Payment Card Industry (PCI) Data Security Standard
Navigating PCI DSS

Understanding the Intent of the Requirements

Ориентирование в PCI DSS:
Понимание требований

Версия 1.1

Редакция: Февраль 2008

Перевод:
ЗАО НИП «ИНФОРМЗАЩИТА»
PCI QSA, PCI ASV
http://www.infosec.ru
pcidss@infosec.ru
7-495-9802345

Translated by:
NIP INFORMZASCHITA
PCI QSA, PCI ASV
http://www.infosec.ru
pcidss@infosec.ru
7-495-9802345

Данный документ является объектом интеллектуальной собственности ЗАО НИП «Информзащита».
ЗАО НИП «Информзащита» предоставляет право на использование этого документа в личных некоммерческих целях и в пределах своей организации. Копирование и/или передача его третьим лицам (в том числе в отредактированном виде) и/или его опубликование могут быть осуществлены только с письменного согласия ЗАО НИП «Информзащита», при этом продажа или любая иная возмездная передача данного документа запрещается.

В случае возникновения замечаний или предложений по переводу просьба направлять их по адресу pcidss@infosec.ru.

Данный документ предоставляется ЗАО НИП «Информзащита» в качестве информационной услуги. Это неофициальный перевод официального документа «Payment Card Industry (PCI) Data Security Standard. Understanding the Intent of the Requirements», находящегося по адресу https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf, собственность PCI Security Standards Council LLC. Текст на английском языке, находящийся по этому адресу, должен рассматриваться в качестве официальной версии документа для любых целей. В случае возникновения каких-либо двусмысленностей или несогласованностей между этим текстом и текстом на английском языке необходимо руководствоваться оригиналом. Данный перевод публикуется в подтверждение и в согласии с условиями, определенными в договоре на разрешение перевода между PCI SSC и ЗАО НИП «Информзащита». Ни PCI Security Standards Council LLC, ни ЗАО НИП «Информзащита» не берут на себя ответственность за какие-либо содержащиеся здесь неточности.

This translated document is provided by *NIP INFORMZASCHITA* as an informational service. This is an unofficial translation of the official document, "Payment Card Industry (PCI) Data Security Standard. Understanding the Intent of the Requirements", located at https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf copyright © February 2008 PCI Security Standards Council LLC. The English text to be found at such address shall for all purposes be regarded as the official version of this document, and to the extent of any ambiguities or inconsistencies between this text and the English text, the English text at such location shall control. This translation is published with acknowledgement of and in agreement with terms specified in a translation permissions agreement between PCI SSC and *NIP INFORMZASCHITA*. Neither PCI Security Standards Council LLC nor *NIP INFORMZASCHITA* assume responsibility for any errors contained herein.

Оглавление

Введение

В данном документе описываются 12 требований стандарта PCI DSS с пояснением их значения. Документ предназначен для предприятий торгово-сервисной сети (merchants), сервис-провайдеров и финансовых учреждений, которые хотят улучшить понимание стандарта PCI DSS, а также дает специфические толкования требований к безопасности системных компонентов (серверы, сеть, приложения и т. д.), которые являются частью среды данных платежных карт.

ПРИМЕЧАНИЕ: Данный документ следует использовать только как руководство. При проведении онсайт-аудита PCI DSS или самооценки необходимо использовать "Стандарт безопасности данных индустрии платежных карт" (PCI DSS v1.1), "Процедуры аудита безопасности" (PCI DSS Security Audit Procedures) и «Листы самооценки» (PCI DSS Self-Assessment Questionnaires v1.1).

Требования стандарта PCI DSS применимы ко всем компонентам системы, которые входят в среду данных платежных карт или непосредственно к ней присоединены. Среда данных платежных карт – это часть сети, в которой обрабатываются данные платежных карт или критичные данные авторизации, включая сетевые компоненты, серверы и приложения.

- Сетевые компоненты включают (но не ограничиваются ими) межсетевые экраны, коммутаторы, маршрутизаторы, беспроводные точки доступа, сетевые устройства и устройства защиты информации.
- Типы серверов включают (но не ограничиваются ими) web-серверы, серверы баз данных, аутентификационные серверы, почтовые серверы, прокси-серверы, NTP- и DNS-серверы.
- Приложения включают (но не ограничиваются ими) все приобретенные и разработанные приложения, как внутренние, так и внешние (подключенные к Интернету).

Продуманная сегментация сети, которая изолирует системы хранения, обработки или передачи данных карт от других систем в организации, может ограничить область оценки среды данных платежных карт. Qualified Security Assessor (QSA, сертифицированная компания, проводящая аудит на соответствие стандарту PCI DSS) может помочь в определении области оценки и дать консультации каким образом можно уменьшить область оценки с помощью правильной сегментацией сети. Вопросы по поводу того, соответствует ли та или иная технология или решение стандарту в целом или какому-то конкретному требованию, PCI SSC рекомендует направлять в компании имеющие статус QSA, которые смогут оценить насколько внедрение технологии или решения соответствуют стандарту PCI DSS. Опыт работы компаний, имеющих статус QSA, со сложными сетями и информационными системами позволяет им давать рекомендации и делиться «лучшими практиками» с торгово-сервисными организациями и сервис-провайдерами по достижению соответствия требованиям стандарта. Список Qualified Security Assessors можно найти по адресу: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Данные платежных карт и элементы критичных данных авторизации

Приведенная ниже таблица иллюстрирует наиболее часто используемые элементы данных платежных карт и критичные данные авторизации (sensitive authentication data); разрешено или запрещено **хранение** каждого элемента данных; должна ли выполняться **защита каждого элемента данных**. Данная таблица не претендует на роль исчерпывающей, она представлена лишь в целях демонстрации различных типов требований, которые применяются к каждому элементу данных.

Данные платежных карт определены как PAN (Primary Account Number, номер карты) и другие данные, полученные в результате транзакций, включая следующие элементы:

- PAN
- Cardholder Name (имя держателя карты)
- Expiration Date (дата истечения срока действия карты)
- Service Code
- *Sensitive authentication data (магнитная дорожка полностью, CAV2/CVC2/CVV2/CID, PIN/PIN-блок)*

Требования стандарта PCI DSS и PA-DSS применяются, если выполняются хранение, обработка или передача номера PAN (Primary Account Number). Если хранение, обработка или передача номера PAN не выполняются, то требования стандарта PCI DSS и PA-DSS не применяются.

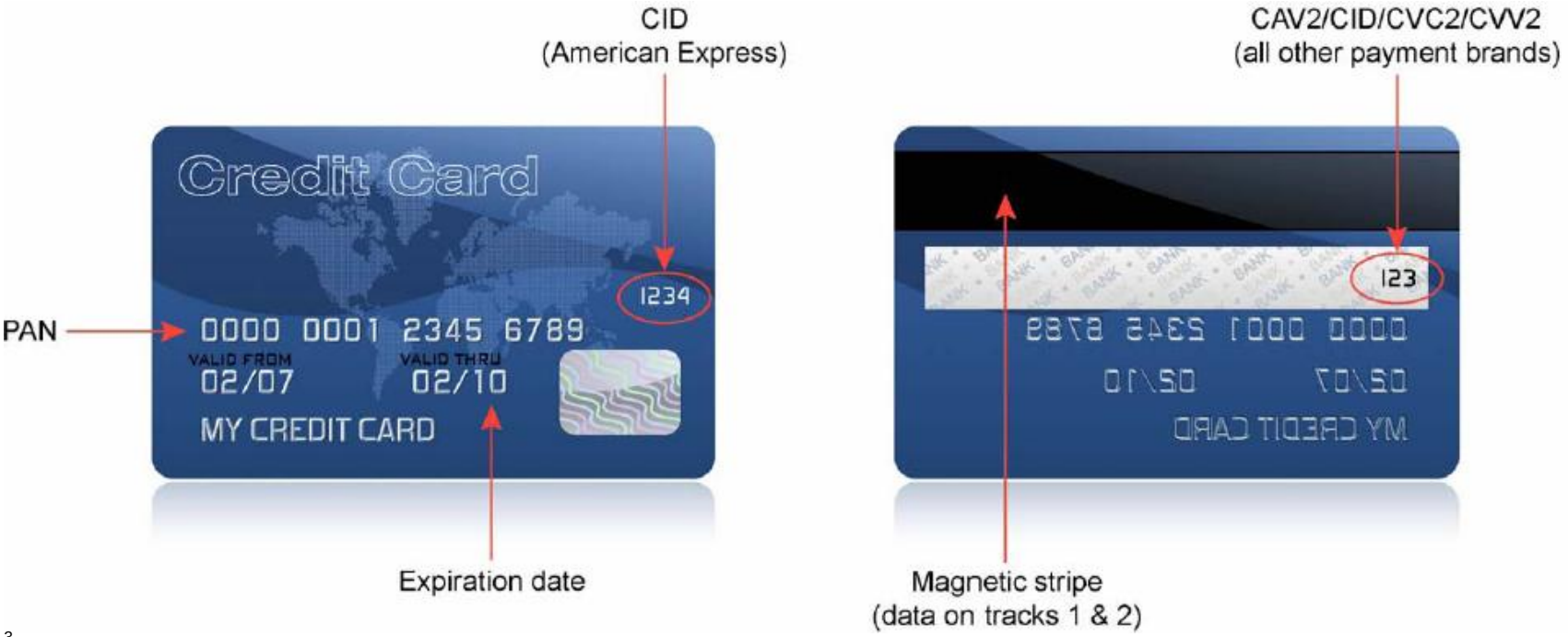
	Элемент данных	Хранение разрешено	Требуется защита	Требование 3.4 стандарта PCI DSS
Данные платежных карт	Номер PAN	ДА	ДА	ДА
	Имя держателя карты[1]	ДА	ДА[1]	НЕТ
	Сервисный код[1]	ДА	ДА[1]	НЕТ
	Дата истечения срока действия[1]	ДА	ДА[1]	НЕТ
Критичные данные авторизации (sensitive authentication data)[2]	Полное содержание магнитной полосы	НЕТ	-	-
	CVC2/CVV2/CID	НЕТ	-	-
	PIN/PIN Block	НЕТ	-	-

[1] *Эти элементы данных должны защищаться, если они хранятся совместно с номером PAN. При этом уровень защиты должен соответствовать требованиям общей защиты среды данных платежных карт стандарта PCI DSS. В соответствии с другими законами (например, связанными с защитой персональных данных клиентов, частной информацией, кражей идентификационной информации или обеспечением безопасности данных) может потребоваться специфическая защита этих данных или оглашение установленных правил компании, если в ходе ведения бизнеса ведется сбор персональных данных клиентов. Однако требования стандарта PCI DSS не применяются, если не выполняются хранение, обработка или передача номеров карт.*

[2] *Критичные данные авторизации (sensitive authentication data) не должны сохраняться после прохождения процедуры авторизации (даже в зашифрованном виде).*

Расположение данных платежных карт и критичных данных авторизации

Критичные данные авторизации состоят из магнитной полосы[3] (трека, дорожки), подтверждающего кода (значения) карты[4] и PIN[5]. **ХРАНИТЬ КРИТИЧНЫЕ ДАННЫЕ АВТОРИЗАЦИИ ЗАПРЕЩЕНО!** Эти данные чрезвычайно ценны для злоумышленников, поскольку позволяют им генерировать поддельную информацию карт и проводить мошеннические транзакции. Полное определение критичных данных авторизации (sensitive authentication data) можно найти в документе «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*). На изображении передней и задней стороны платежной карты ниже показано расположение данных платежных карт и критичных данных авторизации.



[3] Данные, зашифрованные на магнитной полосе, используются для авторизации в течение транзакций с предоставлением карты (card-present transactions). Нет необходимости хранить все данные магнитной полосы после авторизации. Достаточно хранить номер счета, дату истечения срока действия карты и имя держателя.

[4] Трех- или четырехзначное значение, напечатанное на карте справа от места для подписи или на лицевой стороне карты, используемое для проверки транзакций без предоставления карты (card-not-present transactions).

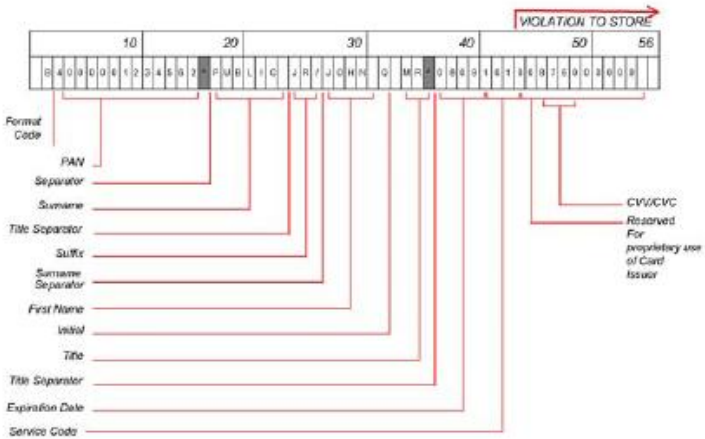
[5] Personal Identification Number (PIN, ПИН – персональный идентификационный номер) вводится держателем карты в течение транзакций с предоставлением карты (card-present transactions) и/или зашифрованный PIN-блок, присутствующий в транзакционном сообщении.

Данные Track 1 и Track 2

Если хранить трек полностью (неважно, трек 1 или трек 2), то хакеры, которые получат эти данные, смогут воспроизвести и продавать данные карт по всему миру. Хранение всех данных трека также нарушает правила работы в платежных системах и может привести к штрафам. Ниже проиллюстрирована информация о треке 1 и треке 2, описывающая различия и показывающая, что именно хранится на магнитной полосе.

