было согласовано руководством.</p>			
<p>6.4.3 Тестирование производственной функциональности</p>	<p>6.4.3 Убедиться, что производственная функциональность была протестирована.</p>			
<p>6.4.4 Процедуру отмены изменения</p>	<p>6.4.4 Убедиться, что предусмотрена процедура отмены изменения.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий	
6.5 Разработка всех веб-приложений (внутренних и внешних, в том числе веб-интерфейсов администрирования 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: <i>Примечание: Уязвимости, перечисленные в 6.5.1 – 6.5.10 были актуальны в руководстве OWASP когда данная версия PCI DSS была опубликована. В случае обновления руководства OWASP следует использовать его актуальную версию.</i>	6.5.a Проверить процесс разработки веб-приложений. Убедиться, что разработчики обязаны проходить обучение безопасному программированию, и что разработка веб-приложений осуществляется в соответствии с руководствами по безопасному программированию, например, такими, как руководства от проекта OWASP.				
	6.5.b Опросить несколько разработчиков программного обеспечения и убедиться, что они знакомы с техникой безопасного программирования.				
	6.5.c Убедиться, что при разработке веб-приложений уделяется внимание защите от таких уязвимостей, как:				
6.5.1 Атаки типа XSS.	6.5.1 Атаки типа XSS (необходима проверка всех параметров перед их включением в код).				
6.5.2 Инъекции, в особенности, SQL-инъекции. Также следует учесть LDAP и Xpath инъекции.	6.5.2 Инъекции, в особенности, SQL-инъекции (необходима проверка того, что введенная пользователями информация не может изменить существующие команды и запросы).				
6.5.3 Исполнение вредоносных файлов.	6.5.3 Исполнение вредоносных файлов (необходима проверка того, что разработанное приложение не принимает такие данные, как имена файлов или файлы).				
6.5.4 небезопасные прямые ссылки.	6.5.4 небезопасные прямые ссылки (прямые ссылки на внутренние объекты не должны предоставляться пользователям).				
6.5.5 Подделка межсайтовых запросов (CSRF).	6.5.5 Подделка межсайтовых запросов (автоматические запросы браузеров о данных учетной записи и идентификаторах должны игнорироваться).				

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
6.5.6 Утечка данных и некорректная обработка ошибок.	6.5.6 Утечка данных и некорректная обработка ошибок (в том числе утечка данных через сообщения об ошибках).			
6.5.7 Обход системы аутентификации и управления сессиями.	6.5.7 Обход системы аутентификации и управления сессиями (необходима корректная аутентификация и защита данных учётной записи и сеансового идентификатора).			
6.5.8 Небезопасное криптографическое хранилище.	6.5.8 Небезопасное криптографическое хранилище (необходима защита от криптографических ошибок).			
6.5.9 Небезопасная передача данных.	6.5.9 Небезопасная передача данных (необходимо шифрование всех критичных соединений и процесса аутентификации).			
6.5.10 Ошибки в контроле доступа по URL.	6.5.10 Ошибки в контроле доступа по URL (необходимо контролировать доступ на уровне приложения и бизнес-логики для всех URL)			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>6.6 Следует обеспечить защиту веб-ориентированных приложений от известных атак (а также регулярно учитывать новые уязвимости) одним из следующих методов:</p> <ul style="list-style-type: none"> ▪ Проверять приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности не реже одного раза в год, а также после внесения изменений. ▪ Установить межсетевой экран прикладного уровня перед веб-ориентированными приложениями. 	<p>6.6 Для общедоступных веб-приложений проверить выполнение одного из следующих требований:</p> <ul style="list-style-type: none"> ▪ Убедиться, что безопасность общедоступных веб-приложений анализируется следующим образом: <ul style="list-style-type: none"> – не реже одного раза в год; – после любых изменений; – организацией, которая специализируется на безопасности приложений; – все уязвимости устраняются; – безопасность приложения анализируется повторно после принятия корректирующих действий; ▪ Убедиться, что перед общедоступным веб-приложением установлен межсетевой экран прикладного уровня (web application firewall). <p><i>Примечание: “Организация, специализирующаяся на безопасности приложений” – как внутренняя, так и сторонняя организация, эксперты которой специализируются на безопасности приложений и не зависят от команды разработчиков.</i></p>			

Внедрение строгих мер контроля доступа

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

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

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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:	7.1 Изучить политику контроля доступа и убедиться, что она регламентирует следующее:			
7.1.1 Доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей.	7.1.1 Доступ пользователям предоставлен только к тем данным, которые необходимы им для выполнения своих должностных обязанностей.			
7.1.2 Назначение привилегий пользователям должно быть основано на их должностных обязанностях.	7.1.2 Назначение привилегий пользователям основано на их должностных обязанностях.			
7.1.3 Подписание руководством заявки о предоставлении прав доступа.	7.1.3 Авторизации подлежат все виды доступа; для получения доступа используются необходимые привилегии, и заявка о предоставлении доступа подписывается руководством.			
7.1.4 Внедрение автоматизированной системы контроля доступа.	7.1.4 Внедрение автоматизированной системы контроля доступа.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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:	7.2 Изучить настройки системы и документацию изготовителя, убедиться, что система контроля доступа включает в себя:			
7.2.1 Покрытие всех системных компонентов.	7.2.1 Покрытие всех системных компонентов.			
7.2.2 Назначение привилегий пользователям должно быть основано на их должностных обязанностях.	7.2.2 Назначение привилегий пользователям основано на их должностных обязанностях.			
7.2.3 По-умолчанию должен быть запрещен любой доступ.	7.2.3 Запрещение любого доступа по умолчанию. <i>Примечание: некоторые механизмы контроля доступа применяют правило «разрешить все» по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.</i>			

Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре

Назначение уникального идентификатора каждому человеку, имеющему доступ к компьютерной сети, позволяет гарантировать, что действия, производимые с критичными данными и системами, производятся известными и авторизованными пользователями и могут быть отслежены.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
8.1 Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.	8.1 Убедиться, что каждому пользователю назначен уникальный идентификатор для доступа к компонентам системы или данным о держателях карт.			
8.2 Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей: <ul style="list-style-type: none"> ▪ Пароль. ▪ Двухфакторная аутентификация (ключи, смарт-карты, биометрические параметры, открытые ключи). 	8.2 Проверить, что для аутентификации пользователей помимо уникального идентификатора применяются дополнительные механизмы аутентификации: <ul style="list-style-type: none"> ▪ изучить документацию, описывающую методы аутентификации; ▪ для каждого типа метода аутентификации и каждого типа системного компонента проверить, что метод аутентификации работает в соответствии с документацией. 			
8.3 Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети (на сетевом уровне извне 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.	8.3 Убедиться в использовании двухфакторной аутентификации при удаленном доступе сотрудников путем наблюдения за подключающимся удаленно к внутренней сети сотрудником (например, администратором сети).			
8.4 Все пароли должны храниться и передаваться только в зашифрованном виде с	8.4.a Для нескольких системных компонентов изучить файлы паролей и убедиться в том, что пароли нечитаемы при передаче и хранении.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
использованием стойких криптографических алгоритмов. <i>Термин «стойкие криптографические алгоритмы» определен в «Глоссарии PCI DSS: Основные определения, аббревиатуры и сокращения»</i>	8.4.b Для поставщиков услуг: изучить файлы паролей, убедиться в том, что клиентские пароли зашифрованы.			
8.5 Должен быть установлен контроль над выполнением процедур аутентификации и управления паролями учетных записей сотрудников и администраторов, включающий в себя:	8.5 Изучить процедуры и опросить сотрудников, убедиться в том, что процедуры аутентификации пользователей и управления паролями учетных записей соответствуют следующим требованиям:			
8.5.1 Контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации.	8.5.1.a Выбрать несколько пользовательских учетных записей, как привилегированных, так и обычных пользователей. Убедиться, что каждый пользователь проходит авторизацию в системе в соответствии с политикой компании: <ul style="list-style-type: none"> ▪ изучить заявку на предоставление доступа для каждой выбранной учетной записи; ▪ убедиться в том, что выбранные учетные записи наделены привилегиями в соответствии с заявками (подписанными и включающими в себя описание привилегий), путем сравнения привилегий, описанных в форме и установленных в системе. 			
8.5.2 Проверку подлинности пользователя перед сменой пароля.	8.5.2 Убедиться в том, что пользователь проходит проверку подлинности перед сменой пароля по телефону, электронной почте, с использованием веб-приложения или иным удаленным способом.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
8.5.3 Установку уникального первоначального пароля для каждого пользователя и его немедленное изменение при первом входе пользователя.	8.5.3 Убедиться в том, что для первого входа в систему пользователю устанавливается уникальный первоначальный пароль, который изменяется при первом входе в систему.			
8.5.4 Немедленный отзыв доступа при увольнении пользователя.	8.5.4 Выбрать несколько уволенных за прошедшие шесть месяцев сотрудников и проанализировать списки контроля доступа, убедиться в том, что их учетные записи заблокированы.			
8.5.5 Удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней.	8.5.5 Убедиться в том, что неактивные более 90 дней учетные записи удаляются или блокируются.			
8.5.6 Включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ.	8.5.6 Убедиться в том, что учетные записи, используемые поставщиками для удаленной поддержки, заблокированы и активируются только на время выполнения работ, в течение которого непрерывно контролируются.			
8.5.7 Доведение правил и процедур использования и хранения пароля до всех пользователей, имеющих доступ к данным о держателях карт.	8.5.7 Опросить несколько пользователей, убедиться в том, что им известны положения парольных политик и процедур.			
8.5.8 Запрет использования групповых, разделяемых и стандартных учетных записей и паролей.	8.5.8.a Для нескольких системных компонентов проверить списки учетных записей пользователей и проверить следующее: <ul style="list-style-type: none"> ▪ стандартные учетные записи заблокированы или не используются; ▪ разделяемые учетные записи для функций администрирования и иных критичных функций не существуют; ▪ разделяемые и стандартные учетные записи не используются для администрирования какого-либо системного компонента. 			
	8.5.8.b Изучить парольные политики и процедуры, убедиться, что они запрещают использование групповых и разделяемых паролей.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	8.5.8.с Опросить системных администраторов, убедиться в том, что пользователям не выдаются групповые и разделяемые пароли, даже если таковые запрашиваются.			
8.5.9 Изменение пароля пользователя не реже одного раза в 90 дней.	8.5.9 Для нескольких системных компонентов проверить настройки и убедиться в том, что пользователь должен менять пароль не реже одного раза в 90 дней. Для поставщиков услуг изучить внутренние процессы и клиентскую документацию, убедиться в том, что клиентский пароль должен меняться регулярно и у клиентов есть инструкция о том, когда и при каких обстоятельствах пароль должен быть изменен.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
8.5.10 Требование использования в пароле не менее семи символов.	<p>8.5.10 Для нескольких системных компонентов проверить настройки и убедиться в том, что длина пароля не менее семи символов.</p> <p>Для поставщиков услуг изучить внутренние процессы и клиентскую документацию, убедиться в том, что к клиентским паролям предъявляется требование минимальной длины.</p>			
8.5.11 Требование использования в пароле как цифр, так и букв.	<p>8.5.11 Для нескольких системных компонентов проверить настройки и убедиться в том, что пароль должен содержать как цифровые, так и буквенные символы.</p> <p>Для поставщиков услуг изучить внутренние процессы и клиентскую документацию, убедиться в том, что пароль должен содержать как цифровые, так и буквенные символы.</p>			
8.5.12 Запрет при смене пароля выбора в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей.	<p>8.5.12 Для нескольких системных компонентов проверить настройки и убедиться в том, что при изменении новый пароль должен отличаться от четырех предыдущих.</p> <p>Для поставщиков услуг изучить внутренние процессы и клиентскую документацию, убедиться в том, что при изменении новый пароль должен отличаться от четырех предыдущих.</p>			
8.5.13 Блокировку учетной записи после шести неудачных попыток ввода пароля.	<p>8.5.13 Для нескольких системных компонентов проверить настройки и убедиться в том, что учетная запись пользователя блокируется после максимум шести неудачных попыток входа.</p> <p>Для поставщиков услуг изучить внутренние процессы и клиентскую документацию, убедиться в том, что учетная запись клиента временно блокируется после максимум шести неудачных попыток входа.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
8.5.14 Установку периода блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором.	8.5.14 Для нескольких системных компонентов проверить настройки и убедиться в том, что учетная запись пользователя блокируется не менее чем на 30 минут либо пока администратор не снимет блокировку.			
8.5.15 Блокировку рабочей сессии пользователя через 15 минут простоя с требованием ввода пароля для разблокировки терминала.	8.5.15 Для нескольких системных компонентов проверить настройки и убедиться в том, что рабочая сессия пользователя блокируется не более чем через 15 минут простоя.			
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.	8.5.16.a Проанализировать настройки баз данных и приложений, проверить, что аутентификация пользователей и разграничение доступа к базам данных включают в себя: <ul style="list-style-type: none"> ▪ аутентификацию всех пользователей перед предоставлением им доступа; ▪ осуществление пользовательских операций с данными (запрос, перемещение, копирование, удаление) только программными методами (например, через хранимые процедуры); ▪ прямой доступ к запросам к базам данных разрешен только для администраторов баз данных. 			
	8.5.16.b Проверить учетные записи приложений и убедиться в том, что учетные записи приложений могут быть использованы только приложениями (но не пользователями или иными процессами).			

