# Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт

## Должны быть разработаны и внедрены стандарты конфигурации брандмауэров и маршрутизаторов, которые должны включать в себя следующее:

### Формальный процесс утверждения и тестирования всех сетевых соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов

### Актуальная схема сети с указанием всех подключений к среде данных держателей карт из других сетей, включая все беспроводные сети

### Актуальная схема, отображающая потоки данных держателей карт во всех системах и сетях

### Требования к межсетевому экранированию каждого Интернет­-соединения и каждого соединения между демилитаризованной зоной (DMZ) и внутренней сетью организации

### Описание групп, ролей и обязанностей по управлению сетевыми компонентами

### Обоснованный документированный перечень всех разрешенных для использования сервисов, протоколов и портов, необходимых для работы бизнес-­приложений, включающий документальное описание внедренных механизмов защиты небезопасных протоколов.

Примеры небезопасных сервисов, протоколов или портов включают помимо прочих, FTP, Telnet, POP3, IMAP и SNMP версии 1 и 2.

### Требование пересмотра наборов правил брандмауэров и маршрутизаторов не реже одного раза в полгода

## Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в среде данных держателей карт

Примечание. Недоверенной является любая сеть, внешняя по отношению к сетям, принадлежащим проверяемой организации и (или) сеть, которая не контролируется проверяемой организацией.

### Входящий и исходящий трафик должен быть ограничен только соединениями, необходимыми для информационной среды держателей карт, а весь остальной трафик должен быть запрещен

### Должна быть обеспечена безопасность и своевременная синхронизация конфигурационных файлов маршрутизаторов

### Установить брандмауэры между каждой беспроводной сетью и информационной средой держателей карт и настроить их на блокирование любого трафика из беспроводной сети либо разрешение только авторизованного трафика между беспроводной сетью и информационной средой данных держателей карт в том случае, если такой трафик необходим в целях совершения операций

## Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом информационной среды держателей карт

### Необходимо внедрить DMZ, чтобы ограничить входящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным сервисам, протоколам и портам

### Необходимо ограничить входящие Интернет-соединения только адресами, находящимися в DMZ

### Примите меры по противодействию подмене IP- адреса, позволяющие определить фальшивые исходные IP-адреса и заблокировать им доступ в сеть

Например, заблокировать Интернет-трафик с внутренним исходным адресом

### Необходимо запретить неавторизованный исходящий трафик из среды данных держателей карт в сеть Интернет

### Необходимо включить динамическую пакетную фильтрацию с сохранением состояния (разрешение прохождения пакетов только для установленных соединений)

### Необходимо размещать системные компоненты (например, базы данных), в которых хранятся данные держателей карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей

## Должно быть запрещено раскрытие частных IP-адресов и данных о маршрутах третьим сторонам, не имеющим авторизованного доступа

Установить персональные брандмауэры на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в сеть Интернет и используемые для доступа к сети. Требования к конфигурации брандмауэров:

* определены конкретные настройки конфигурации для персональных брандмауэров;
* персональные брандмауэры активно работают;
* настройки персональных брандмауэров не могут быть изменены пользователями мобильных и (или) принадлежащих сотрудникам компьютеров;

## Убедиться, что политики безопасности и процедуры управления брандмауэрами по умолчанию документированы, используются и известны всем заинтересованным лицам.

# Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

## Всегда изменяйте значения параметров и пароли, заданные поставщиками по умолчанию, и отключайте или удаляйте учетные записи по умолчанию перед подключением систем к сети

Это требование относится ко ВСЕМ паролям по умолчанию, включая, в том числе, пароли к операционным системам, программам защиты, приложениям и системным учетным записям, кассовым (в точках продаж,) терминалам, а также строки доступа SNMP и т.д.

### Для беспроводных сетей, подключенных к информационной среде держателей карт либо передающих данные держателей карт, необходимо изменить ВСЕ параметры по умолчанию, установленные поставщиком, включая, помимо прочего, ключи шифрования для беспроводного доступа, пароли, строки доступа SNMP

## Должны быть разработаны стандарты конфигурации для всех системных компонентов

Стандарты должны учитывать все известные проблемы безопасности, а также положения общепринятых отраслевых стандартов в области безопасности.

Примеры источников общепринятых отраслевых стандартов в области безопасности включают, но не ограничиваются:

* Центр Интернет-безопасности (CIS);
* Международная организация по стандартизации (ISO);
* Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS);
* Национальный институт стандартов и технологий

### Каждый сервер должен выполнять одну основную функцию, поскольку необходимо исключить совмещение на одном и том же сервере функций, требующих различных уровней защиты (например, веб-серверы, серверы СУБД и DNS-серверы следует размещать на разных компьютерах).

Примечание. При использовании технологии виртуализации необходимо внедрять только одну основную функцию для каждого виртуального системного компонента

### Должны быть включены только необходимые службы, протоколы, управляющие программы и т.д., требующиеся для функционирования системы

### Необходимо обеспечить дополнительные механизмы защиты для всех необходимых служб, протоколов и управляющих программ, которые могут быть небезопасными.