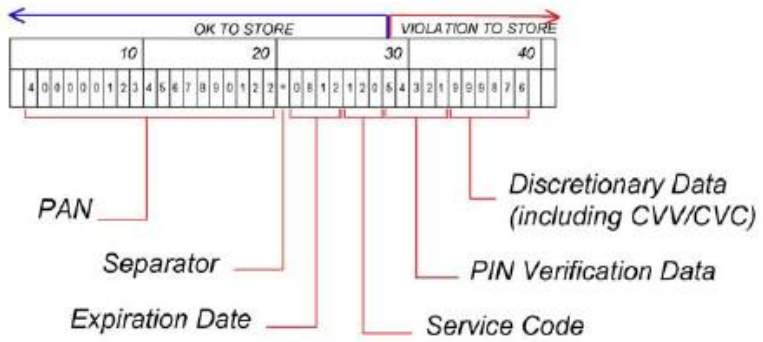
Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters



Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters



PCI Data Security Standard

Построение и поддержание защищенной сети

Требование 1: Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карт
Требование 2: Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию

Защита данных платежных карт

Требование 3: Должна быть обеспечена защита данных платежных карт при хранении
Требование 4: Должно обеспечиваться шифрование данных платежных карт, передаваемых по сетям общего пользования

Реализация программы управления уязвимостями

Требование 5: Должно использоваться и регулярно обновляться антивирусное программное обеспечение
Требование 6: Должна обеспечиваться безопасность при разработке и поддержке систем и приложений

Реализация мер по строгому контролю доступа

Требование 7: Доступ к данным платежных карт должен быть ограничен в соответствии со служебной необходимостью
Требование 8: Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор
Требование 9: Физический доступ к данным платежных карт должен быть ограничен

Регулярный мониторинг и тестирование сетей

Требование 10: Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и данным платежных карт
Требование 11: Должно выполняться регулярное тестирование систем и процессов обеспечения безопасности

Поддержание политики информационной безопасности

Требование 12: Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов

Построение и поддержание защищенной сети

Требование 1: Должны быть обеспечены разработка и управление конфигурацией межсетевых экранов в целях защиты данных платежных карт

Межсетевые экраны – это вычислительные устройства, контролирующие трафик, входящий в корпоративную сеть и исходящий из корпоративной сети, а также трафик к внутренним критичным подсетям. Межсетевой экран анализирует сетевой трафик и блокирует сетевые пакеты, которые не соответствуют определенным критериям безопасности.

Все системы должны быть защищены от несанкционированного доступа из сети Интернет, вне зависимости от способа доступа – посредством приложений электронной коммерции, доступа сотрудников компании к сети Интернет или электронной почте. В некоторых случаях казалось бы несущественные каналы исходящего и входящего интернет-трафика представляют собой незащищенные пути доступа к критичным системам. Межсетевые экраны являются основным механизмом защиты любой компьютерной сети.

Требование	Пояснение
1.1 Должны быть реализованы стандарты конфигурирования межсетевых экранов, включающие следующее:	Межсетевые экраны – это программное или аппаратное обеспечение, которое блокирует нежелательный доступ в сеть. Без наличия действующих политик и процедур, в которых указывается, как персонал должен настраивать межсетевые экраны, организация может легко сдать злоумышленнику свою первую линию обороны в защите данных.
1.1.1 Формализованный[1] процесс утверждения и тестирования всех подключений внешних сетей, а также изменений, вносимых в конфигурацию МЭ	Политика и процесс утверждения и тестирования всех подключений и изменений в конфигурации межсетевых экранов поможет предотвратить проблемы безопасности, вызванные неправильной настройкой сети или межсетевого экрана.
1.1.2 Актуальную схему сети с указанием всех подключений (включая беспроводные сети) к сегментам с данными платежных карт	Схема сети позволяет организации идентифицировать размещение всех сетевых устройств. Без схемы сети некоторые сетевые устройства можно легко упустить из виду и, не обеспечив их должной защиты, подвергнуть угрозе компрометации.
1.1.3 Требования по размещению МЭ на каждом канале подключения к сети Интернет, а также на границе между каждой DMZ и внутренней сетью	Использование межсетевого экрана на каждом входящем (и исходящем) подключении сети позволяет организации выполнять мониторинг и контроль входящего и исходящего трафика и тем самым минимизировать шансы злоумышленника по получению доступа к внутренней сети.
1.1.4 Описание групп, ролей и обязанностей в отношении логического управления сетевыми компонентами	Описание ролей и назначение ответственности позволяет гарантировать, что назначенные лица персонально отвечают за безопасность всех компонентов, осведомлены о своей ответственности, а также свидетельствует об отсутствии неконтролируемых устройств.

[1] Установленный процесс, где исполнители и порядок выполняемых ими действий определены. Обычно такой процесс документирован.

Требование	Пояснение
1.1.5 Документированный перечень сервисов и портов, необходимых для функционирования бизнес-процессов	Компрометации часто происходят вследствие наличия неиспользуемых или незащищенных служб и портов, поскольку они часто содержат общеизвестные уязвимости, а многие организации не устанавливают обновления безопасности для служб и портов, которые они не используют (даже в случае присутствия уязвимостей). Каждая организация должна четко определить, какие службы и порты необходимы для ведения бизнеса, задокументировать их и обеспечить отключение или удаление всех остальных служб и портов. Также организациям необходимо рассмотреть вариант блокирования всего сетевого трафика и последующего открытия лишь тех служб и портов, целесообразность открытия которых определена и задокументирована.
1.1.6 Документирование и обоснование применения для всех использующихся протоколов, за исключением HTTP, SSL, SSH и VPN	
1.1.7 Документирование и обоснование для всех использующихся небезопасных протоколов (например, FTP) с указанием причины использования протокола и реализованных механизмов защиты	Существует большое количество протоколов, которые могут потребоваться для ведения бизнеса (или которые разрешены настройками по умолчанию) и использоваться злоумышленниками для компрометации сети. В добавление к объяснению в п. 1.1.5, если небезопасные протоколы необходимы для ведения бизнеса, то нужно четко понимать риски от их использования, принимать эти риски, обосновывать использование этих протоколов, а также документировать и реализовывать механизмы защиты, которые позволяют безопасно использовать данные протоколы.
1.1.8 Ежеквартальный пересмотр правил МЭ и маршрутизаторов	Данный пересмотр предоставляет организации возможность проведения ежеквартального удаления всех ненужных, истекших или некорректных правил и гарантирует, что все наборы правил разрешают доступ только авторизованным службам и портам, которые соответствуют требованиям бизнеса.
1.1.9 Стандарты конфигурирования для маршрутизаторов	Данные устройства вместе с межсетевыми экранами являются частью архитектуры, которая контролирует точки входа в сеть. Документированные политики помогают сотрудникам настраивать и защищать маршрутизаторы и гарантируют надежность первой линии защиты данных организации.
1.2 Должна быть реализована такая конфигурация МЭ, в которой запрещается любой трафик, поступающий из недоверенных сетей и устройств, **за исключением** протоколов, необходимых для среды данных платежных карт.	Если межсетевой экран установлен, но не содержит правил, которые контролируют или ограничивают определенный трафик, то злоумышленники все равно будут иметь возможность использовать уязвимые протоколы и порты для проведения атак на сеть.
1.3 Должна быть реализована такая конфигурация МЭ, которая ограничивает возможность установления подключений между публично доступными серверами (включая любые подключения из беспроводных сетей) и любыми системными компонентами, в которых хранятся данные платежных карт. Такая конфигурация должна предусматривать:	
1.3.1 Ограничение входящего интернет-трафика IP-адресами	Обычно пакет содержит IP-адрес компьютера, который его отправил. Это позволяет

Требование	Пояснение
внутри DMZ (входная фильтрация)	другим компьютерам в сети узнать, откуда пришел пакет. В определенных ситуациях данный IP-адрес отправителя может быть подменен злоумышленниками. Например, злоумышленники могут отправить пакет с подмененным адресом для того, чтобы (если межсетевой экран не запрещает это) пакет смог попасть во внутреннюю сеть из сети Интернет и выглядел так, как будто он является внутренним и, следовательно, легитимным трафиком. Как только злоумышленники получат возможность проникнуть внутрь сети, они могут начать компрометацию внутренних систем. Входная фильтрация – это способ контроля трафика, который может использоваться на межсетевом экране для фильтрации пакетов, поступающих в сеть, и обеспечения гарантии того, что IP-адреса пакетов не подменены и не выглядят как поступающие из внутренней сети. Для получения дополнительной информации по фильтрации пакетов рекомендуется также изучить способы фильтрации исходящих пакетов «”egress filtering”.
1.3.2 Запрет трафика с адресами отправителя из внутренней сети, поступающего в DMZ из сети Интернет	
1.3.3 Реализацию фильтрации трафика с учетом состояния соединений (stateful inspection), также известной как динамическая фильтрация пакетов (когда доступ в сеть разрешается только для «установленных» соединений)	Межсетевой экран, который выполняет динамическую фильтрацию пакетов, хранит информацию о состоянии (иными словами, статус) для каждого соединения. Сохраняя информацию о состоянии, межсетевой экран знает, являются ли пакеты, которые выглядят как ответ на предыдущее соединение, в действительности ответом (поскольку он «запоминает» предыдущее соединение) или же это попытка обойти межсетевой экран, чтобы он разрешил соединение.
1.3.4 Размещение базы данных во внутреннем сегменте сети, отделенном от DMZ	Информация о счетах платежных карт требует самого высокого уровня защиты информации. Если информация о счетах находится внутри DMZ, то задача получения доступа к этой информации для внешнего злоумышленника упрощается, поскольку ему понадобится преодолеть меньшее количество уровней защиты. При отсутствии межсетевого экрана, защищающего информацию о счетах, эти данные уязвимы как для злоумышленников из внутренней сети, так и для всех злоумышленников, которые могут проникнуть из внешней сети.
1.3.5 Разрешение только такого входящего и исходящего трафика, который является необходимым для среды данных платежных карт	Это требование вводится для предотвращения доступа злоумышленников к сети организации с использованием неавторизованных IP-адресов или предотвращения использования служб, протоколов или портов для выполнения неразрешенных действий (например, отправка данных, полученных из внутренней сети, внешнему серверу).
1.3.6 Обеспечение защиты и синхронизации конфигурационных файлов маршрутизаторов. Например, файлы активной в данный момент времени конфигурации (running configuration) и сохраненной конфигурации (start-up configuration – загружается в оперативную память в качестве активной конфигурации при	В то время как активные конфигурационные файлы обычно содержат безопасные настройки, в файлах сохраненной конфигурации может отсутствовать реализация аналогичных настроек, поскольку они запускаются время от времени (после перезагрузки). Перезагрузка и запуск маршрутизатора без использования безопасных настроек, которые присутствовали в активной конфигурации, может сказаться на

Требование	Пояснение
перезагрузке устройства) должны иметь одинаковую защищенную конфигурацию	ослаблении защиты и может позволить злоумышленнику получить несанкционированный доступ в сеть.
1.3.7 Блокирование любого входящего и исходящего трафика, не разрешенного явно	Все межсетевые экраны должны содержать правило, запрещающее весь входящий и исходящий трафик, который не является необходимым. Это позволит предотвратить случайные ошибки, которые могут разрешать незапланированный и потенциально опасный входящий и исходящий трафик.
1.3.8 Установку МЭ для организации защиты периметра между любыми беспроводными сетями и средой платежных карт и конфигурирование этих МЭ на блокирование любого трафика из беспроводных сетей или контроль этого трафика (если такой трафик необходим для ведения бизнеса)	Известная (или неизвестная) реализация и использование беспроводной технологии в пределах сети компании является распространенным способом получения злоумышленниками доступа в сеть и к данным платежных карт. Если беспроводное устройство или сеть установлены без ведома компании, то злоумышленник может легко и «незаметно» войти в сеть. Если межсетевые экраны не ограничивают доступ из беспроводных сетей в среду данных платежных карт, то злоумышленники, получившие неавторизованный доступ в беспроводную сеть, могут беспрепятственно подключиться к среде данных платежных карт и скомпрометировать информацию о счетах.
1.3.9 Установку персональных межсетевых экранов на все портативные и личные компьютеры сотрудников, которые обладают возможностью прямого доступа к сети Интернет (например, на ноутбуки сотрудников) и используются для доступа к сети организации	Если на компьютере не установлен сетевой экран или антивирусное программное обеспечение, то он может быть заражен вредоносным программным обеспечением (шпионскими программами, троянским программным обеспечением, вирусами или червями). Компьютер является еще более уязвимым при осуществлении прямого подключения к сети Интернет в обход корпоративного межсетевого экрана. Вредоносное программное обеспечение, загруженное на компьютер при подключении в обход корпоративного межсетевого экрана, при последующем подключении к корпоративной сети может поражать информацию в корпоративной сети.
1.4 Должен быть запрещен прямой доступ из публичных внешних сетей к любым системным компонентам, на которых выполняется хранение данных платежных карт (например, базам данных, журналам регистрации событий, файлам трассировки).	Назначением межсетевых экранов является управление и контроль всех подключений между общедоступными и внутренними системами (в особенности теми, в которых хранятся данные платежных карт). Если разрешается прямой доступ между общедоступными системами и системами, в которых хранятся данные платежных карт, то игнорируется предлагаемая межсетевым экраном защита, и системные компоненты, хранящие данные платежных карт, могут быть подвержены компрометации.
1.4.1 Должна быть реализована зона DMZ для фильтрации и экранирования любого трафика и запрета прямых маршрутов для входящего и исходящего интернет-трафика	DMZ – это часть межсетевого экрана, которая обращена к общедоступной сети Интернет и управляет подключениями между сетью Интернет и теми внутренними службами, которые организация считает целесообразным открыть внешнему миру (например, web-сервер). DMZ является первой линией обороны в изоляции и разделении трафика, которому разрешено взаимодействие с внутренней сетью, от трафика, которому это не разрешено.
1.4.2 Исходящий от приложений платежных карт трафик должен быть ограничен IP-адресами внутри DMZ	В DMZ должна проводиться оценка всего исходящего из внутренней сети трафика, чтобы гарантировать, что весь исходящий трафик отвечает установленным правилам.

Требование	Пояснение
	Для того чтобы DMZ эффективно выполняла данную функцию, подключения из внутренней сети к любым адресам за ее пределами не должны разрешаться, прежде чем они не пройдут через DMZ, в которой выполняется их проверка на легитимность.
1.5 Для предотвращения раскрытия структуры внутренней адресации в сети Интернет должен осуществляться IP-маскарадинг и использоваться технологии, реализующие адресное пространство RFC 1918 – PAT (Port Address Translation) или NAT (Network Address Translation).	Скрытие IP-адресов (IP masquerading), которое управляется межсетевым экраном, позволяет организации иметь внутренние адреса, которые видимы только внутри сети, и внешние адреса, которые видимы извне. Если межсетевой экран не скрывает или не маскирует IP-адреса внутренней сети, злоумышленник может обнаружить внутренние IP-адреса и попытаться получить доступ в сеть с помощью подмены IP-адреса.

Требование 2: Не должны использоваться параметры безопасности и системные пароли, установленные производителем по умолчанию

Злоумышленники (внешние и внутренние) для компрометации систем часто используют параметры безопасности и пароли, заданные производителем. Эти параметры и пароли хорошо известны в хакерских сообществах и могут быть получены через открытые источники информации.

