



Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Версия 1.1

Сентябрь 2006

Стандарт PCI DSS © PCI SSC

Перевод © Digital Security



Создание и поддержка безопасной сетевой инфраструктуры

- Требование 1: Разработать и обеспечить поддержку конфигураций межсетевых экранов для защиты данных о держателях карт
- Требование 2: Не использовать установленные производителем системные пароли и иные параметры безопасности

Защита данных о держателях карт

- Требование 3: Обеспечить безопасность хранимых данных о держателях карт
- Требование 4: Шифровать данные о держателях карт при передаче их через открытые общедоступные сети

Поддержка программы управления уязвимостями

- Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение
- Требование 6: Разработать и поддерживать безопасные системы и приложения

Внедрение усиленных средств управления доступом

- Требование 7: Ограничить доступ к данным о держателях карт только служебной необходимостью
- Требование 8: Назначить уникальный идентификатор каждому лицу, имеющему доступ к компьютерной сети
- Требование 9: Ограничить физический доступ к данным о держателях карт

Регулярный мониторинг и тестирование сетевой инфраструктуры

- Требование 10: Отслеживать и контролировать любой доступ к сетевым ресурсам и данным о держателях карт
- Требование 11: Регулярно проверять системы и процессы обеспечения безопасности

Поддержка Политики информационной безопасности

- Требование 12: Поддерживать политику, определяющую правила информационной безопасности для сотрудников и партнеров

Введение

Настоящий документ описывает 12 требований Стандарта безопасности данных индустрии платежных карт (Payment Card Industry (PCI) Data Security Standard (DSS)). Требования PCI DSS объединены в 6 логически связанных групп, которые являются целями выполнения требований (“control objectives”).

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

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

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

* – эти элементы данных должны быть защищены в случае, если хранятся совместно с PAN. Эта защита должна соответствовать требованиям PCI DSS по безопасности среды данных о держателях карт. Иные требования законодательства (например, относящиеся к защите персональных данных клиентов, охране частных сведений, краже личности или безопасности данных) могут предписывать дополнительную защиту этих данных или раскрытие применяемых компанией методов, если персональные данные потребителей накапливаются компанией. Требования PCI DSS, несмотря на это, не применяются, если PAN не хранится, не обрабатывается и не передается.

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

Данные требования безопасности применяются ко всем компонентам системы. Компонентом системы является любое сетевое устройство, сервер или приложение, входящее в состав или подключенное к среде данных о держателях карт. Среда данных о держателях карт – это часть сетевой инфраструктуры, в которой циркулируют данные о держателях карт или критичные аутентификационные данные. Область этой среды может быть значительно сокращена путем использования сегментации сети, которая изолирует системы, хранящие, обрабатывающие и передающие данные о держателях карт, от остальных систем. Сетевые устройства включают в себя в том числе: межсетевые экраны, коммутаторы, маршрутизаторы, беспроводные точки доступа и средства защиты информации. Типы серверов включают в себя в том числе: веб-

серверы, серверы баз данных, аутентификационные серверы, почтовые серверы, прокси-серверы, NTP- и DNS-серверы. Приложения включают в себя все приобретенные и самостоятельно разработанные, включая внутренние и внешние (Интернет) приложения.

Создание и поддержка безопасной сетевой инфраструктуры

Требование 1: Разработать и обеспечить поддержку конфигураций межсетевых экранов для защиты данных о держателях карт

Межсетевые экраны – это средства вычислительной техники, контролирующие сетевой трафик между локальной сетью компании и внешней средой, а также между сегментами локальной сети разного уровня критичности. Межсетевой экран анализирует проходящий через него трафик и блокирует соединения, которые не удовлетворяют определенным критериям безопасности.

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

- 1.1** Должны быть разработаны стандарты конфигурации межсетевых экранов, которые должны включать в себя:
 - 1.1.1** Формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурации межсетевого экрана.
 - 1.1.2** Актуальную схему сети с указанием всех каналов доступа к данным о держателях карт, включая все беспроводные сети.
 - 1.1.3** Требования к межсетевым экранам для каждого Интернет-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью компании.
 - 1.1.4** Описание групп, ролей и ответственности за управление сетевыми устройствами.
 - 1.1.5** Документированный перечень сервисов и портов, необходимых для работы бизнес-приложений.
 - 1.1.6** Обоснование и документирование использования любого протокола передачи данных, кроме HTTP, SSL, SSH и VPN.
 - 1.1.7** Документирование использования любого небезопасного протокола передачи данных (например, FTP), которое включает в себя описание причины использования протокола и применяемых при этом средств защиты.
 - 1.1.8** Ежеквартальный пересмотр настроек межсетевых экранов и маршрутизаторов.
 - 1.1.9** Стандарты конфигурации для маршрутизаторов.
- 1.2** Должна быть создана конфигурация межсетевых экранов, которая запрещает любые соединения, исходящие от недоверенных сетей и узлов, за исключением протоколов, необходимых для среды данных о держателях карт.
- 1.3** Должна быть создана конфигурация межсетевых экранов, ограничивающая соединения между общедоступными серверами и любым компонентом системы, хранящим данные о держателях карт, включая любые беспроводные сети. Эта конфигурация должна включать следующее:
 - 1.3.1** Ограничение входящего трафика на IP-адреса, расположенные в DMZ (входящие фильтры).
 - 1.3.2** Запрет на соединения с внутренних адресов из Интернета к адресам, расположенным в DMZ.
 - 1.3.3** Включение динамической пакетной фильтрации с запоминанием состояния (разрешение прохождения пакетов только для установленных соединений).

