Стандарт безопасности данных индустрии платежных карт

Опросный лист D для самооценки
и свидетельство о соответствии

Все остальные торгово-сервисные компании и поставщики услуг

Версия 2.0

Октябрь 2010 г.

Изменения документа

Дата	Версия	Описание
1 октября 2008 г.	1.2	Обеспечено соответствие стандарту PCI DSS версии 1.2 и внедрены незначительные изменения по сравнению с версией 1.1.
28 октября 2010 г.	2.0	Обеспечено соответствие требованиям и процедурам тестирования по стандарту PCI DSS версии 2.0.

Содержание

Стандарт безопасности данных индустрии платежных карт (PCI DSS): документы по теме

Следующие документы были созданы для помощи торговым организациям и поставщикам услуг в понимании стандарта PCI DSS и того, как заполнять опросные листы для самооценки.

Документ	Целевая аудитория
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Требования и процедура аудита безопасности*	Все торгово-сервисные организации и поставщики услуг
PCI DSS: *Понимание назначения требований*	Все торгово-сервисные организации и поставщики услуг
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Рекомендации и инструкции по заполнению опросных листов для самооценки*	Все торгово-сервисные организации и поставщики услуг
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Опросный лист A для самооценки и свидетельство о соответствии*	Торгово-сервисные организации, имеющие право на участие[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Опросный лист B для самооценки и свидетельство о соответствии*	Торгово-сервисные организации, имеющие право на участие[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Опросный лист C-VT для самооценки и свидетельство о соответствии*	Торгово-сервисные организации, имеющие право на участие[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Опросный лист C для самооценки и свидетельство о соответствии*	Торгово-сервисные организации, имеющие право на участие[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS): *Опросный лист D для самооценки и свидетельство о соответствии*	Торгово-сервисные организации и поставщики услуг, которые имеют право на участие[1]

[1] Чтобы определить, какой опросный лист следует использовать, см. *Стандарт безопасности данных индустрии платежных карт: руководства и инструкции по работе с опросными листами,* раздел “Выбор опросного листа для самооценки и свидетельства о соответствии, которые лучше всего подходят для вашей организации”.

Стандарт безопасности данных индустрии платежных карт и стандарт безопасности данных платежных приложений: *Глоссарий терминов, аббревиатур и сокращений*	Все торгово-сервисные организации и поставщики услуг

До начала работы

Заполнение опросного листа для самооценки

Опросный лист для самооценки (ОЛС) D предназначен для всех поставщиков услуг и торгово-сервисных компаний, которые не подпадают под условия ОЛС типов от A до C (включительно), кратко описанных в приведенной ниже таблице и полностью описанных в документе “Руководствои *инструкции по работе с опросными листами”.*

ОЛС	Описание
A	Торгово-сервисные организации, которые занимаются операциями без предоставления карт (электронная коммерция или прием заказов по почте или телефону), все задачи по работе с данными о держателях карт выполняются сторонними организациями. *Это не относится к торгово-сервисным организациям, которые занимаются операциями с предоставлением карты.*
B	Торгово-сервисные компании, применяющие только системы для чтения данных с банковской карты или автономные терминалы с подключением к телефонной линии, без хранения данных о держателях карт в электронном виде.
C-VT	Торгово-сервисные организации, использующие только виртуальные терминалы с веб-интерфейсом и не хранящие данные о держателях карт в электронном виде
C	Торгово-сервисные организации, использующие платежные системы с подключением к интернету, без хранения данных о держателях карт в электронном виде
D	Все прочие торгово-сервисные организации, не включенные в описания опросных листов A-C, и **все поставщики услуг**, наделенные платежной системой правом заполнения опросного листа.

ОЛС D применяется ко всем торгово-сервисным организациям, не подпадающим под условия ОЛС типов от A до C включительно, и все поставщики услуг, наделенные платежной системой правом заполнения опросного листа. Такие торгово-сервисные организации могут проверить свое соответствие, заполнив опросный лист D и связанное с ним свидетельство о соответствии для подтверждения следующих фактов:

Многим организациям, заполняющим ОЛС D, понадобится проверить выполнение каждого требования PCI DSS, к некоторым организациям с особыми бизнес-моделями могут применяться не все требования. Например, от компании, которая ни в каком виде не использует беспроводные технологии, не потребуется проверять соблюдение стандартов PCI DSS, относящихся к управлению беспроводными технологиями. Сведения об исключениях, касающихся беспроводных технологий и некоторых других вопросов, см. ниже.

Каждый раздел опросника соответствует определенной области безопасности согласно требованиям PCI DSS.

Порядок оформления подтверждения о соответствии стандарту PCI DSS

1. Оцените свою среду на соответствие требованиям PCI DSS.
2. Заполните опросный лист для самооценки (ОЛС) D согласно инструкциям, приведенным в документе *“Руководства и инструкции по работе с опросными листами”.*
3. Пройдите ASV-сканирование уполномоченной организацией (ASV – Approved Scanning Vendor) PCI DSS с положительным результатом и получите подтверждение прохождения такой проверки.
4. Заполните Свидетельство о соответствии.
5. Отправьте ОЛС, результат ASV-сканирования и свидетельство о соответствии вместе со всей требуемой документацией банку-эквайеру (для торгово-сервисных предприятий), платежной системе или другой уполномоченной организации (для поставщиков услуг).

Рекомендации о неприменимости определенных требований

Исключение: если вам необходимо ответить на вопросы ОЛС D для проверки выполнения стандартов PCI DSS, то возможны следующие исключения. См. также раздел “Неприменимость требований”, чтобы выбрать нужный ответ на вопрос.

- На вопросы, относящиеся к беспроводным подключениям, следует отвечать лишь в том случае, если в вашей сети используются беспроводные подключения (например, требования 1.2.3, 2.1.1 и 4.1.1). Обратите внимание, что на вопрос требования 11.1 (применение процессов для идентификации несанкционированных точек беспроводного доступа) необходимо отвечать даже если в вашей сети нет беспроводных подключений, поскольку данный процесс обнаруживает посторонние устройства, которые могли быть добавлены в сеть скрытно.
- На вопросы, относящиеся к индивидуально разработанным приложениям и коду (требования 6.3 и 6.5), нужно отвечать только в случае, если ваша организация самостоятельно разрабатывает такие приложения.
- На вопросы требований с 9.1 по 9.4 включительно нужно отвечать только при наличии “конфиденциальных помещений”. Конфиденциальными являются такие помещения, как центр обработки данных, серверная комната или иное помещение, где расположены системы, которые используются для хранения, обработки или передачи данных о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов, но не являются серверные помещения, в которых хранятся данные о держателях карт, и места массового хранения данных о держателях карт.

Неприменимость: для требований, которые представляются неприменимыми к вашей среде, следует указать “Н/п” в столбце “Комментарии” ОЛС. Для каждого такого требования заполните форму “Причины неприменимости требований”, приведенную в приложении Г к опросному листу.

Свидетельство о соответствии стандарту, ОЛС D, версия для торгово-сервисных организаций

Инструкции по отправке

Торгово-сервисная организация должна заполнить данное Свидетельство о соответствии в знак заявления о соответствии требованиям стандарта *PCI DSS, а также требованиям и процедурам аудита безопасности.* Заполните все необходимые разделы согласно инструкциям, приведенным в разделе “Порядок оформления подтверждения о соответствии стандарту PCI DSS”.

Часть 1. Информация о торгово-сервисной организации и о квалифицированной компании, проверяющей безопасность

Часть 1a. Информация о коммерческой организации

Название компании:			Администраторы баз данных:		
Контактное лицо:			Должность:		
Телефон:			Эл. почта:		
Улица, дом:			Город:		
Область, край:		Страна:		Почтовый индекс:	
URL-адрес:					

Часть 1b. Информация о квалифицированной компании, проверяющей безопасность (если применимо)

Название компании:					
Контактное лицо по проверке безопасности:			Должность:		
Телефон:			Эл. почта:		
Улица, дом:			Город:		
Область, край:		Страна:		Почтовый индекс:	
URL-адрес:					

Часть 2. Область работы торгово-сервисной организации (выберите все применимые ответы):

☐ Розничная торговля питания и супермаркеты ☐ Телекоммуникации ☐ Розничная торговля продуктами

☐ Нефтегазовая отрасль ☐ Электронная торговля ☐ Обработка заказов по почте или по телефону Другое (укажите):

☐ Другое (укажите):

Перечислите все помещения, офисы, магазины и т.п., включенные в данную проверку соответствия

стандартам PCI DSS:

Часть 2a. Взаимоотношения

Поддерживает ли ваша компания взаимоотношения с одной или несколькими сторонними компаниями (например, платежных шлюзов, поставщиков веб-хостинга, агентов по бронированию авиабилетов, агентов программ лояльности клиентов и т.п.)?	☐ Да ☐ Нет
Поддерживает ли ваша компания взаимоотношения с несколькими банками-эквайерами?	☐ Да ☐ Нет

Часть 2b. Обработка транзакций

Как и с какой целью ваша компания хранит, обрабатывает или передает данные о держателях карт?

Укажите следующую информацию, касающуюся платежных приложений, используемых в вашей организации:

Используемое платежное приложение	**Номер версии**	**Дата последней проверки по стандарту PABP/PA-DSS**

Часть 3. Проверка соответствия стандартам PCI DSS

На основе результатов, указанных в ОЛС D от *(дата заполнения)*, *(название торгово-сервисной организации)* заявляет о следующем состоянии соответствия (выберите один вариант):

☐ **Соответствует.** Все разделы ОЛС заполнены, на все вопросы дан ответ “Да”, итоговая оценка **Соответствует**, успешно пройдена проверка, выполненная уполномоченной организацией со статусом PCI SSC Approved Scanning Vendor (ASV). Следовательно, **(название торгово-сервисной организации)** полностью соответствует стандартам PCI DSS.

