



# Стандарт безопасности данных индустрии платежных карт (PCI DSS)

---

**Требования и процедура аудита безопасности**

**Версия 2.0**

Октябрь 2010

**PCI DSS.RU**

## Содержание

<b>Введение и обзор стандарта PCI DSS .....</b>	<b>4</b>
<b>Область применения PCI DSS .....</b>	<b>5</b>
<b>Стандарты PCI DSS и PA-DSS и связь между ними .....</b>	<b>7</b>
<b>Область аудита соответствия требованиям PCI DSS.....</b>	<b>8</b>
Сегментация сети .....	8
Беспроводные сети .....	9
Привлечение третьих сторон.....	9
Выборочная оценка системных компонентов .....	10
Компенсирющие меры.....	11
<b>Инструкции по заполнению и требования к содержанию Отчета о соответствии .....</b>	<b>12</b>
Содержание и формат отчета .....	12
Проведение повторных проверок.....	15
Оценка соответствия PCI DSS – шаги создания отчета .....	16
<b>Детальные требования PCI DSS и процедуры проведения аудита.....</b>	<b>16</b>
<b>Построение и обслуживание защищенной сети .....</b>	<b>17</b>
Требование 1: Установить и обеспечить функционирование межсетевых экранов для защиты данных о держателях карт .....	17
Требование 2: Не использовать пароли и другие системные параметры, заданные производителем по умолчанию.....	23
<b>Защита данных о держателях карт .....</b>	<b>28</b>
Требование 3: Обеспечить безопасное хранение данных о держателях карт .....	28
Требование 4. Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования .....	39
<b>Управление уязвимостями.....</b>	<b>41</b>
Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение .....	41
Требование 6: Разрабатывать и поддерживать безопасные системы и приложения .....	43

<b>Внедрение строгих мер контроля доступа .....</b>	<b>51</b>
Требование 7: Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью .....	51
Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре .....	53
Требование 9: Ограничить физический доступ к данным платежных карт .....	61
<b>Регулярный мониторинг и тестирование сети .....</b>	<b>67</b>
Требование 10: Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт .....	67
Требование 11: Регулярно выполнять тестирование систем и процессов обеспечения безопасности .....	72
<b>Разработка политики информационной безопасности .....</b>	<b>78</b>
Требование 12: Разработать и поддерживать политику информационной безопасности для всего персонала организации .....	78
<b>Приложение А: Дополнительные требования PCI DSS для поставщиков услуг с общей средой .....</b>	<b>88</b>
<b>Приложение В: Компенсирующие меры .....</b>	<b>91</b>
<b>Приложение С: Компенсирующие меры – форма для заполнения .....</b>	<b>92</b>
<b>Приложение D: Определение области аудита и выборки .....</b>	<b>94</b>
<b>Информация о переводе .....</b>	<b>95</b>

## Введение и обзор стандарта PCI DSS

Стандарт безопасности данных индустрии платежных карт (PCI DSS) разработан в целях упрощения внедрения, распространения мер по обеспечению и повсеместному внедрению стандарта безопасности данных о держателях карт. В основе стандарта PCI DSS лежат базовые технические и эксплуатационные требования, обеспечивающие защиту данных о держателях карт. Данный стандарт предназначен для использования аудиторами при проверке всех организаций сферы обработки платежных данных на соответствие данным требованиям, а именно торгово-сервисных предприятий, процессинговых центров, банков-эквайеров, организаций, выпускающих платежные карты и поставщиков услуг, а также других организаций, которые хранят, обрабатывают или передают данные о держателях карт. Стандарт PCI DSS содержит минимальное количество требований, разработанных для защиты данных о держателях карт, которое может быть расширено дополнительными регулирующими мерами и разработками для сокращения рисков в дальнейшем. Ниже приведен общий обзор 12 требований стандарта PCI DSS.

### **Общий 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.

#### **Поддержка политики информационной безопасности**

Требование 12: Разработать и поддерживать политику информационной безопасности.

Данный документ, *Требования и процедура аудита безопасности стандарта PCI DSS*, содержит 12 требований стандарта и соответствующие проверочные процедуры оценки соответствия и предназначается для проведения оценки организаций соответствия стандарту PCI DSS. Он создан для использования в процессе оценки соответствия PCI DSS как элемент аттестации организации. Приведенные ниже разделы содержат детальное руководство и лучшие практики для содействия организациям при подготовке, проведению и написанию отчетных материалов по результатам аудита на соответствие требованиям стандарта PCI DSS. Требования стандарта PCI DSS и Проверочные процедуры начинаются со страницы 18.

На сайте Совета PCI SSC (PCI Security Standards Council) ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)) размещены дополнительные источники информации, включая:

- Аттестаты соответствия
- Исследование PCI DSS: понимание назначение требований PCI DSS
- Словарь терминов, акронимов и сокращений PCI DSS и PA-DSS
- Часто задаваемые вопросы FAQs
- Дополнительная информация и руководство

**Примечание:** Дополнительная информация применима совместно со стандартом PCI DSS и содержит дополнительный анализ и рекомендации по достижению соответствия требованиям PCI DSS, однако они не изменяют, не исключают и не заменяют содержание стандарта или его иное требование.

Для получения более подробной информации посетите [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

## Область применения PCI DSS

Требования PCI DSS применимы к информационной инфраструктуре, если в ней хранятся, обрабатываются или передаются карточные данные. Карточные данные включают в себя Данные о держателях карт и Критичные аутентификационные данные:

<b>Данные о держателях карт:</b>	<b>Критичные аутентификационные данные:</b>
<ul style="list-style-type: none"><li>▪ PAN</li><li>▪ Имя держателя</li><li>▪ Срок действия</li><li>▪ Сервисный код</li></ul>	<ul style="list-style-type: none"><li>▪ Полные данные магнитной полосы карты или её эквивалент на чипе</li><li>▪ CAV2/CVC2/CVV2/CID</li><li>▪ PIN/PIN-блоки</li></ul>

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

Если имя держателя, сервисный код и/или срок действия хранятся, обрабатываются или передаются вместе с PAN, или другим образом присутствуют в инфраструктуре, они должны быть защищены в соответствии с требованиями PCI DSS, за исключением требований 3.3 и 3.4, которые применимы только к PAN.

PCI DSS представляет минимальный набор целей для контроля, который может быть усилен местными, региональными или отраслевыми законами и постановлениями. Также, законодательства или нормативные требования могут требовать особой защиты персональной информации или других элементов данных (например, имени держателя карты), или определять порядок раскрытия организацией информации о потребителях. Примеры включают законы, относящиеся к защите персональных данных, приватности, кражи личных данных или безопасности информации. PCI DSS не заменяет собой местные или региональные законы, правительственные распоряжения или иные законные требования.

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.

	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)	ДА	ДА	НЕТ
	Сервисный код (Service Code)	ДА	ДА	НЕТ
	Дата истечения срока действия карты (Expiration Date)	ДА	ДА	НЕТ
Критичные аутентификационные данные <sup>1</sup>	Вся магнитная полоса карты <sup>2</sup>	НЕТ	Не определено	Не определено
	CAV2/CVC2/CVV2/CID	НЕТ	Не определено	Не определено
	PIN / PIN Block	НЕТ	Не определено	Не определено

<sup>1</sup>критичные аутентификационные данные не должны храниться после авторизации (даже в зашифрованном виде).

<sup>2</sup> полная магнитная полоса карты, её зашифрованное представление в чипе и другие виды представления

Требования 3.3 и 3.4 применяются только к PAN. Если PAN хранится вместе с другими данными о держателях, то в соответствии с требованием 3.4 хранить в нечитаемом виде необходимо только PAN.

Если PAN не хранится, не обрабатывается и не передается, то требования PCI DSS не применяются.

## Стандарты PCI DSS и PA-DSS и связь между ними

Использование приложения, соответствующего стандарту PA-DSS, не является гарантией соответствия организации требованиям стандарта PCI DSS, поскольку данное приложение должно быть внедрено в среду, соответствующую Стандарту PCI DSS и в соответствии с Руководством по внедрению, которое должно быть представлено разработчиком платежного приложения (согласно требованию 13.1 стандарта PA-DSS).

Требования стандарта PA-DSS основаны на Требованиях и процедуре аудита безопасности стандарта PCI DSS (данном документе). Стандарт PA-DSS более детально описывает требования к платежному приложению для упрощения достижения соответствия стандарту PCI DSS.

Безопасные платежные приложения при внедрении в среду соответствия стандарту PCI DSS позволят избежать нарушений безопасности и мошеннических действий, которые могут привести к компрометации полного содержания данных магнитной полосы, проверочных значений (CAV2, CID, CVC2, CVV2), а также PIN и PIN-блоков.

Вот примеры случаев, в которых платежные приложения могут препятствовать достижению соответствия:

- Хранение данных магнитной полосы и/или эквивалентной чиповой информации в клиентской сети после авторизации;
- Приложения, требующие от клиентов отключения различных опций, требуемых стандартом PCI DSS, например, антивирусного программного обеспечения, межсетевых экранов для должной работы приложения;
- Использование разработчиками небезопасных методов подключения, используемых для поддержки клиента.

Стандарт PA-DSS применим к разработчикам программного обеспечения и платежных приложений, которые хранят, обрабатывают или передают данные о держателях карт при выполнении авторизации или платежных операций, в случае продажи данных приложений, их распространения или лицензирования для третьих лиц.

Следует принять во внимание следующие пункты применения стандарта PA-DSS:

- PA-DSS применим к платежным приложениям, которые являются «готовыми продуктами», т.е. подлежат распространению и установке без существенной доработки.
- PA-DSS не применим к платежным приложениям, разработанным торгово-сервисными предприятиями и поставщиками услуг, если они предназначены для использования внутри организации (не подлежат продаже, распространению или лицензированию для третьих лиц), поскольку данные приложения попадают под требования, предъявляемые к торгово-сервисным предприятиям и поставщикам услуг для соответствия требованиям стандарта PCI DSS.

Для получения более подробного руководства и определения области применения стандарта PA-DSS к тому или иному приложению, обратитесь к документу Требования и процедура аудита безопасности стандарта PA-DSS, который доступен на сайте [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## 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. Системные компоненты также включают в себя виртуализованные компоненты, такие как виртуальные серверы, виртуальные коммутаторы и маршрутизаторы, виртуальные приложения и гипервизоры. Среда данных о держателях карт – это совокупность людей, процессов и оборудования, которые хранят, обрабатывают или передают 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).

Первым шагом выполнения оценки соответствия требованиям PCI DSS должно быть определение области аудита. Как минимум один раз в год и перед каждой ежегодной оценкой соответствия, оцениваемая организация должна проверять корректность определения области применения PCI DSS, идентифицируя все места хранения и потоки данных о держателях карт и проверяя, все ли они включены в область применения PCI DSS. Для того чтобы проверить корректность области применения PCI DSS следует выполнить следующие действия:

- Оцениваемая организация идентифицирует все данные о держателях карт в своей информационной инфраструктуре, чтобы убедиться в том, что данные о держателях карт отсутствуют вне определенной среды данных о держателях карт;
- Когда все места нахождения данных о держателях карт определены, организация использует эту информацию, чтобы убедиться в том, что область применения PCI DSS определена корректно;
- Организация признает все обнаруженные данные о держателях карт относящимися к области аудита на соответствие PCI DSS, пока эти данные не будут удалены или перенесены в среду данных о держателях карт, определенную ранее;
- Организация сохраняет документы, описывающие процесс идентификации данных о держателях карт и его результаты, для их пересмотра аудитором и/или до их пересмотра в рамках ежегодной оценки соответствия требованиям PCI DSS.

### 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.

Если сегментация сети присутствует и используется для уменьшения области применения PCI DSS, аудитор должен удостовериться в том, что сегментация адекватно уменьшает область оценки. 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 D: 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 подключена или 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). Перед внедрением беспроводных технологий организация должна тщательно проанализировать необходимость их внедрения и оценить связанные с этим риски. Рекомендуется использовать беспроводные технологии только для передачи некритичных данных.

### **Привлечение 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) Пройти оценку PCI DSS и предоставить доказательство соответствия своим клиентам, или
- 2) Не проходить оценку своей организации PCI DSS и предоставлять возможность анализа своих услуг в ходе оценки соответствия каждого 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**

Выборка не является требованием стандарта PCI DSS. Однако, аудитор, выполняющий проверки PCI DSS, может выбрать несколько бизнес-единиц и системных компонентов для проверок. Размер выборки должен быть определен вначале для бизнес-единиц, а затем для системных компонентов внутри каждой из них. Выборка должна быть репрезентативным выбором как всех типов и размещений бизнес-единиц, так и типов системных компонентов внутри бизнес-единиц. Выборка должна быть достаточно обширной, чтобы аудитор мог удостовериться в выполнении всех требований.

Использование выборочной оценки бизнес-единиц и системных компонентов не уменьшает области хранения данных о держателях карт или применения требований PCI DSS. Вне зависимости от произведения выборки, требования PCI DSS распространяются на всю область хранения данных о держателях карт. Если производится выборка, каждый элемент должен быть проверен на соответствие всем применимым требованиям PCI DSS. Проведение выборки требований PCI DSS запрещено.