Требование	Пояснение
2.1 **До** подключения системы к сети должны быть изменены параметры, заданные производителем по умолчанию, влияющие на защищенность (в том числе пароли, SNMP-строки, а также удалены неиспользуемые учетные записи).	Злоумышленники (внешние и внутренние по отношению к компании) часто для компрометации систем используют настройки, учетные записи и пароли, установленные производителем по умолчанию. Данные параметры широко известны в хакерских сообществах и подвергают систему риску эксплуатации уязвимостей.
2.1.1 Для беспроводных сред должны быть изменены значения, заданные производителем по умолчанию, включая (но не ограничиваясь) следующие параметры: WEP-ключи, идентификаторы сетей (SSID), пароли и SNMP-строки. Необходимо отключать широковещательную рассылку идентификаторов SSID и использовать технологии WPA или WPA2 для шифрования и аутентификации WPA-совместимых устройств	Многие пользователи устанавливают данные устройства без утверждения руководства и не меняют настройки, заданные производителем по умолчанию, или не настраивают параметры безопасности. Если в беспроводных сетях не реализован достаточный уровень безопасности (включая изменение параметров по умолчанию), то существует возможность прослушивания трафика беспроводными анализаторами пакетов, извлечения данных и паролей, атак на сеть. В дополнение протокол обмена ключами для ранней версии шифрования стандарта 802.11x (WEP) может быть взломан и стать бесполезным в отношении защиты.
2.2 Должны быть разработаны стандарты конфигурирования для всех системных компонентов, учитывающие все известные уязвимости и рекомендации по обеспечению безопасности систем (определенные, например, SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST) и Center for Internet Security (CIS)).	У многих операционных систем, баз данных и корпоративных приложений существуют известные уязвимости (или недостатки конфигурирования). Вместе с тем известны способы конфигурирования данных систем для устранения этих недостатков. Для помощи лицам, не являющимся экспертами в области безопасности, организации, специализирующиеся на защите информации, предоставляют специальные рекомендации по повышению уровня защищенности систем, в которых указаны способы устранения уязвимостей и недостатков конфигурирования. Если не происходит устранения известных недостатков в системах (например, недостатков в настройках по ограничению доступа к файлам или отключения служб и протоколов, активированных по умолчанию, которые не являются необходимыми), злоумышленник получает возможность использования многочисленных общеизвестных эксплойтов для проведения атак на уязвимые службы и протоколы и получения доступа к сети организации.
2.2.1 На каждом сервере должна быть реализована только одна основная функция (например, web-сервер, сервер баз данных и DNS-сервер должны быть реализованы на различных серверах)	Назначение данного требования – обеспечение того, что стандарты конфигурирования для систем организации и процессы, связанные с ними, адресуют функции сервера, которые соответствуют различным уровням безопасности, или функции, которые могут являться слабыми местами в организации безопасности по отношению к другим функциям на том же сервере. Примеры: 1. База данных, требующая наличия усиленных мер безопасности, будет подвергаться риску в случае использования сервера совместно с web-приложением, которое должно

Требование	Пояснение
	быть доступным пользователям сети Интернет. 2. Ошибка применения исправления уязвимости к казалось бы незначительной функции может привести к компрометации более важных функций (например, базы данных) на том же сервере. Данное требование предназначено для серверов (обычно Unix, Linux или Windows), но не для мейнфреймов.
2.2.2 Все ненужные и небезопасные сервисы и протоколы (сервисы и протоколы, не являющиеся необходимыми для выполнения назначенных устройствам функций) должны быть отключены	Как упоминалось в п. 1.1.7, существует большое количество протоколов, которые могут потребоваться для ведения бизнеса (или активированы настройками по умолчанию) и которые обычно используются злоумышленниками для компрометации сети. Данное требование должно являться частью стандартов конфигурирования организации и связанных с ними процессов для обеспечения гарантии того, что подобные протоколы и службы отключены при развертывании новых серверов.
2.2.3 Параметры безопасности систем должны быть настроены для предотвращения ненадлежащего использования	Это требование введено для того, чтобы гарантировать, что стандарты конфигурирования систем и связанные с ними процессы уделяют повышенное внимание настройкам безопасности и параметрам, оказывающим существенное влияние на состояние защищенности.
2.2.4 Должен быть удален весь избыточный функционал, например, скрипты, драйверы, функциональные возможности, подсистемы, файловые системы и неиспользуемые web-серверы	Стандарты для повышения защищенности серверов должны включать процессы устранения ненужной функциональности, связанной с потенциальными уязвимостями (например, удаление/отключение служб FTP или web, если они не относятся к функциям сервера).
2.3 Должно выполняться шифрование любого неконсольного административного доступа. Для управления с помощью web-интерфейса и другого неконсольного административного доступа должны использоваться такие технологии, как SSH, VPN или SSL/TLS.	Если при удаленном администрировании не используются безопасная аутентификация и шифрование, то существует возможность перехвата злоумышленником критичной информации (например, паролей администраторов). Злоумышленник затем может использовать данную информацию для получения доступа к сети, административных прав и кражи данных.
2.4 Хостинг-провайдеры должны защищать среду размещения и данные каждой обслуживаемой организации. Хостинг-провайдеры должны соответствовать дополнительным требованиям, описанным в приложении A: «Применимость стандарта PCI DSS к хостинг-провайдерам».	Данное требование предназначено для хостинг-провайдеров, которые предоставляют общую среду размещения данных для нескольких организаций-клиентов на одном и том же сервере. Когда все данные находятся на одном и том же сервере и управляются из единой среды, отдельные клиенты обычно не управляют настройками этих совместно используемых серверов, т.к. разрешение добавления клиентами небезопасных функций и скриптов окажет влияние на защищенность данных всех клиентов, размещенных на том же сервере. При компрометации злоумышленником данных одной категории клиентов подвергнутся риску и возможности получения доступа данные других клиентов. Дополнительные сведения содержатся в Требовании A.1 в конце данного документа.

Защита данных платежных карт

Требование 3: Должна быть обеспечена защита данных платежных карт при хранении

Шифрование является важнейшей составляющей защиты данных платежных карт. В случае обхода мер по защите сети и получения доступа к зашифрованным данным злоумышленник не сможет узнать содержимое данных или воспользоваться ими без наличия корректных криптографических ключей. Также с целью уменьшения рисков должны рассматриваться и другие эффективные методы защиты хранимых данных. Например, методы минимизации риска включают: отказ от хранения данных платежных карт, если только это не является необходимостью, усечение данных платежных карт, если не требуется наличие полного номера PAN, и запрет отправки номеров PAN в незашифрованных сообщениях электронной почты.

Требование	Пояснение
3.1 Хранение данных платежных карт должно быть сведено к минимуму. Должна быть разработана политика хранения и уничтожения данных платежных карт. Также должен быть ограничен объем хранимой информации и период хранения так, как это необходимо исходя из требований бизнеса, правовых и/или нормативных актов, и документировано в политике хранения данных платежных карт.	Хранение расширенной информации платежных карт, выходящей за пределы потребностей бизнеса, представляет собой дополнительный риск. Единственными данными платежных карт, которые могут храниться, являются номер PAN (приведен к нечитаемому виду), дата истечения срока действия, имя и код обслуживания. Необходимо придерживаться принципа: «**Если данные не нужны – не храните их**».
3.2 Запрещено хранение критичных данных авторизации («sensitive authentication data») после прохождения процедуры авторизации (даже в зашифрованном виде). К критичным данным авторизации относятся данные, рассмотренные в требованиях 3.2.1–3.2.3:	Критичные данные авторизации включают: код CVC, данные целого трека и блоки PIN. Хранение критичных данных авторизации запрещено! Эти данные чрезвычайно ценны для злоумышленника, поскольку их знание позволяет производить поддельные платежные карты и выполнять мошеннические транзакции. Определение термина «критичные данные авторизации» содержится в документе «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*).
3.2.1 Запрещается хранить полное содержимое любого трека с магнитной полосы (расположенного, например, на оборотной стороне карты, в чипе или еще где-либо). Эти данные также могут называться полным треком (full track), треком, первым треком (track 1), вторым треком (track 2) или данными магнитной полосы. *Для ведения бизнеса обычно требуется хранение следующих элементов данных с магнитной полосы: имя держателя счета, номер платежной карты (PAN), дата истечения срока действия и сервисный код. Для минимизации рисков должны храниться лишь те элементы данных, которые необходимы для ведения бизнеса. НИКОГДА не должно выполняться хранение элементов Card Verification Code, или Card Verification Value, или PIN verification value.*	Если сохранены данные полного трека, злоумышленник, получивший доступ к этим данным, может воспроизводить и продавать платежные карты по всему миру. Хранение данных полного трека также запрещено действующими нормативными актами платежных систем и может повлечь за собой наказания и штрафы.

Требование	Пояснение
Для получения дополнительной информации необходимо обратиться к документу «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*).	
3.2.2 Запрещается хранить элементы card-validation code или value (трех- или четырехзначное число, напечатанное на карте), использующиеся для проверки транзакций, совершающихся в отсутствие карты. *Для получения дополнительной информации необходимо обратиться к документу* «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*).	Назначение элемента card validation code состоит в защите транзакций, выполняющихся в отсутствие карты, в которых не происходит непосредственного считывания данных с карты (заказ товаров по сети Интернет или почте/заказ по телефону). Данные типы транзакций могут быть аутентифицированы как исходящие от владельца карты лишь по элементу card validation code, поскольку подразумевается, что лишь владелец карты может держать карту в руках и назвать значение данного кода. Если эти запрещенные данные будут храниться и будут украдены, злоумышленник получит возможность совершения мошеннических транзакций по сети Интернет, почте и телефону. Хранение этих данных также запрещено нормативными актами платежных систем и может повлечь за собой наказания и штрафы.
3.2.3 Запрещается хранить PIN-коды или зашифрованные PIN-блоки	Данные значения должны быть известны только владельцу карты или банку, выдавшему карту. Если эти запрещенные данные будут храниться и будут украдены, злоумышленник получит возможность совершения мошеннических дебетовых транзакций, основанных на PIN-кодах (например, получение наличных в банкоматах). Хранение этих данных также запрещено нормативными актами платежных систем и может повлечь за собой наказания и штрафы.
3.3 Номера PAN при отображении должны маскироваться (максимальным количеством разрешенных к отображению цифр являются первые шесть и последние четыре цифры). *Данное требование не распространяется на сотрудников и иные стороны, которым необходимо видеть полный номер PAN для выполнения должностных обязанностей. Оно также не отменяет более строгие требования по отображению данных платежных карт (например, на чеках POS-терминалов).*	Отображение полного номера PAN на экранах компьютеров, квитанциях платежных карт, факсах или бумажных отчетах может привести к тому, что эти данные станут известны неавторизованным лицам и использованы в мошеннических целях. Важно обратить внимание на то, что полный номер PAN может отображаться на копиях квитанций у предприятий торгово-сервисной сети или у лиц, которым нужно видеть полный номер PAN для выполнения определенных задач.
3.4 Номера PAN должны быть приведены к нечитаемому виду вне зависимости от места хранения (включая данные на портативных носителях, резервных копиях, в журналах, а также данные, полученные или сохраненные посредством беспроводных сетей) с помощью одного из перечисленных ниже способов:	Недостаточная защита номеров PAN может привести к тому, что неавторизованные внутренние пользователи и злоумышленники получат возможность просмотра или сохранения этих данных. Все номера PAN, которые хранятся в основных хранилищах (базах данных, неструктурированных файлах), а также во вспомогательных хранилищах (архивных копиях, журналах регистрации событий, журналах неисправностей), должны быть защищены. Последствия кражи или утери резервных носителей в процессе транспортировки могут быть уменьшены, если номера PAN приведены к нечитаемому виду посредством шифрования, усечения или хеширования. Поскольку необходимо хранить журналы регистрации событий и неисправностей, предотвращение раскрытия данных в журналах достигается приведением номеров

Требование	Пояснение
	PAN, сохраняемых в журналах, к нечитаемому виду (посредством их удаления или маскирования).
• стойкие односторонние хеш-функции (хешированные индексы)	Для приведения данных платежных карт к нечитаемому виду могут использоваться односторонние хеш-функции, например, SHA-1. Их использование целесообразно тогда, когда отсутствует необходимость восстановления номера PAN (т.к. односторонние хеш-функции являются необратимыми).
• усечение	Цель усечения заключается в том, что хранится только часть (не больше чем шесть первых и четыре последних цифры) номера PAN. Данный подход отличается от маскирования, при котором хранится полный номер PAN и маскируется лишь при отображении (например, на экранах, в отчетах, в квитанциях и т. д. отображается только часть номера PAN).
• index token и PADs (PAD должны храниться в безопасности)	Индексные "маркеры" и "блокноты" также могут использоваться для приведения данных платежных карт к нечитаемому виду. Индексный "маркер" – это криптографический параметр, который заменяет номер PAN на основе заданного индекса для получения непредсказуемого значения. Одноразовый "блокнот" (one-time pad) – это система, в которой секретный ключ, сгенерированный случайным образом, используется только один раз для шифрования сообщения, которое затем расшифровывается с использованием соответствующего одноразового блокнота и ключа.
• надежная криптография совместно с процессами и процедурами управления ключами ***Из информации, относящейся к счету, ПО КРАЙНЕЙ МЕРЕ номер PAN должен быть приведен к нечитаемому виду.*** *Если по каким-либо причинам компания не может выполнять шифрование данных платежных карт, необходимо обратиться к приложению B: "Компенсационные меры".*	Цель надежной криптографии (см. определение и длины ключей в документе «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*)) заключается в том, что шифрование основывается на использовании протестированных, стандартизованных алгоритмов с высокой стойкостью (а не собственных или "доморощенных" алгоритмов).
3.4.1 При шифровании дисков (вместо шифрования на уровне файлов или на уровне полей базы данных) логический доступ должен управляться независимо от встроенных механизмов контроля доступа операционной системы (например, учетных записей локальной системы или Active Directory). Ключи дешифрования не должны быть привязаны к пользовательским учетным записям	Цель данного требования состоит в акцентировании внимания на приемлемости использования шифрования диска для приведения данных платежных карт к нечитаемому виду. При шифровании дисков шифруются данные, хранящиеся на жестком диске, они автоматически расшифровываются при их запросе авторизованным пользователем. Системы шифрования дисков перехватывают операции чтения и записи операционной системы и выполняют соответствующие криптографические преобразования, не требуя каких-либо дополнительных действий со стороны пользователя, за исключением ввода пароля или парольной фразы в начале сеанса. На основе данных характеристик шифрования дисков для соответствия данному требованию метод шифрования дисков не должен иметь:

Требование	Пояснение
	1) прямой связи с операционной системой либо 2) ключей дешифрования, связанных с учетными записями пользователей.
3.5 Ключи, использующиеся для шифрования данных платежных карт, должны быть защищены от несанкционированного разглашения и ненадлежащего использования:	Ключи шифрования должны быть надежно защищены, поскольку лица, получившие к ним доступ, смогут расшифровать данные.
3.5.1 Доступ к ключам должен быть предоставлен минимальному количеству сотрудников, которым он необходим	Необходимо максимально уменьшить количество лиц, имеющих доступ к ключам шифрования. Обычно это лица, отвечающие за хранение ключей.
3.5.2 Должно выполняться безопасное хранение ключей. Количество мест хранения ключей должно быть минимизировано	Ключи шифрования должны храниться в безопасности. Обычно они шифруются с использованием ключей для шифрования ключей и хранятся в минимально возможном количестве мест.
3.6 Должны быть полностью документированы и реализованы все процессы и процедуры управления ключами для ключей, использующихся при шифровании данных платежных карт, включая следующие:	Способ управления ключами шифрования представляет собой критичную часть непрерывного обеспечения безопасности средством шифрования. Правильно организованный процесс управления ключами, вне зависимости от того, выполняется ли он вручную или автоматически в составе продукта шифрования, включает все элементы с 3.6.1 по 3.6.10.
3.6.1 Генерация стойких ключей	Средство шифрования должно генерировать стойкие ключи, как определено в документе «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*) (“strong cryptography”).
3.6.2 Безопасное распределение ключей	Средство шифрования должно обеспечивать безопасное распределение ключей, здесь подразумевается, что ключи не должны распределяться в открытом виде.
3.6.3 Защищенное хранение ключей	Средство шифрования должно обеспечивать защищенное хранение ключей, здесь подразумевается, что ключи не должны храниться в открытом виде (необходимо шифровать их с использованием ключей для шифрования ключей).
3.6.4 Периодическая замена ключей: • в соответствии с рекомендациями и необходимостью связанного приложения (например, смена ключей шифрования); предпочтительно автоматически; • по крайней мере ежегодно.	Необходимо следовать процессам и рекомендациям по плановой замене ключей, если они предоставляются производителем средства шифрования. Ежегодная замена ключей шифрования является обязательной для минимизации рисков несанкционированного получения ключей шифрования и последующего дешифрования данных.
3.6.5 Уничтожение устаревших ключей	Устаревшие ключи, которые больше не используются или в которых нет необходимости, должны быть уничтожены. Если требуется хранение устаревших ключей (например, для поддержки архивированных зашифрованных данных), то они должны быть надежно защищены (см. п. 3.6.6).
3.6.6 Разделение ключевой информации между несколькими лицами и удвоенный контроль за ключами (чтобы для	Разделение ролей и удвоенный контроль за ключами используются для устранения возможности того, что один человек получит доступ к целому ключу. Такой контроль

Требование	Пояснение
восстановления ключа требовалось присутствие двух или трех человек, каждый из которых знает свою часть ключа)	обычно применяется для систем шифрования с ручным вводом ключа шифрования или в случае, когда управление ключами не реализовано в продукте шифрования. Такой тип контроля обычно реализуется в аппаратных модулях защиты.
3.6.7 Предотвращение несанкционированной подмены ключей	Средство шифрования не должно допускать или принимать подмену ключей, инициированную неавторизованными источниками или неожиданными процессами.
3.6.8 Замена скомпрометированных или заподозренных в компрометации ключей	Средство шифрования должно поддерживать и облегчать процесс замены скомпрометированных или заподозренных в компрометации ключей.
3.6.9 Отзыв истекших или недействительных ключей	Это требование позволяет гарантировать, что ключи не смогут больше использоваться.
3.6.10 Требование подписания соглашения сотрудниками, ответственными за хранение и использование ключей, в котором подтверждается, что они понимают обязанности и принимают ответственность по обеспечению защищенности ключей	Данный процесс позволяет гарантировать передачу роли хранителя ключей определенным лицам, которые признают свою ответственность.

Требование 4: Должно обеспечиваться шифрование данных платежных карт, передаваемых по сетям общего пользования

Критичная информация должна шифроваться при передаче по сетям, в которых велика вероятность перехвата, модификации и изменения маршрута следования данных при их передаче.

Требование	Пояснение
4.1 Для защиты критичных данных платежных карт при их передаче по сетям общего пользования должна использоваться надежная криптография и протоколы, обеспечивающие защиту передаваемых данных, например, SSL/TLS, IPSEC. *Примерами сетей общего пользования, которые находятся в области действия требований стандарта PCI DSS, являются Интернет, Wi-Fi (IEEE 802.11x), GSM и GPRS.*	Критичные данные должны шифроваться при передаче по сетям общего пользования, потому что злоумышленник может перехватить и/или изменить их маршрут при передаче. Необходимо обратить внимание на то, что версии протокола SSL, предшествующие версии 3.0, содержат документированные уязвимости, такие как переполнение буфера, которые могут быть использованы злоумышленником для получения контроля над системой.
4.1.1 Передаваемые в беспроводных сетях данные платежных карт должны шифроваться с использованием технологий WPA или WPA2, IPSEC VPN или SSL/TLS. Для обеспечения конфиденциальности и контроля доступа к беспроводной сети никогда не следует полагаться исключительно на WEP. В случае если используется WEP, необходимо: • в качестве минимально допустимой длины ключа шифрования использовать 104 бит, а вектора инициализации – 24 бит • использовать его только совместно с технологией WPA (или WPA22), VPN или SSL/TLS • проводить ежеквартальную замену WEP-ключей (если позволяет технология – автоматически) • заменять WEP-ключи при любых изменениях в составе персонала, обладающего доступом к ключам • ограничивать доступ на основе MAC-адресов	Злоумышленники используют свободно распространяемые и широкодоступные средства для прослушивания беспроводного трафика. Использование надлежащего шифрования может предотвратить прослушивание и раскрытие критичной информации, передаваемой по сети. При эскалации злоумышленником привилегий доступа из беспроводной сети в проводную возникло большое количество компрометаций данных платежных карт, хранящихся лишь в проводной сети. Запрещается использование WEP-шифрования без дополнительных защитных мер, поскольку оно является уязвимым из-за слабых векторов инициализации (IV), использующихся в процессе обмена WEP-ключами, и недостаточно частой смены ключей. Злоумышленник может воспользоваться свободно распространяемыми инструментами для перебора возможных комбинаций ключей и преодоления защиты, обеспечиваемой шифрованием WEP.
4.2 Никогда не должна выполняться отправка номеров PAN в незашифрованном виде по электронной почте.	Сообщения электронной почты могут быть перехвачены в процессе доставки почты с помощью анализаторов пакетов как во внутренней, так и во внешней общедоступной сети.

[2] Прим. ИЗ. Вероятно, опечатка в стандарте. WPA не может быть использован одновременно с WEP. Скорее всего имелось в виду совместное использование WEP и VPN или SSL|TLS.

Реализация программы управления уязвимостями

Требование 5: Должно использоваться и регулярно обновляться антивирусное программное обеспечение

Большое количество вирусов проникает в сеть компании в результате обмена сообщениями электронной почты. На всех системах, которые подвержены воздействию вирусов, должно быть установлено антивирусное программное обеспечение для их защиты от вредоносного программного обеспечения.

Требование	Пояснение
5.1 Антивирусное программное обеспечение должно быть установлено на всех системах, подверженных воздействию вирусов (персональных компьютерах и серверах). *К системам, подверженным воздействию вирусов, обычно не относят операционные системы на базе ОС UNIX или мейнфреймы.*	Существует большое количество атак, использующих широко известные эксплойты (часто опубликованные и распространяющиеся по сетям в пределах одного часа со времени обнаружения уязвимости), направленных против казалось бы полностью защищенных систем. Без наличия регулярно обновляемого антивирусного программного обеспечения сеть подвержена воздействию новых вирусов, которые могут нарушить ее работу.
5.1.1 Антивирусное программное обеспечение должно обладать способностью обнаружения, удаления и защиты от различных видов вредоносного программного обеспечения (включая spyware, adware)	Важно осуществлять защиту от **всех** типов и видов вредоносного программного обеспечения.
5.2 Должна быть включена постоянная антивирусная защита, механизмы обеспечения антивирусной защиты должны регулярно обновляться и обладать возможностью генерации журналов регистрации событий.	Даже лучшее антивирусное программное обеспечение обладает ограниченной эффективностью в случае, если используются неактуальные базы сигнатур вирусов и если оно не запущено на точках доступа в сеть или на отдельных компьютерах. Журналы регистрации событий предоставляют возможность мониторинга за вирусной активностью и ответными действиями антивирусного программного обеспечения.

Требование 6: Должна обеспечиваться безопасность при разработке и поддержке систем и приложений

Злоумышленники используют уязвимости в системе защиты для получения привилегированного доступа в компьютерные системы. Большинство уязвимостей устраняются с помощью обновлений безопасности, предоставляемых производителями. Для защиты от эксплуатации уязвимостей внутренними и внешними злоумышленниками, а также вирусами на всех системах должны быть установлены последние выпущенные приемлемые обновления безопасности. Приемлемые обновления безопасности – это такие обновления, которые были в достаточной степени проанализированы и протестированы, чтобы определить, что их установка не приведет к конфликтам с действующими защищенными конфигурациями. Если выполняется разработка приложений внутри организации, большого количества уязвимостей можно избежать, используя стандартные процессы разработки систем и приемы безопасного программирования.

Требование	Пояснение
6.1 Для всех системных компонентов и программного обеспечения должны быть установлены самые последние обновления безопасности, предоставленные производителями. Обновления безопасности, относящиеся к используемым системам, должны быть установлены в течение одного месяца с момента их выпуска.	Существует большое количество атак, использующих широко известные эксплойты (часто опубликованные в пределах одного часа со времени обнаружения уязвимости), направленных против казалось бы полностью защищенных систем. Без оперативного внедрения наиболее актуальных обновлений безопасности злоумышленник может использовать эти эксплойты для проведения атак на сеть и нарушения ее работы. Необходимо определить приоритеты применения обновлений таким образом, что критичные обновления безопасности устанавливаются на критичные или подверженные риску системы в течение 30 дней, а обновлениям с меньшим уровнем риска назначается более низкий приоритет.
6.2 Должен существовать процесс идентификации вновь обнаруженных уязвимостей безопасности (например, подписка на рассылки, связанные с информационной безопасностью и обнаружением уязвимостей, свободно доступные в сети Интернет). Должно выполняться обновление стандартов конфигурирования с целью устранения новых обнаруженных уязвимостей.	Цель данного требования состоит в том, что организации должны своевременно узнавать о новых уязвимостях для того, чтобы они могли защищать свои сети и внедрять процедуры устранения вновь обнаруженных и имеющих отношение к их системам уязвимостей в свои стандарты конфигурирования.
6.3 Разработка программного обеспечения должна производиться с учетом накопленного в данной отрасли опыта и учитывать вопросы обеспечения информационной безопасности на всех стадиях процесса разработки.	Если не уделять должного внимания безопасности информации на этапах разработки программного обеспечения (определения требований, проектирования, анализа и тестирования), в среду эксплуатации непреднамеренно или сознательно могут быть внесены уязвимости в системе безопасности.
6.3.1 До внедрения в среду эксплуатации должно выполняться тестирование всех обновлений безопасности, а также изменений в конфигурации систем и программного обеспечения	Необходимо удостовериться, что все инсталляции и изменения выполняются так, как планировалось, и не обладают иными недокументированными, ненужными или вредоносными функциями.
6.3.2 Должны быть разделены среды разработки, тестирования и эксплуатации	Как правило, среда разработки и среда тестирования менее защищены, чем среда эксплуатации. Без надлежащего разделения эксплуатационная среда и данные платежных карт могут подвергаться риску вследствие уязвимостей или ненадежных внутренних процессов.

Требование	Пояснение
6.3.3 Должно существовать разделение обязанностей в средах разработки, тестирования и эксплуатации	Это позволит минимизировать количество сотрудников с доступом к эксплуатационной среде и данным платежных карт и поможет гарантировать, что доступ предоставляется только тем сотрудникам, кому он в действительности нужен.
6.3.4 Для тестирования или разработки не должно использоваться данных из среды эксплуатации (реальных номеров PAN)	В среде разработки обычно осуществляется менее жесткий контроль за обеспечением безопасности. Использование в такой среде реальных данных позволит потенциальным злоумышленникам, равно как и разработчикам, получить неавторизованный доступ к информации, используемой в эксплуатационной среде.
6.3.5 Должно выполняться удаление тестовых учетных записей и данных до внедрения в среду эксплуатации	Тестовые данные и учетные записи должны удаляться из кода перед активацией приложения, поскольку они могут предоставить информацию о функционировании приложения. Обладание такой информацией может облегчить компрометацию приложения и связанных с ним данных платежных карт.
6.3.6 Учетные записи, имена пользователей и пароли в разработанном программном обеспечении должны быть удалены до внедрения этого программного обеспечения в среду эксплуатации или его передачи заказчику	Учетные записи заказных приложений, имена пользователей и пароли должны удаляться из кода перед активацией приложения или его передачей клиентам, поскольку они могут предоставить информацию о функционировании приложения. Обладание такой информацией может облегчить компрометацию приложения и связанных с ним данных платежных карт.
6.3.7 Для идентификации потенциальных уязвимостей в разработанном программном обеспечении должен выполняться анализ кода перед запуском этого ПО в эксплуатацию или его передачей заказчику	Уязвимости безопасности кода заказных приложений обычно эксплуатируются злоумышленниками для получения доступа к сети и компрометации данных платежных карт. Поэтому для идентификации уязвимостей анализ кода должны выполнять лица, владеющие приемами безопасного программирования.
6.4 При внесении любых изменений в системы и программное обеспечение необходимо следовать процедурам управления изменениями. Эти процедуры должны включать:	Без надлежащего контроля изменений программного обеспечения возможности защиты могут быть непреднамеренно или сознательно упущены или отключены, возможно появление ошибок обработки или внедрение вредоносного кода. Если используются недостаточно основательные политики проверки биографии принимаемых на работу сотрудников и контроля доступа к системе, то существует риск того, что неблагонадежные и недостаточно подготовленные сотрудники смогут получить неограниченный доступ к программному коду, а уволившиеся сотрудники будут иметь возможность компрометации систем, при этом определить неавторизованные действия будет невозможно.
6.4.1 Документирование влияния, оказываемого изменением	Необходимо документировать влияние, которое может быть нанесено изменением, чтобы все вовлеченные стороны могли надлежащим образом запланировать все изменения в обработке данных.
6.4.2 Утверждение руководством	Утверждение руководством указывает на то, что изменение является легитимным, авторизованным и санкционированным организацией.
6.4.3 Тестирование работоспособности	Тщательное тестирование должно выполняться для проверки того, что любая