- 1.3.4 Размещение баз данных во внутреннем сегменте сети, отделенном от DMZ.
 - 1.3.5 Ограничение входящего и исходящего трафика. Следует разрешить только необходимый для среды данных о держателях карт трафик.
 - 1.3.6 Обеспечение безопасности и синхронизации конфигурационных файлов маршрутизаторов. Например, файлы текущей рабочей конфигурации (для нормального функционирования маршрутизаторов) и файлы инициализации (используемые при перезагрузке) должны содержать одинаково безопасную конфигурацию.
 - 1.3.7 Запрещение всего входящего и исходящего трафика, который явно не разрешен правилами.
 - 1.3.8 Установку межсетевых экранов между любой беспроводной сетью и средой данных о держателях карт, и конфигурирование этих межсетевых экранов с целью запрещения любого трафика из беспроводной сети, либо его контроля в том случае, если такой трафик необходим для бизнес-приложений.
 - 1.3.9 Установку персональных межсетевых экранов на все мобильные и принадлежащие сотрудникам компьютеры, имеющие доступ в Интернет и используемые для доступа к локальной сети организации.
- 1.4 Должен быть запрещен любой прямой доступ из внешней среды к любому из компонентов системы, содержащих данные о держателях карт (базам данных, журналам протоколирования событий, файлам трассировки).
- 1.4.1 Следует использовать DMZ для фильтрации любого трафика и запрещения прямых маршрутов для входящего и исходящего Интернет-трафика.
 - 1.4.2 Любой исходящий трафик от приложений обработки платежных карт должен быть ограничен только IP-адресами, расположенными в DMZ.
- 1.5 Должен быть реализован механизм трансляции IP-адресов для предотвращения раскрытия внутренних адресов. Для этого следует использовать такие технологии, как PAT и NAT.

Требование 2: Не использовать установленные производителем системные пароли и иные параметры безопасности

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

- 2.1 Всегда следует менять установленные производителем настройки по умолчанию перед установкой системы в сетевую инфраструктуру (например, сменить установленные по умолчанию пароли, строки доступа SNMP, удалить ненужные для работы учетные записи).
 - 2.1.1 **Для беспроводных устройств**, необходимо изменить установленные по умолчанию производителем параметры, такие как: WEP-ключи, идентификатор сети (SSID), административные пароли, строки доступа SNMP, а также отключить широковещательную рассылку SSID. Следует включить WPA или WPA2 для шифрования данных и аутентификации, если устройство поддерживает WPA.
- 2.2 Должны быть разработаны стандарты конфигурации для всех системных компонентов. Стандарты должны учитывать все известные проблемы безопасности, а также положения общепринятых отраслевых стандартов (SANS, NIST, CIS).
 - 2.2.1 Каждый сервер должен выполнять одну основную функцию (например, веб-сервер, сервер баз данных и сервер DNS должны быть установлены на разных компьютерах).

- 2.2.2** Должны быть отключены все небезопасные и ненужные для работы сервисы и протоколы (те сервисы и протоколы, использование которых не требуется для выполнения устройством своей основной функции).
 - 2.2.3** Следует настроить параметры безопасности системы так, чтобы исключить возможность некорректного использования системы.
 - 2.2.4** Из системы должна быть удалена вся ненужная функциональность: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, ненужные для работы веб-серверы.
- 2.3** Следует всегда шифровать канал удаленного административного доступа к системе. Для этого необходимо использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов удаленного административного доступа.
- 2.4** Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным в Приложении А: «Применимость PCI DSS к хостинг-провайдерам».

Защита данных о держателях карт

Требование 3: Обеспечить безопасность хранимых данных о держателях карт

Шифрование – критичный компонент защиты данных о держателях карт. Если взломщик обойдет остальные меры безопасности и получит доступ к зашифрованным данным, не зная ключа шифрования, то эти данные останутся для него нечитаемыми и практически бесполезными. Иные способы защиты хранимых данных должны рассматриваться как средства уменьшения риска. Методы минимизации риска включают в себя: запрет хранения данных о держателях карт, кроме случаев крайней необходимости, хранение укороченного PAN, если не требуется хранение полного PAN, и избегание пересылки PAN по электронной почте в открытом виде.