Примеры бизнес-единиц включают (но не ограничиваются): офисы компании, магазины, франчайзинговые предприятия и географически разнесенные офисные помещения. Необходимо проверить на соответствие системные компоненты в каждой выбранной бизнес-единице. Например, операционные системы или приложения, доступные для проверок.

Например, проверяющий может определить, что выборка внутри бизнес-единицы включает в себя сервера под управлением Sun Solaris, на которых функционирует веб-сервер Apache, Windows-сервера, на которых функционирует СУБД Oracle, мейнфрейм, на котором функционируют платежные приложения предыдущего поколения, сервера передачи данных под управлением HP-UX и Linux-сервера с MySQL. Если все приложения работают на одной операционной системе (например, Windows 7 или Solaris 10), проверке подлежат множество различных приложений (см. Приложение D: *Определение области аудита и выборки*).

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

- При наличии стандартизированных процессов, согласно которым выполняются требования PCI DSS, выборка может быть меньше. При этом, выборка должна быть достаточно большой, чтобы уверенность проверяющего в том, что все бизнес-единицы и системные компоненты настроены корректно, была обоснованной.
- 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.

Для каждого случая применения выборки аудитор должен:

- Документировать обоснование примененного метода выборки и ее размера;

- Документировать и утвердить стандартизованные процессы, рассматриваемые при определении размера выборки;
- Объяснить, насколько сделанная выборка репрезентативна.

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

*Подробнее см. Приложение D: Определение области аудита и выборок.*

### ***Компенсирующие меры***

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

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

Подробности см. в Приложении В и С.

## 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:

- Документ, в котором аудитор подтверждает правильность области применения PCI DSS, включая:
  - Методы или процессы, использованные для идентификации и документации всех мест наличия данных о держателях карт
  - Как были оценены и документированы результаты
  - Как были проверены эффективность и правильность использованных методов
  - Что аудитор утверждает, что область проверки правильна и репрезентативна
  
- 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».

### 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, уточняйте требования отдельных платежных систем к платежным приложениям.*
- Перечень опрошенных лиц, их должности, организации, к которым они относятся, и обсужденные темы.
- 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 торгово-сервисного предприятия или поставщика услуг и аудитора.
- Временной период и длительность проведения оценки соответствия.
- 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 ASV-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 разделе «краткое описание» следует отразить все дополнительные наблюдения, которые могут не попадать под пункты Отчёта 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.
- Убедиться, что все неприменимые пункты однозначно объяснены.
- 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

- Заполнение Отчета о соответствии, согласно требованиям приведенного выше раздела «Инструкции по заполнению и содержание Отчета о соответствии».
- Проверка результатов проведения ASV-сканирования уполномоченной организацией (ASV – *Approved Scanning Vendor*), а также запрос подтверждения его проведения у уполномоченной организации.
- Заполнение Свидетельства о соответствии (Attestation of Compliance). Свидетельства о соответствии доступны на сайте PCI SSC ([www.pcisecuritystandarts.org](http://www.pcisecuritystandarts.org)).
- 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, или в результате того, что требование не применимо.

*Примечание: эта колонка не должна быть использована для тех настроек, которые ещё не работают или того, что будет сделано потом*

- **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. Для дальнейших инструкций по отчетам о несоответствии обратитесь к Свидетельствам о соответствии, доступным на сайте PCI SSC ([www.pcisecuritystandarts.org](http://www.pcisecuritystandarts.org)).
- **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.

Иные системные компоненты, если они отвечают минимальным требованиям к межсетевым экранам, приведенным в требовании 1, могут использоваться для обеспечения функциональности межсетевого экранирования. Системные компоненты, используемые для обеспечения функциональности межсетевого экранирования внутри среды данных о держателях карт, должны быть включены в определение и область действия Требования 1.

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>1.1</b> Должны быть разработаны стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя:	<b>1.1</b> 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:			
<b>1.1.1</b> Формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов.	<b>1.1.1</b> Проверить, что существует формальный процесс утверждения всех сетевых соединений, а также изменений в конфигурациях межсетевых экранов и маршрутизаторов.			
<b>1.1.2</b> Актуальную схему сети с указанием всех каналов доступа к данным о держателях карт, включая все беспроводные сети.	<b>1.1.2.a</b> 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.			
	<b>1.1.2.b</b> Проверить актуальность схемы сети.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>1.1.3</b> Требования к межсетевому экранированию каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании.	<b>1.1.3.a</b> Проверить, что стандарты конфигурации включают требование о необходимости межсетевого экранирования каждого Интернет-соединения, а также между DMZ и внутренней сетью.			
	<b>1.1.3.b</b> Проверить, что конфигурации межсетевых экранов не противоречат схеме сети.			
<b>1.1.4</b> Описание групп, ролей и ответственности за управление сетевыми устройствами.	<b>1.1.4</b> Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат описание ролей, групп и ответственности за управление сетевыми компонентами.			
<b>1.1.5</b> Обоснованный документированный перечень всех разрешенных для использования сервисов, протоколов и портов, необходимых для работы бизнес-приложений, включающий документальное описание внедренных механизмов защиты небезопасных протоколов.  Примеры небезопасных сервисов, протоколов или портов включают, но не ограничиваются FTP, Telnet, POP3, IMAP и SMTP.	<b>1.1.5.a</b> Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов содержат документированный перечень сервисов, протоколов и портов, необходимых для бизнеса (например, HTTP, SSL, SSH, VPN).			
	<b>1.1.5.b</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.			
<b>1.1.6</b> Требование пересмотра настроек межсетевых экранов и маршрутизаторов не реже одного раза в полгода.	<b>1.1.6.a</b> Проверить, что стандарты конфигурации межсетевых экранов и маршрутизаторов требуют пересмотра правил для межсетевых экранов и маршрутизаторов как минимум раз в полгода.			
	<b>1.1.6.b</b> Получить и проверить документацию, подтверждающую, что наборы правил пересматриваются как минимум раз в полгода.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>1.2</b> Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в среде данных о держателях карт.</p> <p><i>Примечание: недоверенной является любая сеть, внешняя по отношению к сетям, принадлежащим проверяемой организации и/или сеть, которая не контролируется проверяемой организацией</i></p>	<p><b>1.2</b> 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:</p>			
<p><b>1.2.1</b> Входящий и исходящий трафик должен быть ограничен только необходимыми соединениями для среды данных о держателях карт.</p>	<p><b>1.2.1.a</b> Проверить, что входящий и исходящий трафик ограничен только необходимыми для среды данных о держателях карт соединениями и что ограничения документированы.</p> <p><b>1.2.1.b</b> Проверить, что весь иной входящий и исходящий трафик явно запрещен.</p>			
<p><b>1.2.2</b> Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов маршрутизаторов.</p>	<p><b>1.2.2</b> Проверить, что конфигурационные файлы маршрутизаторов синхронизированы, например, рабочие конфигурационные файлы и конфигурационные файлы, используемые при перезагрузке маршрутизатора, имеют одинаковую безопасную конфигурацию.</p>			
<p><b>1.2.3</b> 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.</p>	<p><b>1.2.3</b> 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.</p>			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>1.3</b> Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды данных о держателях карт.	<b>1.3</b> Проверить конфигурацию межсетевых экранов и маршрутизаторов, включая (но не ограничиваясь) маршрутизатор на границе с сетью Интернет, маршрутизатор и межсетевой экран DMZ, сегмент DMZ, пограничный маршрутизатор и внутренний сегмент сети данных о держателях карт, 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.			
<b>1.3.1</b> Необходимо внедрить DMZ, чтобы ограничить входящий и исходящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным сервисам, протоколам и портам.	<b>1.3.1</b> Проверить, что DMZ применяется для ограничения входящего и исходящего трафика только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным сервисам, протоколам и портам.			
<b>1.3.2</b> Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ.	<b>1.3.2</b> Проверить, что входящие Интернет-соединения ограничены только адресами, находящимися в DMZ.			
<b>1.3.3</b> Должны быть запрещены любые прямые входящие или исходящие соединения между сетью Интернет и средой данных о держателях карт.	<b>1.3.3</b> Проверить, что отсутствуют прямые входящие и исходящие соединения между сетью Интернет и средой данных о держателях карт.			
<b>1.3.4</b> Необходимо запретить соединения с внутренними адресами от источника из сети Интернет к адресам, расположенным в DMZ.	<b>1.3.4</b> Проверить, что пакеты с внутренними адресами не могут достигнуть DMZ от источника из сети Интернет.			
<b>1.3.5</b> Необходимо запретить неавторизованный исходящий трафик из среды данных о держателях карт в сеть Интернет.	<b>1.3.5</b> Убедиться, что исходящий трафик из среды данных о держателях карт в сеть Интернет является строго авторизованным.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>1.3.6</b> Необходимо включить динамическую пакетную фильтрацию с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений).	<b>1.3.6</b> Убедиться, 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].			
<b>1.3.7</b> Необходимо размещать системные компоненты (например, базы данных), в которых хранятся данные о держателях карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей.	<b>1.3.7</b> Убедиться, что системные компоненты, в которых хранятся данные о держателях карт, располагаются во внутренней сети, отделенной от DMZ и иных недоверенных сетей.			
<b>1.3.8</b> Должно быть запрещено раскрытие частных IP-адресов и данных о маршрутах третьим сторонам, не имеющим авторизованного доступа.  Примечание: правила сокрытия IP-адресации могут включать (но не ограничиваются): <ul style="list-style-type: none"> <li>▪ технология NAT;</li> <li>▪ расположение серверов, содержащих данные о держателях карт за</li> </ul>	<b>1.3.8.a</b> Убедиться, что существуют правила, обеспечивающие предотвращение раскрытия частных IP-адресов и данных о маршрутах из внутренней сети в сеть Интернет.			

Требование PCI DSS	Процедура проведения проверки	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>прокси-серверами/межсетевыми экранами или кэшами содержимого;</i></p> <ul style="list-style-type: none"> <li>▪ <i>удаление или фильтрация объявлений маршрутов для частных сетей, требующих зарегистрированной адресации;</i></li> <li>▪ <i>внутреннее использование адресного пространства RFC1918 вместо зарегистрированных адресов.</i></li> </ul>	<p><b>1.3.8.b</b> Убедиться, что любое раскрытие частных IP-адресов и данных о маршрутах внешним сторонам является авторизованным.</p>			
<p><b>1.4</b> Должны быть установлены персональные межсетевые экраны на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети организации.</p>	<p><b>1.4.a</b> Проверить, что на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети организации, установлены и активированы персональные межсетевые экраны.</p>			
	<p><b>1.4.b</b> Проверить, что настройки персонального меж сетевого экрана выполнены в соответствии со стандартами организации и не могут быть изменены пользователями мобильных и принадлежащих сотрудникам компьютеров.</p>			