Например, следует использовать такие технологии защиты, как SSH, S-FTP, SSL или IPSec VPN для защиты таких незащищенных сервисов как NetBIOS совместное использование файлов, Telnet, FTP и т.д.

Если используется протокол SSL/TLS, должны быть выполнены требования в Приложении A2.

### Следует настроить параметры безопасности системы таким образом, чтобы исключить возможность некорректного использования системы.

### Из системы должен быть удален весь неиспользуемый функционал: сценарии, драйверы, дополнительные возможности, подсистемы, файловые системы, не нужные для работы веб-серверы

## При использовании неконсольного административного доступа к системе следует всегда шифровать канал с использованием стойких криптографических алгоритмов.

## Вести учет системных компонентов, на которые распространяется действие стандарта PCI DSS

## Убедиться, что политики безопасности, процедуры управления учетными данными поставщиков по умолчанию и другие параметры безопасности документированы, используются и известны всем заинтересованным лицам

## Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон. Эти провайдеры должны соответствовать требованиям, описанным в Приложении A1

# Обеспечить безопасное хранение данных держателей карт

## Хранение данных держателей карт должно быть ограничено только необходимым минимумом. Должны быть разработаны политики, процедуры и процессы хранения и уничтожения данных, соответствующие следующим минимальным требованиям к хранению данных держателей карт

* количество данных и сроки их хранения должны быть ограничены только необходимыми для выполнения требований бизнеса, законодательства и иных регулирующих требований
* специфические требования к хранению данных держателей карт
* процессы безопасного удаления данных, хранение которых более не является необходимым
* ежеквартальные процессы обнаружения и безопасного удаления данных держателей карт, которые превышают определенные политикой сроки хранения данных

## Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде). В случае получения критичных аутентификационных данных все данные невозможно будет восстановить по завершении процесса авторизации

### Запрещается хранить полное содержимое дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте). Эти данные также называются "полная дорожка", "дорожка", "дорожка 1", "дорожка 2" и "данные магнитной полосы".

### 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).

### Запрещается хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока

## Следует маскировать основной номер держателя карты при его отображении (максимально возможное количество знаков для отображения - первые шесть и последние четыре), чтобы только сотрудники с обоснованной коммерческой необходимостью могли видеть весь основной номер держателя карты.

## PAN должен быть представлен в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, в резервных копиях и журналах протоколирования событий).

### Если используется шифрование на уровне всего диска (вместо шифрования на уровне отдельных файлов или столбцов базы данных), то управление логическим доступом должно осуществляться отдельно и независимо от механизмов аутентификации и контроля доступа операционной системы (например, локальных баз данных учетных записей или общих учетных данных для входа в сеть). Ключи дешифрования не должны быть связаны с учетными записями пользователей.

## Задокументировать и внедрить процедуры для защиты ключей шифрования данных держателей карт от разглашения или неправильного использования следующим образом

### (Дополнительное требование для поставщиков услуг) Ведение документированного описания криптографической архитектуры, которая включает

* Подробная информация о всех алгоритмах, протоколах и ключах, используемых для защиты данных держателей карт, включая силу ключа и дату истечения срока действия
* Описание использования ключа для каждого ключа
* Инвентаризация любых HSM и других SCD, используемых для управления ключами

### Доступ к ключам шифрования должен быть разрешен наименьшему возможному количеству ответственных за их хранение и использование сотрудников

### Всегда хранить секретные и частные ключи шифрования/дешифрования данных держателей карт в одной (или нескольких) из следующих форм:

* защищенными ключом для шифрования ключей, который имеет такой же уровень защиты, как и ключ для шифрования данных, и хранится отдельно от этого ключа
* в безопасном устройстве для шифрования данных (например, хост-модуле безопасности или платежном терминале, одобренном PTS);
* в безопасном устройстве для шифрования данных (например, хост-модуле безопасности или платежном терминале, одобренном PTS);

### Ключи должны храниться в как можно меньшем количестве мест

## Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных держателей карт, в том числе следующие

### Генерация стойких криптографических ключей

### Безопасное распространение ключей

### Безопасное хранение ключей

### Смена ключей шифрования, криптопериод которых истек (например, когда истек установленный срок и (или) когда данным ключом было зашифровано некоторое количество криптотекста), основана на передовых практических методах индустрии безопасности и руководствах (например, специальное издание 800-57 NIST) и должна производиться согласно предписаниям соответствующего производителя или владельца ключа

### Изъятие или смена ключей (например,архивация, уничтожение и (или) аннуляция) при нарушении целостности (например, увольнение сотрудника, обладающего информацией об открытом компоненте ключа), а также ключей, относительно которых существуют подозрения во взломе.