☐ **Не соответствует.** Заполнены не все разделы ОЛС, ответ “Да” дан не на все вопросы, итоговая оценка **Не соответствует** или не пройдена проверка, выполненная уполномоченной организацией со статусом PCI SSC Approved Scanning Vendor (ASV). Следовательно, **(название торгово-сервисной организации)** не соответствует стандартам PCI DSS.

Дата обеспечения соответствия.

Организации, отправляющей эту форму с состоянием “Не соответствует”, может потребоваться заполнить план действий в части 4 данного документа. *Перед заполнением части 4 обсудите этот вопрос с банком-эквайером или платежными брендами, поскольку заполнение этого раздела требуется не всеми платежными брендами.*

Часть 3a. Подтверждение состояния соответствия

Торгово-сервисная организация подтверждает:

☐	опросный лист для самооценки D PCI DSS версии *(номер версии ОЛС)* был заполнен согласно указанным инструкциям.
☐	Вся информация в указанном ОЛС и в данном свидетельстве соответствует результатам оценки.
☐	Поставщик платежного приложения подтверждает, что платежная система не хранит конфиденциальные данные после авторизации.
☐	Со стандартами PCI DSS ознакомлен(а) и признаю необходимость постоянного соблюдения всех стандартов PCI DSS.
☐	На ВСЕХ системах, проверенных в ходе данного аудита, не обнаружено признаков сохранения данных магнитной полосы[2], CAV2, CVC2, CID, CVV2[3], а также данных ПИН-кода[4] после авторизации операций.

Часть 3b. Подтверждение торгово-сервисной организации

Подпись руководителя торгово-сервисной организации	*Дата*
Имя руководителя торгово-сервисной организации	*Должность*
Представитель торгово-сервисной организации	

Часть 4. План действий при несоответствии

Выберите соответствующее “Состояние соответствия” для каждого требования. Если на какое-либо из требований был дан ответ “Нет”, необходимо указать дату, когда компания будет соответствовать данному требованию, а также привести краткое описание действий, которые будут выполнены для обеспечения соответствия. *Перед заполнением части 4 обсудите этот вопрос с банком-эквайером или платежными брендами, поскольку заполнение этого раздела требуется не всеми платежными брендами.*

Требование PCI DSS	Описание требования	Состояние соответствия (выберите один вариант)		Дата устранения несоответствия и необходимые для этого действия (если указано состояние соответствия “Нет”)
		ДА	НЕТ	

[2] Данные, зашифрованные на магнитной полосе (или эквивалентные данные в чипе карты), используются для авторизации при проведении операций с предоставлением карты. Организации могут не хранить полные данные магнитной полосы после авторизации операции. Достаточно хранить только такие элементы, как номер платежной карты, имя держателя карты и дата истечения срока действия карты.

[3] Трех- или четырехзначное число, напечатанное справа от места для подписи или на лицевой стороне карты, используется для проверки операций без предоставления карты.

[4] Персональный идентификационный номер вводится держателем карты при выполнении операции с предоставлением карты, при этом в сообщении об операции может присутствовать зашифрованный PIN-блок.

Требование PCI DSS	Описание требования	Состояние соответствия (выберите один вариант)		Дата устранения несоответствия и необходимые для этого действия
1	Установить и поддерживать в рабочем состоянии брандмауэры для защиты данных о держателях карт	☐	☐	
2	Не использовать пароли и другие системные параметры, заданные производителем по умолчанию	☐	☐	
3	Обеспечить безопасное хранение данных о держателях карт	☐	☐	
4	Использовать шифрование данных о держателях карт при их передаче через сети общего пользования	☐	☐	
5	Использовать и регулярно обновлять антивирусное программное обеспечение	☐	☐	
6	Разрабатывать и поддерживать безопасные системы и приложения	☐	☐	
7	Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью	☐	☐	
8	Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре	☐	☐	
9	Ограничить физический доступ к данным о держателях карт	☐	☐	
10	Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт	☐	☐	
11	Регулярно проверять системы и процессы, обеспечивающие безопасность.	☐	☐	
12	Разработать и поддерживать политику информационной безопасности для всего персонала организации	☐	☐	

Свидетельство о соответствии стандарту, ОЛС D, версия для поставщиков услуг

Инструкции по отправке

Поставщик услуг должен заполнить данное свидетельство о соответствии в знак заявления о соответствии требованиям стандарта *PCI DSS, а также требованиям и процедурам аудита безопасности.* Заполните все необходимые разделы согласно инструкциям, приведенным в разделе “Оценка соответствия требованиям PCI DSS: шаги создания отчета” в данном документе.

Часть 1. Информация о поставщике услуг и о квалифицированной компании, проверяющей безопасность

Часть 1a. Сведения об организации-поставщике услуг

Название компании:			Администраторы баз данных:		
Контактное лицо:			Должность:		
Телефон:			Эл. почта:		
Улица, дом:			Город:		
Область, край:		Страна:		Почтовый индекс:	
URL-адрес:					

Часть 1b. Информация о квалифицированной компании, проверяющей безопасность (если применимо)

Название компании:					
Контактное лицо по проверке безопасности:			Должность:		
Телефон:			Эл. почта:		
Улица, дом:			Город:		
Область, край:		Страна:		Почтовый индекс:	
URL-адрес:					

Часть 2. Сведения проверке соответствия PCI DSS

Часть 2a. Поставщики услуг, ВКЛЮЧЕННЫЕ в область проверки PCI DSS (выберите все применимые ответы)

☐ Поставщик услуг 3-D Secure	☐ Поставщик услуг хостинга – оборудование	☐ Обработка платежей – банкоматы
☐ Управление работой с	☐ Поставщик услуг хостинга –	☐ Обработка платежей – заказы

клиентами	веб-сайты	по телефону или по почте
☐ Авторизация	☐ Обработка данных эмитентов	☐ Обработка платежей – Интернет
☐ Услуги внутреннего офиса	☐ Программы лояльности	☐ Обработка платежей – POS-терминалы
☐ Управление выставлением счетов	☐ Управляемые услуги	☐ Предоплаченные услуги
☐ Расчетно-кассовые операции	☐ Обслуживание торговых точек	☐ Управление архивами
☐ Подготовка данных	☐ Поставщик сетевых ресурсов и каналов передачи данных	☐ Налоги и государственные платежи
☐ Борьба с мошенничеством и возврат платежей	☐ Платежные шлюзы	
☐ Другое (укажите):		

Перечислите все помещения, офисы, магазины и т.п., включенные в данную проверку соответствия стандартам PCI DSS:

Часть 2b. Если какие-либо услуги предоставляются поставщиком услуг, но *НЕ БЫЛИ ВКЛЮЧЕНЫ* в область проверки PCI DSS, укажите их ниже:		
☐ Поставщик услуг 3-D Secure	☐ Поставщик услуг хостинга – оборудование	☐ Обработка платежей – банкоматы
☐ Управление работой с клиентами	☐ Поставщик услуг хостинга – веб-сайты	☐ Обработка платежей – заказы по телефону или по почте
☐ Авторизация	☐ Обработка данных эмитентов	☐ Обработка платежей – Интернет
☐ Услуги внутреннего офиса	☐ Программы лояльности	☐ Обработка платежей – POS-терминалы
☐ Управление выставлением счетов	☐ Управляемые услуги	☐ Предоплаченные услуги
☐ Расчетно-кассовые операции	☐ Обслуживание торговых точек	☐ Управление архивами
☐ Подготовка данных	☐ Поставщик сетевых ресурсов и каналов передачи данных	☐ Налоги и государственные платежи
☐ Борьба с мошенничеством и возврат платежей	☐ Платежные шлюзы	
☐ Другое (укажите):		

Часть 2c. Взаимоотношения

Поддерживает ли ваша компания взаимоотношения с одной или несколькими сторонними компаниями (например, платежных шлюзов, поставщиков веб-хостинга, агентов по бронированию авиабилетов, агентов программ лояльности клиентов и т.п.)? ☐ Да ☐ Нет

Часть 2d. Обработка транзакций

Как и с какой целью ваша компания хранит, обрабатывает или передает данные о держателях карт?

Используемое платежное приложение	**Номер версии**	**Дата последней проверки по стандарту PABP/PA-DSS**

Укажите следующую информацию, касающуюся платежных приложений, используемых в вашей организации:

Часть 3. Проверка соответствия стандартам PCI DSS

На основе результатов, указанных в ОЛС D от *(дата заполнения)*, *(название поставщика услуг)* заявляет о следующем состоянии соответствия (выберите один вариант):

☐ **Соответствует.** Все разделы ОЛС заполнены, на все вопросы дан ответ “Да”, итоговая оценка **Соответствует**, и также успешно пройдена проверка, выполненная уполномоченной организацией со статусом PCI SSC Approved Scanning Vendor (ASV). Следовательно, **(название поставщика услуг)** полностью соответствует стандартам PCI DSS.

☐ **Не соответствует.** Заполнены не все разделы ОЛС, ответ “Да” дан не на все вопросы, итоговая оценка **Не соответствует** или не пройдена проверка, выполненная уполномоченной организацией со статусом PCI SSC Approved Scanning Vendor (ASV). Следовательно, **(название поставщика услуг)** не соответствует стандартам PCI DSS.

Дата обеспечения соответствия.