Требование 9: Ограничить физический доступ к данным платежных карт

Физический доступ к системам, содержащим данные о держателях карт, предоставляет возможность получить контроль над устройствами и данными, а также украсть устройство или документ, и должен быть соответствующим образом ограничен.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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.</p>	<p>9.1 Проверить наличие средств контроля физического доступа в каждый вычислительный центр, дата-центр и иные помещения, в которых располагаются системы, которые хранят, обрабатывают или передают данные о держателях карт.</p> <ul style="list-style-type: none"> ▪ убедиться, что доступ контролируется при помощи персональных карт или иных устройств, в том числе механических замков; ▪ наблюдать за попыткой системного администратора выполнить консольный вход в случайно выбранные системы в среде данных о держателях карт и убедиться в том, что он заблокирован, чтобы избежать несанкционированного доступа. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>9.1.1 Следует использовать камеры видеонаблюдения или иные механизмы контроля доступа, чтобы следить за критическими местами. Данные, собранные механизмами контроля доступа, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством.</p> <p><i>Примечание: критическими 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.</i></p>	<p>9.1.1 Убедиться в том, что камеры видеонаблюдения либо иные механизмы контроля доступа применяются для мониторинга доступа в критичные помещения. Камеры и иные средства должны быть защищены от подделки или отключения. Убедиться в том, что данные с камер видеонаблюдения и иных механизмов контроля доступа хранятся не менее трех месяцев.</p>			
<p>9.1.2 Доступ к сетевым разъемам, расположенным в общедоступных местах, должен быть ограничен.</p>	<p>9.1.2 Опросить администраторов и изучить сетевые разъемы, чтобы убедиться в том, что сетевые разъемы включены только в случае, если они необходимы авторизованным сотрудникам компании. Проверить, что, например, в комнате для переговоров сетевые разъемы не подключены к портам коммутатора с включенным DHCP. Проверить, что исключено наличие посетителей без сопровождения в помещениях с активными сетевыми разъемами.</p>			
<p>9.1.3 Доступ к беспроводным точкам доступа, шлюзам и портативным устройствам должен быть ограничен.</p>	<p>9.1.3 Убедиться, что физический доступ к беспроводным точкам доступа, шлюзам и портативным устройствам должным образом ограничен.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>9.2 Должны быть внедрены процедуры, позволяющие легко различать сотрудников и посетителей, особенно в помещениях, где циркулируют данные о держателях карт.</p> <p><i>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.</i></p>	<p>9.2.a Проанализировать процессы и процедуры выдачи пропусков сотрудникам и посетителям, в том числе:</p> <ul style="list-style-type: none"> ▪ процедуры предоставления новых пропусков, изменения прав доступа, отзыва пропуска у уволенного сотрудника или посетительского пропуска с истекшим сроком действия; ▪ ограничение доступа к пропускной системе. <p>9.2.b Убедиться, что можно легко отличить сотрудников компании от посетителей.</p>			
<p>9.3 Следует ввести процедуру прохода посетителей на объект, обеспечивающую:</p>	<p>9.3 Проверить процедуру контроля доступа, в том числе:</p>			
<p>9.3.1 Авторизацию посетителя, перед входом в помещения, где циркулируют данные о держателях карт.</p>	<p>9.3.1 Наблюдать за посетителями, чтобы убедиться в использовании ими посетительских пропусков. Попробовать получить доступ к дата-центру с использованием посетительского пропуска, убедиться, что посетитель не может без сопровождения проникнуть в помещения, где циркулируют данные о держателях карт.</p>			
<p>9.3.2 Выдачу посетителю материального идентификатора (например, бейджа или электронного ключа), имеющего ограничение срока действия, при входе на объект. Идентификатор должен обеспечивать отличие посетителя от сотрудника.</p>	<p>9.3.2 Осмотреть пропуска сотрудников и посетителей, убедиться, что они легко различимы и что пропуск посетителя имеет ограниченный срок действия.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
9.3.3 Возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении срока его действия.	9.3.3 Ознакомится с процессом ухода посетителями с территории компании, убедиться, что от посетителей требуется возврат пропуска при уходе либо окончании срока действия.			
9.4 Следует вести журнал учета посетителей и использовать его для анализа посещений. В журнале следует регистрировать имя посетителя, организацию, которую он представляет, а также сотрудника компании, разрешившего доступ посетителю. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством.	9.4.a Убедиться в том, что ведется журнал регистрации посетителей как на входе в офисные помещения, так и на входе в вычислительные центры и дата-центры, в которых хранятся или передаются данные о держателях карт. 9.4.b Убедиться в том, что журнал содержит имя посетителя, название представляемой им организации, а также имя сотрудника компании, предоставившего посетителю физический доступ. Убедиться в том, что журнал хранится не менее трех месяцев.			
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. Безопасность мест хранения должна проверяться не реже одного раза в год.	9.5 Убедиться в том, что безопасность мест хранения резервных копий проверяется не реже одного раза в год.			
9.6 Должна быть обеспечена физическая безопасность всех бумажных и электронных средств, содержащих данные о держателях карт.	9.6 Проверить, что процедуры физической защиты данных о держателях карт включают меры по защите бумажных и электронных носителей, содержащих данные о держателях карт (включая компьютеры, съемные носители, сетевое и коммуникационное оборудование, линии телесвязи, бумажные счета, бумажные отчеты и факсы).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
9.7 Должен быть обеспечен строгий контроль над передачей носителей информации, содержащих данные о держателях карт, включающий:	9.7 Убедиться в наличии политики, регламентирующей порядок передачи носителей информации, содержащих данные о держателях карт.			
9.7.1 Классификацию носителей информации, их маркировку, как содержащих конфиденциальную информацию.	9.7.1 Убедиться в том, что носители информации классифицированы и соответствующим образом промаркированы.			
9.7.2 Пересылку носителей только с доверенным курьером, или иным способом, который может быть тщательно проконтролирован.	9.7.2 Убедиться в том, что вынос носителя за пределы объекта компании должен быть зарегистрирован, согласован с руководством, а пересылка носителей осуществляется только с доверенным курьером или иным способом, который может быть тщательно проконтролирован и отслежен.			
9.8 Должна быть внедрена процедура разрешения руководством выноса за пределы охраняемой территории носителей, содержащих данные о держателях карт (особенно при передаче носителя частным лицам).	9.8 Для нескольких случаев выноса носителя, зарегистрированных в журнале за несколько дней, проверить детальные обстоятельства выноса и наличие согласования выноса с руководством.			
9.9 Должен быть обеспечен строгий контроль хранения носителей, содержащих данные о держателях карт, и управление доступом к ним.	9.9 Изучить политику хранения носителей, содержащих данные о держателях карт, убедиться в том, что она регламентирует регулярную инвентаризацию носителей.			
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.	9.9.1 Убедиться, что инвентаризация носителей проводится не реже одного раза в год.			
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:	9.10 Изучить политику уничтожения носителей, содержащих данные о держателях карты, хранение которых более не требуется; убедиться в том, что её действие распространяется на все носители, содержащие данные о держателях карт, а также:			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
9.10.1 Измельчение, сжигание или растворение бумажного носителя, чтобы данные о держателях карт не могли быть восстановлены.	9.10.1.a Убедиться, что твердые копии документов измельчаются, сжигаются или растворяются способом, исключающим их восстановление.			
	9.10.1.b Осмотреть хранилище документов, приготовленных для уничтожения, убедиться, что доступ к таким документам ограничен.			
9.10.2 Уничтожение данных о держателях карт на электронном носителе, исключающее возможность их восстановления.	9.10.2 Убедиться в том, что уничтожение данных о держателях карт на электронном носителе осуществляется способом, исключающим возможность их восстановления.			

Регулярный мониторинг и тестирование сети

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

Наличие механизмов ведения записей о событиях, а также возможности проследить действия пользователей необходимо для системы, так как они позволяют провести расследование и анализ инцидентов. Определение причин инцидентов затруднено в отсутствие журналов записей о событиях в системе.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
10.1 Должен быть разработан процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам.	10.1 Опросить системного администратора и проверить, что ведутся журналы протоколирования событий системных компонентов.			
10.2 Для каждого системного компонента должен быть включен механизм протоколирования следующих событий:	10.2 Методом интервью, изучения журналов протоколирования событий и настроек систем протоколирования осуществить следующие проверки:			
10.2.1 Любой доступ пользователя к данным о держателях карт.	10.2.1 Убедиться в том, что факты доступа пользователя к данным о держателях карт регистрируются.			
10.2.2 Любые действия, совершенные с использованием административных полномочий.	10.2.2 Убедиться в том, что любые действия, совершенные с использованием административных полномочий, регистрируются.			
10.2.3 Любой доступ к записям о событиях в системе.	10.2.3 Убедиться в том, что факты доступа к записям о событиях в системе регистрируются.			
10.2.4 Неуспешные попытки логического доступа.	10.2.4 Убедиться в том, что неуспешные попытки логического доступа регистрируются.			
10.2.5 Использование механизмов идентификации и аутентификации.	10.2.5 Убедиться в том, что регистрируются факты использования механизмов идентификации и аутентификации.			
10.2.6 Инициализация журналов протоколирования событий.	10.2.6 Убедиться в том, что регистрируются факты инициализации журналов протоколирования событий.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
10.2.7 Создание и удаление объектов системного уровня.	10.2.7 Убедиться в том, что регистрируются факты создания и удаления объектов системного уровня.			
10.3 Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры:	10.3 Убедиться, что для каждого протоколируемого события регистрируются следующие параметры:			
10.3.1 Идентификатор пользователя.	10.3.1 Идентификатор пользователя.			
10.3.2 Тип события.	10.3.2 Тип события.			
10.3.3 Дата и время.	10.3.3 Дата и время.			
10.3.4 Успешным или неуспешным было событие.	10.3.4 Успешным или неуспешным было событие.			
10.3.5 Источник события.	10.3.5 Источник события.			
10.3.6 Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.	10.3.6 Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.			
10.4 Все системные часы на критичных системах должны быть синхронизированы.	10.4 Проанализировать процесс получения и распространения точного времени в организации, равно как и связанные с этим конфигурационные параметры для выборки системных компонентов. Убедиться, что выполнены следующие требования:			
	10.4.a Для синхронизации часов используется NTP или схожая технология, удовлетворяющая требованиям 6.1 и 6.2 стандарта PCI DSS.			
	10.4.b Убедиться, что не все внутренние сервера получают информацию о времени из внешних источников (несколько центральных серверов времени в организации должны получать такую информацию и распространять на другие компьютеры в сети).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	<p>10.4.с Убедиться, что внешние хосты, с которых сервера времени получают информацию, жестко определены (чтобы предотвратить смену времени злоумышленником). Эта информация может быть дополнительно зашифрована симметричным ключом и списками контроля доступа, определяющими адреса машин, которым разрешено получать обновления времени. Дополнительная информация на www.ntp.org.</p>			
<p>10.5 Журналы протоколирования событий должны быть защищены от изменений.</p>	<p>10.5 Опросить системного администратора и изучить права доступа, чтобы убедиться в том, что журналы протоколирования событий защищены от изменений, в том числе:</p>			
<p>10.5.1 Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.</p>	<p>10.5.1 Убедиться в том, что доступом к журналам протоколирования событий обладают только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.</p>			
<p>10.5.2 Журналы протоколирования событий должны быть защищены от неавторизованного изменения.</p>	<p>10.5.2 Убедиться в том, что актуальные журналы протоколирования событий защищены от неавторизованного изменения при помощи механизмов контроля доступа, физической и/или сетевой сегментации.</p>			
<p>10.5.3 Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено.</p>	<p>10.5.3 Убедиться в том, что резервные копии журналов протоколирования событий оперативно сохраняются на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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.	10.5.4 Убедиться в том, что журналы протоколирования событий доступных извне систем (беспроводных сетей, межсетевых экранов, DNS, почтовых систем) сохраняются на сервер протоколирования, находящийся внутри локальной сети.			
10.5.5 Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала).	10.5.5 Убедиться в наличии систем контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений.			
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). <i>Примечание: Для обеспечения соответствия Требованию 10.6 могут быть использованы средства сбора и анализа журналов регистрации событий, а также средства оповещения.</i>	10.6.a Изучить политики и процедуры, проверить, что они регламентируют необходимость анализа журналов систем безопасности не реже одного раза в день, а также необходимость реагирования на исключительные ситуации. 10.6.b Убедиться, что журналы протоколирования событий всех системных компонентов регулярно анализируются.			
10.7 Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев (например – в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии).	10.7.a Изучить политики и процедуры, проверить, что они регламентируют необходимость хранения журналов регистрации событий не менее одного года. 10.7.b Убедиться, что журналы протоколирования событий доступны в течение одного года и находятся в оперативном доступе не менее трех месяцев.			

Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
11.1 Следует ежеквартально проверять наличие беспроводных точек доступа, используя анализатор беспроводных сетей либо беспроводные IDS/IPS для обнаружения всех включенных беспроводных устройств.	11.1.a Убедиться, что беспроводной сканер используется как минимум раз в три месяца, или что беспроводная IDS/IPS функционирует и настроена на обнаружение новых беспроводных устройств.			
	11.1.b Если беспроводная IDS/IPS внедрена, убедиться, что она генерирует уведомления администратору.			
	11.1.c Убедиться, что в политике расследования инцидентов (требование 12.9) упомянуты действия при обнаружении неавторизованного беспроводного устройства.			
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). <i>Примечание: ежеквартальное внешнее сканирование должно</i>	11.2.a За последние четыре квартала проанализировать отчеты результатов сканирования уязвимостей внутренней сети, хостов и приложений, чтобы убедиться в существовании процедуры периодической проверки безопасности. Убедиться, что при устранении проблем производится повторное сканирование. <i>Примечание: внешние сканирования, проводимые после изменений в сети, а также внутренние сканирования могут выполняться собственным квалифицированным персоналом компании, либо внешними сторонами.</i>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>выполняться сторонней компанией (ASV), сертифицированной Советом PCI SSC. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании.</i></p>	<p>11.2.b Убедиться, что внешнее сканирование производится как минимум раз в квартал, в соответствии с Процедурами Сканирования PCI (PCI Security Scanning Procedures) путем анализа отчетов внешних сканирований за последние четыре квартала на предмет следующих проверок:</p> <ul style="list-style-type: none"> ▪ Четыре последних сканирования производились в течение последних 12 месяцев; ▪ Результаты каждого сканирования удовлетворяют требованиям процедур сканирования PCI (например, нет срочных, критических уязвимостей или уязвимостей высокого уровня); ▪ Сканирование производилось компанией ASV, сертифицированной Советом PCI SSC. <p><i>Примечание: для первоначального соответствия PCI DSS не требуется отчетов четырех ежеквартальных сканирований, если аудитор убедился в следующем: 1) последнее сканирование было пройдено успешно, 2) документированные процедуры регламентируют необходимость ежеквартального сканирования, 3) обнаруженные уязвимости были устранены и это подтверждено повторным сканированием. Для последующих проверок, после первоначального подтверждения соответствия PCI DSS, требуется наличие отчетов о ежеквартальных сканированиях.</i></p>			
	<p>11.2.c Убедиться, что внутреннее и внешнее сканирование происходит после любого крупного изменения в сети путем анализа результатов сканирования за последний год. Убедиться, что процедуры сканирования повторяются до тех пор, пока не будет получен положительный результат</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
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). Данные тесты на проникновение должны включать:	11.3.a Изучить результаты последнего теста на проникновение, убедиться в том, что тест на проникновение осуществляется не реже одного раза в год и после всех значительных изменений в инфраструктуре. Убедиться в том, что выявленные уязвимости были устранены и повторный тест проведен.			
	11.3.b Убедиться в том, что тест на проникновение был проведен квалифицированными сотрудниками компании либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно).			
11.3.1 Тесты на проникновение сетевого уровня.	11.3.1 Убедиться в том, что тест на проникновение включает в себя тест на проникновение на сетевом уровне. Тест должен охватывать не только операционные системы, но и другие компоненты, поддерживающие взаимодействие на сетевом уровне.			
11.3.2 Тесты на проникновение уровня приложений.	11.3.2 Убедиться в том, что тест на проникновение включает в себя тест на проникновение на уровне приложений. Для веб-приложений тест должен учитывать, как минимум, проверки на наличие уязвимостей, приведенные в требовании 6.5 PCI DSS.			
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.	11.4.a Проверить, что применяются системы обнаружения и предотвращения вторжений и что весь трафик в среде данных о держателях карт подлежит мониторингу.			
	11.4.b Убедиться в том, что системы IDS/IPS оповещают сотрудников компании о подозрительной активности.			
	11.4.c Изучить конфигурации систем IDS/IPS и убедиться в том, что устройства IDS/IPS настроены, поддерживаются и обновляются в соответствии с рекомендациями производителя.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>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.</p> <p><i>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.</i></p>	<p>11.5 Убедиться в наличии и работоспособности систем контроля целостности файлов в среде данных о держателях карт.</p> <p>Примеры файлов, подлежащих мониторингу:</p> <ul style="list-style-type: none"> ▪ системные исполняемые файлы; ▪ прикладные исполняемые файлы; ▪ конфигурационные файлы и файлы параметров; ▪ централизованно хранимые файлы журналов протоколирования событий. 			