### Если процедуры управления ключами шифрования в открытом виде осуществляются вручную, данные процедуры должны координироваться с использованием принципа разделения знания и двойного контроля

### Защита от неавторизованной замены ключа

### Определение обязанностей и ответственности сотрудников по хранению и использованию ключей с официальным подтверждением их согласия с ознакомлением и принятием таких обязанностей и ответственности

## Убедиться, что политики безопасности и процедуры защиты данных держателей карт документированы, используются и известны всем заинтересованным лицам

# Обеспечить шифрование данных держателей карт при передаче их через сети общего пользования

## Для защиты данных держателей карт во время их передачи через общедоступные сети следует использовать надежные криптографические алгоритмы и протоколы защиты (например, SSL/TLS, IPSEC, SSH и т.д.), соответствующие следующим требованиям

* прием только доверенных ключей и сертификатов
* используемый протокол поддерживает только безопасные версии и конфигурации
* стойкость шифрования соответствует используемой методологии шифрования

### При использовании беспроводных сетей, передающих данные держателей карт либо подключенных к среде данных держателей карт, следует использовать передовые практические методы индустрии безопасности (например, IEEE 802.11i), чтобы обеспечить стойкое шифрование при аутентификации и передаче данных

## Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (электронная почта, системы мгновенной отправки сообщений, чаты и т.д.).

## Убедиться, что политики безопасности и процедуры шифрования передаваемых данных держателей карт документированы, используются и известны всем заинтересованным лицам

# Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО

## Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах)

### Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.

### Проводить периодические проверки для выявления и оценки рисков заражения вредоносным ПО на системах, которые считаются не подверженными заражению вредоносным ПО, с целью подтверждения отсутствия необходимости в антивирусном ПО

## Убедится, что все антивирусные механизмы

* Актуальны
* выполняют периодическое сканирование
* создают журналы регистрации событий, которые хранятся согласно требованию 10.7 стандарта PCI DSS.

## Необходимо убедиться, что антивирусные программы работают в активном режиме и не могут быть отключены или изменены пользователями без явного разрешения руководства на индивидуальной основе и на ограниченный период времени

## Убедиться, что политики безопасности и процедуры защиты систем от вредоносного ПО документированы, используются и известны всем заинтересованным лицам.

# Разрабатывать и поддерживать безопасные системы и приложения

## Должен быть внедрен процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также ранжирования риска например, "высокий", "средний" или "низкий") недавно обнаруженных уязвимостей

## Все системные компоненты и программное обеспечение должны быть защищены от известных уязвимостей путем установки необходимых обновлений системы безопасности, выпущенных поставщиком. Критичные обновления безопасности должны быть установлены в течение месяца с момента их выпуска производителем

## Разработать безопасные внутренние и внешние приложения (включая административный доступ к приложениям через веб-интерфейс) с соблюдением следующих требований

* согласно требованиям PCI DSS (например, в отношении безопасной аутентификации и ведения журнала);
* процесс разработки программного обеспечения должен быть основан на отраслевых стандартах и (или) известных рекомендациях
* информационная безопасность должна учитываться в течение всего цикла разработки ПО

### Удалить все учетные записи разработчиков, тестовые и (или) пользовательские учетные записи приложения, имена пользователей и пароли перед передачей программного обеспечения заказчикам или переводом его в производственный режим.

### Проверить программный код приложений на наличие потенциальных уязвимостей (вручную или автоматически) перед передачей готовых приложений заказчикам или переводом их в производственный режим с соблюдением следующих минимальных требований

* изменения программного кода должны контролироваться лицами, иными, чем создавший его автор, и лицами, знакомыми с методиками контроля кода (code review techniques) и методами безопасного программирования (secure coding practices);
* контроль программного кода обеспечивает его разработку в соответствии с основными принципами безопасного программирования;
* все необходимые корректировки вносятся до выпуска программного обеспечения;
* результаты контроля кода рассматриваются и утверждаются руководством до выпуска программного обеспечения.

## Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов. Это могут быть следующие процедуры

### Отделить среды разработки/тестирования и производственного функционирования программного обеспечения друг от друга и при этом внедрить механизмы разграничения доступа

### Существует разделение обязанностей между сотрудниками, работающими в среде разработки/тестирования, и сотрудниками, работающими в среде эксплуатации

### Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки

### Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.

### Процедуры контроля изменений перед внедрением обновлений безопасности и изменений в конфигурации ПО должны включать следующее

#### Документирование влияния изменений

#### Согласование изменения с руководством

#### Тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы

#### Процедуры отмены изменения

### По завершении значительного изменения все соответствующие требования PCI DSS должны быть реализованы во всех новых или измененных системах и сетях, а документация обновлена в зависимости от ситуации

## Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом

* обучение разработчиков методикам безопасного программирования, включая информацию о том, как избежать распространенных программных уязвимостей и как определить способ хранения критичных данных в памяти;
* разработка приложений в соответствии с основными принципами безопасного программирования

### Инъекции, в особенности, SQL- инъекции. Также следует учесть инъекции OS Command, LDAP и Xpath

### Переполнение буфера

### Небезопасное криптографическое хранилище

### Небезопасная передача данных

### Некорректная обработка ошибок

### Все уязвимости с высокой степенью риска, найденные в процессе обнаружения уязвимостей (в соответствии с требованием 6.1 стандарта PCI DSS).