Организации, отправляющей эту форму с состоянием “Не соответствует”, может потребоваться заполнить план действий в части 4 данного документа. *Перед заполнением части 4 обсудите этот вопрос с банком-эквайером или платежными брендами, поскольку заполнение этого раздела требуется не всеми платежными брендами.*

Часть 3a. Подтверждение состояния соответствия

Поставщик услуг подтверждает:

☐	опросный лист для самооценки D PCI DSS версии *(номер версии ОЛС)* был заполнен согласно указанным инструкциям.
☐	Вся информация в указанном ОЛС и в данном свидетельстве соответствует результатам оценки.
☐	Со стандартами PCI DSS ознакомлен(а) и признаю необходимость постоянного соблюдения всех стандартов PCI DSS.
☐	На ВСЕХ системах, проверенных в ходе данного аудита, не обнаружено признаков сохранения данных магнитной полосы[5], CAV2, CVC2, CID, CVV2[6], а также данных ПИН-кода[7] после авторизации операций.

Часть 3b. Подтверждение поставщика услуг

Подпись руководителя поставщика услуг ☐	*Дата* ☐
Имя руководителя поставщика услуг ☐	*Должность* ☐

Представитель поставщика услуг ☐

Часть 4. План действий при несоответствии

Выберите соответствующее “Состояние соответствия” для каждого требования. Если на какое-либо из требований был дан ответ “Нет”, необходимо указать дату, когда компания будет соответствовать данному требованию, а также привести краткое описание действий, которые будут выполнены для обеспечения соответствия. *Перед заполнением части 4 обсудите этот вопрос с банком-эквайером или платежными брендами, поскольку заполнение этого раздела требуется не всеми платежными брендами.*

[5] Данные, зашифрованные на магнитной полосе (или эквивалентные данные в чипе карты), используются для авторизации при проведении операций с предоставлением карты. Организации могут не хранить полные данные магнитной полосы после авторизации операции. Достаточно хранить только такие элементы, как номер платежной карты, имя держателя карты и дата истечения срока действия карты.

[6] Трех- или четырехзначное число, напечатанное справа от места для подписи или на лицевой стороне карты, используется для проверки операций без предоставления карты.

[7] Персональный идентификационный номер вводится держателем карты при выполнении операции с предоставлением карты, при этом в сообщении об операции может присутствовать зашифрованный PIN-блок.

Требование PCI DSS	Описание требования	Состояние соответствия (выберите один вариант)		Дата устранения несоответствия и необходимые для этого действия (если указано состояние соответствия “Нет”)
		ДА	НЕТ	
1	Установить и поддерживать в рабочем состоянии брандмауэры для защиты данных о держателях карт	☐	☐	
2	Не использовать пароли и другие системные параметры, заданные производителем по умолчанию	☐	☐	
3	Обеспечить безопасное хранение данных о держателях карт	☐	☐	
4	Использовать шифрование данных о держателях карт при их передаче через сети общего пользования	☐	☐	
5	Использовать и регулярно обновлять антивирусное программное обеспечение	☐	☐	
6	Разрабатывать и поддерживать безопасные системы и приложения	☐	☐	
7	Ограничить доступ к данным о держателях карт в соответствии со служебной необходимостью	☐	☐	
8	Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре	☐	☐	
9	Ограничить физический доступ к данным о держателях карт	☐	☐	
10	Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт	☐	☐	
11	Регулярно проверять системы и процессы, обеспечивающие безопасность.	☐	☐	
12	Разработать и поддерживать политику информационной безопасности для всего персонала организации	☐	☐	

Опросный лист D для самооценки

Примечание. *Нумерация следующих вопросов соответствует нумерации требований и процедур проверки PCI DSS согласно документу* Требования и процедуры аудита безопасности PCI DSS.

Дата заполнения:

Построение и обслуживание защищенной сети

Требование 1. Установить и поддерживать в рабочем состоянии брандмауэры для защиты данных

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
1.1	Разработаны ли стандарты конфигурации межсетевых экранов и маршрутизаторов, которые должны включать в себя следующее:				
1.1.1	Существует ли формальный процесс утверждения и тестирования всех внешних соединений и изменений в конфигурациях межсетевых экранов и маршрутизаторов?		☐	☐	
1.1.2	(а) Есть ли в наличии схемы сети (например, отражающей потоки данных о держателях карт через корпоративную сеть) со всеми подключениями к среде данных о держателях карт, в том числе беспроводными?		☐	☐	
	(б) Поддерживается ли актуальность схемы сети.		☐	☐	
1.1.3	(а) Включают ли стандарты конфигурации включают требование о необходимости защиты брандмауэром всех подключений к интернету, а также наличия брандмауэра между DMZ и внутренней сетью?		☐	☐	
	(б) Соответствует ли текущая конфигурация межсетевых экранов схеме сети?		☐	☐	
1.1.4	Содержат ли стандарты конфигурации межсетевых экранов и маршрутизаторов описание ролей, групп и ответственности за управление сетевыми компонентами?		☐	☐	
1.1.5	(а) Содержат ли стандарты конфигурации межсетевых экранов и маршрутизаторов документированный перечень служб, протоколов и портов, необходимых для бизнеса (например, HTTP, SSL, SSH, VPN)?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
		(б) Все ли разрешенные небезопасные службы, протоколы и порты необходимы? Задокументированы ли и применяются ли механизмы защиты для всех этих служб, протоколов и портов? *Примечание. Примеры небезопасных служб, протоколов или портов включают, помимо прочего, FTP, Telnet, POP3, IMAP и SMTP.*	☐	☐	
	1.1.6	(а) Требуют ли стандарты конфигурации межсетевых экранов и маршрутизаторов пересмотра правил для межсетевых экранов и маршрутизаторов как минимум раз в полгода?	☐	☐	
		(б) Выполняется ли пересмотр настроек межсетевых экранов и маршрутизаторов не реже одного раза в полгода?	☐	☐	
1.2		Создана ли конфигурация брандмауэров и маршрутизаторов, которая запрещает все соединения между недоверенными сетями и всеми системными компонентами в среде данных о держателях карт? *Примечание. Недоверенной является любая сеть, внешняя по отношению к сетям, принадлежащим проверяемой организации и/или сеть, которая не контролируется проверяемой организацией.*			
	1.2.1	(а) Входящий и исходящий трафик ограничен только необходимыми для среды данных о держателях карт соединениями, а ограничения документированы?	☐	☐	
		(б) Весь иной входящий и исходящий трафик явно запрещен, например посредством использования явного отказа или подразумеваемого отказа?	☐	☐	
	1.2.2	Обеспечена ли безопасность и своевременная синхронизация конфигурационных файлов маршрутизаторов?	☐	☐	
	1.2.3	Установлены ли брандмауэры любой беспроводной сетью и средой данных о держателях карт, и настроены ли брандмауэры на блокирование любого трафика из беспроводной сети либо его контроль в том случае, если такой трафик необходим для бизнес-приложений?	☐	☐	
1.3		Запрещает ли конфигурация брандмауэров прямой обмен данными между интернетом и любыми компонентами среды данных о держателях карт?			

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
1.3.1	Применяется ли DMZ для ограничения входящего и исходящего трафика только к тем системным компонентам, которые предоставляют авторизованный доступ к общедоступным службам, протоколам и портам?		☐	☐	
1.3.2	Ограничен ли входящий интернет-трафик только IP-адресами, находящимися в DMZ?		☐	☐	
1.3.3	Отсутствуют ли прямые входящие и исходящие подключения между интернетом и средой данных о держателях карт?		☐	☐	
1.3.4	Пакеты с внутренними адресами действительно не могут попасть в DMZ из интернета?		☐	☐	
1.3.5	Является ли исходящий трафик из среды данных о держателях карт в интернет строго авторизованным?		☐	☐	
1.3.6	Применяется ли проверка с сохранением состояния, т.е. динамическая фильтрация пакетов (в сети разрешены только установленные подключения)?		☐	☐	
1.3.7	Размещены ли системные компоненты (например, базы данных), в которых хранятся данные о держателях карт, во внутреннем сегменте сети, отделенном от DMZ и иных недоверенных сетей?		☐	☐	
1.3.8	(а) Существуют ли правила, предотвращающие раскрытие частных IP-адресов и данных о маршрутах из внутренней сети в интернете? ***Примечание**. К числу методов сокрытия IP-адресации относятся:* • *технология Network Address Translation (NAT);* • *расположение серверов, содержащих данные о держателях карт за прокси-серверами/межсетевыми экранами или кэшами содержимого;* • *удаление или фильтрация объявлений маршрутов для частных сетей, требующих зарегистрированной адресации;* • *внутреннее использование адресного пространства RFC1918 вместо зарегистрированных адресов.*		☐	☐	
	(б) Авторизовано ли любое раскрытие частных IP-адресов и данных о маршрутах внешним сторонам?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
1.4	(а) Установлены ли личные брандмауэры на все мобильные и принадлежащие сотрудникам компьютеры (например, ноутбуки), имеющие прямой доступ в интернет и используемые для доступа к сети организации?		☐	☐	
	(б) Соответствуют ли настройки личных брандмауэров стандартам организации (и не могут быть изменены пользователями мобильных и принадлежащих сотрудникам компьютеров)?		☐	☐	