## 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
2.1 Всегда следует менять настройки, установленные производителем по умолчанию, перед установкой системы в сетевую инфраструктуру, включая (но не ограничиваясь) пароли, строки доступа SNMP и удаление ненужных для работы учетных записей.	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).			
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.	2.1.1 Проверить следующие настройки для беспроводных устройств, установленные производителем по умолчанию:			
	2.1.1.a Проверить, что установленные по умолчанию ключи шифрования были изменены при инсталляции и изменяются каждый раз, когда кто-либо, обладающий данными о ключах, уходит из компании либо переходит на другую должность.			
	2.1.1.b Проверить, что установленные по умолчанию строки доступа SNMP беспроводных устройств были изменены.			
	2.1.1.c Проверить, что установленные по умолчанию пароли/парольные фразы точек доступа были изменены.			
	2.1.1.d Проверить, что программное обеспечение беспроводных устройств обновлено до актуальной версии и поддерживает стойкие криптографические алгоритмы для аутентификации и передачи данных через беспроводные сети.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	<b>2.1.1.e</b> Проверить, что прочие настройки безопасности беспроводных устройств, установленные производителем по умолчанию, были изменены, если применимо.			
<b>2.2</b> 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.  Примеры источников общепринятых отраслевых стандартов в области безопасности: <ul style="list-style-type: none"> <li>▪ Центр Интернет-безопасности (CIS);</li> <li>▪ Международная организация по стандартизации (ISO);</li> <li>▪ Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS);</li> <li>▪ Национальный институт стандартов и технологий (NIST).</li> </ul>	<b>2.2.a</b> Изучить стандарты системных конфигураций всех системных компонентов. Проверить, что стандарты конфигурации учитывают положения общепринятых отраслевых стандартов.			
	<b>2.2.b</b> Проверить, что стандарты системных конфигураций обновляются по мере обнаружения новых проблем безопасности, как описывается в требовании 6.2.			
	<b>2.2.c</b> Убедиться, что стандарты системных конфигураций применяются при настройке новых систем.			
	<b>2.2.d</b> Убедиться, что стандарты системных конфигураций включают в себя следующие параметры, указанные ниже (2.2.1-2.2.4).			
<b>2.2.1</b> Для каждого сервера должна быть внедрена одна основная функция для недопущения нахождения на одном и том же сервере функций, требующих различные уровни защиты (например, веб-серверы, серверы СУБД и DNS-серверы следует	<b>2.2.1.a</b> Для нескольких системных компонентов убедиться, что выполняется правило "одна основная функция – один сервер".			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>размещать на разных компьютерах).</p> <p><i>Примечание: при использовании технологии виртуализации необходимо внедрять только одну основную функцию для каждого виртуального системного компонента.</i></p>	<p><b>2.2.1.b</b> При использовании технологии виртуализации убедиться, что выполняется правило "одна основная функция - один виртуальный системный компонент или устройство".</p>			
<p><b>2.2.2</b> Должны быть включены только необходимые и защищенные сервисы, протоколы, управляющие программы и т.д., требующиеся для функционирования системы.</p> <p>Необходимо настроить параметры безопасности для всех указанных сервисов, протоколов и управляющих программ, которые могут быть небезопасными. Например, следует использовать такие защитные технологии, как SSH, S-FTP, SSL или IPSec VPN для защиты таких незащищенных сервисов как NetBIOS, совместное использование файлов, Telnet, FTP и т.д.</p>	<p><b>2.2.2.a</b> Для выборки из нескольких системных компонентов проверить включенные сервисы, управляющие программы и протоколы. Проверить, что включены только необходимые сервисы и протоколы.</p> <p><b>2.2.2.b</b> Определить все включенные небезопасные сервисы, управляющие программы и протоколы. Убедиться, что их использование обосновано, а параметры безопасности внедрены и документированы.</p>			
<p><b>2.2.3</b> Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.</p>	<p><b>2.2.3.a</b> Опросить системных администраторов и/или администраторов безопасности с целью проверки того, что им известны настройки основных параметров безопасности системных компонентов.</p> <p><b>2.2.3.b</b> Проверить, что основные параметры безопасности включены в стандарты конфигурации системных компонентов.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	<b>2.2.3.с</b> Для нескольких системных компонентов проверить, что основные параметры безопасности установлены соответствующим образом.			
<b>2.2.4</b> Из системы должна быть удалена вся ненужная функциональность: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.	<b>2.2.4.а</b> Для нескольких системных компонентов проверить, что ненужная функциональность (например, сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы) удалена.			
	<b>2.2.4.б</b> Проверить, что включенные функции документированы и безопасно настроены.			
	<b>2.2.4.с</b> Убедиться, что в выборке системных компонентов присутствует только документированная функциональность.			
<b>2.3</b> При использовании неконсольного административного доступа к системе, следует всегда шифровать канал с использованием стойких криптографических алгоритмов. Следует использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа.	<b>2.3</b> Для нескольких системных компонентов убедиться, что канал неконсольного административного доступа проходит шифрование следующим образом:			
	<b>2.3.а</b> Изучить записи журнала каждой системы для того, чтобы подтвердить активизацию механизмов шифрования до запроса пароля администратора.			
	<b>2.3.б</b> Проверить сервисы и файлы параметров на системах и убедиться, что Telnet и другие протоколы удаленного доступа к системе не доступны для внутреннего использования.			
	<b>2.3.с</b> Убедиться, что административный доступ к веб-ориентированным системам администрирования подвергается шифрованию с использованием стойких криптографических алгоритмов.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>2.4</b> 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><b>2.4</b> 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 избегание пересылки PAN с использованием пользовательских технологий передачи сообщений, таких как электронная почта и системы мгновенной отправки сообщений.

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
3.1 Хранение данных о держателях карт должно быть ограничено только необходимым минимумом. Должны быть разработаны политики, процедуры и процессы хранения и уничтожения данных, как изложено ниже.	3.1 Изучить политики, процедуры и процессы хранения и уничтожения данных и выполнить следующее:			
3.1.1 Необходимо внедрить политики хранения и уничтожения данных, которые предусматривают: <ul style="list-style-type: none"> <li>▪ Количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований;</li> <li>▪ Процессы безопасного удаления данных, хранение которых более не является необходимым;</li> <li>▪ Специфические требования к</li> </ul>	3.1.1.a Проверить, что политики и процедуры внедрены и содержат требования бизнеса и законодательства к хранению данных, включая специфические требования к хранению данных о держателях карт (например, установлен срок хранения данных о держателях карт X в силу Y бизнес-причин).			
	3.1.1.b Проверить, что политики и процедуры содержат положения о необходимости безопасного уничтожения данных, если их хранение более не является необходимым по требованиям бизнеса, законодательства и иным регулирующим требованиям, включая уничтожение данных о держателях карт.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>хранению данных о держателях карт;</p> <ul style="list-style-type: none"> <li>Ежеквартальные процессы, проводимые вручную или автоматически, которые обнаруживают и безопасно удаляют данные о держателях карт, которые превышают определенные политикой требования хранения данных.</li> </ul>	<p><b>3.1.1.c</b> Проверить, что действие политик и процедур распространяется на все места хранения данных о держателях карт.</p> <p><b>3.1.1.d</b> Проверить, что политики и процедуры содержат, по меньшей мере, один из следующих параметров:</p> <p>Программные процессы (проводимые автоматически или вручную) предусматривают удаление данных о держателях карт, сроки хранения которых превышают определенные политикой требования хранения данных, не реже одного раза в квартал.</p> <p>Требования как минимум ежеквартальной проверки, свидетельствующие о том, что сроки хранения данных о держателях карт не превышают определенные политикой требования хранения данных.</p> <p><b>3.1.1.e</b> Для нескольких системных компонентов, хранящих данные о держателях карт, убедиться, что сроки хранения данных не превышают определенные политикой требования хранения данных.</p>			
<p><b>3.2</b> 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><i>Примечание: эмитенты и компании, обеспечивающие эмиссионные сервисы, могут иметь</i></p>	<p><b>3.2.a</b> Убедиться, что эмитенты и компании, обеспечивающие эмиссионные сервисы, имеют обоснованную с точки зрения бизнеса необходимость хранения критичных аутентификационных данных, а хранимые данные надежно защищены.</p> <p><b>3.2.b</b> В других случаях, если критичные аутентификационные данные получаются и уничтожаются, проверить, что процессы безопасного удаления данных гарантируют невозможность восстановления данных.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>обоснованную необходимость хранения критичных аутентификационных данных. Такая необходимость должна иметь обоснование с точки зрения бизнеса, а хранимые данные должны быть надежно защищены.</i></p>	<p><b>3.2.c</b> Для каждого вида критичных аутентификационных данных выполнить следующие шаги:</p>			
<p><b>3.2.1</b> Запрещается хранить полное содержимое дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте). Эти данные также называются «полная дорожка», «дорожка», «дорожка 1», «дорожка 2» и «данные магнитной полосы».</p> <p><i>Примечание: Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы:</i></p> <ul style="list-style-type: none"> <li>▪ <i>имя держателя карты,</i></li> <li>▪ <i>номер платежной карты (PAN),</i></li> <li>▪ <i>дата истечения срока действия карты,</i></li> <li>▪ <i>сервисный код.</i></li> </ul> <p><i>Для минимизации рисков разрешается хранить только указанные элементы данных.</i></p>	<p><b>3.2.1</b> Для нескольких системных компонентов проверить источники данных, например, перечисленные ниже (но не ограничиваться ими), и убедиться, что полная дорожка магнитной полосы, находящейся на обратной стороне карты (или её аналог на чипе), не сохраняется ни при каких обстоятельствах:</p> <ul style="list-style-type: none"> <li>▪ <i>входящие данные о транзакции;</i></li> <li>▪ <i>все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок);</i></li> <li>▪ <i>файлы истории;</i></li> <li>▪ <i>файлы трассировки;</i></li> <li>▪ <i>несколько схем баз данных;</i></li> <li>▪ <i>содержимое баз данных.</i></li> </ul>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>3.2.2</b> 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).</p>	<p><b>3.2.2</b> Для нескольких системных компонентов проверить следующие элементы (но не ограничиваться ими) и убедиться, что трех- или четырехзначное проверочное значение (CVV2, CVC2, CID, CAV2) не сохраняется ни при каких обстоятельствах:</p> <ul style="list-style-type: none"> <li>▪ входящие данные о транзакции;</li> <li>▪ все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок);</li> <li>▪ файлы истории;</li> <li>▪ файлы трассировки;</li> <li>▪ несколько схем баз данных;</li> <li>▪ содержимое баз данных.</li> </ul>			
<p><b>3.2.3</b> Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.</p>	<p><b>3.2.3</b> Для нескольких системных компонентов проверить следующие элементы (но не ограничиваться ими) 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"> <li>▪ входящие данные о транзакции;</li> <li>▪ все журналы протоколирования (журналы транзакций, журналы истории, журналы отладки, журналы ошибок);</li> <li>▪ файлы истории;</li> <li>▪ файлы трассировки;</li> <li>▪ несколько схем баз данных;</li> <li>▪ содержимое баз данных.</li> </ul>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>3.3</b> Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4).</p> <p><i>Примечание:</i></p> <ul style="list-style-type: none"> <li>• Данное требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть весь PAN;</li> <li>• Данное требование не заменяет собой иные более строгие требования к отображению данных о держателях карт (например, на чеках POS-терминалов).</li> </ul>	<p><b>3.3</b> 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>			
<p><b>3.4</b> PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий). Для этого следует использовать любой из следующих методов:</p> <ul style="list-style-type: none"> <li>▪ стойкая однонаправленная хэш-функция (должен быть хеширован весь PAN);</li> <li>▪ укорачивание (хеширование не может использоваться для замещения укороченного сегмента PAN);</li> <li>▪ использование механизмов One-Time-Pad («одноразовых блокнотов», хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных</li> </ul>	<p><b>3.4.a</b> Изучить документацию о системе, используемой для защиты PAN, в том числе информацию о ее производителе, типе системы/процесса, 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"> <li>▪ стойкая однонаправленная хэш-функция;</li> <li>▪ укорачивание (truncation);</li> <li>▪ использование механизмов One-Time-Pad («одноразовых блокнотов», хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных (index tokens);</li> <li>▪ стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами.</li> </ul> <p><b>3.4.b</b> Изучить несколько таблиц или файлов из нескольких хранилищ данных и убедиться, что PAN представлен в нечитаемом виде (т.е. не хранится в открытом виде).</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>(index tokens);</p> <ul style="list-style-type: none"> <li>▪ стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами.</li> </ul> <p><i>Примечание: При наличии доступа одновременно к маскированному и хешированному номерам карты для злоумышленника не составит большого труда восстановить данные исходного PAN. Если маскированное и хешированное значение одного и того же PAN содержатся внутри среды какой-либо структуры, необходимо ввести дополнительные средства контроля для недопущения корреляции между маскированным и хешированным значениями, так как при этом исходный PAN становится легко восстановим.</i></p>	<p><b>3.4.c</b> Изучить несколько съемных носителей (например, кассеты с резервными копиями данных) и убедиться, что PAN представлен в нечитаемом виде.</p> <p><b>3.4.d</b> Изучить несколько журналов регистрации событий и убедиться, что PAN из них удален или представлен в нечитаемом виде.</p>			
<p><b>3.4.1</b> 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</p>	<p><b>3.4.1.a</b> 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><b>3.4.1.b</b> Проверить, что криптографические ключи хранятся безопасно (например, на съемном носителе, который защищен соответствующими процедурами контроля доступа).</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
(например, локальных учетных записей). Ключи шифрования не должны быть привязаны к учетным записям пользователей.	<p><b>3.4.1.c</b> Проверить, что данные о держателях карт на съемных носителях хранятся только в зашифрованном виде.</p> <p><i>Примечание: Если шифрование диска не используется для шифрования съемных носителей, данные на съемных носителях должны быть представлены в нечитаемом виде путем использования других методов шифрования.</i></p>			
<p><b>3.5</b> Следует обеспечить защиту всех ключей шифрования данных о держателях карт от их компрометации или неправильного использования:</p> <p><i>Примечание: Данное требование также применимо к ключам шифрования ключей, используемых для защиты ключей шифрования данных. Такие ключи шифрования ключей должны быть, как минимум, не менее стойкими, чем ключи шифрования данных.</i></p>	<p><b>3.5</b> Проверить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования следующим образом:</p>			
<p><b>3.5.1</b> Доступ к ключам шифрования должен быть разрешен наименьшему возможному количеству ответственным за их хранение и использование сотрудникам.</p>	<p><b>3.5.1</b> Изучить списки доступа и убедиться, что доступ к ключам предоставлен наименьшему возможному количеству ответственных за их хранение и использование сотрудников.</p>			
<p><b>3.5.2</b> Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.</p>	<p><b>3.5.2.a</b> Изучить системные конфигурационные файлы, убедиться, что ключи хранятся в зашифрованном виде и ключи шифрования ключей хранятся отдельно от ключей шифрования данных.</p>			
	<p><b>3.5.2.b</b> Определить места хранения ключей и убедиться, что они хранятся только в строго определенных защищенных хранилищах и строго определенном виде.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>3.6</b> Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе:  <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 <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>).</i>	<b>3.6.a</b> Проверить наличие процедур управления ключами шифрования данных о держателях карт.			
	<b>3.6.b</b> Только для поставщиков услуг: Убедиться, что поставщики услуг при предоставлении клиентам ключей шифрования для передачи или хранения данных о держателях карт также предоставляют документацию по условиям их безопасной передачи, хранения и обработки, в соответствии с требованиями 3.6.1-3.6.8, приведенными ниже.			
	<b>3.6.c</b> Изучить процедуры управления ключами и выполнить следующие проверки:			
<b>3.6.1</b> Генерация стойких ключей.	<b>3.6.1</b> Убедиться, что процедуры управления ключами обеспечивают генерацию стойких ключей.			
<b>3.6.2</b> Безопасное распространение ключей.	<b>3.6.2</b> Убедиться, что процедуры управления ключами обеспечивают безопасное распространение ключей.			
<b>3.6.3</b> Безопасное хранение ключей.	<b>3.6.3</b> Убедиться, что процедуры управления ключами обеспечивают безопасное хранение ключей.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>3.6.4</b> Смена ключей шифрования, криптопериод которых истек (например, когда истек установленный срок, и/или когда данным ключом было зашифровано некоторое количество криптотекста), основана на передовых практических методах индустрии безопасности и руководствах (например, специальное издание 800-57 NIST) и должна производиться согласно предписаниям соответствующего производителя или владельца ключа.	<b>3.6.4</b> Убедиться, что внедренные процедуры управления ключами обеспечивают их периодическое изменение по завершении установленного криптопериода ключей.			
<b>3.6.5</b> Изъятие или смена ключей (например, архивация, уничтожение или/и аннуляция) при нарушении его целостности	<b>3.6.5.a</b> Убедиться, что процедуры управления ключами обеспечивают изъятие из обращения старых ключей (архивацию, уничтожение, отзыв).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>(например, увольнение сотрудника, обладающего информацией об открытом коде ключа), а также ключей, относительно которых существуют подозрения в их компрометации.</p> <p><i>Примечание: Если существует необходимость сохранения изъятых или замененных ключей, они должны быть надежно заархивированы (например, посредством ключа шифрования ключей). Помещенные в архив криптографические ключи должны использоваться только в целях дешифрования/ верификации.</i></p>	<p><b>3.6.5.b</b> Убедиться, что процедуры управления ключами обеспечивают изменение скомпрометированных ключей, а также ключей, относительно которых существуют подозрения в их компрометации.</p>			
<p><b>3.6.6</b> Если процедуры управления криптографическими ключами в открытом виде осуществляются вручную, данные процедуры должны управляться с использованием раздельного знания и двойного контроля (например, таким образом, чтобы для расшифровки данных требовался составной ключ, компоненты которого хранятся у 2-3 сотрудников).</p> <p><i>Примечание: Примеры процедур управления ключами включают (но не ограничиваются): генерацию ключа, его передачу, загрузку в устройство, хранение и уничтожение.</i></p>	<p><b>3.6.6</b> Убедиться, что процедуры управления ключами в открытом виде обеспечивают раздельное владение частями ключей.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>3.6.7</b> Защита от неавторизованной смены ключа.	<b>3.6.7</b> Убедиться, что процедуры управления ключами обеспечивают защиту от неавторизованного изменения ключа.			
<b>3.6.8</b> Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с официальным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности.	<b>3.6.8</b> Убедиться, что внедренные процедуры управления ключами обеспечивают согласие (в письменном или электронном виде) 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><b>4.1</b> Для защиты данных о держателях карт во время передачи их через общедоступные сети следует использовать стойкие криптографические алгоритмы и безопасные протоколы (например, такие как SSL/TLS, IPSEC, SSH и т.д.).</p> <p><i>Примерами общедоступных сетей, на которые распространяются требования PCI DSS, могут служить:</i></p> <ul style="list-style-type: none"> <li>▪ Интернет;</li> <li>▪ Беспроводные технологии;</li> <li>▪ GSM;</li> <li>▪ GPRS.</li> </ul>	<p><b>4.1</b> Проверить использование протоколов безопасности в случае передачи данных о держателях карт через общедоступные сети. Убедиться, что во время передачи данных используются стойкие криптографические алгоритмы следующим образом:</p>			
	<p><b>4.1.a</b> Выбрать несколько входящих транзакций и проверить, что данные о держателях карт передаются в зашифрованном виде.</p>			
	<p><b>4.1.b</b> Убедиться, что принимаются только доверенные ключи и сертификаты.</p>			
	<p><b>4.1.c</b> Убедиться, что протокол использует только безопасные конфигурации и не поддерживает незащищенные версии или конфигурации.</p>			
	<p><b>4.1.d</b> Проверить, что для шифрования данных применяются стойкие алгоритмы (учесть рекомендации производителя и наиболее прогрессивные методы).</p>			
<p><b>4.1.e</b> Для внедрения протоколов SSL/TLS необходимо:</p> <ul style="list-style-type: none"> <li>- Проверить, что строка URL содержит HTTPS;</li> <li>- Проверить, что данные о держателях карт не передаются, когда URL не содержит HTTPS.</li> </ul>				