### Межсайтовый скриптинг (XSS)

### Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, отсутствие ограничения доступа по URL, обход директорий и отсутствие ограничения прав доступа пользователя к функциям)

### Подделка межсайтовых запросов (CSRF)

### Противодействие взлому механизмов аутентификации и управления сеансами

## Следует обеспечить защиту общедоступных веб-приложений от известных атак (а также регулярно учитывать новые угрозы и уязвимости) одним из следующих методов

* проверять приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности приложений не реже одного раза в год, а также после внесения изменений. Данное требование отличается от сканирования на наличие уязвимостей (п.11.2)
* Перед общедоступным веб­приложением должно быть установлено техническое средство для постоянной проверки всего трафика (например, веб-брандмауэр) с целью обнаружения и предупреждения веб­атак.

## Убедиться, что политики безопасности и процедуры разработки для обеспечения безопасности систем и приложений документированы, используются и известны всем заинтересованным лицам

# Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью

## Доступом к вычислительным ресурсам и данным держателей карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями

### Определение прав доступа для каждой должности, включая

* системные компоненты и ресурсы данных, доступ к которым необходим для каждой должности для выполнения должностных обязанностей
* необходимый уровень привилегий (например, пользователь, администратор и т.д.) для доступа к ресурсам

### Предоставить пользователям с учетными записями с широкими полномочиями доступ только к тем полномочиям, которые необходимы им для выполнения своих должностных обязанностей

### Назначать права доступа пользователям на основании классификации должностей и их должностных обязанностей

### Требовать документального утверждения прав доступа уполномоченными лицами с указанием необходимых полномочий

## Следует установить систему контроля доступа к системным компонентам, основанную на принципе необходимых полномочий и применить принцип "запрещено все, что явно не разрешено” ("deny all"). Система контроля доступа должна включать следующее

### Покрытие всех системных компонентов

### Назначение полномочий пользователям должно быть основано на их должностных обязанностях

### По умолчанию должен быть запрещен любой доступ

## Убедиться, что политики безопасности и процедуры ограничения доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам

# Определять и подтверждать доступ к системным компонентам

## Определить и внедрить политики и процедуры управления идентификацией сотрудников (не клиентов) и администраторов на всех системных компонентах, регламентирующие следующие требования:

### Каждому пользователю должен быть назначен уникальный идентификатор до предоставления ему доступа к системным компонентам или данным держателей карт

### Контроль добавления, удаления и изменения идентификаторов пользователей, аутентификационных данных и иных объектов идентификации

### Немедленный отзыв доступа при увольнении пользователя

### Проводить удаление/блокировку неактивных учетных записей не реже одного раза в 90 дней

### Управлять учетными записями, используемыми внешними пользователями для удаленного доступа, поддержки и обслуживания системных компонентов, следующим образом

* включать только на необходимый промежуток времени и отключать, когда они не используются
* проводить мониторинг во время их использования

### Блокировать учетные записи после не более чем шести неудачных попыток входа подряд

### Установить период блокировки учетной записи равным 30 минутам или до разблокировки учетной записи администратором

### Блокировать сеанс работы пользователя через 15 минут простоя с требованием ввода пароля для разблокировки, повторной активации терминала или сеанса

## Помимо назначения уникального идентификатора, для обеспечения надлежащего управления аутентификацией сотрудников (не пользователей) и администраторов на уровне всех системных компонентов должен применяться хотя бы один из следующих методов аутентификации всех пользователей

* то, что вы знаете (например, пароль или парольная фраза);
* то, что у вас есть (например, ключи или смарт-карты);
* то, чем вы обладаете (например, биометрические параметры).

### Все учетные данные для проверки подлинности (например, пароли/парольные фразы) должны храниться и передаваться только в зашифрованном виде с использованием стойкого шифрования на всех компонентах системы

### Перед изменением учетных данных для проверки подлинности (например, сбросом пароля, предоставлением новых токенов или генерацией новых ключей) необходимо установить личность пользователя

### Пароли/парольные фразы должны соответствовать следующим требованиям:

* наличие в пароле не менее семи символов
* наличие в пароле и цифр, и букв;
* как вариант, пароли/парольные фразы должны иметь сложность и стойкость, сравнимые с указанными выше параметрами

### Изменение паролей/парольных фраз пользователей не реже одного раза в 90 дней.

### Запрет смены пароля/парольной фразы на какие- либо из четырех последних паролей/парольных фраз данного пользователя, использованных им ранее

### Установка уникального первоначального пароля/парольной фразы для каждого пользователя и их немедленное изменение при первом входе пользователя в систему

## Для средств удаленного доступа сотрудников (включая пользователей и администраторов) и любых третьих лиц (включая доступ поставщиков для поддержки или техобслуживания) во внутреннюю сеть из внешней сети должен быть реализован механизм многофакторной аутентификации

### Включить многофакторную аутентификацию со всех средств удалённого доступа в CDE для персонала с административным доступом

### Включить многофакторную аутентификацию для всего удаленного доступа к сети (как пользователя, так и администратора, включая сторонний доступ для поддержки или обслуживания), из-за пределов сети предприятия.