- 3.1** Хранение данных о держателях карт должно быть ограничено только необходимым минимумом данных. Должна быть разработана политика хранения и обращения с данными. Количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований параметрами, эти параметры должны быть отражены в политике хранения данных.
- 3.2** Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). К критичным аутентификационным данным относятся данные, перечисленные в требованиях 3.2.1 – 3.2.3.
- 3.2.1** Запрещается хранить полное содержимое любой дорожки магнитной полосы, находящейся на обратной стороне карты, на чипе, либо ином месте, («полная дорожка», «дорожка», «дорожка 1», «дорожка 2»).
- Для ведения бизнеса, может быть необходимо хранение следующих элементов данных магнитной полосы: имя держателя счета, номер платежной карты (PAN), дата истечения срока действия карты и сервисный код. Для минимизации рисков разрешается хранить только указанные элементы данных. НИКОГДА нельзя сохранять элементы данных, содержащие код CVC или PIN. Дополнительная информация приведена в «Глоссарии PCI DSS».*
- 3.2.2** Запрещается хранение кода CVC или значения, используемого для подтверждения транзакций, выполняемых без непосредственного считывания информации с кредитной карты (трех- или четырехзначного числа, изображенного на лицевой или обратной стороне карты).
- Дополнительная информация приведена в «Глоссарии PCI DSS».*
- 3.2.3** Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока.
- 3.3** Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4 знака).
- Это требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть полный PAN, также это требование не заменяет собой иные более строгие требования к отображению данных о держателях карт (например, на чеках POS-терминалов).*
- 3.4** Из всех данных о держателе карты, как минимум, PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий, а также данные, получаемые по беспроводным сетям). Для этого следует использовать любой из следующих методов:
- стойкая однонаправленная хэш-функция;
 - укорачивание (truncation);

- использование механизмов One-Time-Pad («одноразовые блокноты») и использование и хранение ссылок на данные вместо самих данных (index tokens);
- стойкие криптографические алгоритмы, совместно с процессами и процедурами управления ключами.

Из всей информации о держателе карты, КАК МИНИМУМ, PAN должен быть преобразован в нечитаемый вид.

Если, по каким-то причинам, компания не может шифровать данные о держателях карты, то компенсирующие меры отражены в Приложении В: «Компенсирующие меры для шифрования хранимых данных».

- 3.4.1** Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или полей базы данных), то управление логическим доступом должно осуществляться независимо от механизмов разграничения доступа операционной системы (например, локальных учетных записей или учетных записей Active Directory). Ключи шифрования не должны быть привязаны к учетным записям пользователей.
- 3.5** Следует обеспечить защиту ключей шифрования данных о держателях карт от их компрометации или неправильного использования.
- 3.5.1** Доступ к ключам шифрования должен быть разрешен только нескольким ответственным за их хранение и использование сотрудникам.
- 3.5.2** Ключи должны храниться только в строго определенных защищенных хранилищах и строго определенном виде.
- 3.6** Должны быть документированы все процессы и процедуры управления ключами шифрования данных о держателях карт, в том числе:
- 3.6.1** Генерация стойких ключей.
- 3.6.2** Безопасное распространение ключей.
- 3.6.3** Безопасное хранение ключей.
- 3.6.4** Периодическая смена ключей:
- насколько часто это видится необходимым и требуется применяемыми приложениями, предпочтительно автоматически;
 - не реже одного раза в год.
- 3.6.5** Уничтожение старых (просроченных) ключей.
- 3.6.6** Раздельное владение частями ключей (так, чтобы для расшифровки данных требовался составной ключ, компоненты которого хранятся у 2-3 сотрудников).
- 3.6.7** Защита от неавторизованной смены ключа.
- 3.6.8** Замена скомпрометированного ключа, а также предположительно скомпрометированного ключа.
- 3.6.9** Отзыв просроченных и недействительных ключей.
- 3.6.10** Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с письменным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности.

Требование 4: Шифровать данные о держателях карт при передаче их через открытые общедоступные сети

Критичная информация должна передаваться через общедоступные сети, где ее легко перехватить, изменить или перенаправить, только в зашифрованном виде.

- 4.1** Для защиты критичных данных о держателях карт во время передачи их через общедоступные сети, следует использовать стойкие криптографические алгоритмы и протоколы, такие как SSL/TLS и IPSEC.

Примерами общедоступных сетей, на которые распространяются требования PCI DSS, являются Интернет, Wi-Fi (IEEE 802.11x), GSM, GPRS.