Разработка политики информационной безопасности

Требование 12: Разработать и поддерживать политику информационной безопасности

Строгая политика безопасности задает атмосферу безопасности для всей компании и информирует сотрудников о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите. В контексте данного требования термином «сотрудники» обозначаются постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.1 Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика информационной безопасности.	12.1 Изучить политику информационной безопасности и убедиться в том, что она опубликована и распространена среди всех пользователей (включая поставщиков, подрядчиков и бизнес-партнеров).			
12.1.1 Политика информационной безопасности должна учитывать все требования настоящего стандарта.	12.1.1 Убедиться в том, что политика информационной безопасности учитывает все требования PCI DSS.			
12.1.2 Политика информационной безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков.	12.1.2 Убедиться в том, что политика информационной безопасности регламентирует ежегодное выполнение анализа информационных рисков.			
12.1.3 Политика информационной безопасности должна пересматриваться не реже одного раза в год и обновляться в случае изменения инфраструктуры.	12.1.3 Убедиться в том, что политика информационной безопасности пересматривается не реже одного раза в год и обновляется в случае изменения бизнес-целей и среды данных о держателях карт.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>12.2 Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов протоколирования событий).</p>	<p>12.2.а Изучить ежедневные процедуры безопасности. Убедиться в том, что они соответствуют требованиям настоящего стандарта и включают административные и технические процедуры по каждому требованию.</p>			
<p>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 сеть Интернет), чтобы определить корректный порядок использования этих устройств сотрудниками. Эти правила должны включать следующее:</p>	<p>12.3 Изучить правила эксплуатации критичных технологий, с которыми непосредственно работают сотрудники, и осуществить следующие проверки:</p>			
<p>12.3.1 Процедуру явного одобрения руководством.</p>	<p>12.3.1 Убедиться в том, что использование технологий требует утверждения руководством.</p>			
<p>12.3.2 Аутентификацию перед использованием устройства.</p>	<p>12.3.2 Убедиться в том, что перед использованием технологии пользователь должен пройти аутентификацию по имени и паролю, либо иному средству аутентификации (например, токену).</p>			
<p>12.3.3 Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.</p>	<p>12.3.3 Убедиться в наличии перечня используемых устройств и сотрудников, имеющих доступ к таким устройствам.</p>			
<p>12.3.4 Маркировку устройств с указанием владельца, контактной информации и назначения.</p>	<p>12.3.4 Убедиться, что правила эксплуатации регламентируют маркировку устройств с указанием владельца, контактной информации и назначения.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.3.5 Допустимые варианты использования устройств.	12.3.5 Убедиться, что правила эксплуатации регламентируют допустимые варианты использования устройств.			
12.3.6 Допустимые точки размещения устройств в сети.	12.3.6 Убедиться, что правила эксплуатации регламентируют допустимые точки размещения устройств в сети.			
12.3.7 Перечень одобренных компаний устройств.	12.3.7 Убедиться в наличии перечня одобренных компаний устройств.			
12.3.8 Автоматическое отключение сессий удаленного доступа после определенного периода простоя.	12.3.8 Убедиться, что правила эксплуатации регламентируют автоматическое отключение сессий удаленного доступа после определенного периода простоя.			
12.3.9 Включение механизмов удаленного доступа для службы поддержки (производителям) только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	12.3.9 Убедиться, что правила эксплуатации регламентируют включение механизмов для доступа службы поддержки (производителя) только в случае необходимости такого доступа с немедленным выключением механизмов после использования.			
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.	12.3.10 Убедиться, что правила эксплуатации запрещают копирование, перемещение и хранение данных о держателях карт на локальных дисках, дискетах и иных съемных носителях при удаленном доступе к данным.			
12.4 Политика и процедуры безопасности должны однозначно определять обязанности всех сотрудников и партнеров, относящиеся к информационной безопасности.	12.4 Убедиться в том, что политики однозначно определяют обязанности всех сотрудников и партнеров, относящиеся к информационной безопасности.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.5 Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:	12.5 Убедиться в том, что ответственность за обеспечение информационной безопасности формально возложена на CSO или другого члена правления, компетентного в области информационной безопасности. Изучить политики и выполнить следующие проверки:			
12.5.1 Разработка, документирование и распространение политики и процедур безопасности.	12.5.1 Убедиться в том, что определена ответственность за разработку и распространение политик и процедур безопасности.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.5.2 Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных.	12.5.2 Убедиться в том, что определена ответственность за мониторинг, анализ и доведение до сведения соответствующего персонала (специалистов по информационной безопасности и представителей бизнес-подразделений) информации о событиях, имеющих отношение к информационной безопасности.			
12.5.3 Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.	12.5.3 Убедиться в том, что определена ответственность за разработку, документирование и распространение процедур реагирования на инциденты и процедур эскалации.			
12.5.4 Администрирование учетных записей пользователей, включая их добавление, удаление и изменение.	12.5.4 Убедиться в том, что определена ответственность за управление учетными записями пользователей.			
12.5.5 Мониторинг и контроль любого доступа к данным.	12.5.5 Убедиться в том, что определена ответственность за мониторинг и контроль доступа к данным.			
12.6 Должна быть внедрена официальная программа повышения осведомленности сотрудников о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт.	12.6.a Проверить наличие формальной программы повышения осведомленности сотрудников о вопросах безопасности.			
	12.6.b Изучить программу повышения осведомленности сотрудников о вопросах безопасности и выполнить следующие проверки:			
12.6.1 Обучение сотрудников должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год.	12.6.1.a Убедиться в том, что программа повышения осведомленности сотрудников использует различные методы доведения информации до сотрудников (плакаты, письма, заметки, системы дистанционного обучения, специальные кампании).			
	12.6.1.b Убедиться в том, что сотрудники проходят обучение по вопросам информационной безопасности при приеме на работу, а также не реже одного раза в год.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.6.2 Сотрудники должны не реже одного раза в год подтверждать своё знание и понимание политики и процедур информационной безопасности компании.	12.6.2 Убедиться в том, то программа повышения осведомленности сотрудников регламентирует подтверждение сотрудниками их знания и понимания политики информационной безопасности компании (например, в виде теста в письменной или электронной форме).			
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.	12.7 Убедиться в том, что при приеме на работу новых сотрудников осуществляются кадровые проверки (с учетом особенностей законодательства). Примером кадровых проверок являются изучение послужного списка, изучение записей правоохранительных органов, изучение кредитной истории, проверки рекомендаций.			
12.8 В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними, включающие:	12.8 Если проверяемая организация передает данные о держателях карт поставщикам услуг (например, хранилище носителей резервных копий, дата-центр или хостинг провайдер), необходимо изучить политики и процедуры взаимодействия с поставщиками услуг и выполнить следующие проверки:			
12.8.1 Поддержку перечня поставщиков услуг.	12.8.1 Убедиться в том, что поддерживается перечень поставщиков услуг.			
12.8.2 Поддержку письменного соглашения о том, что поставщики услуг ответственны за безопасность переданных им данных о держателях карт.	12.8.2 Убедиться, что письменное соглашение с поставщиком услуг предусматривает возложение на поставщика услуг ответственности за безопасность переданных ему данных о держателях карт.			
12.8.3 Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним.	12.8.3 Убедиться в выполнении всех политик и процедур, а также проведении тщательной проверки поставщика услуг перед началом взаимодействия с ним.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.8.4 Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS.	12.8.4 Убедиться в наличии программы проверки статуса соответствия поставщиков услуг требованиям PCI DSS.			
12.9 Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы.	12.9 Изучить план реагирования на инциденты, выполнить следующие проверки:			
12.9.1 Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум: <ul style="list-style-type: none"> ▪ 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; <ul style="list-style-type: none"> ▪ охват всех критических системных компонентов; ▪ ссылки или включение процедур реагирования на инциденты международных платежных систем. 	12.9.1 Убедиться, что план реагирования на инциденты включает в себя: <ul style="list-style-type: none"> ▪ 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; ▪ охват всех критических системных компонентов; ▪ ссылки или включение процедур реагирования на инциденты международных платежных систем. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
12.9.2 План должен тестироваться не реже одного раза в год.	12.9.2 Убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год.			
12.9.3 Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7.	12.9.3 Убедиться в наличии персонала, способного реагировать на сигналы тревоги в режиме 24/7.			
12.9.4 Персонал, ответственный за реагирование на нарушения безопасности, должен быть обучен соответствующим образом.	12.9.4 Убедиться в том, что персонал, ответственный за реагирование на нарушения безопасности, проходит периодическое обучение.			
12.9.5 План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов.	12.9.5 Убедиться в том, что план реагирования на инциденты включает в себя процедуры реагирования на сигналы тревоги систем безопасности, в том числе обнаружение неавторизованных беспроводных точек доступа.			
12.9.6 Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	12.9.6 Убедиться в том, что налажен процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.			