## Задокументировать и проинформировать всех пользователей о процедурах и политиках аутентификации, включая

* рекомендации по выбору стойких учетных данных для аутентификации
* рекомендации по защите учетных данных для аутентификации
* указания не использовать ранее использованные пароли
* инструкции по смене пароля в случае подозрения на взлом

## Не использовать групповые, общие и стандартные учетные записи и пароли, а также прочие подобные методы аутентификации и убедиться в том, что

* стандартные учетные записи заблокированы или удалены
* общие учетные записи для системного администрирования и иных критичных функций не существуют
* общие и стандартные учетные записи не используются для администрирования каких-либо системных компонентов

### Дополнительное требование для поставщиков услуг: поставщики услуг, имеющие удаленный доступ к помещению клиента (например, для поддержки систем или серверов кассовых терминалов), обязаны использовать уникальные учетные данные для аутентификации (например, пароль/парольная фраза) для каждого клиента

## В случае использования других механизмов аутентификации (например, физических или логических токенов безопасности, смарт-карт, сертификатов и т.д.), эти механизмы должны назначаться следующим образом

* механизмы аутентификации должны назначаться для каждой учетной записи в отдельности, а не для нескольких учетных записей сразу
* необходимо использовать физические и (или) логические механизмы контроля, чтобы только авторизованный пользователь мог использовать такие механизмы для получения доступа

## Любой доступ к базе данных держателей карт (включая доступ со стороны приложений, администраторов и любых других пользователей) должен быть ограничен следующим образом

* доступ, запросы и операции с базами данных должны осуществляться только программными методами
* разрешение запросов и прямого доступа к базам данных только для администраторов баз данных
* учетные записи приложений по управлению базами данных могут использоваться только приложениями (но не пользователями или иными процессами).

## Убедиться, что политики безопасности и процедуры идентификации и аутентификации документированы, используются и известны всем заинтересованным лицам

# Ограничить физический доступ к данным держателей карт

## Следует использовать средства контроля доступа в помещение, чтобы ограничить и отслеживать физический доступ к системам, которые хранят, обрабатывают или передают данные держателей карт

### Следует использовать камеры видеонаблюдения или иные механизмы контроля доступа, чтобы следить за критичными помещениями. Данные, собранные механизмами контроля доступа, должны анализироваться и сопоставляться с другими фактами. Эти данные следует хранить не менее трех месяцев, если иной срок не предписан законодательством.

### Внедрить механизмы физического и (или) логического контроля для ограничения доступа к сетевым разъемам, расположенным в общедоступных местах

### Доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи должен быть ограничен

## Разработать процедуры, позволяющие легко различать персонал организации и посетителей и включающие

* идентификацию новых сотрудников или посетителей (например, путем выдачи бейджей)
* внесение изменений в права доступа
* процедуры отзыва или отключения средств идентификации уволенного сотрудника или средств идентификации посетителей с истекшим сроком действия (например, бейджей)

## Контролировать физический доступ сотрудников к критичным помещениям следующим образом

* права доступа сотрудников должны быть утверждены на основании классификации должностей и их должностных обязанностей
* доступ должен быть отозван сразу после его прекращения и все механизмы физического доступа (например, ключи, карты доступа и т.д.) должны быть возвращены или отключены

## Внедрить процедуры идентификации и авторизации посетителей. Процедуры должны быть следующими

### Посетители должны проходить авторизацию перед входом в помещения, где обрабатываются или хранятся данные держателей карт, и сопровождаться во время пребывания в них

### Идентифицировать посетителей и выдавать им бейдж или другое средство идентификации, имеющее ограничение срока действия и позволяющее отличить посетителя от сотрудника организации.

### Требовать от посетителей возврата выданного бейджа или другого средства идентификации при выходе с объекта или при истечении срока его действия.

### Ведется журнал регистрации посетителей как на входе в офисные помещения, так и на входе в вычислительные центры и центры обработки данных, в которых хранятся или передаются данные держателей карт. В журнале следует регистрировать имя посетителя, организацию, которую он представляет, а также сотрудника организации, разрешившего доступ посетителю. Этот журнал следует хранить не менее трех месяцев, если иной срок не предписан законодательством

## Должна быть обеспечена физическая безопасность всех видов носителей

### Носители с резервными копиями данных следует хранить в безопасных местах (желательно вне объекта), таких как запасной центр обработки данных, или же воспользовавшись услугами организаций, обеспечивающих безопасное хранение. Безопасность мест хранения должна проверяться не реже одного раза в год.

## Должен быть обеспечен строгий контроль за передачей всех видов носителей информации внутри организации и вне ее, в том числе следующее

### Классифицировать носители информации для определения уровня критичности хранимых данных

### Пересылку носителей осуществлять только с доверенным курьером или иным способом, который может быть тщательно проконтролирован

### Убедиться, что любой вынос носителей за пределы охраняемой территории (включая передачу носителя частным лицам) утверждается руководством

## Должен быть обеспечен строгий контроль хранения носителей и управление доступом к ним

### Должны поддерживаться в актуальном состоянии журналы инвентаризации всех носителей данных держателей карт; инвентаризация носителей должна проводиться не реже одного раза в год.