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

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
2.1	Значения параметров и пароли, заданные производителями по умолчанию, всегда изменяются перед установкой систем в сети? *К таким параметрам относятся, помимо прочего, пароли, строки доступа SNMP; к данной процедуре относится и удаление ненужных для работы учетных записей.*		☐	☐	
2.1.1	Изменены ли параметры по умолчанию для беспроводных сред, подключенных к среде с данными о держателях карт или передающих данные о держателях карт, следующим образом:				
	(a) Изменены ли при установке используемые по умолчанию ключи шифрования? Изменяются ли ключи шифрования всякий раз, когда кто-либо, обладающий данными о ключах, уходит из компании либо переходит на другую должность?		☐	☐	
	(b) Изменены ли установленные по умолчанию строки доступа SNMP беспроводных устройств?		☐	☐	
	(c) Изменены ли установленные по умолчанию пароли/парольные фразы точек доступа?		☐	☐	
	(г) Обновлены ли микропрограммы беспроводных устройств обновлено до актуальной версии с поддержкой стойкого шифрования для аутентификации и передачи данных через беспроводные сети?		☐	☐	
	(д) Изменены ли прочие настройки безопасности беспроводных устройств, установленные производителем по умолчанию (если применимо)?		☐	☐	
2.2	(a) Разработаны ли стандарты конфигураций всех системных компонентов, и соответствуют ли эти стандарты принятым отраслевым стандартам повышенной безопасности? В число источников отраслевых стандартов входят, помимо прочего, институт SANS, Национальный институт стандартов и технологий США (NIST), Международная организация по стандартизации (ISO) и Центр безопасности в Интернете (CIS).		☐	☐	
	(b) (б) Обновляются ли стандарты системных конфигураций по мере обнаружения новых проблем безопасности, как описывается в требовании 6.2?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(c) (в) Применяются ли стандарты системных конфигураций применяются при настройке новых систем?		☐	☐	
	(d) Включают ли стандарты конфигураций систем следующее:				
2.2.1	(а) Используется ли каждый сервер для выполнения только одной основной функции (чтобы избежать ситуации, когда на одном сервере выполняется несколько функций, которым требуется разный уровень безопасности)? (Например, веб-серверы, серверы СУБД и DNS-серверы следует размещать на разных компьютерах).		☐	☐	
	(б) При использовании виртуализации: выполняется ли правило “одна основная функция — один виртуальный системный компонент или устройство”?		☐	☐	
2.2.2	(а) Включены ли только те службы, протоколы и т.п., которые необходимы для работы системы (а службы и протоколы, не связанные напрямую с выполнением необходимых функций, отключены)?		☐	☐	
	(б) Все ли разрешенные небезопасные службы, протоколы и порты необходимы? Задокументированы ли и применяются ли механизмы защиты для всех этих служб, протоколов и портов? *Например, следует использовать такие защитные технологии, как SSH, S-FTP, SSL или IPSec VPN для защиты таких незащищенных служб как NetBIOS, совместное использование файлов, Telnet, FTP и т.д.*		☐	☐	
2.2.3	(а) Знают ли администраторы систем и другие сотрудники, настраивающие компоненты систем, об общих параметрах безопасности этих компонентов?		☐	☐	
	(б) Включены ли общие параметры безопасности в стандарты конфигурации системных компонентов?		☐	☐	
	(в) Применены ли параметры безопасности должным образом к системным компонентам?		☐	☐	
2.2.4	(а) Исключены ли из систем все ненужные компоненты, сценарии, драйверы, подсистемы, файловые системы, ненужные для работы веб-серверы?		☐	☐	
	(б) Документированы ли включенные компоненты? Поддерживают ли они безопасную конфигурацию?		☐	☐	
	(с) Поддерживают ли системные компоненты только документированные функции?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
2.3	Применяется ли шифрование для административного доступа (исключая консольный доступ) следующими способами: *Следует использовать такие технологии, как SSH, VPN или SSL/TLS для веб-ориентированных систем администрирования и иных способов неконсольного административного доступа.*				
	(а) Применяется ли для защиты административного доступа стойкие алгоритмы шифрования (с включением шифрования до запроса пароля администратора)?		☐	☐	
	(б) Настроены ли системные службы и файлы параметров таким образом, чтобы исключить возможность использования Telnet и других небезопасных команд входа в систему?		☐	☐	
	(в) Применяется ли стойкое шифрование для защиты административного доступа к веб-системам управления?		☐	☐	
2.4	Если ваша организация является поставщиком услуг хостинга, настроены ли ваши системы для обеспечения безопасности сред и данных о держателях карт, принадлежащих каждой из обслуживаемых сторон? См. *Приложение А. "Дополнительные требования PCI DSS для поставщиков услуг с общей средой (хостинг-провайдеров)".*		☐	☐	

Защита данных о держателях карт

Требование 3. Обеспечить безопасное хранение данных о держателях карт

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
3.1	Применяются ли политика и процедуры хранения и уничтожения данных следующим образом:				
3.1.1	(а) Применяются ли политика и процедуры хранения и уничтожения данных, и включают ли они определенные требования к хранению данных о держателях карт в соответствии с требованиями бизнеса, по юридическим соображениям или по нормативным требованиям? *Например, данные о держателях карт может требоваться хранить в течение периода X по причинам Y.*		☐	☐	
	(б) Содержат ли политика и процедуры положение о необходимости безопасного уничтожения данных, если их хранение более не является необходимым по требованиям бизнеса, законодательства и иным регулирующим требованиям, включая уничтожение данных о держателях карт?		☐	☐	
	(в) Распространяется ли действие политики и процедур на все места хранения данных о держателях карт?		☐	☐	
	(г) Содержат ли политика и процедуры содержат, по меньшей мере, один из следующих компонентов? • Программные процессы (проводимые автоматически или вручную) предусматривают удаление данных о держателях карт, сроки хранения которых превышают определенные политикой требования хранения данных, не реже одного раза в квартал. • Требования как минимум ежеквартальной проверки, свидетельствующие о том, что сроки хранения данных о держателях карт не превышают определенные политикой требования хранения данных.		☐	☐	
	(е) Все ли хранящиеся данные о держателях карт отвечают требованиям, указанным в политике хранения данных?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
3.2	(а) Для эмитентов и компаний, обеспечивающих эмиссионные услуги и хранящих конфиденциальные аутентификационные данные: имеется ли обоснованная с точки зрения бизнеса необходимость хранения таких данных, и защищены ли эти данные?		☐	☐	
	(б) Для всех прочих организаций: если конфиденциальные аутентификационные данные принимаются и уничтожаются, существуют ли процессы безопасного удаления данных, гарантирующие невозможность восстановления данных?		☐	☐	
	(в) Во всех ли системах соблюдается запрет на хранение конфиденциальных аутентификационных данных после авторизации (даже если такие данные зашифрованы)?				
3.2.1	Хранение полного содержимого дорожки (содержимое магнитной полосы, находящейся на обратной стороне карты, его аналог на чипе либо в ином месте) запрещено в любом случае? Эти данные также называются “полная дорожка”, “дорожка”, “дорожка 1”, “дорожка 2” и “данные магнитной полосы”. *Примечание. Для ведения бизнеса может быть необходимо хранение следующих элементов данных магнитной полосы:* • *имя держателя карты;* • *номер платежной карты (PAN);* • *дата истечения срока действия карты;* • *сервисный код.* *Для минимизации рисков разрешается хранить только указанные элементы данных.*		☐	☐	
3.2.2	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), запрещено в любом случае?		☐	☐	
3.2.3	Хранение персонального идентификационного номера (PIN), а также зашифрованного PIN-блока запрещено в любом случае?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
3.3	Применяется ли маскировка номера PAN при его отображении (максимально возможное количество знаков PAN для отображения – первые 6 и последние 4)? *Примечания.* • *Данное требование не относится к сотрудникам и иным сторонам, для работы которых необходимо видеть весь номер PAN.* • *Это требование не заменяет более строгие требования относительно отображения данных о держателях карт, например, для чеков POS-систем.*		☐	☐	
3.4	Представлен ли PAN в нечитаемом виде во всех местах хранения (включая данные на съемных носителях, резервных копиях и журналах протоколирования событий) с помощью любого из следующих методов? • Стойкая однонаправленная хеш-функция (должен быть хеширован весь PAN). • Укорачивание (хеширование не может использоваться для замещения укороченного сегмента PAN). • Использование механизмов One-Time-Pad (“одноразовых блокнотов”, хранение которых должно быть безопасным) и использование и хранение ссылок на данные вместо самих данных (index tokens). • Стойкие криптографические алгоритмы совместно с процессами и процедурами управления ключами. *Примечание. При наличии доступа одновременно к маскированному и хешированному номерам карты для злоумышленника не составит большого труда восстановить данные исходного PAN. Если маскированное и хешированное значение одного и того же PAN содержатся внутри среды какой-либо структуры, необходимо ввести дополнительные средства контроля для недопущения корреляции между маскированным и хешированным значениями, так как при этом исходный PAN становится легко восстановим.*		☐	☐	
3.4.1	Если применяется шифрование дисков (вместо шифрования файлов или полей баз данных), осуществляется ли управление доступом следующим образом?				
	(a) Происходит ли управление логическим доступом независимо от механизмов управления доступом операционной системы (например, локальных учетных записей)?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
		(б) Безопасно ли хранятся ключи шифрования (например, на съемном носителе, который защищен соответствующими процедурами контроля доступа)?	☐	☐	
		(в) Данные о держателях карт на съемных носителях хранятся только в зашифрованном виде? ***Примечание**. Если шифрование диска не используется для шифрования съемных носителей, данные на съемных носителях должны быть представлены в нечитаемом виде путем использования других методов шифрования.*	☐	☐	
3.5	Защищены ли любые ключи, используемые для защиты данных о держателях карт, от раскрытия или неправильного использования следующим образом? ***Примечание**. Требование по защите ключей от раскрытия и неправильного использования применяется как к ключам для шифрования ключей, так и к ключам для шифрования данных. Подобные ключи для шифрования ключей должны обладать таким же уровнем защиты, как и ключи для шифрования данных.*				
3.5.1		Доступ к ключам шифрования разрешен наименьшему возможному количеству сотрудников, ответственных за их хранение и использование?	☐	☐	
3.5.2		(а) Ключи хранятся в зашифрованном виде? Ключи шифрования ключей хранятся отдельно от ключей шифрования данных?	☐	☐	
		(б) Ключи хранятся только в строго определенных защищенных хранилищах и строго определенном виде?	☐	☐	
3.6	(a)	Все процессы и процедуры управления ключами шифрования данных о держателях карт полностью документированы и внедрены?	☐	☐	
	(b)	Только для поставщиков услуг: Если ключи предоставляются клиентам для передачи или хранения данных о держателях карт, предоставляется ли также документация по условиям их безопасной передачи, хранения и обработки, в соответствии с требованиями 3.6.1-3.6.8, приведенными ниже?	☐	☐	
	(c)	Применяемые процессы и процедуры управления ключами включают в себя следующие требования?			
3.6.1		Создание стойких ключей шифрования.	☐	☐	