Требование	Пояснение
	активность ожидаема, данные в отчетах точны и выполняется корректная обработка всех ошибочных состояний и т. п.
6.4.4 Процедуры отката	Для каждого изменения должна существовать процедура отката, которая в случае сбоя при применении изменения позволит вернуть систему в первоначальное состояние.
6.5 Все web-приложения должны разрабатываться с учетом рекомендаций по программированию защищенных web-приложений, например, рекомендаций OWASP. С целью идентификации уязвимостей, связанных с ошибками программирования, должен выполняться анализ кода разработанных приложений, при этом должно выполняться предотвращение следующих распространенных уязвимостей:	Прикладной уровень подвержен высокому риску и может являться целью как внутренних, так и внешних угроз. Без надлежащей защиты данные платежных карт и другая конфиденциальная информация компании могут быть раскрыты, что приведет к нанесению ущерба компании, ее клиентам и ее репутации.
6.5.1 Отсутствие проверки корректности вводимых данных	Необходимо выполнять проверку данных, получаемых от web-запросов, перед их передачей web-приложению – например, выполнять проверки на то, что введены только буквы, буквы и цифры и т. д. Без выполнения подобных проверок злоумышленник сможет передать приложению неверные данные и атаковать компоненты внутренней сети с использованием этого приложения.
6.5.2 Уязвимости механизмов контроля доступа (например, злоумышленное использование идентификаторов пользователей)	Злоумышленники часто пытаются просканировать и перечислить существующие в приложениях пользовательские учетные записи для того, чтобы найти точку входа для проведения атаки. Как только существующая учетная запись будет обнаружена, злоумышленник может попытаться использовать пароли, заданные по умолчанию, или выполнить подбор паролей методом перебора для получения доступа к приложению.
6.5.3 Уязвимости подсистемы аутентификации и управления сеансами (использование учетных данных и сеансовых cookie)	Учетные данные и "маркеры" сеанса должны быть надежно защищены. Атаки, направленные на пароли, ключи, сеансовые файлы “cookie” или другие маркеры, могут помочь злоумышленнику обойти требования аутентификации и попробовать угадать идентификаторы других пользователей. Кроме того, файлы “cookie” могут содержать информацию платежных карт и по умолчанию сохраняться в открытом виде.
6.5.4 Атаки типа Cross-Site Scripting (XSS)	При атаке данного типа web-приложение используется для отправки атаки браузеру конечного пользователя, что может привести к раскрытию маркера сеанса конечного пользователя, атаке на его компьютер, а также отправке подмененного содержимого для обмана пользователя.
6.5.5 Переполнение буфера	Злоумышленник может повредить компоненты web-приложения, которые не обрабатывают должным образом данные, введенные пользователем (см. п. 6.5.1), и получить контроль над процессами на сервере с web-приложением.
6.5.6 Инъекции (например, SQL-инъекции)	Для повышения скорости подключения и уменьшения нагрузки на стороне сервера часто требуется выполнять проверку и обработку вводимых пользователем данных на

Требование	Пояснение
	стороне клиента. Обычно обход данной проверки является относительно тривиальной задачей для злоумышленника, после чего web-приложение используется для отправки вредоносных команд серверу для запуска атак на переполнение буфера, получения конфиденциальной информации или выявления особенностей функционирования серверного приложения. Данная уязвимость также является популярным средством для выполнения мошеннических транзакций на сайтах электронной коммерции.
6.5.7 Некорректная обработка ошибок	Зачастую некорректная обработка ошибок может предоставить злоумышленнику информацию, которая поможет ему скомпрометировать систему. Если злоумышленник сможет вызвать появление ошибок, которые web-приложение не сможет правильно обработать, существует возможность получения злоумышленником подробной информации о системе, возникновения ситуации отказа в обслуживании, нарушения работы системы безопасности или сбоя сервера. Например, сообщение «введен неправильный пароль» говорит о том, что использовалось верное имя пользователя и необходимо сфокусировать свои усилия только на подборе пароля. *Необходимо использовать сообщения об ошибках более общего характера, например, «данные не могут подтверждены».*
6.5.8 Небезопасное хранение	Это имеет отношение к ненадежному использованию криптографии. Приложения, использующие криптографию, являются сложными для правильного программирования, что обычно сказывается на слабой защите хранимых данных и использовании криптографии, которая легко взламываются.
6.5.9 Отказ в обслуживании	Злоумышленники могут использовать ресурсы web-приложения до их полного исчерпания для того, чтобы другие пользователи не смогли использовать приложение. Злоумышленники также могут заблокировать пользовательские учетные записи или вызвать сбой приложения.
6.5.10 Небезопасное управление конфигурациями	Наличие надежного стандарта конфигурирования сервера критично для защиты web-приложений. Существует большое количество параметров конфигурации для управления безопасностью серверов, которые по умолчанию не настроены.
6.6 Все web-приложения должны быть защищены от известных атак, используя один из приведенных ниже методов:	Атаки, направленные на web-приложения, являются распространенными и обычно успешными, если при разработке web-приложений не использовались приемы безопасного программирования. Целью требования анализа кода приложений или использования межсетевых экранов прикладного уровня является значительное снижение количества компрометаций web-приложений, которые приводят к утечке данных платежных карт.
• Выполнение анализа кода всех разработанных приложений организацией, специализирующейся в области безопасности приложений, на предмет наличия	Также для удовлетворения данному требованию может использоваться инструментарий, выполняющий анализ кода и/или мониторинга его изменений.

Требование	Пояснение
распространенных уязвимостей.	
• Установка межсетевого экрана прикладного уровня перед web-приложениями. *Требование 6.6 до 30 июня 2008 г. носит рекомендательный характер, после чего становится обязательным.*	Межсетевые экраны прикладного уровня используются для фильтрации и блокировки ненужного трафика на уровне приложений. Работая вместе с межсетевым экраном сетевого уровня, правильно сконфигурированный межсетевой экран прикладного уровня позволит предотвратить атаки уровня приложений.

Реализация мер по строгому контролю доступа

Требование 7: Доступ к данным платежных карт должен быть ограничен в соответствии со служебной необходимостью

Данное требование обеспечивает то, что доступ к критичным данным может быть осуществлен только авторизованными сотрудниками.

Требование	Пояснение
7.1 Доступ к вычислительным ресурсам и данным платежных карт должен быть предоставлен только тем сотрудникам, которым он необходим для выполнения должностных обязанностей.	Чем больше людей имеют доступ к данным платежных карт, тем выше риск злонамеренного использования пользовательских учетных записей. Предоставление доступа лишь тем сотрудникам, которым он необходим для выполнения должностных обязанностей, позволит организации предотвратить ненадлежащее обращение с данными платежных карт, связанное с отсутствием опыта или со злым умыслом. В организации должна быть разработана политика контроля доступа к данным, определяющая, как и кому предоставляется доступ.
7.2 Для многопользовательских систем должен быть реализован механизм предоставления доступа, ограничивающий доступ по принципу необходимого знания (need-to-know), запрещающий любой доступ, не разрешенный явно.	Без механизма предоставления доступа по принципу минимальной достаточности пользователь может получить доступ к данным платежных карт, в действительности не нуждаясь в этом для выполнения должностных обязанностей.

Требование 8: Каждому лицу, имеющему доступ к вычислительным ресурсам, должен быть назначен уникальный идентификатор

Назначение уникального идентификатора каждому лицу с правом доступа обеспечит возможность выполнения действий над критичными данными и системами авторизованными пользователями и отслеживания действий, выполненных конкретными авторизованными пользователями.

Требование	Пояснение
8.1 Каждому пользователю должно быть назначено уникальное имя пользователя до предоставления доступа к системным компонентам или данным платежных карт.	Уникально идентифицируя каждого пользователя – вместо использования одного идентификатора для нескольких сотрудников – организация может поддерживать индивидуальную ответственность сотрудников за свои действия и эффективно отслеживать все действия, выполняемые каждым сотрудником. Это поможет ускорить разрешение и предотвращение происходящих инцидентов, связанных с информационной безопасностью.
8.2 В дополнение к назначению уникального идентификатора для всех пользователей должен использоваться по крайней мере один из следующих механизмов аутентификации: • Пароль • Устройства аутентификации (например, SecureID, сертификаты или открытые ключи) • Биометрия	Данные элементы аутентификации при использовании совместно с уникальными идентификаторами помогают защитить уникальные идентификаторы пользователей от компрометации (поскольку злоумышленнику нужно знать и уникальный идентификатор, и пароль или другой элемент аутентификации).
8.3 Для предоставления удаленного доступа в сеть служащим компании, администраторам или третьим лицам должна быть реализована двухфакторная аутентификация. Должны использоваться такие технологии, как RADIUS или TACACS с аппаратными устройствами аутентификации; либо VPN (на базе протоколов SSL/TLS или IPSEC) с пользовательскими сертификатами.	Одна из технологий двухфакторной аутентификации – двухфакторная аутентификация с использованием одноразовых паролей (one-time passwords) применяется в тех случаях, когда требуется дополнительный элемент аутентификации для осуществления доступа из сред с высоким риском, например, при доступе из внешней сети. Для повышения уровня безопасности организация может также использовать двухфакторную аутентификацию при осуществлении доступа из сетей с более низким уровнем безопасности в сети с более высоким уровнем безопасности (например, при обращении с корпоративных рабочих станций (более низкий уровень безопасности) к серверам/базам данных с данными платежных карт (более высокий уровень безопасности)).
8.4 Все пароли должны находиться в зашифрованном виде как при передаче, так и при хранении на любых системных компонентах.	Многие сетевые устройства и приложения передают пользовательский идентификатор и незашифрованный пароль по сети и/или хранят пароли в открытом виде (без применения шифрования). Злоумышленник может перехватить незашифрованные идентификатор пользователя и пароль при их передаче, используя анализатор пакетов, или получить прямой доступ к идентификаторам и незашифрованным паролям в файлах, в которых они хранятся, и использовать эти данные для получения несанкционированного доступа.
8.5 Для учетных записей сотрудников и администраторов на всех системных компонентах должны обеспечиваться надежная	Поскольку одним из первых действий, которые злоумышленник предпринимает при компрометации системы, является эксплуатация слабых или отсутствующих паролей,

Требование	Пояснение
аутентификация и управление паролями, как описано в нижеследующих пунктах:	важно правильно реализовать процессы для аутентификации пользователей и управления паролями.
8.5.1 Должно контролироваться добавление, удаление и изменение пользовательских идентификаторов, учетных данных и других объектов идентификации	Для обеспечения гарантии, что добавляемые к системам пользователи действительны и правомочны, операциями добавления, удаления и изменения пользовательских идентификаторов должна управлять небольшая группа сотрудников со специальными полномочиями. Только члены этой небольшой группы должны управлять идентификаторами пользователей.
8.5.2 Должна выполняться проверка подлинности пользователей перед сбросом их паролей	Многие злоумышленники используют социальную инженерию – например, звонят в службу поддержки для изменения пароля и действуют как легитимный пользователь, чтобы затем получить возможность использовать идентификатор пользователя. Необходимо продумать использование секретного вопроса, ответ на который может дать только реальный пользователь, для помощи администраторам в идентификации пользователя при восстановлении его пароля. Необходимо гарантировать, что эти вопросы должным образом защищены и не являются общими.
8.5.3 Первоначальные пароли для каждого пользователя должны быть уникальными и изменяться сразу же после первого использования	Если для каждого нового пользователя устанавливается один и тот же пароль, то внутренний пользователь, бывший сотрудник или злоумышленник могут знать или легко обнаружить этот пароль и использовать его для получения доступа к учетным записям.
8.5.4. Доступ для каждого сотрудника при его увольнении должен немедленно аннулироваться	Если сотрудник уволился из компании и все еще имеет доступ к ее ресурсам с использованием своей учетной записи, возможен несанкционированный и злонамеренный доступ к данным платежных карт. Такой доступ может получить как бывший сотрудник, так и злоумышленник, использующий его учетную запись или другие неиспользуемые учетные записи. Рассмотрите возможность организации процесса увольнения вместе с департаментом по управлению персоналом таким образом, чтобы происходило немедленное уведомление об увольнении сотрудника, для того чтобы его учетные записи были сразу заблокированы.
8.5.5 Должно выполняться удаление неактивных учетных записей пользователей по крайней мере каждые 90 дней	Существование неактивных учетных записей может предоставить возможность эксплуатации неавторизованным пользователем неиспользуемой учетной записи и осуществления доступа к данным платежных карт.
8.5.6 Учетные записи, использующиеся производителями для осуществления удаленной поддержки, должны активироваться только на период оказания поддержки	Предоставление производителям (например, производителям POS-терминалов) круглосуточного доступа в сеть организации семь дней в неделю для поддержки систем увеличивает вероятность несанкционированного доступа, осуществляемого пользователями среды производителя или злоумышленником, который обнаружит и сможет использовать внешнюю, готовую к приему подключений, точку входа в сеть. За более подробными сведениями по данной теме необходимо обратиться к пп. 12.3.8 и 12.3.9.
8.5.7 Парольные политики и процедуры должны быть доведены	Информирование всех пользователей об используемых процедурах управления