Приложение А: Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)

Требование А.1: Поставщики услуг с общей средой должны защищать среду данных платежных карт

Согласно требованию 12.8, все поставщики услуг, имеющие доступ к данным о держателях карт, должны выполнять требования PCI DSS. В дополнение к этому, требование 2.4 говорит о том, что поставщики услуг с общей средой (хостинг-провайдеры) должны защищать данные каждого клиента. Таким образом, поставщики услуг с общей средой (хостинг-провайдеры) должны дополнительно выполнять требования, перечисленные в этом приложении.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>А.1 Обеспечить защиту данных каждого клиента, согласно требованиям с А.1.1 по А.1.4: Хостинг-провайдер должен удовлетворять всем этим требованиям, помимо требований PCI DSS</p> <p><i>Примечание: не смотря на то, что хостинг-провайдер будет соответствовать требованиям PCI DSS, каждый его клиент должен, тем не менее, проходить собственный аудит.</i></p>	<p>А.1 Чтобы убедиться, что хостинг-провайдер обеспечивает должный уровень защиты своих клиентов, выберите несколько серверов (под управлением Windows и Unix/Linux) и проведите проверки, перечисленные в пунктах с А.1.1 по А.1.4.</p>			
<p>А.1.1 Ограничить доступ приложений каждого клиента только к своей среде данных о держателях карт.</p>	<p>А.1.1 Если хостинг-провайдер позволяет клиентам запускать приложения (например, скрипты), следует убедиться, что эти приложения запущены под уникальным идентификатором. Например:</p> <ul style="list-style-type: none"> ▪ Ни одно приложение и ни один пользователь не может использовать имени пользователя, от которого работает разделяемый веб-сервер. ▪ Все CGI-скрипты, используемые клиентом, должны быть созданы и запущены от имени идентификатора клиента. 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
A.1.2 Ограничить доступ клиента только к своей среде данных о держателях карт.	A.1.2.a Убедиться, что ни один из клиентов не обладает правами администратора/суперпользователя.			
	A.1.2.b Убедиться, что каждый клиент имеет права чтения, записи и выполнения только своих утилит и данных. Для этого ограничения могут применяться средства типа chroot, jail и т.п. ВАЖНО: файлы клиента не должны быть доступны группе пользователей.			
	A.1.2.c Убедиться, что у клиента отсутствует право записи в разделяемые системные библиотеки и исполняемые файлы.			
	A.1.2.d Убедиться, что просмотр журналов протоколирования доступен только владельцу.			
	A.1.2.e Чтобы убедиться, что ни один клиент не может использовать все ресурсы сервера для эксплуатации уязвимостей, убедиться, что для каждого клиента установлены системные лимиты на: <ul style="list-style-type: none"> ▪ Использование дискового пространства ▪ Использование канала ▪ Использование памяти ▪ Использование ресурсов ЦПУ 			
A.1.3 Убедиться, что протоколирование действий и событий включено для каждого клиента и соответствует требованию 10 стандарта.	A.1.3.a Убедиться, что протоколирование событий удовлетворяет следующим критериям: <ul style="list-style-type: none"> ▪ Протоколирование настроено для всех типичных используемых на сервере приложений сторонних производителей ▪ Протоколирование включено по умолчанию ▪ Журналы доступны для просмотра администратору и клиенту, для которого выполняется протоколирование ▪ Журналы расположены в каталогах, доступных клиенту 			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
A.1.4 Убедиться в наличии процессов, позволяющих провести расследование инцидентов каждого клиента.	A.1.4 Убедиться в наличии у хостинг-провайдера политик, описывающих правила проведения расследования в случае компрометации данных клиентов.			

Приложение В: Компенсирующие меры

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

Компенсирующие меры должны удовлетворять следующим требованиям:

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

При анализе избыточности следует руководствоваться следующими моментами:

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

- a) Существующее требование PCI DSS НЕ МОЖЕТ рассматриваться как компенсирующая мера, если она уже описана в отчете. Например, пароли на административный удаленный доступ должны передаваться в зашифрованном виде, для защиты от перехвата. Использование других мер, таких как использование стойких паролей и т.п., не решает указанную проблему, так как не снижает риска перехвата.
 - b) Существующее требование PCI DSS МОЖЕТ рассматриваться как компенсирующая мера, если оно снижает существующий риск. Например, двухфакторная аутентификация, являющаяся требованием при удаленном доступе, также может использоваться и внутри сети для защиты административного доступа, если шифрование аутентификационных данных невозможно. В случае если это требование снижает указанный риск и корректно реализовано, оно может рассматриваться как компенсирующая мера.
 - c) Существующие требования PCI DSS могут использоваться совместно с другими мерами как компенсирующие. Например, если компания не может реализовать нечитаемое хранение карточных данных (например, путем внедрения шифрования), компенсирующей мерой может считаться использование устройства или комбинации устройств, приложений и проверок, направленных на 1) сегментацию сети 2) фильтрацию по IP или MAC адресам 3) использование двухфакторной аутентификации во внешней сети.
4. Быть соизмеримыми с дополнительным риском, вызванным невозможностью выполнить требование PCI DSS.

Аудитор должен проверить каждую компенсирующую меру, чтобы убедиться, что она адекватно соотносится с риском, который призвано уменьшить оригинальное требование PCI DSS, руководствуясь вышеперечисленными пунктами. Следует также иметь установленные процедуры и проверки, чтобы убедиться, что компенсирующие меры остаются эффективными с течением времени.

Приложение С: Компенсирующие меры – форма для заполнения

Пользуйтесь этой таблицей для определения компенсирующей меры для каждого требования PCI DSS. Следует помнить, что компенсирующие меры должны быть отражены в Отчете о соответствии в соответствующем пункте требования PCI DSS.

Примечание: Только организации, выполнившие оценку рисков, могут пользоваться компенсирующими мерами для достижения статуса соответствия.

Номер требования и определение:

	Требуемая информация	Описание
1. Ограничение	Перечислите ограничения, препятствующие выполнению оригинального требования стандарта.	
2. Цель	Определите цель оригинального требования и компенсирующей меры.	
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением оригинального требования.	
4. Определение компенсирующих мер	Опишите компенсирующую меру и то, как она закрывает требование и создает дополнительные риски (если создает).	
5. Проверка компенсирующих мер	Опишите, как компенсирующие меры были проверены и протестированы.	
6. Поддержка	Опишите, как контролируется процесс поддержания компенсирующей меры.	

Перечень компенсирующих мер – пример заполнения

Пользуйтесь этой таблицей для описания компенсирующих мер для требований, имеющих статус «Выполнено» благодаря использованию компенсирующих мер.

Номер требования: *8.1 – все ли пользователи имеют уникальный идентификатор для получения доступа к системным компонентам карточной среды?*

	Требуемая информация	Описание
1. Ограничение	Перечислите ограничения, препятствующие выполнению оригинального требования стандарта.	<i>Компания XYZ использует Unix-сервера без LDAP-авторизации. Таким образом, на каждый из них требуется заходить под учетной записью суперпользователя («root»). Следить за использованием этой учетной записи всеми администраторами не представляется возможным.</i>
2. Цель	Определите цель оригинального требования и компенсирующей меры.	<i>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.</i>
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением оригинального требования.	<i>Дополнительный риск связан с тем, что не всем пользователям назначен уникальный идентификатор и их действия не могут быть отслежены.</i>
4. Определение компенсирующих мер	Опишите компенсирующую меру и то, как она закрывает требование и создает дополнительные риски (если создает).	<i>Пользователям предписано использовать команду «su» для получения доступа с правами суперпользователя. Все действия, связанные с запуском этой команды, протоколируются в отдельный лог-файл.</i>
5. Проверка компенсирующих мер	Опишите, как компенсирующие меры были проверены и протестированы.	<i>Аудиторам было продемонстрировано использование утилиты «su» и журнал регистрации событий SU-Log.</i>
6. Поддержка	Опишите, как контролируется процесс поддержания компенсирующей меры.	<i>Компания XYZ документировала процесс и процедуры, чтобы гарантировать неизменность использования утилиты «su» для получения административных прав на серверах.</i>



Приложение D: Оценка соответствия – торгово-сервисные предприятия

Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Свидетельство о соответствии. Оценка соответствия торгово-сервисного предприятия

Версия 1.2.1

Июль 2009

PCI DSS.RU

Инструкции по предоставлению отчета в регулирующие органы

Этот документ должен быть заполнен QSA-аудитором или представителем торгово-сервисного предприятия (в случае проведения внутреннего аудита) как свидетельство того, что торгово-сервисное предприятие имеет статус соответствия стандарту PCI DSS. Заполните все поля и передайте банку-эквайеру или МПС.