Вопрос PCI DSS		Ответ:	Да	Нет	Комментарии*
3.6.2	Защищенное распространение ключей шифрования.		☐	☐	
3.6.3	Защищенное хранение ключей шифрования.		☐	☐	
3.6.4	Смена ключей шифрования, криптопериод которых истек (например, когда истек установленный срок, или когда данным ключом было зашифровано некоторое количество криптотекста), основана на передовых практических методах индустрии безопасности и руководствах (например, специальное издание 800-57 NIST) согласно предписаниям о предписаниям соответствующего производителя или владельца ключа.		☐	☐	
3.6.5	(a) Изъятие или смена ключей (например, архивация, уничтожение или аннулирование) при нарушении целостности (например, увольнение сотрудника, обладающего информацией об открытом коде ключа), а также ключей, относительно которых существуют подозрения в их компрометации.		☐	☐	
	(b) Замена ключей шифрования, которые были или могли быть скомпрометированы.		☐	☐	
	(c) Если удаленные или замененные ключи сохраняются, эти ключи не используются для шифрования.		☐	☐	
3.6.6	Включают ли процедуры управления криптографическими ключами раздельное знание и двойной контроль (например, таким образом, чтобы для расшифрования данных требовался составной ключ, компоненты которого хранятся у 2-3 сотрудников) для управления ключами в открытом виде? ***Примечание**. Примеры процедур управления ключами включают (но не ограничиваются): генерацию ключа, его передачу, загрузку в устройство, хранение и уничтожение.*		☐	☐	
3.6.7	Включают ли процедуры управления криптографическими ключами предотвращение неавторизовнной подстановки ключей?		☐	☐	
3.6.8	Обязаны ли сотрудники по хранению и использованию ключей официально подтверждать (в электронном виде или письменно), что они поняли свою ответственность и принимают свои обязанности?		☐	☐	

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

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
4.1	(a) Применяются ли стойкие алгоритмы шифрования и протоколы безопасности, такие как SSLTLS, SSH или IPSEC, для защиты конфиденциальных данных о держателях карт при передаче таких данных по сетям общего пользования? *Примерами общедоступных сетей, на которые распространяется стандарт PCI DSS, являются интернет, беспроводные и мобильные сети.*		☐	☐	
	(b) Принимаются ли только доверенные ключи и сертификаты?		☐	☐	
	(c) Используют ли протоколы только безопасные конфигурации, без поддержки незащищенных версий и конфигураций?		☐	☐	
	(d) Применяются ли нужные алгоритмы стойкого шифрования (согласно рекомендациям поставщиков и отраслевым методикам)?		☐	☐	
	(e) Для протоколов SSL/TLS: • Входит ли в строку URL-адреса префикс HTTPS? • Данные о держателях карт передаются только в том случае, если URL-адрес содержит префикс HTTPS?		☐	☐	
	4.1.1 Применяются ли отраслевые рекомендации (например, IEEE 802.11i) по использованию стойкого шифрования при аутентификации и передаче данных в беспроводных сетях, по которым передаются данные о держателях карт или подключенных к среде с данными о держателях карт? ***Примечание**. Использование протокола WEP в качестве протокола безопасности запрещено с 30 июня 2010 г.*		☐	☐	
4.2	(a) PAN передается в нечитаемом виде или защищен посредством стойких криптографических механизмов при использовании пользовательских технологий передачи сообщений (электронная почта, мгновенные сообщения, чат)?		☐	☐	
	(b) Применяются ли политики, запрещающие отправку незашифрованного PAN при помощи пользовательских технологий передачи сообщений?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

Программа для устранения уязвимостей

Требование 5. Использовать и регулярно обновлять антивирусное программное обеспечение

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
5.1	Развернуто ли антивирусное программное обеспечение на всех системах, подверженных воздействию вирусов?		☐	☐	
5.1.1	Обеспечивает ли антивирусное ПО защиту от всех известных видов вредоносного ПО (например, вирусов, троянских программ, червей, шпионских программ, рекламных модулей, руткитов)?		☐	☐	
5.2	Поддерживаются ли антивирусные программы в актуальном состоянии, они постоянно включены и ведут журналы аудита:				
	(a) Политика антивируса требует обновления антивирусной программы и определений вирусов?		☐	☐	
	(b) Включено ли автоматическое обновление и регулярные проверки в установочных образах используемых систем?		☐	☐	
	(c) Включено ли автоматическое обновление и периодическая проверка?		☐	☐	
	(d) Создают ли все антивирусные программы журналы аудита, и хранятся ли такие журналы согласно требованию 10.7 стандарта PCI DSS?		☐	☐	

Требование 6. Разрабатывать и поддерживать безопасные системы и приложения

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
6.1	(a) На все системные компоненты и программное обеспечение установлены самые свежие обновления безопасности, выпущенные производителем?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(б) Важные обновления безопасности устанавливаются в течение месяца с момента их выпуска? ***Примечание**. Организация может применять подход к распределению приоритетов при установке обновлений, основанный на оценке рисков. Например, для более приоритетных критичных приложений (общедоступные устройства и системы, базы данных) убедиться, что срок установки обновлений не превышает одного месяца, для менее критичных внутренних устройств – три месяца.*		☐	☐	
6.2	(а) Внедрен процесс выявления и оценки вновь обнаруженных уязвимостей по уровню риска? Как минимум, самые важные уязвимости с высоким уровнем риска должны иметь отметку “Высокий уровень риска”. ***Примечание**. Ранжирование рисков должно быть основано на передовых методах индустрии безопасности. Например, к уязвимостям высокого риска относятся те, которые имеют уровень 4.0 и выше по шкале CVSS; уязвимости, для закрытия которых производитель выпустил обновление категории “важное”, а также уязвимости, поражающие важные компоненты системы.* *До 30 июня 2012 года ранжирование уязвимостей по уровню риска носит рекомендательный характер, а после этой даты становится обязательным требованием.*		☐	☐	
	(б) Процессы выявления новых уязвимостей включают в себя использование для этого внешних источников информации?		☐	☐	
6.3	(а) Процесс разработки программного обеспечения основан на передовых практических методах и стандартах индустрии безопасности?		☐	☐	
	(b) Информационную безопасность учитывается в течение всего цикла разработки программ?		☐	☐	
	(c) Программные приложения разрабатываются согласно требованиям PCI DSS (например, в отношении безопасной проверки подлинности и ведения журнала)?		☐	☐	
	(d) Обеспечивает ли процесс разработки программ выполнение следующих требований?				
6.3.1	Все индивидуальные учетные записи, имена пользователей и пароли должны быть удалены перед передачей программного обеспечения заказчикам или переводом его в производственный режим.		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	6.3.2	Применяется ли изучение программного кода приложений на наличие потенциальных уязвимостей (вручную или автоматически) перед передачей готовых приложений заказчикам или переводом их в производственный режим с соблюдением следующих правил? • Изменения программного кода анализируются сотрудниками, не принимавшими участие в его написании и знакомыми с методами безопасного программирования. • Анализ программного кода обеспечивает его разработку в соответствии с основными принципами безопасного кодирования (см. требование 6.5 PCI DSS). • Все необходимые корректировки вносятся до выпуска программного обеспечения. • Результаты анализа программного кода проверяются и утверждаются руководством до выпуска программного обеспечения. ***Примечание**. Данное требование применимо ко всем разрабатываемым приложениям (как внутренним, так и общедоступным) как элемент обеспечения безопасности цикла разработки. Оценка программного кода может проводиться как компетентным персоналом, так и третьими сторонами. Веб-приложения также являются объектом применения дополнительных мер по защите; если они находятся в публичном доступе, следует учесть угрозы и уязвимости, в соответствии с требованием 6.6 PCI DSS.*	☐	☐	
6.4		Разработаны ли процедуры управления изменениями системных компонентов, включающие следующие правила?			
	6.4.1	Среды разработки, тестирования и производственного функционирования программного обеспечения должны быть отделены друг от друга, и при этом должны быть внедрены механизмы разграничения доступа.	☐	☐	
	6.4.2	Обязанности по разработке, тестированию и производственному функционированию программного обеспечения должны быть разделены.	☐	☐	
	6.4.3	***Производственные данные (действующие PAN) не должны использоваться для тестирования и разработки.***	☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	6.4.4	Все тестовые данные и платежные счета должны быть удалены из системы перед переводом ее в производственный режим.	☐	☐	
	6.4.5	(а) Процедуры управления изменениями, относящиеся к обновлениям безопасности и изменениям в конфигурации, документированы и требуют выполнения представленных ниже п.п. 6.4.5.1 – 6.4.5.4?	☐	☐	
		(б) Выполняются ли следующие правила при всех изменениях?			
	6.4.5.1	Документирование влияния изменения на систему.	☐	☐	
	6.4.5.2	Согласование изменения с руководством.	☐	☐	
	6.4.5.3	(а) Тестирование производственной функциональности с целью убедиться в том, что внесенные изменения не оказывают неблагоприятного воздействия на безопасность системы.	☐	☐	
		(б) Для изменений программного кода все обновления должны быть протестированы на соответствие требованию 6.5 PCI DSS перед их запуском в производственный режим.	☐	☐	
	6.4.5.4	Для каждого изменения должна быть предусмотрена процедура отмены.	☐	☐	
6.5		(a) Разработка приложений производится в соответствии с основными принципами безопасного программирования? (К таким принципам можно отнести *руководство OWASP, SANS CWE Top 25, правила написания безопасного кода CERT и пр.*).	☐	☐	
		(b) Разработчики знакомы с техникой безопасного программирования?	☐	☐	
		(c) Процесс разработки приложений должен предупреждает возникновение общеизвестных уязвимостей программного кода, в том числе следующих? *Примечание. Уязвимости, перечисленные в требованиях 6.5.1 – 6.5.9 соответствовали передовым практическим методам индустрии безопасности, когда была опубликована данная версия стандарта PCI DSS. В случае обновления рекомендаций по безопасности для данных требований следует использовать их актуальную версию.*			