Требование	Пояснение
до всех пользователей, обладающих возможностью доступа к данным платежных карт	паролями поможет пользователям понять эти процедуры и следовать политикам, а также предупреждать обо всех злоумышленниках, которые могут попытаться использовать их пароли для получения доступа к данным платежных карт (например, звонящих сотруднику с просьбой дать его пароль для решения какой-либо проблемы).
8.5.8. Не должны использоваться групповые, разделяемые или встроенные учетные записи и пароли	При использовании несколькими пользователями одной и той же учетной записи и пароля становится невозможным назначить ответственность за действия, выполненные индивидуальным пользователем, или эффективно регистрировать события, связанные с этими действиями, поскольку эти действия могут быть совершены любым членом группы.
8.5.9. Пользовательские пароли должны изменяться по крайней мере каждые 90 дней	Надежные пароли являются первой линией обороны в сети, поскольку злоумышленник обычно сначала пытается найти учетные записи со слабыми или отсутствующими паролями. У злоумышленника больше шансов найти слабо защищенные учетные записи и скомпрометировать сеть под видом настоящего пользователя, если используются короткие, легко угадываемые или не изменяемые в течение длительного времени пароли. Можно принудительно применить перечисленные к надежным паролям требования, активируя встроенные возможности защиты учетных записей и паролей операционной системы (например, Windows), сетей, баз данных и других платформ.
8.5.10 Минимальная длина паролей должна составлять не менее 7 символов	
8.5.11 Пароли должны состоять из числовых и буквенных символов	
8.5.12 Должно быть запрещено задание нового пароля, если он совпадает с любым из последних четырех ранее использовавшихся паролей	
8.5.13 Количество неудачных попыток получения доступа должно быть ограничено блокированием идентификатора пользователя по крайней мере после шести неудачных попыток	Без реализованного механизма блокировки учетных записей злоумышленник может непрерывно пытаться подобрать пароль или вручную, или с использованием автоматизированных средств (программ взлома паролей) до достижения успеха и получения доступа к пользовательской учетной записи.
8.5.14 Продолжительность блокирования идентификатора пользователя должна составлять 30 минут или до активации учетной записи администратором	Если учетная запись пользователя блокируется в результате непрекращающихся попыток подбора пароля, защитные меры в виде задержки активации заблокированных учетных записей помогут остановить злоумышленника от непрерывного подбора пароля (он будет вынужден остановиться по крайней мере на 30 минут до автоматической активации учетной записи). Кроме того, если требуется вмешательство администратора или службы «Help Desk» для активации учетной записи, может быть установлено, действительно ли владелец учетной записи (из-за опечаток) является причиной блокировки.
8.5.15 При отсутствии активности во время пользовательского сеанса более чем 15 минут должен выполняться повторный запрос пароля пользователя для разблокирования терминала	Когда пользователи отлучаются от работающих компьютеров, имеющих доступ к критичным данным сети или данным платежных карт, эти компьютеры могут использоваться кем-нибудь в их отсутствие, что приведет к несанкционированному доступу к учетной записи и/или ненадлежащему ее использованию.
8.5.16 Должен аутентифицироваться любой доступ к любой	Без использования аутентификации базы данных увеличивается потенциальная

Требование	Пояснение
базе данных, содержащей данные платежных карт, в том числе доступ, осуществляемый приложениями, администраторами и любыми другими пользователями	возможность неавторизованного или злонамеренного доступа к ней. Кроме того, события, связанные с таким доступом, не могут быть зарегистрированы, поскольку пользователь не аутентифицируется и, следовательно, неизвестен системе. Кроме того, доступ к базам данных должен всегда осуществляться посредством запрограммированных хранимых процедур, а не посредством прямого доступа к базе данных конечными пользователями (за исключением администраторов баз данных, которые могут иметь прямой доступ к базе данных для выполнения своих административных обязанностей).

Требование 9: Физический доступ к данным платежных карт должен быть ограничен

Любой физический доступ к данным или системам, содержащим данные платежных карт, предоставляет возможность получения контроля над устройствами или данными, в том числе возможность удаления систем или печатных копий, и должен строго ограничиваться.

Требование	Пояснение
9.1 Для ограничения и отслеживания физического доступа к системам, в которых хранятся, обрабатываются или передаются данные платежных карт, должен использоваться надежный механизм контроля доступа в помещения.	Без контроля физического доступа существует возможность получения доступа к помещению и к критичной информации неавторизованными лицами, а также возможность изменения ими конфигураций систем, внесения уязвимостей в сеть, уничтожения или кражи оборудования.
9.1.1 Для наблюдения за критичными помещениями должны использоваться видеокамеры. Должен проводиться анализ собранных данных и их сопоставление с другими событиями. Данные видеонаблюдения должны храниться по крайней мере в течение 3 месяцев, если это не противоречит законодательству	При отсутствии наблюдения за критичными системами гораздо труднее предотвратить и расследовать нарушения физического периметра и невозможно идентифицировать злоумышленников.
9.1.2 Физический доступ к сетевым разъемам, расположенным в публично доступных местах, должен быть ограничен	Ограничение доступа к сетевым разъемам предотвратит подключение злоумышленника к легкодоступным сетевым разъемам и, следовательно, от возможности подключения к внутренним сетевым ресурсам. Необходимо отключать сетевые разъемы, когда они не используются, и включать их только при возникновении необходимости. В общественных помещениях, таких как конференц-залы, необходимо реализовывать частные сети для предоставления производителям и посетителям доступа в сеть Интернет лишь таким образом, чтобы у них не было доступа во внутреннюю сеть.
9.1.3 Физический доступ к беспроводным точкам доступа, маршрутизаторам и портативным устройствам должен быть ограничен	Без обеспечения защиты доступа к беспроводным компонентам и устройствам злоумышленники могут использовать неконтролируемые беспроводные устройства компании для получения доступа к сетевым ресурсам или даже подключать собственные устройства к беспроводной сети и получать возможность неавторизованного доступа. Необходимо продумать размещение беспроводных точек доступа и маршрутизаторов в надежных местах хранения, например, в запираемых шкафах. Необходимо гарантировать использование надежного шифрования, также необходимо активировать автоматическую блокировку на беспроводных портативных устройствах, наступающую после периода бездействия, и настроить требование ввода пароля при включении.
9.2 Должны быть разработаны процедуры, позволяющие персоналу легко отличать сотрудников компании от посетителей, особенно в тех помещениях, в которых существует возможность получения доступа к данным платежных карт. *В данном контексте под «сотрудником» понимаются сотрудники, работающие в компании полный рабочий день, или*	Без систем идентификации сотрудников (например, бейджей) и контроля за входом в помещения неавторизованные и злонамеренные пользователи могут легко получить доступ к помещениям с целью кражи, отключения, разрушения и уничтожения критичных систем и данных платежных карт. Для оптимального контроля необходимо рассмотреть реализацию системы контроля доступа с использованием бейджей или карточек при входе и выходе из помещений, содержащих данные платежных карт.

Требование	Пояснение
частично занятые сотрудники, временные сотрудники и персонал, а также консультанты, постоянно находящиеся в компании. Термин «посетитель» относится к производителям, гостям сотрудников, обслуживающему персоналу или лицам, которым необходимо посетить помещение в течение непродолжительного промежутка времени, обычно не превышающего один день.	
9.3 В отношении всех посетителей должно выполняться следующее:	Контроль над посетителями очень важен для уменьшения возможности получения доступа в помещения компании неавторизованными пользователями и злоумышленниками (а потенциально и к данным платежных карт).
9.3.1 Авторизация до входа в помещения, в которых обрабатываются данные платежных карт 9.3.2 Выдача физического средства идентификации (например, идентификационной карточки или устройства доступа) с ограниченным сроком действия, отличающего посетителей от сотрудников компании 9.3.3 Изъятие физического средства идентификации перед уходом или по истечении срока действия	Контроль над посетителями очень важен для гарантии того, что посетители смогут входить лишь в те помещения, полномочия на вход в которые им предоставлены; что они идентифицируются именно как посетители и сотрудники смогут наблюдать за их деятельностью; и что продолжительность их доступа ограничена допустимым временем посещения.
9.4 Должен использоваться журнал регистрации посетителей с целью хранения записей о посетителях. Данный журнал должен храниться по крайней мере в течение 3 месяцев, если это не противоречит законодательству.	Журнал регистрации посетителей является недорогим и несложным в поддержке и может оказать помощь во время расследования потенциальных инцидентов, в идентификации физического доступа в здание или помещение и потенциального доступа к данным платежных карт. Необходимо предусмотреть реализацию журналов на входах в помещения, в особенности, в те зоны, где присутствуют данные платежных карт.
9.5 Носители с резервными копиями должны храниться в защищенных местах, предпочтительно во внешних помещениях, например, альтернативном или резервном помещении или в коммерческом хранилище информации.	Резервные копии могут содержать данные платежных карт и в случае их хранения в незащищенных помещениях они могут быть легко утеряны, украдены или скопированы со злым умыслом. Для обеспечения защищенного хранения необходимо рассмотреть возможность заключения договора с коммерческой компанией, занимающейся хранением данных, или, для небольших компаний, использовать сейф.
9.6 Должна обеспечиваться физическая защита всех бумажных и электронных носителей (включая компьютеры, электронные носители, сетевое и коммуникационное оборудование, телекоммуникационные линии, чеки, распечатанные отчеты и факсы), содержащих данные платежных карт.	Данные платежных карт восприимчивы к неавторизованному просмотру, копированию или сканированию, если они не защищены должным образом на портативных носителях, распечатаны или оставлены без присмотра у какого-либо сотрудника на столе. Необходимо продумать процедуры и процессы защиты данных платежных карт на носителях, передаваемых внутренним или внешним пользователям. В отсутствие таких процедур данные могут быть утеряны, украдены и использованы в мошеннических целях.

Требование	Пояснение
9.7 Должен обеспечиваться строгий контроль над внутренним или внешним перемещением носителей всех видов, содержащих данные платежных карт, включая следующее:	
9.7.1 Маркировку носителей, чтобы они могли быть идентифицированы как содержащие конфиденциальную информацию	С носителем, который не маркирован как конфиденциальный, сотрудники могут обращаться без должного внимания, что может привести к его утере или краже. Необходимо включить процесс классификации носителей в процедуры п. 9.6.
9.7.2 Отправку носителей с доверенным курьером или с помощью другого способа доставки, который можно проконтролировать	Носитель может быть утерян или украден при отправке с использованием неотслеживаемого метода, такого как обычная почта. Необходимо заключить договор со службой безопасной доставки для доставки всех носителей, которые содержат данные платежных карт, для того, чтобы иметь возможность использовать их систему слежения для поддержки инвентаризации и местонахождения отправлений.
9.8 Руководство должно утверждать перемещение всех носителей за пределы защищенной территории (в особенности если носители передаются отдельным лицам).	Перемещение данных платежных карт за пределы защищенной территории вне рамок процесса, утвержденного руководством, может привести к их утере или краже. Без наличия жесткого процесса не отслеживается размещение носителей, а также отсутствует процесс контроля над перемещением данных и их защитой. Необходимо включить разработку утвержденного руководством процесса перемещения носителей в процедуры, рекомендованные п. 9.6.
9.9 Должен обеспечиваться строгий контроль хранения и доступности носителей, содержащих данные платежных карт	Без точных методов инвентаризации и контроля за хранением факт кражи или утери носителя может оставаться незамеченным в течение неопределенного периода времени. Необходимо включить разработку процесса ограничения доступа к носителям с данными платежных карт в процедуры, рекомендованные п. 9.6.
9.9.1 Должны выполняться инвентаризация и защищенное хранение всех носителей	Если инвентаризация носителей не выполняется, то факт кражи или утери носителя может оставаться незамеченным в течение длительного периода времени. Необходимо включить разработку процесса инвентаризации носителей и их защищенного хранения в процедуры, рекомендованные п. 9.6.
9.10 Носители, содержащие данные платежных карт, должны уничтожаться перечисленными ниже способами, если их хранение больше не обосновано с точки зрения соблюдения требований законодательства или выполнения бизнес-задач:	Если не выполняется уничтожение информации, содержащейся на жестких дисках компьютеров, компакт-дисках или на бумаге, использование подобной информации может привести к компрометации, а следовательно, к финансовым потерям, а также потере репутации. Например, злоумышленники могут использовать прием, известный под названием «разгребание мусора» (“dumpster diving”), при котором они просматривают мусор и используют найденную информацию для начала проведения атаки. Необходимо включить разработку процесса надлежащего уничтожения носителей с данными платежных карт, включая надежное хранение носителей до уничтожения, в процедуры, рекомендованные п. 9.6.
9.10.1. Перекрестным измельчением, сожжением или преобразованием в целлюлозную массу печатных документов	
9.10.2 Удалением без возможности восстановления, размагничиванием, измельчением или уничтожением иным способом электронных носителей для исключения возможности воссоздания данных платежных карт	

Регулярный мониторинг и тестирование сетей

Требование 10: Должен отслеживаться и контролироваться любой доступ к сетевым ресурсам и данным платежных карт

Механизмы регистрации событий и возможность отслеживания действий пользователей крайне необходимы. Наличие зарегистрированных событий во всех средах предоставляет возможность расследования и анализа при инцидентах. Определение причины компрометации является крайне затруднительным без журналов регистрации событий.

Требование	Пояснение
10.1 Должен быть реализован процесс, связывающий осуществление любого доступа к системным компонентам (в особенности доступа с использованием административных привилегий, например, root) с конкретными пользователями.	Важно иметь процесс или систему, которые связывают пользовательский доступ с системными компонентами, к которым он осуществлен, в особенности для пользователей с административными привилегиями. Данная система будет генерировать журналы регистрации выполненных действий и будет предоставлять возможность выяснения происхождения подозрительной активности до конкретного пользователя. Группы, расследующие инциденты, полагаются на подобные журналы для начала проведения расследования.
10.2 Для всех системных компонентов должна выполняться регистрация событий с целью восстановления: 10.2.1 Любого пользовательского доступа к данным платежных карт 10.2.2 Всех действий, выполненных с использованием административных привилегий 10.2.3 Доступа ко всем журналам регистрации событий 10.2.4 Неудачных попыток логического доступа 10.2.5 Использования механизмов идентификации и аутентификации 10.2.6 Инициализации журналов регистрации событий 10.2.7 Создания и удаления системных объектов	Злоумышленники обычно предпринимают многочисленные попытки доступа к целевым системам. Генерация журналов регистрации событий подозрительной деятельности позволит предупредить системного администратора, может отправить данные к другим устройствам мониторинга (например, системам обнаружения вторжений), а также может предоставить хронологию событий для расследования инцидентов безопасности.
10.3 В регистрируемых событиях для каждого системного компонента должны записываться по крайней мере следующие элементы: 10.3.1 Идентификатор пользователя 10.3.2 Тип события 10.3.3 Дата и время 10.3.4 Индикатор успеха или отказа 10.3.5 Источник события 10.3.6 Идентификатор или название задействованных данных, системного компонента или ресурса	Записывая перечисленные элементы для контролируемых событий, перечисленных в п. 10.2, можно быстро идентифицировать потенциальную компрометацию и иметь достаточно сведений о том, кто, что, когда, где и как сделал.