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>4.1.1</b> При использовании беспроводных сетей, передающих данные о держателях карт либо подключенных к среде данных о держателях карт, следует использовать передовые практические методы индустрии безопасности (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных.</p> <p><i>Примечание: Использование протокола WEP в качестве протокола безопасности запрещено с 30 июня 2010 г.</i></p>	<p><b>4.1.1</b> Для беспроводных сетей, передающих данные о держателях карт либо подключенных к среде данных о держателях карт, проверить, используются ли передовые практические методы и стандарты индустрии безопасности (например, IEEE 802.11i) по обеспечению стойкого шифрования при аутентификации и передаче данных.</p>			
<p><b>4.2</b> Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты и т.д.).</p>	<p><b>4.2.a</b> Проверить, что PAN передается в нечитаемом виде или защищен посредством стойких криптографических механизмов защиты при использовании пользовательских технологий передачи сообщений.</p>			
	<p><b>4.2.b</b> Проверить наличие политики, запрещающей отправку незашифрованного PAN при помощи пользовательских 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
<b>5.1</b> Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).	<b>5.1</b> Для нескольких системных компонентов, включая все типы операционных систем, подверженных воздействию вирусов, проверить, что используется антивирусная защита (если подходящая антивирусная технология существует).			
<b>5.1.1</b> Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.	<b>5.1.1</b> Для нескольких системных компонентов проверить, что антивирусное программное обеспечение обеспечивает защиту от всех известных форм вредоносного программного обеспечения, включая шпионские и рекламные программы.			
<b>5.2</b> Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий.	<b>5.2</b> Проверить, что антивирусные механизмы актуальны, постоянно включены и ведут журналы протоколирования событий, а именно:			
	<b>5.2.a</b> Изучить политику и убедиться, что она регламентирует регулярное обновление антивирусного программного обеспечения и антивирусных баз.			
	<b>5.2.b</b> Убедиться, что в установочном образе используемых систем включено автоматическое обновление и регулярное сканирование.			
	<b>5.2.c</b> 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
	<b>5.2.d</b> 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
<b>6.1</b> На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем. Критичные 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. Например, для более приоритетных критичных приложений (общедоступные устройства и системы, базы данных) убедиться, что срок установки обновлений не превышает одного месяца, для менее критичных внутренних устройств – три месяца.</i>	<b>6.1.a</b> Для нескольких системных компонентов и программного обеспечения проверить, установлены ли актуальные обновления безопасности, выпущенные производителем.			
	<b>6.1.b</b> Изучить политики, убедиться, что они регламентируют установку всех критичных обновлений безопасности в течение одного месяца.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>6.2</b> Должен быть внедрен процесс выявления и определения вновь обнаруженных уязвимостей по уровню риска.</p> <p><i>Примечание:</i></p> <ul style="list-style-type: none"> <li>▪ <i>Ранжирование рисков должно быть основано на передовых методах индустрии безопасности. Например, к уязвимостям высокого риска относятся те, которые имеют уровень 4.0 и выше по шкале CVSS, и/или те из них, для закрытия которых производитель выпустил обновление категории «критическое» и/или уязвимости, поражающие критичные компоненты системы;</i></li> <li>▪ <i>До 30 июня 2012 года ранжирование уязвимостей по уровню риска, как определено в п.п. 6.2, носит рекомендательный характер, а после этой даты становится обязательным требованием.</i></li> </ul>	<p><b>6.2.a</b> Опросить ответственных лиц, убедиться, что в компании внедрены процессы выявления новых уязвимостей, и что обнаруженные уязвимости ранжируются по уровню связанного с ними риска. Как минимум, самые критичные уязвимости с высоким уровнем риска должны иметь отметку «Высокий (уровень критичности)».</p> <p><b>6.2.b</b> Убедиться, что процессы выявления новых уязвимостей включают в себя использование для этого внешних источников информации.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>6.3</b> Приложения (внутренние и внешние и включительно сетевой административный доступ к приложениям) должны разрабатываться в соответствии с требованиями PCI DSS (например, безопасная аутентификация и регистрация событий). Разработка приложений должна быть основана на передовых практических методах индустрии безопасности и принимать во внимание информационную безопасность в течение всего цикла разработки, в том числе:</p>	<p><b>6.3.a</b> Изучить документацию по разработке программного обеспечения и убедиться, что процесс разработки программного обеспечения основан на передовых практических методах или/и стандартах индустрии безопасности.</p>			
	<p><b>6.3.b</b> Изучить документацию по разработке программного обеспечения и убедиться, что она принимает во внимание информационную безопасность в течение всего цикла разработки.</p>			
	<p><b>6.3.c</b> Изучить документацию по разработке программного обеспечения и убедиться, что разработка программных приложений учитывает требования стандарта PCI DSS.</p>			
	<p><b>6.3.d</b> Путем изучения документации, опроса разработчиков программного обеспечения, а также иных наблюдений, проверить следующее:</p>			
<p><b>6.3.1</b> Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчиком или переводом его в производственный режим</p>	<p><b>6.3.1</b> Убедиться в том, что все индивидуальные учетные записи, имена пользователей и пароли удаляются перед передачей программного обеспечения заказчиком или переводом его в производственный режим.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>6.3.2</b> Программный код приложений должен быть исследован на наличие потенциальных уязвимостей перед передачей готовых приложений заказчиком или переводом их в производственный режим.</p> <p><i>Примечание: данное требование применимо ко всем разрабатываемым приложениям (как внутренним, так и общедоступным) как элемент обеспечения безопасности цикла разработки. 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><b>6.3.2.a</b> Изучить политики и убедиться, что они регламентируют необходимость анализа изменений программного кода всех внутренних приложений (автоматически, либо вручную) следующим образом:</p> <ul style="list-style-type: none"> <li>▪ Изменения программного кода анализируются сотрудниками, не принимавшими участие в его написании и знакомыми с методами безопасного программирования;</li> <li>▪ Анализ программного кода обеспечивает его разработку в соответствии с основными принципами безопасного кодирования (см. Требование 6.5 PCI DSS);</li> <li>▪ Все необходимые корректировки вносятся до выпуска программного обеспечения;</li> <li>▪ Результаты анализа программного кода проверяются и утверждаются руководством до выпуска программного обеспечения.</li> </ul> <p><b>6.3.2.b</b> Для нескольких недавних изменений приложений проверить, что программный код был проанализирован согласно требованию 6.3.2.a, представленному выше.</p>			
<p><b>6.4</b> Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов, включающие в себя:</p>	<p><b>6.4</b> Путем изучения процедур управления изменениями, опроса системных и сетевых администраторов, а также анализа соответствующих данных (документация по сетевой конфигурации, данные разработки и тестирования и пр.) убедиться в следующем:</p>			
<p><b>6.4.1</b> Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга.</p>	<p><b>6.4.1</b> Убедиться в том, что среды разработки, тестирования и производственного функционирования программного обеспечения отделены друг от друга, и при этом внедрены механизмы разграничения доступа.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>6.4.2</b> Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть разделены.	<b>6.4.2</b> Убедиться в том, что обязанности по разработке, тестированию и производственному функционированию программного обеспечения разделены.			
<b>6.4.3</b> Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.	<b>6.4.3</b> Убедиться в том, что производственные данные (действующие PAN) не используются для тестирования и разработки.			
<b>6.4.4</b> Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.	<b>6.4.4</b> Убедиться в том, что все тестовые данные и платежные счета удаляются из системы перед переводом ее в производственный режим.			
<b>6.4.5</b> Все обновления безопасности и изменения в конфигурации должны быть протестированы перед внедрением; тестирование должно включать в себя:	<b>6.4.5.a</b> Убедиться, что процедуры управления изменениями, относящиеся к обновлениям безопасности и изменениям в конфигурации, документированы и требуют выполнения представленных ниже п.п. 6.4.5.1 – 6.4.5.4.			
	<b>6.4.5.b</b> Для нескольких системных компонентов и нескольких изменений/обновлений изучить записи процедур управления изменениями. Для каждого изменения выполнить следующие проверки:			
<b>6.4.5.1</b> Документирование влияния изменения на систему.	<b>6.4.5.1</b> Убедиться, что влияние изменения на систему документировано для каждого из выбранных изменений.			
<b>6.4.5.2</b> Согласование изменения с руководством.	<b>6.4.5.2</b> Убедиться, что изменение было согласовано уполномоченными лицами.			
<b>6.4.5.3</b> Тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятное воздействие на безопасность системы.	<b>6.4.5.3.a</b> Для каждого изменения проверить, что производственная функциональность была протестирована, чтобы убедиться, что внесенные изменения не оказывают неблагоприятное воздействие на безопасность системы.			
	<b>6.4.5.3.b</b> Для изменений программного кода убедиться, что все обновления протестированы на соответствие требованию 6.5 PCI DSS перед их запуском в производственный режим.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>6.4.5.4</b> Процедуру отмены изменения.	<b>6.4.5.4</b> Убедиться, что предусмотрена процедура отмены для каждого изменения.			
<b>6.5</b> Разработка приложений должна проходить в соответствии с основными принципами безопасного программирования. Процесс разработки приложений должен предупреждать возникновение общеизвестных уязвимостей программного кода, и включать следующее:  <i>Примечание: Уязвимости, перечисленные в требованиях 6.5.1 – 6.5.9 соответствовали передовым практическим методам индустрии безопасности, когда была опубликована данная версия стандарта PCI DSS. В случае обновления передовых практических методов индустрии безопасности (таких как, руководство OWASP, SANS CWE Top 25, CERT Secure Coding и т.д.) для данных требований следует использовать их актуальную версию.</i>	<b>6.5.a</b> Проверить процесс разработки приложений. Убедиться, что разработчики обязаны проходить обучение технике безопасного программирования, и что разработка веб-приложений осуществляется в соответствии с передовыми практическими методами и руководствами индустрии безопасности.			
	<b>6.5.b</b> Опросить несколько разработчиков программного обеспечения и убедиться, что они знакомы с техникой безопасного программирования.			
	<b>6.5.c</b> Убедиться, что при разработке приложений уделяется внимание защите по меньшей мере от таких уязвимостей, как:			
<b>6.5.1</b> Инъекции, в особенности, SQL-инъекции. Также следует учесть OS Command, LDAP и Xpath инъекции.	<b>6.5.1</b> Инъекции, в особенности, SQL-инъекции (необходима проверка того, что введенная пользователями информация не может изменить существующие команды и запросы, использовать параметризованные запросы и т.д.).			
<b>6.5.2</b> Переполнение буфера.	<b>6.5.2</b> Переполнение буфера (убедиться в наличии границ буфера и усечения стоки ввода).			
<b>6.5.3</b> Небезопасное криптографическое хранилище.	<b>6.5.3</b> Небезопасное криптографическое хранилище (необходима защита от криптографических ошибок).			
<b>6.5.4</b> Небезопасная передача данных.	<b>6.5.4</b> Небезопасная передача данных (необходимо шифрование всех критичных соединений и процесса аутентификации).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>6.5.5</b> Некорректная обработка ошибок.	<b>6.5.5</b> Некорректная обработка ошибок (необходимо не допускать утечки данных через сообщения об ошибках).			
<b>6.5.6</b> Все уязвимости, имеющие «Высокую» степень риска, найденные в процессе обнаружения уязвимостей (в соответствии с требованием 6.2 PCI DSS).  <i>Примечание: До 30 июня 2012 г. данное требование носит рекомендательный характер, а после этой даты становится обязательным требованием.</i>	<b>6.5.6</b> Все уязвимости, отмеченные «Высокой» степенью риска в соответствии с требованием 6.2 PCI DSS.			
<i>Примечание: Требования 6.5.7-6.5.9, приведенные ниже, распространяются на веб-приложения и интерфейсы приложений (внешние или внутренние):</i>				
<b>6.5.7</b> Межсайтовый скриптинг (XSS).	<b>6.5.7</b> Межсайтовый скриптинг (XSS) (необходимо проверить все параметры перед их включением в код, использовать контекстно-зависимое экранирование и т.п.)			
<b>6.5.8</b> Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий).	<b>6.5.8</b> Ошибки в контроле доступа, такие как небезопасные прямые ссылки на объект, невозможность ограничения доступа по URL и обход директорий (необходимо надлежащим образом аутентифицировать пользователей и удалять входные данные. Пользователям не должны предоставляться прямые ссылки на внутренние объекты).			
<b>6.5.9</b> Подделка межсайтовых запросов (CSRF).	<b>6.5.9</b> Подделка межсайтовых запросов (CSRF) (автоматические запросы браузеров о данных учетной записи и идентификаторах должны игнорироваться).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>6.6</b> Следует обеспечить защиту общедоступных веб-приложений от известных атак (а также регулярно учитывать новые угрозы и уязвимости) одним из следующих методов:</p> <ul style="list-style-type: none"> <li>▪ Проверять приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности приложений не реже одного раза в год, а также после внесения изменений.</li> <li>▪ Установить межсетевой экран прикладного уровня перед веб-ориентированными приложениями.</li> </ul>	<p><b>6.6</b> Для общедоступных веб-приложений проверить выполнение одного из следующих требований:</p> <ul style="list-style-type: none"> <li>▪ Убедиться, что анализ (с использованием методов ручного или автоматического анализа защищенности приложений) общедоступных веб-приложений проходит следующим образом:               <ul style="list-style-type: none"> <li>– не реже одного раза в год;</li> <li>– после любых изменений;</li> <li>– организацией, которая специализируется на безопасности приложений;</li> <li>– все уязвимости устраняются;</li> <li>– безопасность приложения анализируется повторно после принятия корректирующих действий.</li> </ul> </li> <li>▪ Убедиться, что перед общедоступным веб-приложением установлен межсетевой экран прикладного уровня (web application firewall) для обнаружения и предупреждения веб-ориентированных атак.</li> </ul> <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 уполномоченными лицами заявки о предоставлении прав доступа.	7.1.3 Авторизации подлежат все виды доступа; заявка о предоставлении доступа подлежит документальному согласию (в рукописной или электронной форме) уполномоченных лиц и детально описывает необходимые привилегии.			
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
<b>7.2</b> Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания и применяющий принцип «запрещено все, что явно не разрешено». Механизм контроля доступа должен включать следующее:	<b>7.2</b> Изучить настройки системы и документацию изготовителя, убедиться, что система контроля доступа включает в себя:			
<b>7.2.1</b> Покрытие всех системных компонентов.	<b>7.2.1</b> Подтвердить, что система контроля доступа внедрена на всех системных компонентах.			
<b>7.2.2</b> Назначение привилегий пользователям должно быть основано на их должностных обязанностях.	<b>7.2.2</b> Назначение привилегий пользователям основано на их должностных обязанностях.			
<b>7.2.3</b> По-умолчанию должен быть запрещен любой доступ.  <i>Примечание: Некоторые механизмы контроля доступа применяют правило «разрешить все» по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.</i>	<b>7.2.3</b> Запрещение любого доступа по умолчанию.			