## Носители, хранение которых более не требуется для выполнения бизнес­задач или требований законодательства, должны быть уничтожены следующим образом

### Измельчение, сжигание или преобразование бумажного носителя в целлюлозную массу, чтобы данные держателей карт не могли быть восстановлены. Контейнеры для материалов, приготовленных для уничтожения, должны быть защищены

### Уничтожение данных держателей карт на электронном носителе, исключающее возможность их восстановления

## Обеспечить защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой, от подделки и подмены

### Составление и регулярное обновление списка устройств. Список должен включать следующую информацию

* марка и модель устройства
* местонахождение устройства (например, адрес объекта, в котором находится устройство);
* серийный номер устройства или другой уникальный идентификатор

### Периодически проверять поверхность устройств для обнаружения признаков взлома (например, прикрепленных к устройствам "скиммеров") или подмены (например, путем проверки серийного номера или других характеристик устройств, чтобы убедиться, что устройство не было заменено на мошенническое).

### Обучать сотрудников распознаванию признаков взлома или подмены устройств. Обучение должно включать следующую информацию

* следует установить личность третьих лиц, выдающих себя за ремонтников или специалистов техобслуживания, перед предоставлением им доступа для внесения изменений или устранения проблем с устройствами
* не следует устанавливать, заменять или возвращать устройство поставщику без такой проверки
* следует следить за подозрительным поведением вблизи устройств (например, попытками посторонних лиц отключить или открыть устройство)
* сотрудники должны сообщать о признаках взлома или подмены устройств соответствующим лицам (например, руководителю или сотруднику службы безопасности)

## Убедиться, что политики безопасности и процедуры ограничения физического доступа к данным держателей карт документированы, используются и известны всем заинтересованным лицам.

# Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт

## Внедрить журнал регистрации событий, связывающий любой доступ к системным компонентам с конкретным пользователем

## Для каждого системного компонента должен быть включен механизм протоколирования следующих событий

### Любой доступ пользователя к данным держателей карт

### Любые действия, совершенные с использованием административных полномочий

### Любой доступ к записям о событиях в системе

### Неуспешные попытки логического доступа

### Использование и изменение механизмов идентификации и аутентификации, включая, помимо прочего, создание новых учетных записей, расширение привилегий, а также все изменения, добавления, удаления учетных записей с правами суперпользователя ("root") или администратора

### Инициализация, остановка или приостановка ведения журналов протоколирования событий

### Создание и удаление объектов системного уровня

## Для каждого события каждого системного компонента должны быть записаны как минимум следующие параметры

### Идентификатор пользователя

### Тип события

### Дата и время

### Успешным или неуспешным было событие

### Источник события

### Идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие

## Все системные часы и системное время на критичных системах должны быть синхронизированы, Необходимо убедиться в исполнении данного требования для получения, распространения и хранения данных о времени

### На критичных системах установлено точное и согласованное время

### Данные о времени защищены

### Получение настроек времени происходит из признанных индустрией безопасности источников

## Журналы протоколирования событий должны быть защищены от изменений

### Доступом к журналам протоколирования событий должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями

### Журналы протоколирования событий должны быть защищены от неавторизованного изменения

### Резервные копии журналов протоколирования событий должны оперативно сохраняться на централизованный сервер протоколирования или отдельный носитель, где их изменение было бы затруднено

### Копии журналов протоколирования событий для технологий, к которым возможен доступ извне, должны сохраняться на безопасный и централизованный внутренний сервер протоколирования или носитель

### Следует использовать приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала)

## Изучать журналы протоколирования событий и события безопасности всех системных компонентов с целью обнаружения аномалий или подозрительной активности

### Проверяйте не реже одного раза в день

* все события безопасности
* журналы всех системных компонентов, осуществляющих хранение, обработку или передачу данных держателей карт и (или) критичных аутентификационных данных, или влияющих на их безопасность
* журналы всех критичных системных компонентов
* журналы всех серверов и системных компонентов, выполняющих функции безопасности (например, брандмауэров, систем обнаружения и предотвращения вторжений, серверов аутентификации, серверов перенаправления электронной торговли и т.д.

### Периодически изучать журналы других системных компонентов на основании политик и стратегии управления рисками, определяемой в рамках ежегодной оценки рисков

### Изучить исключительные ситуации (exceptions) и аномалии, обнаруженные во время проверки

## Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев (например, они могут находиться в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии)

## Дополнительные требования только для поставщиков услуг: Внедрение процесса для своевременного обнаружения и отчетности о сбоях критических систем управления безопасностью, включая, но не ограничиваясь:

* Брандмауэры
* IDS / IPS
* FIM
* Антивирус
* Контроль физического доступа
* Контроль логического доступа
* Механизмы ведения журналов
* Элементы управления сегментацией (если используются)

### Дополнительные требования только для поставщиков услуг: своевременно реагировать на сбои любых критических элементов управления безопасностью. Процессы реагирования на сбои в средствах контроля безопасности должны включать

* Восстановление функций безопасности
* Идентификация и документирование продолжительности (даты и времени начала до конца) сбоя в системе безопасности
* Идентификация и документирование причин(-ы) сбоя, включая основную причину, и документирование исправления, требуемого для устранения первопричины
* Определение и устранение любых проблем безопасности, возникших во время сбоя
* Выполнение оценки риска для определения необходимости дальнейших действий в результате сбоя в системе безопасности
* Внедрение контроля для предотвращения отказов по выявленным ранее причинам
* Возобновление мониторинга элементов управления безопасностью