4.1.1 При использовании беспроводных сетей для передачи данных о держателях карт, следует использовать технологию WPA (WPA2), IPSEC VPN, либо SSL/TLS. Никогда не следует полагаться только на WEP для защиты конфиденциальных данных в беспроводных сетях. При использовании WEP, следует предпринять следующие меры:

- использовать только 104-битные ключи шифрования и 24-битное инициализирующее значение (IV);
- использовать WEP только совместно с технологиями WPA (WPA2), VPN, или SSL/TLS.

Примечание: использовать WEP совместно с WPA технически невозможно. В настоящий момент рекомендуется игнорировать эту часть пункта.

- менять WEP ключи ежеквартально (или автоматически, если технология это позволяет);
- менять WEP ключи при кадровых изменениях среди персонала, имеющего доступ к ключам.
- ограничить доступ по MAC-адресам.

- 4.2** Никогда не следует пересылать незашифрованный PAN по электронной почте.

Поддержка программы управления уязвимостями

Требование 5: Использовать и регулярно обновлять антивирусное программное обеспечение

Большинство вредоносных вирусов проникают в сеть через электронную почту сотрудников. Антивирусное программное обеспечение должно быть установлено на всех подверженных воздействию вирусов системах, чтобы защитить их от вредоносного кода.

- 5.1** Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).
Обычно UNIX-системы и мэйнфреймы не подвержены воздействию вирусов.
 - 5.1.1** Следует убедиться в том, что антивирусное программное обеспечение также способно обнаруживать и защищать от иных форм вредоносного кода, включая шпионские и рекламные программы.
- 5.2** Антивирусные механизмы должны быть актуальными, постоянно включенными и должны вести журналы протоколирования событий.

Требование 6: Разработать и поддерживать безопасные системы и приложения

Злоумышленники используют уязвимости в безопасности для получения привилегированного доступа к системе. Большинство из таких уязвимостей закрываются путем установки обновлений безопасности, выпускаемых производителем. На все системы должны быть установлены самые свежие подходящие обновления программного обеспечения для защиты от использования уязвимостей внутренними и внешними злоумышленниками, а также вирусами. Подходящими являются те обновления, которые протестированы на совместимость с текущей конфигурацией безопасности. В случае самостоятельной разработки приложений, множество уязвимостей удастся избежать, используя стандартные процессы разработки систем и приемы безопасного написания программного кода.

- 6.1** На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем. Обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем.
- 6.2** Должен быть внедрен процесс определения вновь обнаруженных уязвимостей безопасности (например, подписка на бесплатную рассылку сообщений о новых уязвимостях). Стандарты конфигурации системных компонентов (Требования 1.1 и 2.2 PCI DSS) должны обновляться для учета вновь обнаруженных уязвимостей.
- 6.3** Приложения должны разрабатываться в соответствии с накопленным в данной отрасли опытом, с учетом требований информационной безопасности в течение всего цикла разработки.
 - 6.3.1** Все обновления безопасности и изменения в конфигурации должны быть протестированы перед внедрением.
 - 6.3.2** Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга.
 - 6.3.3** Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть отделены друг от друга.
 - 6.3.4** Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.
 - 6.3.5** Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.

- 6.3.6** Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчику или переводом его в производственный режим.
- 6.3.7** Программный код приложений должен быть исследован на наличие потенциальных уязвимостей перед передачей готовых приложений заказчику или переводом их в производственный режим.
- 6.4** Должны быть разработаны и внедрены процедуры управления изменениями, которые должны включать в себя:
 - 6.4.1** Документирование влияния изменения на систему;
 - 6.4.2** Согласование изменения с руководством;
 - 6.4.3** Тестирование производственной функциональности;
 - 6.4.4** Процедуру отмены изменения.
- 6.5** Разработка веб-приложений должна проходить в соответствии с руководствами по безопасному программированию, например, такими как руководства от проекта OWASP. Программный код приложений должен быть исследован на наличие потенциальных уязвимостей, в частности таких как:
 - 6.5.1** Отсутствие проверки входных данных;
 - 6.5.2** Обход системы контроля доступа (например, возможность использования чужих учетных записей);
 - 6.5.3** Обход системы аутентификации и управления сессиями (возможность использования чужих аутентификационных данных и файлов cookie);
 - 6.5.4** Атаки типа XSS;
 - 6.5.5** Переполнение буфера;
 - 6.5.6** Инъекции (например, SQL-инъекции);
 - 6.5.7** Некорректная обработка ошибок;
 - 6.5.8** Небезопасное хранение данных;
 - 6.5.9** Отказ в обслуживании;
 - 6.5.10** Небезопасное управление конфигурацией.
- 6.6** Следует обеспечить защиту веб-ориентированных приложений от известных атак одним из следующих методов:
 - Проверить программный код на наличие уязвимостей, воспользовавшись услугами компаний, специализирующихся на безопасности приложений.
 - Установить межсетевой экран прикладного уровня перед веб-ориентированными приложениями.