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
6.5.1	Уязвимости для инъекций, в особенности, SQL-инъекции. (необходима проверка того, что введенная пользователями информация не может изменить существующие команды и запросы, использовать параметризованные запросы и т.д.). *Также следует учесть инъекции команд ОС, LDAP и Xpath .*		☐	☐	
6.5.2	Переполнение буфера. Убедиться в наличии границ буфера и усечения строки ввода.		☐	☐	
6.5.3	Небезопасное криптографическое хранилище. (Необходима защита от криптографических ошибок).		☐	☐	
6.5.4	Незащищенная передача данных. (Необходимо шифрование всех важных передаваемых данных).		☐	☐	
6.5.5	Некорректная обработка ошибок. (Необходимо не допускать утечки данных через сообщения об ошибках).		☐	☐	
6.5.6	Все уязвимости, имеющие “высокую” степень риска, найденные в процессе обнаружения уязвимостей (в соответствии с требованием 6.2 PCI DSS). ***Примечание**. До 30 июня 2012 года данное требование носит рекомендательный характер, а после этой даты становится обязательным требованием.*		☐	☐	
Для веб-приложений и интерфейсов приложений (внутренних или внешних) применяются следующие дополнительные требования:					
6.5.7	Межсайтовые сценарии (XSS). (Необходимо проверить все параметры перед их включением в код, использовать контекстно-зависимое экранирование и т.п.)		☐	☐	
6.5.8	Ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход каталогов). (Следует проверять подлинность пользователей и вводимые данные. Пользователям не должны предоставляться прямые ссылки на внутренние объекты).		☐	☐	
6.5.9	Подделка межсайтовых запросов (CSRF). (Автоматические запросы браузеров о данных учетной записи и идентификаторах должны игнорироваться).		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
6.6	*Осуществляется ли защита общедоступных веб-приложений от известных атак (с учетом новых угроз и уязвимостей)* любым из следующих методов? ☐ Проверка приложений на наличие уязвимостей (вручную или автоматически): o не реже одного раза в год o после любых изменений o организацией, которая специализируется на безопасности приложений o Все уязвимости должны быть устранены o Безопасность приложения анализируется повторно после исправления проблем. *– или –* ☐ Перед общедоступным веб-приложением должен быть установлен межсетевой экран прикладного уровня для обнаружения и предупреждения веб-атак. ***Примечание**. Организацией, которая специализируется на безопасности приложений, может быть сторонняя компания или внутренняя организация, сотрудники которой специализируются на безопасности приложений и независимы от группы разработчиков.*		☐	☐	

Внедрение строгих мер контроля доступа

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

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
7.1	Доступом к вычислительным ресурсам и данным о держателях карт обладают только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями?				
7.1.1	Доступ пользователям предоставлен только к тем данным, которые необходимы сотрудникам для выполнения своих должностных обязанностей?		☐	☐	
7.1.2	Назначение прав доступа пользователям основано на их должностных обязанностях?		☐	☐	
7.1.3	Требуется ли документальное утверждение полномочными сторонами (в рукописной или электронной форме) уполномоченных лиц с описанием необходимых прав?		☐	☐	
7.1.4	Применяется ли автоматизированная система контроля доступа?		☐	☐	
7.2	Используется ли для многопользовательских систем механизм разграничения доступа, основанный на факторе знания и применяющий принцип “запрещено все, что явно не разрешено”?				
7.2.1	Система контроля доступа внедрена на всех системных компонентах?		☐	☐	
7.2.2	Назначение прав пользователям основано на их должностных обязанностях?		☐	☐	
7.2.3	По умолчанию системы управления доступом работают по принципу “запрещено все, что явно не разрешено”? ***Примечание**. Некоторые механизмы контроля доступа применяют правило “разрешить все” по умолчанию до тех пор, пока явно не прописано правило запрещения доступа.*		☐	☐	

* *“Неприменимо” (Н/п) или “Использованы компенсирующие меры”. Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

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

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
8.1	Каждому ли пользователю назначается уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт?		☐	☐	
8.2	Помимо идентификатора, применяется ли хотя бы один из следующих методов для аутентификации всех пользователей? • То, что вы знаете (пароль и парольная фраза) • То, что у вас есть (ключи или смарт-карты) • То, что вы есть (биометрические параметры)		☐	☐	
8.3	Применяется ли двухфакторная аутентификация для удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети (для доступа к сети снаружи)? *Например, можно использовать такие технологии, как RADIUS с ключами; системы управления доступом к контроллеру терминального доступа TACACS с ключами, прочие технологии, способствующие двухфакторной аутентификации.* ***Примечание**. Для двухфакторной аутентификации требуется применение двух из трех методов аутентификации (описание методов аутентификации см. в требовании PCI DSS 8.2). Использование одного метода дважды (например, использование двух различных паролей) не считается двухфакторной аутентификацией.*		☐	☐	
8.4	Все пароли хранятся и передаются только в зашифрованном виде с использованием стойких криптографических алгоритмов?		☐	☐	
	(б) Только для поставщиков услуг: Пароли клиентов зашифрованы?		☐	☐	
8.5	Применяются ли меры контроля над выполнением процедур идентификации и аутентификации пользователей и управления паролями учетных записей сотрудников и администраторов на всех системных компонентах, включающие в себя следующее:				

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
8.5.1	Добавление, удаление и изменение идентификаторов пользователей, учетных данных и других аналогичных объектов контролируется таким образом, что работа с идентификаторами пользователей (в том числе с расширенными правами) ведется только при авторизации?		☐	☐	
8.5.2	Проводится ли идентификация пользователей перед сбросом пароля без личного присутствия пользователя (например, по телефону, по электронной почте, в интернете)?		☐	☐	
8.5.3	Применяется ли установка уникального начального пароля для каждого пользователя и немедленное изменение пароля при первом входе пользователя в систему?		☐	☐	
8.5.4	Применяется ли немедленный отзыв доступа при увольнении пользователя?		☐	☐	
8.5.5	Происходит ли удаление (или отключение) учетных записей пользователей, неактивных в течение 90 дней или более?		☐	☐	
8.5.6	(а) Учетные записи, используемых поставщиками для удаленного доступа, обслуживания и поддержки, включаются только на время выполнения работ?		☐	☐	
	(б) Отслеживаются ли учетные записи удаленного доступа, используемые поставщиками во время работ?		☐	☐	
8.5.7	Правила и процедуры аутентификации доведены до до всех пользователей, имеющих доступ к данным о держателях карт?		☐	☐	
8.5.8	Использование групповых, общих и стандартных учетных записей и паролей, а также прочих методов аутентификации, запрещено (с соблюдением следующих правил)? • Стандартные учетные записи заблокированы или удалены. • Не существует общих учетных записей для администрирования и иных важных функций. • Общие и стандартные учетные записи не используются для администрирования каких-либо системных компонентов.		☐	☐	
8.5.9	(а) Пароли пользователей изменяются не реже чем через каждые 90 дней?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(б) Только для поставщиков услуг: Происходит ли регулярная смена неклиентских паролей? Получают ли пользователи инструкции о том, когда и при каких обстоятельствах пароль должен быть изменен?		☐	☐	
8.5.10	(а) Установлена ли для паролей минимальная длина в 7 символов?		☐	☐	
	(б) Только для поставщиков услуг: Действует ли для неклиентских паролей требование минимальной длины?		☐	☐	
8.5.11	(а) Должны ли пароли содержать и цифры, и буквы?		☐	☐	
	(б) Только для поставщиков услуг: (а) Должны ли неклиентские пароли содержать и цифры, и буквы?		☐	☐	
8.5.12	(а) Новый пароль пользователя должен отличаться от любого из последних четырех паролей этого пользователя?		☐	☐	
	(б) Только для поставщиков услуг: Новый пароль неклиентского пользователя должен отличаться от любого из последних четырех паролей этого пользователя?		☐	☐	
8.5.13	(а) Применяется ли блокировка учетной записи после шести (или менее) неудачных попыток входа в систему?		☐	☐	
	(б) Только для поставщиков услуг: Применяется ли временная блокировка неклиентских паролей записи после шести (или менее) неудачных попыток входа в систему?		☐	☐	
8.5.14	Блокировка учетных записей действует по крайней мере 30 минут или до разблокировки учетной записи администратором?		☐	☐	
8.5.15	Требуется ли пользователям заново проходить проверку подлинности (например, вводить пароль) для возобновления сеанса или работы с терминалом в случае бездействия в течение 15 минут?		☐	☐	
8.5.16	(а) Применяется ли аутентификацию доступа к любой базе данных, содержащей данные о держателях карт? (Это требование касается доступа приложений, администраторов и любых других пользователей).		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(б) Настройки баз данных и приложений обеспечивают осуществление доступа, запроса и операций с данными (перемещение, копирование, удаление) только программными методами (например, с помощью хранимых процедур)?		☐	☐	
	(с) Прямые запросы и прямой доступ к базам данных разрешен только администраторам баз данных?		☐	☐	
	(г) Учетные записи приложений могут быть использованы только приложениями (но не пользователями или иными процессами)?		☐	☐	