## Убедиться, что политики безопасности и процедуры мониторинга любого доступа к сетевым ресурсам и данным держателей карт документированы, используются и известны всем заинтересованным лицам

# Регулярно выполнять тестирование систем и процессов обеспечения безопасности

## Внедрить процессы для проведения ежеквартальной проверки наличия беспроводных точек доступа (802.11) и для обнаружения авторизованных и неавторизованных беспроводных точек доступа

### Вести список авторизованных беспроводных точек доступа с указанием их необходимости для ведения дел

### Внедрить процедуры реагирования на обнаружение неавторизованных беспроводных точек доступа

## Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений (например, установки новых системных компонентов, изменения топологии сети, изменения правил межсетевых экранов, обновления продуктов)

### Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей и, при необходимости, повторные сканирования, пока не будут устранены все уязвимости, представляющие высокий риск (согласно определению в требовании 6.1). Сканирование должны выполнять квалифицированные специалисты

### Следует проводить ежеквартальное внешнее сканирование на наличие уязвимостей посредством авторизованного поставщика услуг сканирования (ASV), сертифицированного Советом по стандартам безопасности индустрии платежных карт (PCI SSC). Проводить повторные сканирования до достижения удовлетворительного результата

### Проводить внутреннее и внешнее сканирования и, при необходимости, повторное сканирование после любого значительного изменения в сети. Сканирование должны выполнять квалифицированные специалисты

## Внедрить методологию проведения тестирования на проникновение которая:

* основана на общепринятых отраслевых подходах к проведению тестирования на проникновение (например, NIST SP800-115)
* охватывает весь периметр информационной среды держателей карт и критичные системы
* включает тестирование как снаружи сети, так и внутри сети
* включает тестирование на наличие механизмов сегментации и уменьшения охвата
* требует, чтобы тесты на проникновение на уровне приложения включали, как минимум, проверку на наличие уязвимостей, приведенных в требовании 6.5
* требует, чтобы тесты на проникновение на уровне сети охватывали не только операционные системы, но и другие компоненты, поддерживающие взаимодействие на сетевом уровне
* включает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев
* регламентирует хранение результатов тестов на проникновение и мер, предпринятых для устранения уязвимостей

### Следует проводить внешний тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера).

### Следует проводить внутренний тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера).

### Необходимо исправлять опасные уязвимости, обнаруженные во время тестирования на возможность проникновения и проводить повторное тестирование для проверки исправлений

### В случае использования сегментации для изолирования информационной среды держателей карт от других сетей необходимо проводить тестирование на возможность проникновения не реже одного раза в год и после любого изменения механизмов/методов сегментации для проверки функционирования и эффективности методов сегментации и изолирования всех непроверенных систем от проверенных

#### Дополнительные требования только для поставщиков услуг: если используется сегментация, подтвердите область PCI DSS, выполнив тестирование на проникновение в элементы управления сегментацией не реже одного раза в шесть месяцев и после любых изменений в элементах управления / методах сегментации.

## Следует использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Следует осуществлять мониторинг сетевого трафика по периметру среды данных держателей карт и в критичных точках внутри среды данных держателей карт, и оповещать сотрудников о подозрительных действиях. Системы обнаружения и предотвращения вторжений и их сигнатуры должны поддерживаться в актуальном состоянии

## Следует внедрить механизм защиты от изменений (например, мониторинг целостности файлов) для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных; сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю

### Внедрить процесс реагирования на любое срабатывание механизма защиты от изменений

## Убедиться, что политики безопасности и процедуры мониторинга и проверки безопасности документированы, используются и известны всем заинтересованным лицам

# Разработать и поддерживать политику информационной безопасности для всего персонала организации

## Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика безопасности

### Политика безопасности должна пересматриваться по меньшей мере ежегодно и обновляться в случае изменения среды организации

## Внедрить процесс оценки рисков, который

* осуществляется не реже, чем раз в год и после значительного изменения среды (например, покупки, слияния, перемещения и т.д.);
* выявляет критические активы, угрозы и уязвимости
* завершается официальной оценкой рисков

## Разработать правила эксплуатации критичных технологий и определить надлежащее применение для этих технологий

Примечание. К критичным технологиям относятся в том числе: технологии удаленного доступа, беспроводные технологии, использование ноутбуков, планшетов, съемных носителей информации, электронной почты и Интернета.

Изучить правила эксплуатации критичных технологий и осуществить следующие проверки:

### Процедуру явного одобрения уполномоченными лицами

### Аутентификацию перед использованием устройства

### Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам

### Способ точного и оперативного определения владельца, контактных данных и назначения(например, маркировка, кодирование и (или) инвентаризация устройств

### Допустимые варианты использования технологий

### Допустимые точки размещения технологий в сети

### Перечень одобренных компанией продуктов

### Автоматическое отключение сессий удаленного доступа после определенного периода простоя

### Включение механизмов удаленного доступа для производителей и деловых партнеров только в случае необходимости такого доступа с немедленным выключением механизмов после использования

### Персоналу, имеющему удаленный доступ к данным держателей карт, запрещается копировать, перемещать и хранить данные держателей карт на локальных жестких дисках и съемных электронных носителях, если это не обусловлено служебной необходимостью. При наличии подтвержденной служебной необходимости политики эксплуатации должны регламентировать защиту данных в соответствии со всеми действующими требованиями стандарта PCI DSS.