Часть 1. Информация о QSA

Название компании:					
Контактное лицо (QSA):			Должность:		
Телефон:			E-mail:		
Юридический адрес:			Город:		
Регион:		Страна:		Индекс:	
Адрес сайта в Интернете:					

Часть 2. Информация о проверяемой организации

Название компании:			Роль в МПС:		
Контактное лицо:			Должность:		
Телефон:			E-mail:		
Юридический адрес:			Город:		
Регион:		Страна:		Индекс:	
Адрес сайта в Интернете:					

Часть 2а. Виды деятельности (отметить необходимые)

- Розничная торговля
 Телекоммуникации
 Продовольствие
 Нефть
 Электронная коммерция
 Заказы по телефону
 Путешествия и развлечения
 Другие (укажите):

Перечень помещений, в которых проведен аудит:

Part 2b. Связи

Имеются ли связи со сторонними организациями (платежными шлюзами, хостинговыми компаниями и т.п.)? Да Нет

Имеются ли связи более чем с одним банком-эквайером? Да Нет

Part 2c. Обработка транзакций

Используемое платежное приложение: Версия приложения:

Часть 3. Проверка соответствия PCI DSS

На основании результатов, описанных в Отчете о соответствии (“ROC”) датированном (*дата создания отчета*), (*Имя QSA/Название торгового-сервисного предприятия*) подтверждает, что компания, описанная в части 2 настоящего документа, по состоянию на (*дата*) имеет статус (выберите):

- Соответствует:** Все требования помечены как “выполненные⁴,” и ASV-сканирование было выполнено (*имя ASV*), таким образом, (*имя компании*) продемонстрировала полное соответствие требованиям PCI DSS (*версия стандарта*).
- Не соответствует:** Некоторые требования PCI DSS помечены как “невыполненные”, что приводит к общему статусу **НЕСООТВЕТСТВИЯ**, или не было проведено успешное ASV-сканирование уполномоченным лицом, таким образом, (*Имя компании*) не продемонстрировала полного статуса соответствия PCI DSS

Дата, на которую запланировано достижение статуса соответствия:

При предъявлении данного отчета со статусом несоответствия требуется также предоставить заполненный План Мероприятий (Action Plan) части 4 данного документа. *Проконсультируйтесь с банком-эквайером или платежной системой, так как не все платежные системы требуют заполнения этой части*

Часть 3а. Подтверждения статуса соответствия

QSA/Торгово-сервисное предприятие подтверждает:

- Отчет о соответствии заполнен в соответствии с документом «*Требования и процедура аудита безопасности*», версии (*вставить номер версии*).
- Вся информация в Отчете является достоверной и передает реальную ситуацию
- Торгово-сервисное предприятие подтвердило у поставщика платежных приложений, что их приложение не сохраняет критичных аутентификационных данных после авторизации
- Торгово-сервисное предприятие ознакомлено со стандартом PCI DSS и понимает необходимость наличия статуса соответствия.
- В процессе аудита не обнаружено никаких следов хранения магнитного трека⁵, CAV2, CVC2, CID, или CVV2 кодов⁶, или информации о PIN коде⁷.

Part 3b. Подписи QSA-аудитора и проверяемой организации

Подпись QSA-аудитора ↑		Дата:
ФИО:	Должность:	
Подпись руководителя проверяемой организации ↑		Дата:
ФИО:	Должность:	

⁴ Выполненные требования должны включать компенсирующие меры, утвержденные аудитором QSA/внутренним аудитором торгового-сервисного предприятия. Если компенсирующие меры должным образом минимизируют риски связанные с требованием, QSA аудитор должен отметить эти требования, как «выполненные».

⁵ Данные, закодированные в магнитной полосе карты, используются для аутентификации в ходе транзакции с предъявлением карты. Организации не требуется хранение этих данных после проведения авторизации. Потребоваться может только хранение PAN, срока действия карты и имени владельца.

⁶ Трех- или четырехзначное число, напечатанное рядом с местом для подписи или на лицевой стороне карты, используется для авторизации в ходе транзакции без предъявления карты.

⁷ PIN, введенный держателем карты в ходе транзакции с предъявлением карты, и/или зашифрованный PIN-блок, содержащийся в транзакционном сообщении.

Часть 4. План Мероприятий для устранения несоответствий

Выберите нужный статус выполнения для каждого требования. Если вы ответили “Не выполнено” на какое-либо из требований, следует предоставить дату приведения требования в соответствие и краткое описание планируемых мероприятий. *Проконсультируйтесь с банком-эквайером или платежной системой, так как не все платежные системы требуют заполнения этой части.*

Требование PCI	Описание	Статус выполнения (Выбрать)	Дата устранения и план действий (если отмечено “Не выполнено”)
1	Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
2	Не использовать пароли и другие системные параметры, заданные производителем по умолчанию	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
3	Обеспечить безопасное хранение данных о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
4	Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
5	Использовать и регулярно обновлять антивирусное ПО	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
6	Разрабатывать и поддерживать безопасные системы и приложения	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
7	Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
8	Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
9	Ограничить физический доступ к данным о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
10	Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
11	Регулярно выполнять тестирование систем и процессов обеспечения безопасности	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
12	Разработать и поддерживать политику информационной безопасности	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	





Приложение Е: Оценка соответствия – поставщики услуг
**Стандарт безопасности данных
индустрии платежных карт (PCI DSS)**

**Свидетельство о соответствии. Оценка
соответствия поставщика услуг**

Версия 1.2.1

Июль 2009

PCI DSS.RU

Инструкция по предоставлению отчета в регулирующие органы

Этот документ должен быть заполнен QSA-аудитором и поставщиком услуг как свидетельство того, что поставщик услуг имеет статус соответствия стандарту PCI DSS. Заполните все поля и передайте в МПС.

Часть 1. Информация о QSA

Название компании:					
Контактное лицо (QSA):			Должность:		
Телефон:			E-mail:		
Юридический адрес:			Город:		
Регион:		Страна:		Индекс:	
Адрес сайта в Интернете:					

Часть 2. Информация о поставщике услуг

Название компании:			Роль в МПС:		
Контактное лицо:			Должность:		
Телефон:			E-mail:		
Юридический адрес:			Город:		
Регион:		Страна:		Регион:	
Адрес сайта в Интернете:					

Часть 2а. Предоставляемые услуги (выбрать необходимые)

- | | | |
|--|--|---|
| <input type="checkbox"/> Авторизация | <input type="checkbox"/> Программы лояльности | <input type="checkbox"/> Сервер контроля доступа 3-D Secure |
| <input type="checkbox"/> Коммутация | <input type="checkbox"/> Электронная коммерция | <input type="checkbox"/> Обработка магнитной полосы |
| <input type="checkbox"/> Платежный шлюз | <input type="checkbox"/> Клиринг и урегулирование платежей | |
| <input type="checkbox"/> Обработка заказов по телефону или почте | <input type="checkbox"/> Хостинг | |
| <input type="checkbox"/> Выпуск карт | <input type="checkbox"/> Другое (укажите): | |

Перечень помещений, в которых проведен аудит:

Часть 2б. Связи

Имеются ли связи со сторонними организациями (платежными шлюзами, хостинговыми компаниями и т.п.)? Да Нет

Часть 2с. Обработка транзакций

Как и в каком количестве обрабатываются или хранятся данные о держателях карт?