Данный метод становится обязательным требованием с 30 июня 2008 года.

Внедрение усиленных мер по управлению доступом

Требование 7: Ограничить доступ к данным о держателях карт только служебной необходимостью

Это требование гарантирует, что доступ к критичным данным имеют только авторизованные сотрудники.

- 7.1 Доступом к вычислительным ресурсам и информации о держателях карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.
- 7.2 Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания, и применяющий принцип «запрещено всё, что явно не разрешено».

Требование 8: Назначить уникальный идентификатор каждому человеку, имеющему доступ к компьютерной сети

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

- 8.1 Каждому пользователю должно быть назначено уникальное имя учетной записи, до предоставления ему доступа к компонентам системы и данным о держателях карт.
- 8.2 Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей:
 - Пароль;
 - Ключи (например, SecureID, сертификаты, открытый ключ);
 - Биометрические параметры.
- 8.3 Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети должен быть реализован механизм двухфакторной аутентификации. Для этого следует использовать такие технологии, как RADIUS и TACACS с ключами; или VPN (SSL/TLS или IPSEC) с индивидуальными сертификатами.
- 8.4 Все пароли должны храниться и передаваться только в зашифрованном виде.
- 8.5 Должен быть установлен контроль над выполнением процедур аутентификации и управления паролями учетных записей сотрудников и администраторов, включающий в себя:
 - 8.5.1 Контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации.
 - 8.5.2 Проверку подлинности пользователя перед сменой пароля.
 - 8.5.3 Установку уникального первоначального пароля для каждого пользователя и его немедленное изменение при первом входе пользователя.
 - 8.5.4 Немедленный отзыв доступа при увольнении пользователя.
 - 8.5.5 Удаление заблокированных учетных записей не реже одного раза в 90 дней.
 - 8.5.6 Включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ.
 - 8.5.7 Доведение правил и процедур использования и хранения пароля до всех пользователей, имеющих доступ к данным о держателях карт.

- 8.5.8 Запрет использования групповых, разделяемых и стандартных учетных записей и паролей.
- 8.5.9 Изменение пароля пользователя не реже одного раза в 90 дней.
- 8.5.10 Требование использования в пароле не менее семи символов.
- 8.5.11 Требование использования в пароле как цифр, так и букв.
- 8.5.12 Запрет при смене пароля выбора в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей.
- 8.5.13 Блокировку учетной записи после шести неудачных попыток ввода пароля.
- 8.5.14 Установку периода блокировки учетной записи равным 30 минутам, или до разблокировки учетной записи администратором.
- 8.5.15 Блокировку рабочей сессии пользователя через 15 минут простоя, с требованием ввода пароля для разблокировки терминала.
- 8.5.16 Аутентификацию всех вариантов доступа к любой базе данных, содержащей данные о держателях карт, в том числе доступ со стороны приложений, администраторов и любых других пользователей.

Требование 9: Ограничить физический доступ к данным о держателях карт

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

- 9.1 Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные о держателях карт.
 - 9.1.1 Следует использовать камеры видеонаблюдения, чтобы следить за критичными местами. Данные, собранные камерами видеонаблюдения, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством.
 - 9.1.2 Доступ к сетевым разъемам, расположенным в общедоступных местах, должен быть ограничен.
 - 9.1.3 Доступ к беспроводным точкам доступа, шлюзам и портативным устройствам должен быть ограничен.
- 9.2 Должны быть внедрены процедуры, позволяющие легко различать сотрудников и посетителей, особенно в помещениях, где циркулируют данные о держателях карт.

Под термином «сотрудники» в данном случае понимаются постоянные и временные сотрудники, а также консультанты, работающие на объекте. Под термином «посетители» понимаются поставщики, гости сотрудников, сервисный персонал и иные люди, кратковременно находящиеся на объекте, обычно не более одного дня.
- 9.3 Следует ввести процедуру прохода посетителей на объект, обеспечивающую:
 - 9.3.1 Авторизацию посетителя, перед входом в помещения, где циркулируют данные о держателях карт;
 - 9.3.2 Выдачу посетителю материального идентификатора (например, бейджа или электронного ключа), имеющего ограничение срока действия, при входе на объект.
 - 9.3.3 Возвращение посетителем выданного материального идентификатора при выходе с объекта или при истечении его срока действия.