Требование	Пояснение
10.4 Должна выполняться синхронизация времени на всех критичных системах.	Если злоумышленнику удалось войти в сеть, обычно он пытается изменить временные отметки своих действий в журналах регистрации событий для предотвращения обнаружения своей активности. Для групп, расследующих инциденты, время совершения каждого действия является критичным для определения способов компрометации систем. Злоумышленник может также попытаться напрямую изменить время на сервере времени, если отсутствуют надлежащие ограничения доступа, и установить время равным времени до его проникновения в сеть.
10.5 Журналы регистрации событий должны быть защищены от внесения изменений.	Обычно злоумышленники, проникшие в сеть, пытаются внести изменения в журналы регистрации событий для того, чтобы скрыть свои действия. При недостаточной защите журналов гарантировать их полноту, точность и целостность будет невозможно, и они будут бесполезны в качестве средства расследования после компрометации.
10.5.1 Просмотр журналов регистрации событий должен быть разрешен только тем сотрудникам, кому это необходимо для выполнения должностных обязанностей 10.5.2 Файлы журналов регистрации событий должны быть защищены от несанкционированных изменений 10.5.3 Должно выполняться своевременное резервирование файлов с зарегистрированными событиями на централизованный log-сервер или носители, где их сложнее изменить 10.5.4 Журналы регистрации событий для беспроводных сетей должны копироваться на log-сервер во внутренней сети	Достаточная защита журналов аудита включает строгий контроль доступа (ограничение доступа к журналам по принципу необходимого знания) и использование внутренней сегрегации (чтобы затруднить поиск и модификацию журналов).
10.5.5 Для журналов регистрации событий должно использоваться программное обеспечение контроля целостности файлов и обнаружения изменений для обеспечения того, что существующие данные в журналах не смогут быть изменены без генерации предупреждения (при этом добавление новых данных не должно вызывать генерации предупреждения)	Обычно системы мониторинга целостности файлов выполняют проверку на внесение изменений в критичные файлы и генерируют предупреждения при обнаружении изменений. В целях мониторинга целостности файлов система выполняет мониторинг файлов, которые обычно не меняются, но изменение которых может свидетельствовать о компрометации. Для файлов журналов (которые часто меняются) необходимо проводить мониторинг операций удаления, неожиданного увеличения или уменьшения и любых других показателей изменения файла журнала злоумышленником. Для мониторинга целостности файлов существуют как коммерческие продукты, так и программы с открытым исходным кодом.
10.6 Должен выполняться по крайней мере ежедневный просмотр журналов зарегистрированных событий для всех системных компонентов. Просмотр журналов регистрации событий должен включать журналы серверов, выполняющих функции обеспечения безопасности, например, систем обнаружения вторжений (IDS) и серверов аутентификации, авторизации и учета (Authentication, Authorization, Accounting, AAA), например, RADIUS.	Большое количество компрометаций существуют дни или даже месяцы до обнаружения. Ежедневная проверка журналов регистрации событий позволяет минимизировать время обнаружения и подверженности потенциальной компрометации. Процесс анализа журналов не должен выполняться вручную. Необходимо продумать возможность использования специальных средств сбора и анализа событий, также уведомляющих о потенциальных инцидентах, особенно для организаций с большим количеством серверов.

Требование	Пояснение
Для достижения соответствия требованию 10.6 может использоваться инструментарий для сбора, анализа событий и уведомления.	
10.7 Журналы регистрации событий должны храниться по крайней мере в течение 1 года, при этом в течение 3 месяцев журналы должны быть доступны в режиме оперативного доступа.	Хранение журналов по крайней мере в течение года связано с тем фактом, что на обнаружение компрометации требуется время, а журналы предоставляют достаточную хронологию событий при расследовании инцидентов и возможность более точного определения продолжительности существования потенциальной компрометации и систем, подверженных ее воздействию.

Требование 11: Должно выполняться регулярное тестирование систем и процессов обеспечения безопасности

Уязвимости постоянно обнаруживаются злоумышленниками и исследователями, а также вносятся вместе с новым программным обеспечением. Системы, процессы и разрабатываемое программное обеспечение должны периодически тестироваться в целях поддержания с течением времени, а также при любых изменениях в программном обеспечении надлежащего уровня защищенности.

Требование	Пояснение
11.1 (a) Должно проводиться ежегодное тестирование защитных мер, ограничений и сетевых подключений для обеспечения уверенности в их способности идентифицировать и блокировать любые попытки несанкционированного доступа.	Если не выполнять регулярное тестирование защитных мер, то в них могут возникнуть недостатки (дыры), которыми могут воспользоваться злоумышленники.
(b) Для идентификации всех использующихся беспроводных устройств должен по крайней мере ежеквартально использоваться анализатор беспроводных сетей.	Реализация и/или использование беспроводной технологии в пределах сети компании является одним из наиболее распространенных способов получения злоумышленниками доступа в сеть и к данным платежных карт. Если беспроводное устройство или сеть установлены без ведома компании, то злоумышленник может легко и «незаметно» проникнуть в сеть. В дополнение к анализаторам беспроводной сети для определения беспроводных устройств можно использовать "nmap" и другие сетевые утилиты, которые способны обнаруживать беспроводные устройства.
11.2 Внутренние и внешние сканирования уязвимостей сети должны проводиться по крайней мере ежеквартально или после любого значительного изменения в инфраструктуре сети (например, при установке новых системных компонентов, изменениях в сетевой топологии, модификации правил межсетевого экранирования или обновлении версий продуктов). *Ежеквартальное внешнее сканирование уязвимостей сети должно выполняться организацией, квалификация которой подтверждена платежными системами. Сканирования, проводимые после внесения изменений в сеть, могут выполняться внутренним персоналом компании.*	Сканирование на наличие уязвимостей выполняется автоматизированными средствами в отношении внутренних и внешних точек доступа в сеть, устройств и серверов в сети для обнаружения потенциальных уязвимостей и идентификации портов в сети, которые могут быть обнаружены и эксплуатированы злоумышленниками. После идентификации уязвимостей организации устраняют их для увеличения защищенности сети.
11.3 По крайней мере ежегодно, а также после любых значительных модернизаций или модификаций инфраструктуры или приложений (например, обновление версии ОС, добавление подсети или web-сервера) должны проводиться тесты на проникновение. Данные тесты на проникновение должны включать: 11.3.1 Тесты на проникновение на сетевом уровне 11.3.2 Тесты на проникновение на уровне приложений	Тесты на проникновение на сетевом и прикладном уровнях отличаются от сканирования на наличие уязвимостей тем, что тесты на проникновение в большей степени выполняются вручную, действительно являются попытками эксплуатации каких-либо уязвимостей, обнаруженных при сканировании, и соответствуют деятельности злоумышленников, предпринимаемой для того, чтобы воспользоваться недостаточной защищенностью систем или процессов. Перед передачей приложений, сетевых устройств и систем в среду эксплуатации они должны быть защищены в соответствии с лучшими рекомендациями по обеспечению безопасности (согласно требованию 2.2). С помощью сканирования на наличие уязвимостей и тестов на проникновение обнаруживаются все оставшиеся уязвимости,

Требование	Пояснение
	которые позже могут быть обнаружены и эксплуатированы злоумышленниками.
11.4 (a) Для мониторинга всего сетевого трафика и предупреждения персонала о возможных компрометациях должны использоваться системы обнаружения вторжений на уровне сети, системы обнаружения вторжений на уровне хоста и системы предотвращения вторжений.	Эти средства сравнивают поступающий в сеть трафик с известными сигнатурами большого количества атак (инструментарий злоумышленников, троянское программное обеспечение и т. д.), отправляют предупреждения и/или блокируют попытку проведения атаки в режиме реального времени. Без активного подхода к обнаружению несанкционированной деятельности с помощью данных средств атаки на (или ненадлежащее использование) компьютерные ресурсы могут быть не замечены в момент выполнения. Необходимо вести мониторинг сообщений (предупреждений), генерируемых данными средствами, для возможности блокирования предпринятых вторжений.
(b) Должно выполняться регулярное обновление всех систем обнаружения и предотвращения вторжений	Существует большое разнообразие атак, и количество обнаруженных атак увеличивается с каждым днем. Устаревшие версии систем обнаружения и предотвращения вторжений будут иметь неактуальные сигнатуры и не смогут идентифицировать новые уязвимости, что приведет к необнаруженным компрометациям. Производители данных продуктов предоставляют регулярные, зачастую ежедневные, обновления.
11.5 Должно использоваться программное обеспечение контроля целостности файлов, уведомляющее персонал о несанкционированных изменениях критичных системных файлов или файлов данных и выполняющее по крайней мере еженедельное сравнение критичных файлов. Критичные файлы – это необязательно только файлы, содержащие данные платежных карт. С точки зрения контроля целостности файлов под критичными файлами обычно понимаются файлы, которые редко изменяются, но изменение которых может служить признаком компрометации системы или указывать на попытку компрометации. Средства контроля целостности файлов обычно предварительно сконфигурированы перечнем критичных файлов для соответствующей операционной системы. Другие критичные файлы, например, для разработанного ПО, должны быть оценены и определены самой компанией (например, предприятием торгово-сервисной сети или сервис-провайдером).	Обычно системы мониторинга целостности файлов выполняют проверку на внесение изменений в критичные файлы и генерируют предупреждения при обнаружении изменений. Для мониторинга целостности файлов существуют как коммерческие продукты, так и программы с открытым исходным кодом. Если мониторинг целостности файлов не выполняется, то злоумышленник или злонамеренный пользователь может незаметно изменить содержимое файлов или украсть данные.

Поддержание политики информационной безопасности

Требование 12: Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов

Продуманная политика информационной безопасности определяет стратегию защиты информации в компании и распределяет обязанности за обеспечение безопасности. Все сотрудники должны быть осведомлены о необходимости защиты данных и своих обязанностях по их защите.

Требование	Пояснение
12.1 Должна быть разработана, опубликована, утверждена и доведена до сотрудников политика информационной безопасности, которая включает следующее: 12.1.1 Учитывает все требования данного стандарта. 12.1.2 Содержит описание ежегодного процесса идентификации угроз и уязвимостей, завершающегося формализованной оценкой рисков. 12.1.3 Проведение по крайней мере ежегодного пересмотра политики ИБ и ее обновления при изменении инфраструктуры.	Политика информационной безопасности компании создает план по реализации мер защиты наиболее ценных активов. Надежная политика информационной безопасности определяет стратегию и тактику построения корпоративной защиты информации и информирует сотрудников об их обязанностях. Все сотрудники должны быть осведомлены о конфиденциальности данных и своей ответственности за защиту этих данных. Угрозы безопасности и методы защиты быстро развиваются с каждым годом. Без обновления политики безопасности для отражения этих изменений не будут приняты актуальные меры защиты против новых угроз.
12.2 Должны быть разработаны типовые периодически выполняемые процедуры обеспечения безопасности, соответствующие требованиям данного стандарта (например, процедуры управления пользовательскими учетными записями и процедуры анализа журналов регистрации событий).	Действующие постоянно процедуры защиты выступают в качестве «настольных инструкций» для использования сотрудниками при выполнении своих повседневных обязанностей по администрированию и поддержке систем. Недокументированные действующие процедуры защиты могут привести к тому, что сотрудники не будут знать полный круг своих обязанностей, к процессам, которые не смогут быть воспроизведены в кратчайшие сроки новыми сотрудниками, а также к потенциальным уязвимостям в этих процессах, которые могут предоставить злоумышленнику возможность получения доступа к критичным системам и ресурсам.
12.3 Должны быть разработаны политики допустимого использования персональных устройств, которые могут быть использованы сотрудниками (например, модемов и беспроводных устройств), чтобы определить допустимое использование этих устройств для всех сотрудников и контрагентов. Политики допустимого использования должны содержать следующие требования:	Политики использования могут либо запрещать использование определенных устройств, либо содержать инструкции для сотрудников по корректному использованию и внедрению. Если политики использования отсутствуют, то сотрудники могут использовать устройства в нарушение политики компании, могут установить модемы и/или беспроводные сети без реализации защитных мер и, следовательно, предоставить возможность доступа злоумышленникам к критичным системам и данным платежных карт. Для гарантии того, что осуществляется следование стандартам компании и внедряются только утвержденные технологии, необходимо ограничить возможность их внедрения только определенными сотрудниками (специализированными отделами) и запретить их внедрение обычным сотрудникам, которые не являются специалистами.
12.3.1 Явное утверждение руководством	Без утверждения у руководства необходимости внедрения этих технологий сотрудник

Требование	Пояснение
	может реализовать решение для потребностей бизнеса, при этом открыв брешь в системе безопасности и подвергнув критичные системы и данные риску вследствие действий злоумышленника.
12.3.2 Прохождение аутентификации перед использованием устройства	Если технология реализована без надлежащей аутентификации (идентификаторы пользователей и пароли, электронные ключи, VPN и т. д.), злоумышленник может воспользоваться ей для получения доступа к критичным системам и данным платежных карт.
12.3.3 Перечень используемых устройств и сотрудников, имеющих к ним доступ	Злоумышленники могут преодолеть защиту физического периметра и поместить свои собственные устройства в сеть в качестве «черного хода» (“back door”). Сотрудники также могут обойти процедуры защиты и установить свои собственные устройства. Тщательная инвентаризация и маркировка устройств позволит быстро идентифицировать несанкционированно установленные устройства. Необходимо разработать официальное соглашение об именовании устройств, маркировать и регистрировать все устройства в соответствии с установленными процедурами инвентаризации.
12.3.4 Маркировка устройств с указанием имени владельца, контактной информации и назначения	
12.3.5 Допустимое использование устройств	Определяя допустимое для реализации целей ведения бизнеса использование и размещение устройств и технологий, утвержденных руководством, компания может улучшить управление и контроль над появлением брешей в конфигурациях и действующих защитных мерах для того, чтобы исключить возможность появления «черных ходов» для злоумышленника и получения им доступа к критичным системам и данным платежных карт.
12.3.6 Допустимое размещение используемых устройств в сети	
12.3.7 Перечень разрешенных к использованию типов устройств	
12.3.8 Автоматическое отключение сеансов модемов по истечении определенного периода бездействия	Модемы зачастую могут являться «черными ходами» к критичным ресурсам и данным платежных карт. Отключение модемов, когда они не используются (например, модемы, использующиеся для поддержки систем производителями POS-терминалов или другими производителями), позволит минимизировать доступ к сетям и, следовательно, риски. Необходимо использовать стандартные настройки модемов для их отключения после 15 минут бездействия. За более подробными сведениями по данной теме необходимо обратиться к п. 8.5.6.
12.3.9 Включение модемов для осуществления поддержки производителями только при наличии необходимости и немедленное отключение после использования	
12.3.10 Запрет сохранения данных платежных карт на локальных дисках, флоппи-дисках или других внешних носителях при осуществлении удаленного доступа к данным платежных карт. Запрещение операций копирования/вставки и печати во время сеанса удаленного доступа.	Для того чтобы быть уверенными в том, что пользователи знают о запрете хранения и копирования данных платежных карт на свои персональные компьютеры или носители информации, в компании должна быть документированная политика, явно запрещающая такого рода действия.
12.4 Политика и процедуры информационной безопасности должны явно определять обязанности по обеспечению ИБ для сотрудников и контрагентов.	Без явно определенных ролей и обязанностей по обеспечению информационной безопасности взаимодействие между сотрудниками будет неэффективным, что может привести к небезопасному внедрению информационных технологий или