### **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.

*Примечание: Данные требования применимы ко всем учетным записям, включая учетные записи на терминалах оплаты, имеющие административные полномочия, и все учетные записи, использующиеся для просмотра или доступа к данным о держателях карт или системам, содержащим данные о держателях карт. Однако, требования 8.1, 8.2 и 8.5.8-8.5.15 не относятся к учетным записям пользователей терминальных платежных приложений (например, кассовых приложений), которые обладают единовременным доступом только к одному номеру карты для проведения единой транзакции.*

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>8.1</b> Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.</p>	<p><b>8.1</b> Убедиться, что каждому пользователю назначен уникальный идентификатор для доступа к компонентам системы или данным о держателях карт.</p>			
<p><b>8.2</b> Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей:</p> <ul style="list-style-type: none"> <li>▪ То, что вы знаете (пароль и парольная фраза).</li> <li>▪ То, что у вас есть (ключи или смарт-карты).</li> <li>▪ То, что вы есть (биометрические параметры).</li> </ul>	<p><b>8.2</b> Проверить, что для аутентификации пользователей помимо уникального идентификатора применяются дополнительные механизмы аутентификации (например, пароль) для доступа к среде данных о держателях карт:</p> <ul style="list-style-type: none"> <li>▪ изучить документацию, описывающую метод(ы) аутентификации;</li> <li>▪ для каждого типа метода аутентификации и каждого типа системного компонента проверить, что метод аутентификации работает в соответствии с документацией.</li> </ul>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>8.3</b> 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 с ключами; системы контроля доступа контроллера терминального доступа TACACS с ключами и прочие технологии, способствующие двухфакторной аутентификации.</p> <p><i>Примечание: Двухфакторная аутентификация требует, чтобы для аутентификации использовались два из трех методов аутентификации (описание методов аутентификации см. в Требовании 8.2). Использование одного метода дважды (например, использование двух различных паролей) не считается двухфакторной аутентификацией.</i></p>	<p><b>8.3</b> Убедиться в использовании двухфакторной аутентификации при удаленном доступе сотрудников путем наблюдения за подключающимся удаленно к внутренней сети сотрудником (например, администратором сети) и удостовериться, что используются два из трех методов аутентификации.</p>			
<p><b>8.4</b> Все пароли должны храниться и передаваться только в зашифрованном виде с использованием стойких криптографических алгоритмов.</p>	<p><b>8.4.a</b> Для нескольких системных компонентов изучить файлы паролей и убедиться в том, что пароли нечитаемы при передаче и хранении.</p> <p><b>8.4.b</b> Для поставщиков услуг: изучить файлы паролей, убедиться в том, что клиентские пароли зашифрованы.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>8.5</b> Должен быть установлен контроль над выполнением процедур идентификации и аутентификации пользователей и управления паролями учетных записей сотрудников и администраторов на всех системных компонентах, включающий в себя:	<b>8.5</b> Изучить процедуры и опросить сотрудников, убедиться в том, что процедуры идентификации и аутентификации пользователей и управления паролями учетных записей соответствуют следующим требованиям:			
<b>8.5.1</b> Контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации.	<b>8.5.1</b> 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"> <li>▪ изучить заявку на предоставление доступа для каждой выбранной учетной записи;</li> <li>▪ 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.</li> </ul>			
<b>8.5.2</b> Проверку подлинности пользователя перед сменой пароля.	<b>8.5.2</b> Изучить парольные процедуры и процедуры аутентификации и убедиться в том, что пользователь проходит проверку подлинности перед сменой пароля по телефону, электронной почте, с использованием веб-приложения или иным удаленным способом.			
<b>8.5.3</b> Установку уникального первоначального пароля для каждого пользователя и его немедленное изменение при первом входе пользователя.	<b>8.5.3</b> Изучить парольные процедуры и убедиться в том, что для первого входа в систему новому пользователю устанавливается, а для существующих пользователей преустанавливается, уникальный первоначальный пароль, который изменяется при первом входе в систему.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>8.5.4</b> Немедленный отзыв доступа при увольнении пользователя.	<b>8.5.4</b> Выбрать несколько уволенных за прошедшие шесть месяцев сотрудников и проанализировать списки контроля доступа, убедиться в том, что их учетные записи заблокированы и удалены.			
<b>8.5.5</b> Удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней.	<b>8.5.5</b> Убедиться в том, что неактивные более 90 дней учетные записи удаляются или блокируются.			
<b>8.5.6</b> Включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ. Отслеживать удаленные учетные записи, используемые поставщиками, во время работ.	<b>8.5.6.a</b> Убедиться в том, что любые учетные записи, используемые поставщиками для доступа, удаленной поддержки и обслуживанию системных компонентов, заблокированы и активируются только на время выполнения работ.			
	<b>8.5.6.b</b> Убедиться, что во время выполнения работ удаленные учетные записи, используемые поставщиками, контролируются.			
<b>8.5.7</b> Доведение правил и процедур аутентификации до всех пользователей, имеющих доступ к данным о держателях карт.	<b>8.5.7</b> Опросить несколько пользователей, убедиться в том, что им известны положения аутентификационных политик и процедур.			
<b>8.5.8</b> Запрет использования групповых, разделяемых и стандартных учетных записей и паролей и прочих методов аутентификации.	<b>8.5.8.a</b> Для нескольких системных компонентов проверить списки учетных записей пользователей и проверить следующее: <ul style="list-style-type: none"> <li>▪ стандартные учетные записи заблокированы или удалены;</li> <li>▪ разделяемые учетные записи для функций администрирования и иных критичных функций не существуют;</li> <li>▪ разделяемые и стандартные учетные записи не используются для администрирования каких-либо системных компонентов.</li> </ul>			
	<b>8.5.8.b</b> Изучить парольные политики и процедуры, убедиться, что они запрещают использование групповых и разделяемых паролей и прочих методов аутентификации.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	<b>8.5.8.с</b> Опросить системных администраторов, убедиться в том, что пользователям не выдаются групповые и разделяемые пароли и прочие методы аутентификации, даже если таковые запрашиваются.			
<b>8.5.9</b> Изменение пароля пользователя не реже одного раза в 90 дней.	<b>8.5.9.а</b> Для нескольких системных компонентов проверить настройки и убедиться в том, что пользователь должен менять пароль не реже одного раза в 90 дней.			
	<b>8.5.9.б</b> Только для поставщиков услуг: изучить внутренние процессы и клиентскую/пользовательскую документацию, убедиться в том, что неклиентские пароли должны меняться регулярно и у них 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.	8.5.10.а Для нескольких системных компонентов проверить настройки и убедиться в том, что длина пароля не менее семи символов.			