- 9.4** Следует вести журнал учета посетителей и использовать его для анализа посещений. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством.
- 9.5** Носители с резервными копиями данных следует хранить в безопасных местах, желательно вне объекта, таких как запасной центр обработки данных, или же воспользовавшись услугами компаний, обеспечивающих безопасное хранение.
- 9.6** Должна быть обеспечена физическая безопасность всех бумажных и электронных средств (включая компьютеры, электронные носители информации, сетевое оборудование, линии телекоммуникаций, бумажные отчеты, чеки и факсимильные сообщения), содержащих данные о держателях карт.
- 9.7** Должен быть обеспечен строгий контроль над перемещением носителей информации, содержащих данные о держателях карт, включающий:
 - 9.7.1** Классификацию носителей информации, их маркировку, как содержащих конфиденциальную информацию;
 - 9.7.2** Пересылку носителей только с доверенным курьером, или иным способом, который может быть тщательно проконтролирован.
- 9.8** Должна быть внедрена процедура разрешения руководством выноса за пределы охраняемой территории носителей, содержащих данные о держателях карт.
- 9.9** Должен быть обеспечен строгий контроль за хранением носителей, содержащих данные о держателях карт, и доступом к ним.
 - 9.9.1** Носители, содержащие данные о держателях карты, должны быть инвентаризованы, а также должна быть обеспечена их физическая безопасность.
- 9.10** Носители, содержащие данные о держателях карты, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства, должны быть уничтожены следующими способами:
 - 9.10.1** Измельчение, сжигание или растворение бумажного носителя.
 - 9.10.2** Очищение, размагничивание, измельчение или иное разрушение электронного носителя, исключающее возможность восстановления данных о держателях карт.

Регулярный мониторинг и тестирование сетевой инфраструктуры

Требование 10: Отслеживать и контролировать любой доступ к сетевым ресурсам и данным о держателях карт

Наличие механизмов протоколирования событий, а также возможности отслеживать действия пользователей необходимо для системы, так как они позволяют провести расследование и анализ инцидентов. Определение причин инцидентов затруднено при отсутствии журналов протоколирования событий в системе.

- 10.1** Должен быть разработан процесс распределения доступа к компонентам системы (особенно доступа с административными полномочиями) между сотрудниками.
- 10.2** Для каждого системного компонента должен быть включен механизм протоколирования следующих событий:
 - 10.2.1** Любой доступ пользователя к данным о держателях карт;
 - 10.2.2** Любые действия, совершенные с использованием административных полномочий;
 - 10.2.3** Любой доступ к записям о событиях в системе;
 - 10.2.4** Неуспешные попытки логического доступа;
 - 10.2.5** Использование механизмов идентификации и аутентификации;
 - 10.2.6** Инициализация журналов протоколирования событий;
 - 10.2.7** Создание и удаление объектов системного уровня.
- 10.3** Для каждого события каждого системного компонента должны быть записаны следующие параметры:
 - 10.3.1** Идентификатор пользователя;
 - 10.3.2** Тип события;
 - 10.3.3** Дата и время;
 - 10.3.4** Успешным или неуспешным было событие;
 - 10.3.5** Источник события;
 - 10.3.6** Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.
- 10.4** Все критичные системные часы должны быть синхронизированы.
- 10.5** Журналы протоколирования событий должны быть защищены от изменений.
 - 10.5.1** Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.
 - 10.5.2** Журналы протоколирования событий должны быть защищены от неавторизованного изменения.
 - 10.5.3** Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования, или отдельный носитель, где их изменение было бы затруднено.
 - 10.5.4** Копии журналов протоколирования активности в беспроводных сетях должны сохраняться на сервер протоколирования, находящийся внутри локальной сети.
 - 10.5.5** Следует использовать приложения контроля целостности файлов для защиты журналов протоколирования событий от несанкционированных изменений.

- 10.6** Следует просматривать журналы протоколирования событий не реже одного раза в день. Следует анализировать журналы систем обнаружения вторжений (IDS) и серверов, осуществляющих аутентификацию, авторизацию и аудит (например, RADIUS).
- Для обеспечения соответствия Требованию 10.6 могут быть использованы средства сбора и анализа журналов протоколирования событий, а также средства оповещения.*
- 10.7** Журналы протоколирования событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев.

Требование 11: Регулярно проверять системы и процессы обеспечения безопасности

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

- 11.1** Меры обеспечения безопасности и сетевые соединения должны ежегодно тестироваться на их способность обнаруживать попытки несанкционированного доступа и противостоять им. Следует не реже одного раза в квартал анализировать беспроводные сети с целью идентификации всех используемых устройств.
- 11.2** Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значимых изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления системных компонентов).
- Примечание: ежеквартальное сканирование должно производиться сторонней сертифицированной компанией. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании.*
- 11.3** Следует проводить тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера). Эти тесты на проникновение должны включать:
- 11.3.1** Тесты на проникновение сетевого уровня;
- 11.3.2** Тесты на проникновение уровня приложений.
- 11.4** Следует использовать системы обнаружения вторжений на уровне узла и на уровне сети, а также системы предупреждения вторжений для контроля всего сетевого трафика и оповещения персонала о подозрительных действиях. Системы обнаружения и предотвращения вторжений должны быть актуальными.
- 11.5** Следует использовать приложения контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов и файлов данных, проверка целостности критичных файлов должна проводиться не реже одного раза в неделю.