Требование 9. Ограничить физический доступ к данным о держателях карт

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
9.1	Используются ли 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	(a) Используются ли камеры видеонаблюдения или иные механизмы контроля доступа, чтобы следить за конфиденциальными областями? ***Примечание**. Конфиденциальными являются области, относящиеся к любому центру обработки данных, серверной комнате или иному помещению, в котором расположены системы, хранящие данные о держателях карт. Исключением являются места расположения POS-терминалов, такие как кассовые зоны торговых комплексов.*		☐	☐	
	(b) Камеры и иные средства контроля защищены от взлома или отключения?		☐	☐	
	(c) Данные, полученные от видеокамер и других средств контроля, проверяются и сопоставляются с другими данными? Хранятся ли данные в течение по крайней мере 3 месяцев (если иные нормы не установлены законодательством)?		☐	☐	
9.1.2	Ограничен ли физический доступ к общедоступным сетевым разъемам? (Например, посещаемые помещения не должны иметь действующих сетевых портов, если сетевой доступ не является однозначно авторизованным). Посетители могут находиться в помещениях с действующими сетевыми разъемами только с сопровождением?		☐	☐	
9.1.3	Ограничен ли доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
9.2	Применяются ли процедуры, позволяющие легко различать персонал организации и посетителей? *К понятию "персонал" относятся постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на территории компании. Под термином "посетитель" следует понимать поставщиков, гостей сотрудников, обслуживающий персонал и иных лиц, кратковременно находящихся на территории компании, как правило, не более одного дня.*				
	(a) Включают ли процессы и процедуры выдачи пропусков персоналу и посетителям следующие этапы: • Выдача новых пропусков • Изменение требований доступа • Отзыв пропусков уволенных сотрудников и гостевых пропусков с истекшим сроком действия		☐	☐	
	(b) Доступом к пропускной системе обладает только авторизованный персонал?		☐	☐	
	(в) Пропуска позволяют четко идентифицировать посетителей, и можно легко отличать персонал компании от посетителей?		☐	☐	
9.3	Процедура прохода посетителей на объект устроена следующим образом:				
9.3.1	Проводится ли авторизация посетителей перед входом в помещения, где обрабатываются или циркулируют данные о держателях карт?		☐	☐	
9.3.2	(a) Выдается ли посетителям материальный идентификатор (например, карточка или электронный ключ), внешне отличный от идентификатора персонала?		☐	☐	
	(б) Ограничен ли срок действия гостевых карточек?		☐	☐	
9.3.3	Обязаны ли посетители возвращать выданное материальные идентификаторы при выходе с объекта или при истечении срока действия?		☐	☐	
9.4	(a) Ведется ли 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 о держателях карт?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(b) Журнал содержит имя посетителя, название представляемой им организации, а также имя сотрудника компании, предоставившего посетителю физический доступ? Журнал хранится не менее трех месяцев?		☐	☐	
9.5	(a) Носители с резервными копиями данных хранятся в безопасных местах (желательно вне объекта), таких как запасной центр обработки данных, или же в коммерческих хранилищах?		☐	☐	
	(б) Безопасность мест хранения должна проверяется не реже одного раза в год?		☐	☐	
9.6	Процедуры физической защиты данных о держателях карт включают меры по защите всех видов носителей (например, компьютеров, съемных электронных носителей, бумажных счетов, бумажных отчетов и факсов)? *Термин "носитель данных" включает в себя бумажные и электронные носители, которые содержат данные о держателях карт.*		☐	☐	
9.7	(a) Обеспечен ли строгий контроль над внутренним и внешним распространением всех видов носителей информации?		☐	☐	
	(b) Включает ли контроль следующие меры?				
9.7.1	Носители информации классифицированы для определения уровня конфиденциальности хранимых данных?		☐	☐	
9.7.2	Пересылка носителей осуществляется только с доверенным курьером или иным способом, который может быть тщательно проконтролирован?		☐	☐	
9.8	Ведутся ли журналы для отслеживания всех носителей, перемещенных из безопасного места, и требуется ли получение согласия руководства перед перемещением носителей (особенно при распространении носителей частным лицам)?		☐	☐	
9.9	Поддерживается ли строгий контроль хранения носителей и доступа к ним?		☐	☐	
9.9.1	Поддерживаются ли в актуальном состоянии журналы инвентаризации всех носителей данных о держателях карт? Инвентаризация носителей проводится не реже одного раза в год?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
9.10	Уничтожаются ли носители, содержащие данные о держателях карт, хранение которых более не требуется для выполнения бизнес-задач или требований законодательства?		☐	☐	
	Выполняется ли уничтожение следующими способами?				
9.10.1	(а) Уничтожаются ли бумажные материалы путем измельчения, сожжения или растворения таким образом, чтобы данные о держателях карт не могли быть восстановлены?		☐	☐	
	(б) Обеспечивается ли безопасность контейнеров, в которых хранится подлежащая уничтожению информации, чтобы предотвратить доступ к содержимому контейнеров? (Например, оборудован ли контейнер с материалами, подлежащими измельчению, замком?)		☐	☐	
9.10.2	Уничтожение данных о держателях карт на электронном носителе осуществляется способом, исключающим возможность их восстановления?		☐	☐	

Регулярный мониторинг и тестирование сети

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

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
10.1	Применяется ли процесс мониторинга доступа к компонентам системы (особенно доступа с административными полномочиями), а также привязки событий к определенным сотрудникам?		☐	☐	
10.2	Действует ли механизм протоколирования следующих событий для каждого системного компонента?				
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	Записываются ли следующие параметры для каждого события каждого системного компонента?				
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.		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
10.4	(а) Применяется ли синхронизация всех важных системных часов и системного времени? Поддерживается ли технология синхронизации в актуальном состоянии? ***Примечание**. Примером технологии синхронизации времени является протокол синхронизации времени (Network Time Protocol).*		☐	☐	
	(б) Применяются ли следующие средства для получения, распространения и хранения данных времени?				
10.4.1	(а) Только назначенные центральные серверы времени получают информацию о времени из внешних источников, а данная информация основывается на Международном атомном времени (International Atomic Time) или Всемирном координированном времени (UTC)?		☐	☐	
	(б) Точное время на назначенных центральных серверах времени совпадает, и только от них поступает информация о времени на другие внутренние серверы?		☐	☐	
10.4.2	Данные времени защищены следующим образом? (а) Доступ к данным о времени разрешен только персоналу, имеющему служебную необходимость?		☐	☐	
	(б) Все изменения параметров времени важных систем заносятся в журнал, отслеживаются и проверяются?		☐	☐	
10.4.3	Получение настроек времени происходит из признанных индустрией безопасности источников? (В этом случае злоумышленники не смогут перевести часы). Данные обновления могут быть дополнительно зашифрованы симметричным ключом и списками контроля доступа, определяющими IP-адреса машин, которым разрешено получать обновления времени (чтобы предупредить неавторизованное использование внутренних серверов времени).		☐	☐	
10.5	Журналы аудита защищены от изменений следующим образом?				
10.5.1	Доступом к журналам аудита обладают только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	10.5.2	Журналы аудита защищены от неавторизованного изменения при помощи механизмов контроля доступа, физической или сетевой сегментации?	☐	☐	
	10.5.3	Резервные копии журналов аудита оперативно сохраняются на централизованном сервере протоколирования или на отдельном носителе, где их изменение было бы затруднено?	☐	☐	
	10.5.4	Убедиться в том, что журналы аудита доступных извне систем (беспроводных сетей, межсетевых экранов, DNS, почтовых систем) сохраняются на безопасном центральном сервере протоколирования или на носителях, находящихся внутри локальной сети?	☐	☐	
	10.5.5	Применяются ли приложения контроля целостности файлов для защиты журналов регистрации событий от несанкционированных изменений (однако добавление новых данных не должно вызывать тревожного сигнала)?	☐	☐	
10.6		Производится ли проверка журналов всех системных компонентов по крайней мере один раз в день? Требуется ли выполнять реагировать на исключительные ситуации? *Следует анализировать журналы систем обнаружения вторжений (IDS) и серверов, осуществляющих аутентификацию, авторизацию и учет (например, RADIUS).* ***Примечание.** Для обеспечения соответствия требованию 10.6 могут быть использованы средства сбора и анализа журналов регистрации событий, а также средства оповещения.*	☐	☐	
10.7		(а) Применяются ли политика и процедуры сохранения журнала аудита, требующие хранения истории аудита в течение по крайней мере одного года?	☐	☐	
		(б) Доступны ли журналы аудита в течение по крайней мере одного года? Можно ли быстро восстановить журналы по крайней мере за последние 3 месяца для анализа?	☐	☐	

Требование 11. Регулярно проверять системы и процессы, обеспечивающие безопасность