## Политика и процедуры обеспечения безопасности должны однозначно определять обязанности всего персонала организации, относящиеся к информационной безопасности

### Дополнительные требования только для поставщиков услуг: руководство должно установить ответственность за защиту данных держателей карт и программу соответствия PCI DSS, включая:

* Кто несёт общую ответственность за поддержание соответствия PCI DSS
* Кто является руководителем программы соответствия PCI DSS и его взаимодействие с исполнительным руководством

## Определенному сотруднику или группе сотрудников должны быть назначены следующие обязанности в области управления информационной безопасностью:

### Разработка, документирование и распространение политики и процедур обеспечения безопасности

### Мониторинг, анализ и доведение до сведения соответствующего персонала информации о событиях, имеющих отношение к безопасности данных

### Разработка, документирование и распространение процедур реагирования на инциденты и сообщения о них, чтобы гарантировать быструю и эффективную обработку всех ситуаций

### Администрирование учетных записей пользователей, включая их добавление, удаление и изменение

### Мониторинг и контроль любого доступа к данным

## Должна быть внедрена официальная программа повышения осведомленности персонала по вопросам безопасности с целью донести до них важность обеспечения безопасности данных держателей карт

### Обучение персонала организации должно проводиться при приеме на работу, а также не реже одного раза в год

### Персонал организации должен не реже одного раза в год подтверждать свое знание и понимание политики и процедур обеспечения информационной безопасности организации

## Следует тщательно проверять кандидатов (будущий персонал)при приеме на работу для минимизации риска внутренних атак. (Примером кадровых проверок является изучение послужного списка, записей правоохранительных органов, кредитной истории, проверки рекомендаций)

Примечание. Для кандидатов на определенные должности, такие как, например, кассир в магазине, которые имеют доступ только к одному номеру карты только в момент проведения транзакции, это требование носит рекомендательный характер.

## Внедрить и поддерживать следующие политики и процедуры взаимодействия с поставщиками услуг, которые имеют доступ к данным держателей карт или могут повлиять на безопасность данных держателей карт

### Составление и регулярное обновление перечня поставщиков услуг

### Составление письменного соглашения, включающего положение о том, что поставщики услуг ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, или на безопасность которых они могут повлиять

### Гарантию проведения тщательной проверки поставщика услуг перед началом взаимодействия с ним

### Поддержку программы проверки статуса соответствия поставщика услуг требованиям PCI DSS по меньшей мере один раз в год

### Хранить информацию о том, за какие требования стандарта PCI DSS несет ответственность каждый поставщик услуг, а за какие несет ответственность сама организация

## Дополнительное требование для поставщиков услуг: поставщики услуг дают клиентам письменное согласие с тем, что они ответственны за безопасность имеющихся у них данных держателей карт, которые они хранят, обрабатывают или передают от имени клиента, или на безопасность которых они могут повлиять

## Должен быть внедрен план реагирования на инциденты. Организация должна быть готова немедленно отреагировать на нарушение в работе системы

### Следует разработать план реагирования на инциденты, применяемый в случае взлома системы. План должен содержать:

* описание ролей, обязанностей и схем оповещения в случае компрометации, включая, как минимум, оповещение международных платежных систем
* описание процедур реагирования на определенные инциденты
* описание процедур восстановления и обеспечения непрерывности бизнеса
* описание процессов резервного копирования данных
* анализ требований законодательства об оповещении о фактах компрометации
* описание всех критичных системных компонентов
* процедуры реагирования на инциденты международных платежных систем или ссылки на них

### План следует тестировать не реже одного раза в год

### Должен быть назначен соответствующий персонал, готовый реагировать на сигналы тревоги круглосуточно и ежедневно

### Сотрудники, ответственные за реагирование на нарушения безопасности, должны быть обучены соответствующим образом

### План должен включать в себя процедуры реагирования на предупреждения систем мониторинга безопасности, включая, но не ограничиваясь: системы обнаружения и предупреждения вторжений, брандмауэры, а также системы мониторинга целостности файлов

### Должен быть разработан процесс изменения и улучшения плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли

## Дополнительные требования только для поставщиков услуг: по крайней мере ежеквартально подтверждать, что персонал следит за политиками безопасности и операционными процедурами. Обследование должно охватывать следующие процессы:

* Ежедневные обзоры журналов
* Пересмотр правил брандмауэра
* Применение стандартов конфигурации к новым системам
* Реагирование на предупреждения о безопасности
* Процессы управления изменениями

### Дополнительные требования только для поставщиков услуг: Должна вестись документация по квартальному анализу, которая включает:

* Документирование результатов обследования
* Рассмотрение и подписание результатов персоналом, ответственным за программу соблюдения стандартов PCI DSS