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>8.5.14</b> Установку периода блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором.	<b>8.5.14</b> 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.			
<b>8.5.15</b> Блокировку рабочей сессии пользователя через 15 минут простоя с требованием ввода пароля для разблокировки, повторной активации терминала или сессии.	<b>8.5.15</b> Для нескольких системных компонентов проверить настройки и убедиться в том, что рабочая сессия пользователя блокируется не более чем через 15 минут простоя.			
<b>8.5.16</b> 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.  Разрешение запросов и прямого доступа к базам данных только для администраторов баз данных.	<b>8.5.16.a</b> Проанализировать настройки баз данных и приложений, проверить, что пользователи проходят аутентификацию перед предоставлением доступа.			
	<b>8.5.16.b</b> Убедиться, что настройки баз данных и приложений обеспечивают осуществление пользовательских операций с данными (доступ, запрос, перемещение, копирование, удаление) только программными методами (например, через хранимые процедуры).			
	<b>8.5.16.c</b> Убедиться, что настройки баз данных и приложений разрешают запросы и прямой доступ к базам данных только для администраторов баз данных.			
	<b>8.5.16.d</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

Любой физический доступ к данным или 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. Согласно Требованию 9, к понятию «персонал» относятся постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании. Под термином «посетитель» понимаются поставщики, гости сотрудников, сервисный персонал и иные люди, кратковременно находящиеся на объекте, как правило, не более одного дня. Термин «носитель данных» включает в себя бумажные или электронные носители, хранящие данные о держателях карт.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>9.1</b> 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><b>9.1</b> 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"> <li>▪ убедиться, что доступ контролируется при помощи персональных карт или иных устройств, в том числе механических замков;</li> <li>▪ 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.</li> </ul>			
<b>9.1.1</b> Следует использовать камеры видеонаблюдения или иные механизмы контроля доступа, чтобы следить за критическими местами. Данные, собранные механизмами контроля доступа, должны	<p><b>9.1.1.a</b> Убедиться в том, что камеры видеонаблюдения и/или иные механизмы контроля доступа применяются для мониторинга доступа к критическим помещениям/выхода из критических помещений.</p> <p><b>9.1.1.b</b> Убедиться, что камеры и/или иные средства защищены от взлома или отключения.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p>анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством.</p> <p><i>Примечание: Критичными являются места, относящиеся к любому дата-центру, серверной комнате или иному помещению, в котором расположены системы, хранящие, обрабатывающие или передающие данные о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов.</i></p>	<p><b>9.1.1.с</b> Убедиться в том, что данные с камер видеонаблюдения и/или иных механизмов контроля доступа хранятся не менее трех месяцев.</p>			
<p><b>9.1.2</b> Доступ к сетевым разъемам, расположенным в общедоступных местах, должен быть ограничен. Например, посещаемые помещения не должны иметь действующих сетевых портов, если сетевой доступ не является однозначно авторизованным.</p>	<p><b>9.1.2</b> Опросить администраторов и изучить сетевые разъемы, чтобы убедиться в том, что сетевые разъемы включены только в случае, если они необходимы авторизованному персоналу организации. Проверить, что исключено наличие персонала без сопровождения в помещениях с активными сетевыми разъемами.</p>			
<p><b>9.1.3</b> Доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи должен быть ограничен.</p>	<p><b>9.1.3</b> Убедиться, что физический доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи должным образом ограничен.</p>			

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

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>9.3.3</b> Возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении срока его действия.	<b>9.3.3</b> Ознакомится с процессом ухода посетителями с территории компании, убедиться, что от посетителей требуется возврат пропуска при уходе либо окончании срока действия.			
<b>9.4</b> Следует вести журнал учета посетителей и использовать его для анализа посещений. В журнале следует регистрировать имя посетителя, организацию, которую он представляет, а также сотрудника организации, разрешившего доступ посетителю. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством.	<b>9.4.a</b> 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.			
	<b>9.4.b</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.			
<b>9.5</b> 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.	<b>9.5.a</b> Необходимо соблюдать физическую безопасность мест хранения, чтобы убедиться в безопасности мест хранения резервных копий.			
	<b>9.5.b</b> Убедиться в том, что безопасность мест хранения резервных копий проверяется не реже одного раза в год.			
<b>9.6</b> Должна быть обеспечена физическая безопасность всех видов носителей.	<b>9.6</b> Проверить, что процедуры физической защиты данных о держателях карт включают меры по защите всех видов носителей (например, компьютеров, съемных электронных носителей, бумажных счетов, бумажные отчетов и факсов).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>9.7</b> Должен быть обеспечен строгий контроль над передачей всех видов носителей информации, включающий:	<b>9.7</b> Убедиться в наличии политики, регламентирующей порядок передачи всех видов носителей информации, а также распространение носителей информации среди отдельных лиц.			
<b>9.7.1</b> Классификацию носителей информации для определения уровня критичности хранимых данных.	<b>9.7.1</b> Убедиться в том, что носители информации классифицированы для определения уровня критичности хранимых данных.			
<b>9.7.2</b> Пересылку носителей только с доверенным курьером, или иным способом, который может быть тщательно проконтролирован.	<b>9.7.2</b> 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.			
<b>9.8</b> Должна быть внедрена процедура разрешения руководством выноса за пределы охраняемой территории носителей (особенно при передаче носителя частным лицам).	<b>9.8</b> Для нескольких случаев выноса носителя, зарегистрированных в журнале за несколько дней, проверить детальные обстоятельства выноса и наличие согласования выноса с руководством.			
<b>9.9</b> Должен быть обеспечен строгий контроль хранения носителей, и управление доступом к ним.	<b>9.9</b> Изучить политику хранения носителей, убедиться в том, что она регламентирует регулярную инвентаризацию носителей.			
<b>9.9.1</b> Должны поддерживаться в актуальном состоянии журналы инвентаризации всех носителей данных о держателях карт; инвентаризация носителей должна проводиться не реже одного раза в год.	<b>9.9.1</b> Убедиться, что инвентаризация носителей проводится не реже одного раза в год.			
<b>9.10</b> Носители, содержащие данные о держателях карт, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, должны быть уничтожены следующими способами:	<b>9.10</b> 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
<b>9.10.1</b> Измельчение, сжигание или растворение бумажного носителя, чтобы данные о держателях карт не могли быть восстановлены.	<b>9.10.1.a</b> Убедиться, что твердые копии документов измельчаются, сжигаются или растворяются способом, исключающим их восстановление.			
	<b>9.10.1.b</b> Осмотреть хранилище документов, приготовленных для уничтожения, убедиться, что доступ к таким документам ограничен.			
<b>9.10.2</b> Уничтожение данных о держателях карт на электронном носителе, исключающее возможность их восстановления.	<b>9.10.2</b> 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
<b>10.1</b> Должен быть разработан процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам.	<b>10.1</b> Опросить системного администратора и проверить, что ведутся журналы протоколирования событий системных компонентов.			
<b>10.2</b> Для каждого системного компонента должен быть включен механизм протоколирования следующих событий:	<b>10.2</b> Методом интервью, изучения журналов протоколирования событий и настроек систем протоколирования осуществить следующие проверки:			
<b>10.2.1</b> Любой доступ пользователя к данным о держателях карт.	<b>10.2.1</b> Убедиться в том, что факты доступа пользователя к данным о держателях карт регистрируются.			
<b>10.2.2</b> Любые действия, совершенные с использованием административных полномочий.	<b>10.2.2</b> Убедиться в том, что любые действия, совершенные с использованием административных полномочий, регистрируются.			
<b>10.2.3</b> Любой доступ к записям о событиях в системе.	<b>10.2.3</b> Убедиться в том, что факты доступа к записям о событиях в системе регистрируются.			
<b>10.2.4</b> Неуспешные попытки логического доступа.	<b>10.2.4</b> Убедиться в том, что неуспешные попытки логического доступа регистрируются.			
<b>10.2.5</b> Использование механизмов идентификации и аутентификации.	<b>10.2.5</b> Убедиться в том, что регистрируются факты использования механизмов идентификации и аутентификации.			
<b>10.2.6</b> Инициализация журналов протоколирования событий.	<b>10.2.6</b> Убедиться в том, что регистрируются факты инициализации журналов протоколирования событий.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>10.2.7</b> Создание и удаление объектов системного уровня.	<b>10.2.7</b> Убедиться в том, что регистрируются факты создания и удаления объектов системного уровня.			
<b>10.3</b> Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры:	<b>10.3</b> Убедиться, что для каждого протоколируемого события регистрируются следующие параметры:			
<b>10.3.1</b> Идентификатор пользователя.	<b>10.3.1</b> Идентификатор пользователя.			
<b>10.3.2</b> Тип события.	<b>10.3.2</b> Тип события.			
<b>10.3.3</b> Дата и время.	<b>10.3.3</b> Дата и время.			
<b>10.3.4</b> Успешным или неуспешным было событие.	<b>10.3.4</b> Успешным или неуспешным было событие.			
<b>10.3.5</b> Источник события.	<b>10.3.5</b> Источник события.			
<b>10.3.6</b> Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.	<b>10.3.6</b> Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.			
<b>10.4</b> Необходимо использовать технологию синхронизации времени. Все системные часы и системное время на критичных системах должны быть синхронизированы, Необходимо убедиться в исполнении данного требования для получения, распространения и хранения данных о времени.  <i>Примечание: Примером технологии синхронизации времени является Протокол синхронизации времени (Network Time Protocol).</i>	<b>10.4.a</b> Для синхронизации часов используется технология синхронизации времени, удовлетворяющая требованиям 6.1 и 6.2 стандарта PCI DSS.			
	<b>10.4.b</b> Проанализировать процесс получения, распространения и хранения точного времени в организации, равно как и связанные с этим конфигурационные параметры для выборки системных компонентов. Убедиться, что в процесс включены и выполнены следующие требования:			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>10.4.1</b> На критичных системах установлено точное и согласованное время.	<b>10.4.1.a</b> Убедиться, что только назначенные центральные серверы времени получают информацию о времени из внешних источников, а данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC). <b>10.4.1.b</b> Убедиться в том, что точное время на назначенных центральных серверах времени совпадает, и только от них поступает информация о времени на другие внутренние серверы.			
<b>10.4.2</b> Данные о времени защищены.	<b>10.4.2.a</b> Проверить конфигурацию системы и настройки синхронизации времени и убедиться, что доступ к данным о времени разрешен только персоналу, имеющему служебную необходимость. <b>10.4.2.b</b> Проверить конфигурацию системы, настройки и процессы синхронизации времени и убедиться, что любые изменения в настройках времени на критичных системах отслеживаются, контролируются и регистрируются.			
<b>10.4.3</b> Получение настроек времени происходит из признанных индустрией безопасности источников.	<b>10.4.3</b> Убедиться, что временные серверы принимают обновления времени от специализированных, признанных индустрией безопасности, внутренних источников (чтобы предотвратить смену времени злоумышленником). Данные обновления могут быть дополнительно зашифрованы симметричным ключом и списками контроля доступа, определяющими IP-адреса машин, которым разрешено получать обновления времени (чтобы предупредить неавторизованное использование внутренних серверов времени).			
<b>10.5</b> Журналы протоколирования событий должны быть защищены от изменений.	<b>10.5</b> Опросить системного администратора и изучить права доступа, чтобы убедиться в том, что журналы протоколирования событий защищены от изменений, в том числе:			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>10.5.1</b> Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.	<b>10.5.1</b> Убедиться в том, что доступом к журналам протоколирования событий обладают только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.			
<b>10.5.2</b> Журналы протоколирования событий должны быть защищены от неавторизованного изменения.	<b>10.5.2</b> Убедиться в том, что актуальные журналы протоколирования событий защищены от неавторизованного изменения при помощи механизмов контроля доступа, физической и/или сетевой сегментации.			
<b>10.5.3</b> Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено.	<b>10.5.3</b> Убедиться в том, что резервные копии журналов протоколирования событий оперативно сохраняются на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено.			
<b>10.5.4</b> Копии журналов протоколирования активности событий доступных извне технологий (беспроводных сетей, межсетевых экранов, DNS, почтовых систем) должны сохраняться на сервер протоколирования, находящийся внутри локальной сети.	<b>10.5.4</b> 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.			
<b>10.5.5</b> Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала).	<b>10.5.5</b> Убедиться в наличии систем контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>10.6</b> 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).</p> <p><i>Примечание: Для обеспечения соответствия Требованию 10.6 могут быть использованы средства сбора и анализа журналов регистрации событий, а также средства оповещения.</i></p>	<p><b>10.6.a</b> 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.</p> <p><b>10.6.b</b> Убедиться, что журналы протоколирования событий всех системных компонентов регулярно анализируются.</p>			
<p><b>10.7</b> 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).</p>	<p><b>10.7.a</b> Изучить политики и процедуры, проверить, что они включают в себя политику хранения журналов регистрации и регламентируют необходимость хранения журналов регистрации событий не менее одного года.</p> <p><b>10.7.b</b> Убедиться, что журналы протоколирования событий доступны в течение одного года и находятся в оперативном доступе для анализа не менее трех месяцев.</p>			