Критичные файлы – это не только файлы с данными о держателях карт. Обычно контролируется целостность файлов, которые изменяются нечасто, но изменение которых может служить признаком компрометации или попытки компрометации системы. Средства контроля целостности обычно содержат предустановленный перечень файлов, подлежащих контролю, в зависимости от используемой операционной системы. Другие критичные файлы, такие как файлы специализированных приложений, должны быть определены самой компанией.

Поддержка Политики информационной безопасности

Требование 12: Поддерживать политику, определяющую правила информационной безопасности для сотрудников и партнеров

Политика безопасности создает атмосферу безопасности во всей компании и информирует сотрудников о том, что от них требуется. Все сотрудники должны быть осведомлены о критичности данных и своих обязанностях по их защите.

- 12.1** Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности.
 - 12.1.1** Политика безопасности должна учитывать все требования настоящего стандарта;
 - 12.1.2** Политика безопасности должна описывать ежегодно выполняемый процесс идентификации угроз, уязвимостей и результатов их реализации, в рамках формальной оценки рисков;
 - 12.1.3** Политика безопасности должна пересматриваться не реже одного раза в год и обновляться в случае изменения инфраструктуры.
- 12.2** Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов протоколирования событий).
- 12.3** Должны быть разработаны правила эксплуатации для критичных устройств, с которыми непосредственно работают сотрудники (таких как модемы и беспроводные сети), чтобы определить корректный порядок использования этих устройств сотрудниками. Эти правила должны включать следующее:
 - 12.3.1** Процедуру явного одобрения руководством;
 - 12.3.2** Аутентификацию перед использованием устройства;
 - 12.3.3** Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам;
 - 12.3.4** Маркировку устройств, с указанием владельца, контактной информации и назначения;
 - 12.3.5** Допустимые варианты использования устройств;
 - 12.3.6** Допустимые точки размещения устройств в сети;
 - 12.3.7** Перечень одобренных компанией устройств;
 - 12.3.8** Автоматическое отключение модемных сессий после определенного периода простоя;
 - 12.3.9** Включение модемов для доступа службы поддержки производителей, только в случае необходимости такого доступа, с немедленным выключением модемов после использования.
 - 12.3.10** Запрет хранения данных о держателях карт на локальных дисках, дискетах и иных съемных носителях при удаленном доступе к данным, а также запрет использования функций копирования-вставки данных и вывода данных на принтер во время сеанса удаленного доступа.
- 12.4** Политика и процедуры безопасности должны однозначно определять обязанности всех сотрудников и партнеров, относящиеся к информационной безопасности.
- 12.5** Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:

- 12.5.1** Разработка, документирование и распространение политики и процедур безопасности;
 - 12.5.2** Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных;
 - 12.5.3** Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций;
 - 12.5.4** Администрирование учетных записей пользователей, включая их добавление, удаление и изменение;
 - 12.5.5** Мониторинг и контроль любого доступа к данным.
- 12.6** Должна быть внедрена официальная программа повышения осведомленности сотрудников о вопросах безопасности, чтобы донести до них важность обеспечения безопасности данных о держателях карт.
- 12.6.1** Обучение сотрудников должно проводиться при приеме их на работу, продвижении по службе, а также не реже одного раза в год, например, при помощи писем, плакатов, заметок или собраний.
 - 12.6.2** С сотрудников должно быть взято письменное подтверждение того, что они ознакомились и поняли политику и процедуры безопасности компании.
- 12.7** Следует тщательно проверять кандидатов при приеме на работу, для минимизации риска внутренних атак.
- Для таких сотрудников, как кассиры в магазине, которые имеют доступ к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.*
- 12.8** В случае, когда данные о держателях карт становятся доступны поставщику услуг, то в договоре с ним следует урегулировать следующие положения:
- 12.8.1** Поставщик услуг должен соблюдать требования PCI DSS;
 - 12.8.2** Поставщик услуг ответственен за безопасность данных о держателях карт, которые он обрабатывает.
- 12.9** Должен быть внедрен план реагирования на инциденты. Компания должна быть готова немедленно отреагировать на нарушение в работе системы.
- 12.9.1** Следует разработать план реагирования на инциденты, применяемый в случае компрометации системы. План должен содержать, как минимум, процедуры реагирования на определенные инциденты, процедуры восстановления и обеспечения непрерывности бизнеса, процессы резервного копирования данных, роли и ответственность, а также схемы оповещения (например, информирование эквайеров и ассоциаций кредитных карт).
 - 12.9.2** План должен тестироваться не реже одного раза в год.
 - 12.9.3** Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7.
 - 12.9.4** Персонал, ответственный за реагирование на нарушения безопасности, должен быть обучен соответствующим образом.
 - 12.9.5** План должен включать в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов.
 - 12.9.6** Должен быть разработан процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли.