Требование	Пояснение
	использованию незащищенных технологий.
12.5 Должны быть назначены следующие обязанности по управлению ИБ на индивидуальных сотрудников или группы сотрудников: 12.5.1 Разработка, документирование и доведение до сотрудников политик и процедур безопасности 12.5.2 Мониторинг и анализ событий ИБ, а также информирование соответствующего персонала 12.5.3 Разработка, документирование и распределение процедур реагирования на инциденты безопасности и процедуры эскалации для обеспечения своевременной и эффективной обработки инцидентов, связанных с безопасностью 12.5.4 Администрирование пользовательских учетных записей, включая добавление, удаление и модификацию 12.5.5 Мониторинг и контроль любого доступа к данным.	Каждое лицо или группа лиц, которые отвечают за управление информационной безопасностью, должны совершенно точно понимать свои обязанности и связанные с ними задачи посредством определенной политики. Без такой ответственности уязвимости в процессах могут открыть доступ к критичным ресурсам или данным платежных карт.
12.6 Должна быть реализована формализованная программа повышения осведомленности сотрудников в вопросах ИБ для обеспечения понимания сотрудниками важности защиты данных платежных карт.	Если сотрудники не осведомлены о своей ответственности, связанной с информационной безопасностью, реализованные меры и процессы могут потерять свою эффективность вследствие их непреднамеренных ошибок или умышленных действий.
12.6.1 Должно выполняться обучение сотрудников при найме на работу и по крайней мере ежегодно (например, с использованием рассылки, плакатов, заметок, собраний и т. д.)	Если программа осведомленности сотрудников об угрозах и проблемах, связанных с информационной безопасностью, не будет включать дополнительные ежегодные напоминания, то сотрудники могут забыть или пренебречь основными процессами и процедурами обеспечения безопасности, что приведет к уязвимости критичных ресурсов и данных платежных карт.
12.6.2 Сотрудники должны письменно подтверждать прочтение и понимание политики и процедур ИБ	Требование наличия подписи сотрудника позволит гарантировать то, что он действительно прочитал и понял все политики и процедуры обеспечения безопасности, а также то, что он обязуется действовать в соответствии с этими документами.
12.7 Должны выполняться проверки потенциальных сотрудников для минимизации риска внутренних атак. *Для таких сотрудников, как кассиры магазинов, которые имеют доступ только к одному номеру карты единовременно при проведении транзакции, это требование носит рекомендательный характер.*	Детальное изучение биографии сотрудников, которые имеют доступ к данным платежных карт, уменьшает риск неавторизованного использования номеров счетов сотрудниками с сомнительным или криминальным прошлым. Предполагается, что в компании имеется политика и процесс наведения справок, включая собственный процесс принятия решений, с помощью которого результаты проверки оказывают влияние на решение о найме или отказе в приеме на работу (или другие решения).
12.8 При наличии возможности получения доступа к данным платежных карт сервис-провайдером в договорах с сервис-провайдерами должно содержаться следующее:	Если предприятие торгово-сервисной сети или сервис-провайдер совместно используют данные платежных карт с сервис-провайдером, тогда сервис-провайдер, получающий данные платежных карт, должен подписать юридический документ, в

Требование	Пояснение
12.8.1 Необходимость соблюдения сервис-провайдерами положений стандарта PCI DSS 12.8.2 Соглашение, подтверждающее признание сервис-провайдерами обязанностей по обеспечению безопасности данных платежных карт, к которым они получают доступ	котором указывается его ответственность за соответствие политикам безопасности данных платежных карт и который подтверждает признание этим сервис-провайдером своей ответственности. Это позволит гарантировать непрерывную защиту данных, осуществляемую внешними сторонами.
12.9 Должен быть создан план реагирования на инциденты ИБ и обеспечена готовность немедленного реагирования на нарушение информационной безопасности какой-либо системы. 12.9.1 (a) Должен быть разработан план реагирования на инциденты ИБ, выполняемый при компрометации системы.	При отсутствии детального плана реагирования на инциденты безопасности, его распределения, чтения и понимания ответственными сторонами замешательство и отсутствие унифицированного подхода к реагированию могут увеличить время вынужденного бездействия для бизнеса, привести к появлению в средствах массовой информации нежелательной информации, а также к возникновению дополнительной юридической ответственности.
(b) План должен содержать по крайней мере конкретные процедуры реагирования на инциденты ИБ, процедуры восстановления и обеспечения непрерывности бизнеса, процессы резервирования данных, роли и обязанности, а также стратегии уведомления при инциденте (например, информирование банков-эквайреров и ассоциаций платежных карт)	План реагирования на инциденты должен быть детальным и содержать все ключевые элементы, которые позволят компании эффективно реагировать на обнаруженные инциденты, подвергающие риску данные платежных карт.
12.9.2 Должно проводиться по крайней мере ежегодное тестирование плана	Без надлежащего тестирования можно пропустить ключевые пункты, что может ограничить область действия плана во время инцидента.
12.9.3 Должны быть назначены сотрудники, реагирующие на инциденты ИБ 7 дней в неделю 24 часа в сутки.	Без наличия обученной и легкодоступной группы реагирования на инциденты сети может быть нанесен серьезный ущерб, а критичные данные и системы могут быть повреждены вследствие ненадлежащего обращения с целевыми системами. Это может препятствовать успешному процессу расследования, проводимому после обнаружения инцидента. Если компания не располагает внутренними ресурсами, необходимо рассмотреть возможность заключения договора с компанией, предоставляющей подобные услуги.
12.9.4 Должно выполняться соответствующее обучение персонала, ответственного за реагирование на инциденты ИБ	
12.9.5 Должно выполняться наблюдение за событиями от систем IDS, IPS и систем контроля целостности	Данные системы мониторинга предназначены для концентрации на потенциальном риске в отношении данных и критичны к быстрому реагированию для предотвращения инцидента. *Необходимо гарантировать, что системы мониторинга включаются в процессы реагирования на инциденты безопасности.*
12.9.6 Должен быть реализован процесс изменения и развития плана реагирования на инциденты ИБ в соответствии с приобретенным опытом и с учетом развития отрасли ИБ	Внесение «полученных уроков» в план реагирования на инциденты ИБ после инцидента поможет поддерживать актуальность плана и реагировать на тенденции в области безопасности.
12.10 Все процессинговые центры и сервис-провайдеры должны реализовать и поддерживать политики и процедуры управления	Подключенная организация – это вышестоящая организация, которая связана с процессинговым центром или сервис-провайдером с целью получения данных

Требование	Пояснение
подключенными организациями, включая следующее:	платежных карт, включая процессинговые центры, агенты, предприятия торгово-сервисной сети и другие сервис-провайдеры. Данное определение подключенных организаций не включает «нижестоящие» организации, такие как предприятия торгово-сервисной сети и другие сервис-провайдеры и процессинговые центры, которые создали данные и теперь получают их обратно от рассматриваемой организации. Для эффективного управления этими подключенными организациями процессинговые центры и сервис-провайдеры должны использовать соответствующие политики.
12.10.1 Поддержание перечня подключенных организаций	Для предоставления информации о каждой подключенной организации и для помощи в устранении проблем, если таковые возникли, необходимо поддерживать реестр подключенных организаций.
12.10.2 Необходимость выполнения проверок до подключения организации	Политика должна включать процесс детальной проверки в соответствии с необходимым уровнем проверки для организации.
12.10.3 Необходимость соответствия подключаемой организации требованиям стандарта PCI DSS	Данное требование удовлетворяется, если компания заключает договор с подключенной организацией согласно п. 12.8.1.
12.10.4 Определенная процедура подключения и отключения организаций	Политика должна включать перечень действий, которые необходимо предпринять при процессах подключения и отключения.

Приложение A: Применимость стандарта PCI DSS к хостинг-провайдерам

Требование A.1: Хостинг-провайдеры должны защищать среду данных платежных карт

Как упоминалось в требовании 12.8, все сервис-провайдеры, имеющие доступ к данным платежных карт (в том числе хостинг-провайдеры), должны соблюдать положения стандарта PCI DSS. Кроме того, в требовании 2.4 говорится о том, что хостинг-провайдеры должны защищать среду размещения и данные каждой обслуживаемой организации. Поэтому хостинг-провайдеры должны придавать большое значение выполнению следующих требований:

Требование	Пояснение
A.1 Должна выполняться защита среды размещения и данных каждой обслуживаемой организации (предприятия торгово-сервисной сети, сервис-провайдера или другой организации) с учетом требований A.1.1–A.1.4:	Это приложение предназначено для хостинг-провайдеров, предоставляющих своим клиентам среду размещения данных, которая соответствует требованиям стандарта PCI DSS. Хостинг-провайдерам необходимо в дополнение к другим применяемым требованиям стандарта PCI DSS соответствовать и требованиям, изложенным в пп. A.1.1–A.1.4.
A.1.1 Каждая организация должна иметь доступ только к собственной среде данных платежных карт	Если предприятию торгово-сервисной сети или сервис-провайдеру разрешается выполнять свои собственные приложения на совместно используемом сервере, то они должны выполняться под учетной записью предприятия торгово-сервисной сети или сервис-провайдера, а не под учетной записью привилегированного пользователя. Привилегированный пользователь в дополнение к доступу к собственной среде имел бы доступ к средам данных платежных карт всех других предприятий торгово-сервисной сети и сервис-провайдеров.
A.1.2 Права доступа и привилегии каждой организации должны ограничиваться только собственной средой платежных карт	Чтобы гарантировать, что доступ и привилегии предоставляются так, что каждое предприятие торгово-сервисной сети или сервис-провайдер имеют доступ только к собственной среде данных платежных карт, необходимо рассмотреть: 1) привилегии учетной записи, от имени которой запускается web-сервер предприятия торгово-сервисной сети или сервис-провайдера; 2) разрешения на чтение, запись и выполнение файлов; 3) разрешения на запись в исполняемые системные файлы; 4) разрешения на доступ к журналам регистрации событий предприятия торгово-сервисной сети или сервис-провайдера услуг; 5) меры для обеспечения гарантии того, что единственное предприятие торгово-сервисной сети или сервис-провайдер не сможет завладеть всеми системными ресурсами.
A.1.3 Аудит и регистрация событий должны быть включены индивидуально для среды платежных карт каждой организации и в соответствии с требованием 10 стандарта PCI DSS	Журналы должны быть доступны в общей среде размещения данных платежных карт так, что предприятия торгово-сервисной сети и сервис-провайдеры имеют к ним доступ и могут просматривать журналы регистрации событий, относящиеся к собственной среде размещения данных платежных карт.
A.1.4 Должны быть реализованы процессы, позволяющие провести своевременное расследование инцидентов при компрометации размещенных данных любого предприятия торгово-сервисной сети или сервис-провайдера	Хостинг-провайдеры с общей средой размещения должны активировать процесс быстрого и удобного реагирования в случае компрометации, если требуется расследование инцидентов, вплоть до определенного уровня детализации для того, чтобы были доступны подробности об индивидуальном предприятии торгово-сервисной сети или сервис-провайдере.

Приложение Б: Компенсационные меры

Компенсационные меры – Общие положения

Использование компенсационных мер может быть обосновано для большинства требований стандарта PCI DSS в том случае, когда организация не может соответствовать технической спецификации требования, но может в значительной мере снизить связанный с данным требованием риск. За полным определением компенсационных мер необходимо обратиться к документу «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*).
Эффективность компенсационной меры зависит от конкретной среды, в которой реализуется мера, смежных защитных мер и конфигурации меры. Компании должны отдавать себе отчет в том, что какая-то конкретная компенсационная мера не будет эффективной во всех средах. Каждая компенсационная мера должна быть основательно оценена после реализации для подтверждения своей эффективности.
Ниже представлены компенсационные меры для компаний, которые не способны привести данные платежных карт к нечитаемому виду в соответствии с требованием 3.4.

Компенсационные меры для требования 3.4
Использование компенсационных мер можно рассматривать для тех компаний, которые не могут привести данные платежных карт к нечитаемому виду (например, при помощи шифрования) ввиду объективных технических ограничений или требований бизнеса. Условием обеспечения соответствия стандарту PCI DSS для требований, в отношении которых использованы компенсационные меры, является документирование требований бизнеса или технологических ограничений, не позволяющих выполнить соответствующее требование, и проведение анализа рисков для данного требования[3].

Компании, которые рассматривают возможность использования компенсационных мер, связанных с требованием приведения данных платежных карт к нечитаемому виду, должны понимать риск, вызываемый хранением данных платежных карт в читаемом виде. Обычно меры должны предоставлять дополнительную защиту для снижения любого дополнительного риска, вызываемого хранением данных платежных карт в читаемом виде. Меры, предполагаемые к использованию в качестве компенсационных, должны применяться в дополнение к мерам стандарта PCI DSS и должны удовлетворять определению компенсационных мер, которое дается в документе «PCI DSS: Термины, аббревиатуры и акронимы» (*PCI DSS Glossary, Abbreviations, and Acronyms*). Компенсационные меры могут представлять собой устройство, комбинацию устройств, приложений и мер, удовлетворяющих **всем** перечисленным ниже условиям:

1. Обеспечение дополнительного уровня сегментации/абстракции (например, на сетевом уровне)
2. Обеспечение возможности ограничения доступа к данным платежных карт или базам данных на основе следующих критериев:
   - IP-адреса/MAC-адреса
   - Приложения/сервисы
   - Учетные записи пользователей/групп
   - Тип данных (фильтрация пакетов)
3. Ограничение логического доступа к базе данных
   - Логический доступ к базе данных должен контролироваться независимо от Active Directory или LDAP (Lightweight Directory Access Protocol)
4. Предотвращение/обнаружение распространенных атак на приложения или базы данных (например, SQL-инъекции).

[3] Прим. ИЗ. Результаты анализа рисков рекомендуется оформлять в шаблоне Compensating controls Worksheet, приведенном в **Security Audit Procedures, Приложение С**.