Используемое платежное приложение: _____ Версия приложения: _____

Часть 3. Проверка соответствия PCI DSS

На основании результатов, описанных в Отчете о соответствии (“ROC”) датированном (*дата создания отчета*), (*Имя QSA*) подтверждает, что компания, описанная в части 2 настоящего документа, по состоянию на (*дата*) имеет статус (выберите):

- Соответствует:** Все требования помечены как “выполненные⁸,” и ASV-сканирование было выполнено (*имя ASV*), таким образом, (*имя компании*) продемонстрировала полное соответствие требованиям PCI DSS (*версия стандарта*).
- Не соответствует:** Некоторые требования PCI DSS помечены как “невыполненные”, что приводит к общему статусу **НЕСООТВЕТСТВИЯ**, или не было проведено успешное ASV-сканирование уполномоченным лицом, таким образом, (*Имя компании*) не продемонстрировала полного статуса соответствия PCI DSS

Дата, на которую запланировано достижение статуса соответствия:

При предъявлении данного отчета со статусом несоответствия требуется также предоставить заполненный План Мероприятий (Action Plan) части 4 данного документа. *Проконсультируйтесь с банком-эквайером или платежной системой, так как не все платежные системы требуют заполнения этой части*

Часть 3а. Подтверждение статуса соответствия

QSA-аудитор и поставщик услуг подтверждает:

- Отчет о соответствии заполнен в соответствии с документом «*Требования и процедура аудита безопасности*», версии (*вставить номер версии*).
- Вся информация в Отчете является достоверной и передает реальную ситуацию
- Поставщик услуг ознакомлен со стандартом PCI DSS и понимает необходимость наличия статуса соответствия
- В процессе аудита не обнаружено никаких следов хранения магнитного трека⁹, CAV2, CVC2, CID, или CVV2 кодов¹⁰, или информации о PIN коде¹¹.

Часть 3б. Подписи QSA-аудитора и проверяемой организации

Подпись QSA-аудитора ↑		Дата:
ФИО:	Должность:	
Подпись руководителя проверяемой организации: ↑		Дата:
ФИО:	Должность:	

⁸ Выполненные требования должны включать компенсирующие меры, утвержденные QSA аудитором. Если компенсирующие меры должным образом минимизируют риски связанные с требованием, QSA аудитор должен отметить это требование, как «выполненное».

⁹ Данные, закодированные в магнитной полосе карты, используются для аутентификации в ходе транзакции с предъявлением карты. Организации не требуется хранение этих данных после проведения авторизации. Потребоваться может только хранение PAN, срока действия карты и имени владельца.

¹⁰ Трех- или четырехзначное число, напечатанное рядом с местом для подписи или на лицевой стороне карты, используется для авторизации в ходе транзакции без предъявления карты.

¹¹ PIN, введенный держателем карты в ходе транзакции с предъявлением карты, и/или зашифрованный PIN-блок, содержащийся в транзакционном сообщении.

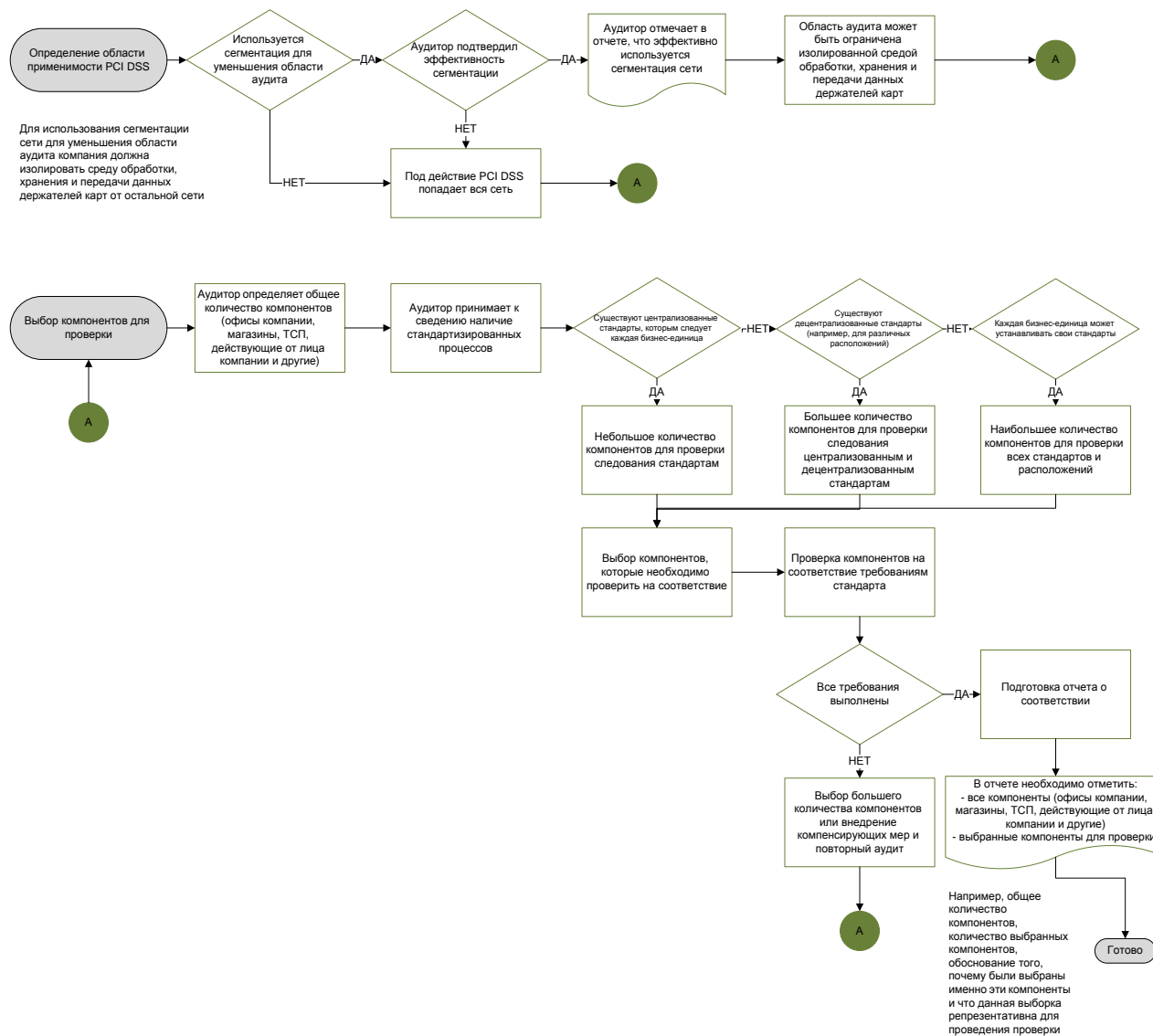
Часть 4. План Мероприятий для устранения несоответствий

Выберите нужный статус выполнения каждого требования. Если вы ответили “Не выполнено” на какое-либо из требований, следует предоставить дату приведения требования в соответствие и краткое описание планируемых мероприятий. *Проконсультируйтесь с банком-эквайером или платежной системой, не все платежные системы требуют заполнения этой части.*

Требование PCI	Описание	Статус выполнения (Выбрать)	Дата устранения и план действий (если отмечено “Не выполнено”)
1	Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
2	Не использовать пароли и другие системные параметры, заданные производителем по умолчанию	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
3	Обеспечить безопасное хранение данных о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
4	Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
5	Использовать и регулярно обновлять антивирусное ПО	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
6	Разрабатывать и поддерживать безопасные системы и приложения	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
7	Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
8	Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
9	Ограничить физический доступ к данным о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
10	Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
11	Регулярно выполнять тестирование систем и процессов обеспечения безопасности	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	
12	Разработать и поддерживать политику информационной безопасности	<input type="checkbox"/> Выполнено <input type="checkbox"/> Не выполнено	



Приложение F: Определение области аудита и выборки



Информация о переводе

Перевод текста Стандарта безопасности данных индустрии платежных карт (PCI DSS) версии 1.2.1 с английского языка на русский выполнили:

Антон Карпов
Сергей Шустиков
Александр Поляков
Юлия Зозуля
Алексей Ендовский

© 2009, Сообщество профессионалов PCIDSS.RU
info@pcidss.ru,
<http://www.pcidss.ru>

Санкт-Петербург,
2009