- 12.10** Все центры обработки данных и поставщики услуг должны внедрить и поддерживать политики и процедуры управления связанными с ними сторонами, включая:
- 12.10.1** Поддержку в актуальном состоянии перечня связанных сторон;
 - 12.10.2** Обеспечение проведения тщательной проверки связанной стороны перед подключением;
 - 12.10.3** Гарантию соответствия связанной стороны требованиям PCI DSS;
 - 12.10.4** Подключение и отключение связанных сторон в соответствии с установленными процедурами.

Приложение А: Применимость PCI DSS к хостинг-провайдерам

Требование А.1: Поддерживать политику, определяющую правила информационной безопасности для сотрудников и партнеров

Как указано в Требовании 12.8, все поставщики услуг, имеющие доступ к данным о держателях карт (включая хостинг-провайдеров), должны соответствовать PCI DSS. Дополнительно к этому, Требование 2.4 указывает, что хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Следовательно, хостинг-провайдеры должны учитывать следующие требования:

- A.1** Обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон (которая может быть торгующей организацией, поставщиком услуг или иной стороной) в соответствии с требованиями А.1.1 – А.1.4:
 - A.1.1** Обеспечивать условия, при которых каждая из обслуживаемых сторон имеет доступ только к своей среде данных о держателях карт.
 - A.1.2** Ограничивать доступ и привилегии каждой обслуживаемой стороны только принадлежащей ей средой данных о держателях карт.
 - A.1.3** Обеспечивать ведение соответствующих Требованию 10 PCI DSS журналов протоколирования событий, уникальных для каждой среды данных о держателях карт.
 - A.1.4** Обеспечивать своевременное проведение расследования инцидентов в случае компрометации для любого из обслуживаемых торгующих организаций или поставщиков услуг.

Хостинг-провайдер должен соответствовать указанным требованиям в дополнение к остальным разделам PCI DSS.

Даже если хостинг-провайдер может соответствовать указанным требованиям, это не гарантирует соответствие обслуживаемой стороны стандарту PCI DSS. Каждая сторона должна соответствовать PCI DSS и подтверждать соответствие применимым требованиям.

Приложение В: Компенсирующие меры

Компенсирующие меры – Общие

В случае, если компания не может выполнить требование стандарта, она может выбрать компенсирующие меры, снижающие риск. Полное определение компенсирующей меры приведено в «Глоссарии PCI DSS».

Эффективность компенсирующей меры зависит от специфики среды, в которой компенсирующая мера внедрена, существующих средств управления и конфигурации. Компании должны иметь в виду, что определенная мера не будет эффективна во всех средах. Каждая мера должна быть тщательно оценена после внедрения с целью доказательства её эффективности.

Следующая инструкция описывает компенсирующие меры для того случая, когда компания не способна обеспечить нечитаемое представление данных о держателях карт в соответствии с Требованием 3.4.

Компенсирующие меры для Требования 3.4

Компании, которые неспособны обеспечить нечитаемое представление данных о держателях карт (например, при помощи шифрования) по причине технической невозможности или бизнес-ограничений, могут выбрать компенсирующие меры. *Только компании, которые провели анализ рисков и имеют обоснованные технологические или документированные бизнес-ограничения, могут рассматривать компенсирующие меры для достижения соответствия Требованию 3.4.*

Компании, выбравшие компенсирующие меры для обеспечения нечитаемого представления данных о держателях карт, должны осознавать риск для данных, который создается в том случае, если данные о держателях карты остаются в читаемом виде. Компенсирующие меры призваны обеспечить дополнительную защиту, чтобы уменьшить этот риск. Выбранные компенсирующие меры должны прилагаться к средствам управления, предписанным PCI DSS, и должны удовлетворять определению «компенсирующих мер» «Глоссария PCI DSS». Компенсирующие меры могут представлять собой устройство или комбинацию устройств, приложений и средств управления, которые соответствуют **всем** следующим условиям:

1. Обеспечивают дополнительную сегментацию/разделение (например, сетевого уровня);
2. Дают возможность разграничить доступ к данным о держателях карт, основываясь на следующих критериях:
 - IP-адрес/MAC-адрес;
 - Приложение/сервис;
 - Учетные записи пользователей/группы;
 - Тип данных (фильтрация пакетов);
3. Разграничивают логический доступ к базе данных
 - Контроль доступа к базе данных независимо от Active Directory или LDAP;
4. Предупреждают/обнаруживают наиболее распространенные атаки на приложения или базы данных (например, SQL-инъекции).