### 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	
<b>11.1</b> Следует ежеквартально проверять наличие беспроводных точек доступа и отслеживать неавторизованные беспроводные точки доступа.  <i>Примечание: Используемые процессы включают в себя, например, сканирование беспроводной сети, физическое/логическое обследование системных компонентов и инфраструктуры, контроль сетевого доступа (NAC) или беспроводные IDS/IPS. Какие бы методы не использовались, они должны быть достаточно эффективными в отслеживании и обнаружении неавторизованных беспроводных устройств.</i>	<b>11.1.a</b> Убедиться, что в организации имеется документированный процесс ежеквартального отслеживания и обнаружения беспроводных точек доступа.				
	<b>11.1.b</b> Убедиться, что применяемая методика способна отслеживать и обнаруживать любые неавторизованные беспроводные точки доступа, включая, по меньшей мере, следующее: <ul style="list-style-type: none"> <li>▪ Помещение карт WLAN внутри системных компонентов;</li> <li>▪ Подключение переносных беспроводных устройств к системным компонентам (например, посредством USB и т.п.);</li> <li>▪ Подключение беспроводных устройств к сетевому порту или устройству.</li> </ul>				
	<b>11.1.c</b> Убедиться в ежеквартальном проведении документированного процесса обнаружения неавторизованных беспроводных точек доступа для всех системных компонентов и оборудования.				
	<b>11.1.d</b> Если внедрен автоматизированный контроль (например, беспроводные IDS/IPS, контроль сетевого доступа и т.п.), убедиться, что он генерирует уведомления персоналу организации.				
	<b>11.1.e</b> Убедиться, что в политике расследования инцидентов (требование 12.9) упомянуты действия при обнаружении неавторизованного беспроводного устройства.				

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>11.2</b> Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов).</p> <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><b>11.2</b> Убедиться, что внешнее и внутреннее сканирование сети на наличие уязвимостей проводится следующим образом:</p>			
<p><b>11.2.1</b> Следует проводить ежеквартальное внутреннее сканирование сети на наличие уязвимостей.</p>	<p><b>11.2.1.a</b> Изучить отчеты о сканированиях и убедиться, что четыре последних сканирования производились в течение последних 12 месяцев.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
	<p><b>11.2.1.b</b> Изучить отчеты о сканированиях и убедиться, что процедура сканирования предусматривает повторные сканирования до тех пор, пока не будут получены положительные результаты, или срочные, критические уязвимости или уязвимости высокого уровня, определенные в требовании 6.2 PCI DSS, не будут закрыты.</p> <p><b>11.2.1.c</b> Убедиться, что сканирование проводилось квалифицированными сотрудниками компании либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или ASV не требуется).</p>			
<p><b>11.2.2</b> Следует проводить ежеквартальное внешнее сканирование на наличие уязвимостей посредством сторонней компании (ASV), сертифицированной Советом PCI SSC.</p> <p><i>Примечание: Ежеквартальное внешнее сканирование на наличие уязвимостей должно выполняться сторонней компанией (ASV), сертифицированной Советом PCI SSC. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании.</i></p>	<p><b>11.2.2.a</b> Изучить результаты четырех последних внешних сканирований на наличие уязвимостей и убедиться, что четыре последних сканирования производились ежеквартально в течение последних 12 месяцев.</p> <p><b>11.2.2.b</b> Изучить результаты каждого ежеквартального сканирования и убедиться в их соответствии требованиям Программного руководства по ASV-сканированию (ASV Program Guide) (например, уязвимости со степенью критичности выше 4.0, согласно Общей системе оценки уязвимостей (CVSS), и автоматические нарушения отсутствуют).</p> <p><b>11.2.2.c</b> Изучить отчеты о сканированиях и убедиться, что сканирование производилось компанией ASV, сертифицированной Советом PCI SSC.</p>			
<p><b>11.2.3</b> Убедиться, что внутреннее и внешнее сканирование происходит после любого крупного изменения в сети.</p>	<p><b>11.2.3.a</b> Изучить документацию по контролю изменений в сети и отчеты о сканировании и убедиться, что выполняются сканирование системных компонентов, подверженных значительным изменениям.</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>Примечание: Сканирования, проводимые после любых значительных изменений, могут производиться внутренними силами компании.</i></p>	<p><b>11.2.3.b</b> Изучить отчеты о сканировании и убедиться, что процедура сканирования предусматривает повторные сканирования до тех пор, пока:</p> <ul style="list-style-type: none"> <li>▪ для внутреннего сканирования – присутствуют уязвимости со степенью критичности выше 4.0, согласно Общей системе оценки уязвимостей (CVSS);</li> <li>▪ для внутреннего сканирования – не получены положительные результаты, или не закрыты срочные, критические уязвимости или уязвимости высокого уровня, определенные в требовании 6.2 PCI DSS.</li> </ul> <p><b>11.2.3.c</b> Проверить, что сканирование проводилось квалифицированными сотрудниками компании либо квалифицированной третьей стороной, а также убедиться в их организационной независимости (если это возможно; при этом наличие статуса QSA или ASV не требуется).</p>			
<p><b>11.3</b> 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:</p>	<p><b>11.3.a</b> 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.</p> <p><b>11.3.b</b> Убедиться в том, что выявленные уязвимости были устранены и проведен повторный тест.</p> <p><b>11.3.c</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; при этом наличие статуса QSA или ASV не требуется).</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>11.3.1</b> Тесты на проникновение сетевого уровня.	<b>11.3.1</b> 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.			
<b>11.3.2</b> Тесты на проникновение уровня приложений.	<b>11.3.2</b> Убедиться в том, что тест на проникновение включает в себя тест на проникновение на уровне приложений. Тест должен учитывать, как минимум, проверки на наличие уязвимостей, приведенных в требовании 6.5 PCI DSS.			
<b>11.4</b> Следует использовать системы обнаружения вторжений и/или системы предотвращения вторжений для контроля сетевого трафика по периметру среды данных о держателях карт и критичных точек внутри среды данных о держателях карт, а также для оповещения персонала о подозрительных действиях. Системы обнаружения и предотвращения вторжений и их сигнатуры должны поддерживаться в актуальном состоянии.	<b>11.4.a</b> Проверить, что применяются системы обнаружения и/или предотвращения вторжений, и что весь трафик по периметру среды данных о держателях карт и критичные точки в среде данных о держателях карт подлежат мониторингу.			
	<b>11.4.b</b> Убедиться в том, что системы IDS и/или IPS оповещают сотрудников компании о подозрительной активности.			
	<b>11.4.c</b> Изучить конфигурации систем IDS/IPS и убедиться в том, что устройства IDS/IPS настроены, поддерживаются и обновляются в соответствии с рекомендациями производителя для обеспечения оптимальной защиты.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><b>11.5</b> Следует использовать средства контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных; сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю.</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 для клиентских приложений, должны быть определены самой компанией (т.е. торгово-сервисным предприятием или поставщиком услуг).</i></p>	<p><b>11.5.a</b> Убедиться в наличии и работоспособности средств контроля целостности файлов в среде данных о держателях карт путем изучения системных настроек и контролируемых файлов, а также проверки результатов мониторинга.</p> <p>Примеры файлов, подлежащих мониторингу:</p> <ul style="list-style-type: none"> <li>▪ системные исполняемые файлы;</li> <li>▪ прикладные исполняемые файлы;</li> <li>▪ конфигурационные файлы и файлы параметров;</li> <li>▪ централизованно хранимые, хронологические или архивные файлы, файлы данных аудита и журналов протоколирования событий.</li> </ul> <p><b>11.5.b</b> Убедиться, что средства контроля целостности файлов оповещают сотрудников компании о неавторизованных изменениях критичных файлов, и что сопоставительный анализ критичных файлов проводится не реже одного раза в неделю.</p>			

## Разработка политики информационной безопасности

### **Требование 12: Разработать и поддерживать политику информационной безопасности для всего персонала организации**

Строгая политика безопасности задает атмосферу безопасности для всей компании и информирует персонал организации о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите. В контексте данного требования термином «персонал» обозначаются постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании или так или иначе имеющие доступ к среде данных о держателях карт.

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>12.1</b> Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика информационной безопасности.	<b>12.1</b> Изучить политику информационной безопасности и убедиться в том, что она опубликована и распространена среди всех пользователей (включая поставщиков, подрядчиков и бизнес-партнеров).			
<b>12.1.1</b> Политика информационной безопасности должна учитывать все требования настоящего стандарта.	<b>12.1.1</b> Убедиться в том, что политика информационной безопасности учитывает все требования PCI DSS.			
<b>12.1.2</b> Политика информационной безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков. (Примеры методик оценки информационных рисков включают, например, OCTAVE, ISO 27005 и NIST SP 800-30).	<b>12.1.2.a</b> Убедиться в том, что процедура ежегодного анализа информационных рисков документирована и предусматривает обнаружение угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков. <b>12.1.2.b</b> Изучить документацию по оценке информационных рисков и убедиться в ежегодном проведении процедуры анализа информационных рисков.			
<b>12.1.3</b> Политика информационной безопасности должна пересматриваться, по меньшей мере, ежегодно и обновляться в случае изменения инфраструктуры.	<b>12.1.3</b> Убедиться в том, что политика информационной безопасности пересматривается, по меньшей мере, ежегодно 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
<b>12.2</b> Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов протоколирования событий).	<b>12.2.a</b> Изучить ежедневные процедуры безопасности. Убедиться в том, что они соответствуют требованиям настоящего стандарта и включают административные и технические процедуры по каждому требованию.			
<b>12.3</b> Должны быть разработаны правила эксплуатации для критичных технологий (таких как системы удаленного доступа, беспроводные технологии, съемные носители информации, мобильные компьютеры, планшетные компьютеры, карманные компьютеры, электронная почта и сеть Интернет), чтобы определить корректный порядок использования этих устройств. Эти правила должны включать следующее:	<b>12.3</b> Изучить правила эксплуатации критичных технологий и осуществить следующие проверки:			
<b>12.3.1</b> Процедуру явного одобрения уполномоченными лицами.	<b>12.3.1</b> Убедиться в том, что использование технологий требует утверждения уполномоченными лицами.			
<b>12.3.2</b> Аутентификацию перед использованием устройства.	<b>12.3.2</b> Убедиться в том, что перед использованием технологии пользователь должен пройти аутентификацию по имени и паролю, либо иному средству аутентификации (например, токену).			
<b>12.3.3</b> Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.	<b>12.3.3</b> Убедиться в наличии перечня используемых устройств и сотрудников, имеющих доступ к таким устройствам.			
<b>12.3.4</b> Маркировку устройств с указанием информации, которую можно связать с владельцем носителя, контактных данных и назначения.	<b>12.3.4</b> Убедиться, что правила эксплуатации регламентируют маркировку устройств с указанием информации, которую можно связать с владельцем носителя, контактных данных и назначения.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>12.3.5</b> Допустимые варианты использования устройств.	<b>12.3.5</b> Убедиться, что правила эксплуатации регламентируют допустимые варианты использования устройств.			
<b>12.3.6</b> Допустимые точки размещения устройств в сети.	<b>12.3.6</b> Убедиться, что правила эксплуатации регламентируют допустимые точки размещения устройств в сети.			
<b>12.3.7</b> Перечень одобренных компанией устройств.	<b>12.3.7</b> Убедиться в наличии перечня одобренных компанией устройств.			
<b>12.3.8</b> Автоматическое отключение сессий удаленного доступа после определенного периода простоя.	<b>12.3.8</b> Убедиться, что правила эксплуатации регламентируют автоматическое отключение сессий удаленного доступа после определенного периода простоя.			
<b>12.3.9</b> Включение механизмов удаленного доступа для производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.	<b>12.3.9</b> Убедиться, что правила эксплуатации регламентируют включение механизмов для доступа производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования.			
<b>12.3.10</b> Запрет копирования, перемещения, хранения данных о держателях карт на локальных дисках и иных съемных электронных носителях персоналу, имеющему доступ к данным о держателях карт, если предоставление этого доступа не обусловлено служебной необходимостью.	<b>12.3.10.a</b> Убедиться, что правила эксплуатации запрещают копирование, перемещение и хранение данных о держателях карт на локальных дисках и иных съемных электронных носителях при удаленном доступе к данным.			
	<b>12.3.10.b</b> Для авторизованных сотрудников убедиться, что правила эксплуатации предписывают обеспечение защиты данных о держателях карт в соответствии с требованиями стандарта PCI DSS.			
<b>12.4</b> Политика и процедуры безопасности должны однозначно определять обязанности всего персонала организации, относящиеся к информационной безопасности.	<b>12.4</b> Убедиться в том, что политики однозначно определяют обязанности всего персонала организации, относящиеся к информационной безопасности.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>12.5</b> Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:	<b>12.5</b> 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:			
<b>12.5.1</b> Разработка, документирование и распространение политики и процедур безопасности.	<b>12.5.1</b> 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
<b>12.5.2</b> Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных.	<b>12.5.2</b> 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.			
<b>12.5.3</b> Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций.	<b>12.5.3</b> Убедиться в том, что определена ответственность за разработку, документирование и распространение процедур реагирования на инциденты и процедур эскалации.			
<b>12.5.4</b> Администрирование учетных записей пользователей, включая их добавление, удаление и изменение.	<b>12.5.4</b> Убедиться в том, что определена ответственность за управление учетными записями пользователей.			
<b>12.5.5</b> Мониторинг и контроль любого доступа к данным.	<b>12.5.5</b> Убедиться в том, что определена ответственность за мониторинг и контроль доступа к данным.			
<b>12.6</b> Должна быть внедрена официальная программа повышения осведомленности персонала компании о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт.	<b>12.6.a</b> Проверить наличие формальной программы повышения осведомленности персонала о вопросах безопасности.			
	<b>12.6.b</b> Изучить программу повышения осведомленности персонала о вопросах безопасности и выполнить следующие проверки:			
<b>12.6.1</b> Обучение персонала организации должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год.	<b>12.6.1.a</b> Убедиться в том, что программа повышения осведомленности персонала использует различные методы доведения информации до персонала (плакаты, письма, заметки, системы дистанционного обучения, специальные кампании).			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<p><i>Примечание: Методики обучения могут варьироваться в зависимости от обязанностей персонала и уровня доступа к данным о держателях карт.</i></p>	<p><b>12.6.1.b</b> Убедиться в том, что персонал организации проходит обучение по вопросам информационной безопасности при приеме на работу, а также не реже одного раза в год.</p>			
<p><b>12.6.2</b> Персонал организации должен не реже одного раза в год подтверждать свое знание и понимание политики и процедур информационной безопасности организации.</p>	<p><b>12.6.2</b> Убедиться в том, что программа повышения осведомленности персонала регламентирует подтверждение персоналом их знания и понимания политики информационной безопасности организации (например, в виде теста в письменной или электронной форме).</p>			
<p><b>12.7</b> Следует тщательно проверять кандидатов (будущий персонал) при приеме на работу, для минимизации риска внутренних атак. (Примером кадровых проверок являются изучение послужного списка, изучение записей правоохранительных органов, изучение кредитной истории, проверки рекомендаций).</p> <p><i>Примечание: Для кандидатов на определенные должности, такие как, например, кассир в магазине, которые имеют доступ только к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.</i></p>	<p><b>12.7</b> Убедиться в том, что при приеме на работу нового персонала, которому будет предоставляться доступ к данным о держателях карт или среде данных о держателях карт, осуществляются кадровые проверки (с учетом особенностей законодательства).</p>			
<p><b>12.8</b> В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними, включающие:</p>	<p><b>12.8</b> Если 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:</p>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>12.8.1</b> Поддержку перечня поставщиков услуг.	<b>12.8.1</b> Убедиться в том, что поддерживается перечень поставщиков услуг.			
<b>12.8.2</b> Поддержку письменного соглашения о том, что поставщики услуг ответственны за безопасность переданных им данных о держателях карт.	<b>12.8.2</b> Убедиться, что письменное соглашение с поставщиком услуг предусматривает возложение на поставщика услуг ответственности за безопасность переданных ему данных о держателях карт.			
<b>12.8.3</b> Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним.	<b>12.8.3</b> 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
<b>12.8.4</b> Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS, по меньшей мере, один раз в год.	<b>12.8.4</b> Убедиться, что в организации имеется программа проверки статуса соответствия поставщиков услуг требованиям PCI DSS, по меньшей мере, один раз в год.			
<b>12.9</b> Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы.	<b>12.9</b> Изучить план реагирования на инциденты, выполнить следующие проверки:			
<b>12.9.1</b> Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум: <ul style="list-style-type: none"> <li>▪ роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем;</li> <li>▪ процедуры реагирования на определенные инциденты;</li> <li>▪ процедуры восстановления и обеспечения непрерывности бизнеса;</li> <li>▪ процессы резервного</li> </ul>	<b>12.9.1.a</b> Убедиться, что план реагирования на инциденты включает в себя: <ul style="list-style-type: none"> <li>▪ роли, обязанности и схемы оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем;</li> <li>▪ процедуры реагирования на определенные инциденты;</li> <li>▪ процедуры восстановления и обеспечения непрерывности бизнеса;</li> <li>▪ процессы резервного копирования данных;</li> <li>▪ анализ требований законодательства об оповещении о фактах компрометации;</li> <li>▪ охват всех критических системных компонентов;</li> <li>▪ ссылки или включение процедур реагирования на инциденты международных платежных систем.</li> </ul>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
копирования данных; <ul style="list-style-type: none"> <li>▪ анализ требований законодательства об оповещении о фактах компрометации;</li> <li>▪ охват всех критичных системных компонентов;</li> <li>▪ ссылки или включение процедур реагирования на инциденты международных платежных систем.</li> </ul>	<b>12.9.1.b</b> Изучить документацию по последнему инциденту или оповещению безопасности и убедиться в соблюдении документированного плана реагирования на инциденты и соответствующих процедур.			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>12.9.2</b> План должен тестироваться не реже одного раза в год.	<b>12.9.2</b> Убедиться в том, что план реагирования на инциденты тестируется не реже одного раза в год.			
<b>12.9.3</b> Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7.	<b>12.9.3</b> Убедиться путем изучения и проверки политики в наличии персонала, способного реагировать на оповещения безопасности и отслеживать информацию для доказательства неавторизованных действий, обнаружения неавторизованных беспроводных точек доступа, критичных оповещений безопасности системы обнаружения вторжений и/или отчетов о неавторизованных критичных системах или изменений содержания данных в режиме 24/7.			
<b>12.9.4</b> Персонал, ответственный за реагирование на нарушения безопасности, должен быть обучен соответствующим образом.	<b>12.9.4</b> Убедиться в том, что персонал, ответственный за реагирование на нарушения безопасности, проходит периодическое обучение.			
<b>12.9.5</b> План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов.	<b>12.9.5</b> 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.			
<b>12.9.6</b> Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.	<b>12.9.6</b> 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><b>A.1</b> 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><b>A.1</b> 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><b>A.1.1</b> Ограничить доступ приложений каждого клиента только к своей среде данных о держателях карт.</p>	<p><b>A.1.1</b> 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"> <li>▪ Ни одно приложение и ни один пользователь не может использовать имени пользователя, от которого работает разделяемый веб-сервер.</li> <li>▪ Все CGI-скрипты, используемые клиентом, должны быть созданы и запущены от имени идентификатора клиента.</li> </ul>			

Требование PCI DSS	Проверочные процедуры	Выполнено	Не выполнено	Дата устранения недостатков / Комментарий
<b>A.1.2</b> Ограничить доступ клиента только к своей среде данных о держателях карт.	<b>A.1.2.a</b> Убедиться, что ни один из клиентов не обладает правами администратора/суперпользователя.			
	<b>A.1.2.b</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.			
	<b>A.1.2.c</b> Убедиться, что у клиента отсутствует право записи в разделяемые системные библиотеки и исполняемые файлы.			
	<b>A.1.2.d</b> Убедиться, что просмотр журналов протоколирования доступен только владельцу.			
	<b>A.1.2.e</b> 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"> <li>▪ Использование дискового пространства</li> <li>▪ Использование канала</li> <li>▪ Использование памяти</li> <li>▪ Использование ресурсов ЦПУ</li> </ul>			
<b>A.1.3</b> Убедиться, что протоколирование действий и событий включено для каждого клиента и соответствует требованию 10 стандарта.	<b>A.1.3.a</b> Убедиться, что протоколирование событий удовлетворяет следующим критериям: <ul style="list-style-type: none"> <li>▪ Протоколирование настроено для всех типичных используемых на сервере приложений сторонних производителей</li> <li>▪ Протоколирование включено по умолчанию</li> <li>▪ Журналы доступны для просмотра администратору и клиенту, для которого выполняется протоколирование</li> <li>▪ Журналы расположены в каталогах, доступных клиенту</li> </ul>			

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.	

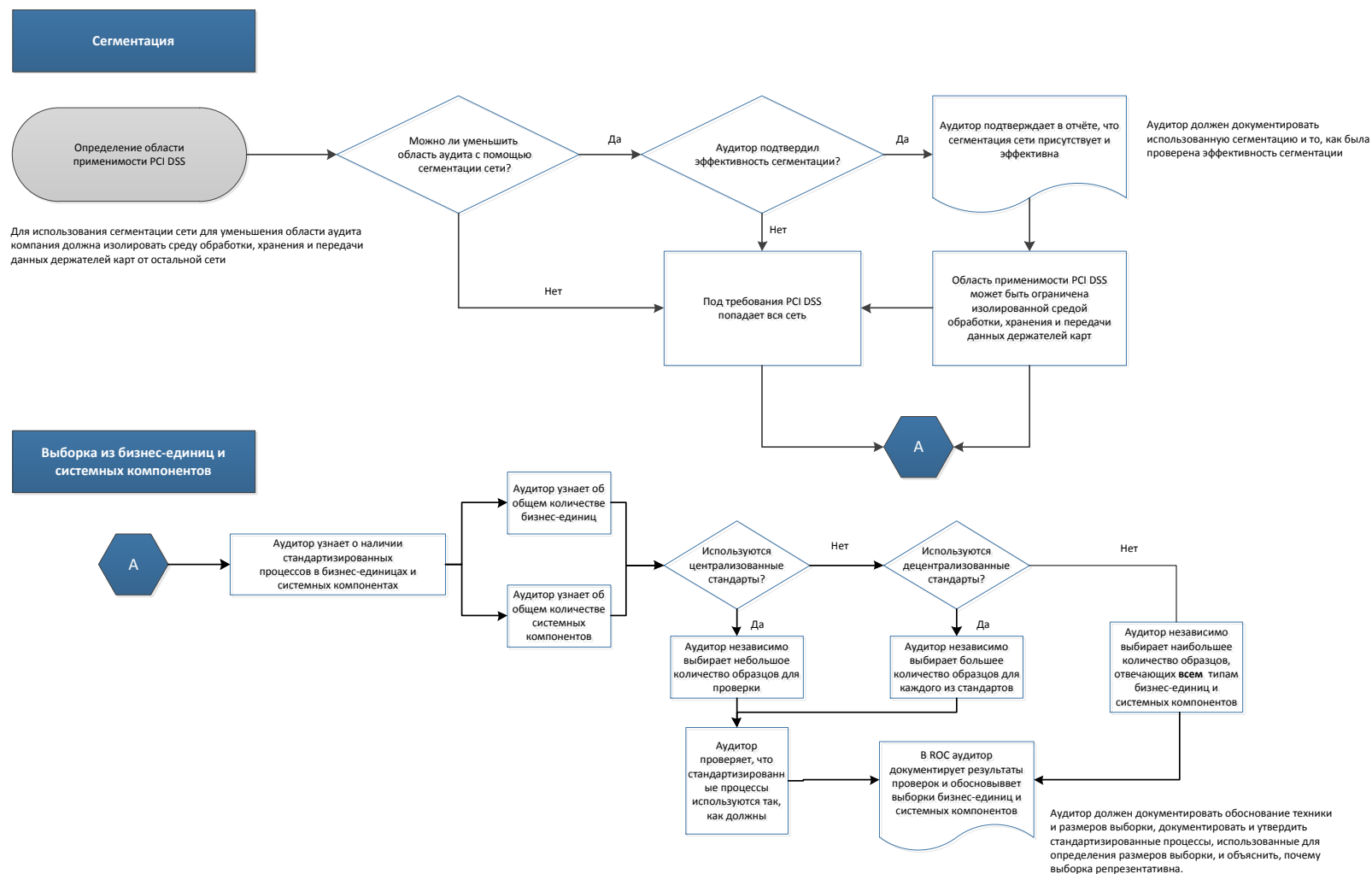
## Перечень компенсирующих мер – пример заполнения

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?

	<b>Требуемая информация</b>	<b>Описание</b>
<b>1. Ограничение</b>	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>
<b>2. Цель</b>	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>
<b>3. Определение риска</b>	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>
<b>4. Определение компенсирующих мер</b>	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>
<b>5. Проверка компенсирующих мер</b>	Опишите, как компенсирующие меры были проверены и протестированы.	<i>Аудиторам было продемонстрировано использование утилиты «su» и журнал регистрации событий SU-Log.</i>
<b>6. Поддержка</b>	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: Определение области аудита и выборки



## Информация о переводе

Перевод текста Стандарта безопасности данных индустрии платежных карт (PCI DSS) версии 2.0 с английского языка на русский выполнили:

Антон Карпов  
Сергей Шустиков  
Александр Поляков  
Ольга Юрова  
Юлия Зозуля  
Алексей Ендовский  
Павел Федоров

© 2010, Сообщество профессионалов PCIDSS.RU  
[info@pcidss.ru](mailto:info@pcidss.ru),  
<http://www.pcidss.ru>

Санкт-Петербург,  
2011