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
11.1	(а) Имеется ли в организации имеется документированный процесс ежеквартального отслеживания и обнаружения беспроводных точек доступа? ***Примечание**. Используемые процессы включают в себя, например, сканирование беспроводной сети, обследование физических и логических системных компонентов и инфраструктуры, контроль сетевого доступа (NAC) или беспроводные IDS/IPS.* *Какие бы методы ни использовались, они должны быть достаточно эффективными в отслеживании и обнаружении неавторизованных беспроводных устройств.*		☐	☐	
	(б) Способна ли применяемая методика отслеживать и обнаруживать любые неавторизованные беспроводные точки доступа, включая, по меньшей мере, следующее: • платы WLAN, вставленные в системные компоненты; • подключение переносных беспроводных устройств к системным компонентам (например, посредством USB и т.п.); • подключение беспроводных устройств к сетевым портам или устройствам?		☐	☐	
	(с) Выполняется ли процедура обнаружения неавторизованных беспроводных точек доступа по крайней мере ежеквартально?		☐	☐	
	(г) Если используется система автоматического мониторинга (например, беспроводные IDS/IPS, контроль сетевого доступа и т.п.), создает ли она оповещения для персонала?		☐	☐	
	(д) Содержит ли политика расследования инцидентов (требование 12.9) действия при обнаружении неавторизованного беспроводного устройства?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
11.2	Проводится ли 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 брандмауэров, обновления продуктов)? ***Примечание**. Для первоначального соответствия PCI DSS не требуется отчетов четырех ежеквартальных сканирований, если аудитор убедился в следующем: 1) последнее сканирование было пройдено успешно, 2) документированные процедуры регламентируют необходимость ежеквартального сканирования, 3) обнаруженные уязвимости были устранены и это подтверждено повторным сканированием. Для последующих проверок, после первоначального подтверждения соответствия PCI DSS, требуется наличие отчетов о ежеквартальных сканированиях.*				
	11.2.1 (а) Проводится ли ежеквартальное внутреннее сканирование сети на наличие уязвимостей?		☐	☐	
	(б) Включает ли ежеквартальный процесс внутреннего сканирования повторное сканирование вплоть до достижения положительного результата или до закрытия всех уязвимостей высокого уровня, определенных в требовании 6.2 PCI DSS?		☐	☐	
	(в) Проводится ли ежеквартальное сканирование квалифицированными сотрудниками компании либо квалифицированной третьей стороной? Также, если применимо, насколько независима эта третья сторона с точки зрения организационной структуры (наличие статуса QSA или ASV не требуется)?		☐	☐	
	11.2.2 (а) Проводится ли ежеквартальное внешнее сканирование сети на наличие уязвимостей?		☐	☐	
	(б) Соответствуют ли результаты каждого ежеквартального внешнего сканирования требованиям программного руководства по ASV-сканированию (ASV Program Guide) (например, не должно быть уязвимостей со степенью важности выше 4.0 по общей системе оценки уязвимостей (CVSS), не должно быть автоматических нарушений)?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
		(в) Проводится ли ежеквартальное внешнее сканирование на наличие уязвимостей сторонней компанией (ASV), сертифицированной советом PCI SS?	☐	☐	
	11.2.3	(а) Проводится ли 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 брандмауэров, обновления продуктов)? **Примечание**. Сканирования после изменений в сетевой инфраструктуре могут производиться внутренними силами компании.	☐	☐	
		(б) Включает ли процесс сканирования повторное сканирование вплоть до достижения следующих результатов: • для внешнего сканирования – нет уязвимостей со степенью важности выше 4.0 по общей системе оценки уязвимостей (CVSS); • для внутреннего сканирования – получены положительные результаты, закрыты срочные, критические уязвимости или уязвимости высокого уровня, определенные в требовании 6.2 PCI DSS.	☐	☐	
		(в) Проводится ли ежеквартальное сканирование квалифицированными сотрудниками компании либо квалифицированной третьей стороной? Также, если применимо, насколько независима эта третья сторона с точки зрения организационной структуры (наличие статуса QSA или ASV не требуется)?	☐	☐	
11.3	(а)	Проводится ли внешний и внутренний тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления инфраструктуры и приложений (например, обновления операционной системы, добавления подсети, установки веб-сервера)?	☐	☐	
	(b)	Были ли устранены выявленные уязвимости с проведением повторного теста?	☐	☐	
	(c)	Проводится ли ежеквартальное сканирование квалифицированными сотрудниками компании либо квалифицированной третьей стороной? Также, если применимо, насколько независима эта третья сторона с точки зрения организационной структуры (наличие статуса QSA или ASV не требуется)?	☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	Данные тесты на проникновение должны включать:				
	11.3.1	Тесты на проникновение сетевого уровня. ***Примечание**. Тест должен охватывать не только операционные системы, но и другие компоненты, поддерживающие взаимодействие на сетевом уровне.*	☐	☐	
	11.3.2	Тесты на проникновение уровня приложений. ***Примечание**. Тест должен учитывать, как минимум, проверки на наличие уязвимостей, приведенных в требовании 6.5 PCI DSS.*	☐	☐	
11.4	(a)	Используются ли системы обнаружения и предотвращения вторжений для контроля сетевого трафика по периметру среды данных о держателях карт и критичных точек внутри среды данных о держателях карт?	☐	☐	
	(b)	Системы IDS и/или IPS оповещают сотрудников компании о подозрительных действиях?	☐	☐	
	(c)	Поддерживаются ли системы обнаружения и предотвращения вторжений и их сигнатуры в актуальном состоянии?	☐	☐	
11.5	(a)	Развернуты ли в среде с данными о держателях карт средства отслеживания целостности файлов? Примеры файлов, подлежащих отслеживанию: • системные исполняемые файлы; • исполняемые файлы приложений; • файлы конфигураций и параметров; • централизованно хранимые, хронологические или архивные файлы, файлы данных аудита и журналов протоколирования событий.	☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(b) Применяются ли средства контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных? Проводится ли сопоставительный анализ критичных файлов должен проводиться не реже одного раза в неделю? ***Примечание**. Обычно контролируется целостность файлов, которые изменяются нечасто, но изменение которых может служить признаком компрометации или попытки компрометации системы. Средства контроля целостности обычно содержат предустановленный перечень файлов, подлежащих контролю, в зависимости от используемой операционной системы. Другие критичные файлы, такие как файлы для клиентских приложений, должны быть определены самой компанией (т.е. торгово-сервисным предприятием или поставщиком услуг).*		☐	☐	

Регулярно выполнять тестирование систем и процессов обеспечения безопасности

Требование 12. Разработать и поддерживать политику информационной безопасности для всего персонала организации

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
12.1	Существует ли установленная, опубликованная, постоянно поддерживаемая и доведенная до сведения всего надлежащего персонала политика безопасности? *В контексте данного требования термином "персонал" обозначаются постоянные сотрудники, временные сотрудники, сотрудники, работающие по совместительству, и консультанты, находящиеся на объекте компании или так или иначе имеющие доступ к среде данных о держателях карт.*		☐	☐	
12.1.1	Учитывает ли политика информационной безопасности все требования PCI DSS?		☐	☐	
12.1.2	(а) Убедиться в том, что процедура ежегодного анализа информационных рисков документирована и предусматривает обнаружение угроз, уязвимостей и результатов их реализации в рамках формальной оценки рисков? (Примеры методик оценки информационных рисков включают, например, OCTAVE, ISO 27005 и NIST SP 800-30).		☐	☐	
	(б) Процедура анализа информационных рисков выполняется по крайней мере один раз в год?		☐	☐	
12.1.3	Политика информационной безопасности пересматривается, по меньшей мере, ежегодно и обновляется в случае изменения бизнес-целей и среды данных о держателях карт?		☐	☐	
12.2	Разработаны ли ежедневные процедуры безопасности, соответствующие требованиям настоящего стандарта (например, процедуры управления учетными записями пользователей, процедуры анализа журналов событий)?		☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
12.3	Разработаны ли правила эксплуатации для критичных технологий (таких как системы удаленного доступа, беспроводные технологии, съемные носители информации, мобильные компьютеры, планшеты, карманные компьютеры, электронная почта и интернет), чтобы определить корректный порядок использования этих устройств всеми сотрудниками? Применяются ли следующие требования?				
	12.3.1	Явное одобрение использования устройств уполномоченными лицами.	☐	☐	
	12.3.2	Аутентификация перед использованием устройства.	☐	☐	
	12.3.3	Перечень используемых устройств и сотрудников, имеющих доступ к таким устройствам.	☐	☐	
	12.3.4	Маркировка устройств с указанием информации, которую можно связать с владельцем носителя, а также контактных данных 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 сеансов удаленного доступа после определенного периода бездействия.	☐	☐	
	12.3.9	Включение удаленного доступа для поставщиков и деловых партнеров только в случае необходимости такого доступа с немедленным отключением после использования.	☐	☐	
	12.3.10	(а) Для персонала, имеющего доступ к данным о держателях карт с помощью удаленного доступа: запрещает ли политика копирование, перемещение, хранение данных о держателях карт на локальных дисках и иных съемных электронных носителях, если это не обусловлено служебной необходимостью?	☐	☐	
		(б) Для авторизованных сотрудников: предусматривает ли политика защиту данных о держателях карт в соответствии с требованиями стандарта PCI DSS?	☐	☐	
12.4	Политика и процедуры обеспечения безопасности однозначно определяют обязанности всего персонала организации, относящиеся к информационной безопасности?		☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
12.5		Ответственность за обеспечение информационной безопасности официально возложена на руководителя службы безопасности или другого члена правления, компетентного в области информационной безопасности?	☐	☐	
		Назначены ли определенному сотруднику или группе сотрудников следующие обязанности в области управления информационной безопасностью:			
	12.5.1	Создание, документирование и распространение политик 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		(а) Внедрена ли официальная программа повышения осведомленности персонала по вопросам безопасности с целью донести до них важность обеспечения безопасности данных о держателях карт?	☐	☐	
		(б) Включает ли программа повышения осведомленности персонала по вопросам безопасности следующее?			
	12.6.1	В программе повышения осведомленности персонала используются различные методы доведения информации до персонала (плакаты, письма, заметки, системы дистанционного обучения, специальные кампании)? ***Примечание.*** *Методики обучения могут варьироваться в зависимости от обязанностей персонала и уровня доступа к данным о держателях карт.*	☐	☐	
		Обучение персонала организации проводится при приеме на работу, продвижении по службе, а также не реже одного раза в год?	☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	12.6.2	Персонал организации должен не реже одного раза в год подтверждать свое знание и понимание политики и процедур обеспечения информационной безопасности организации?	☐	☐	
12.7		Проводится ли тщательная проверка кадров 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.*	☐	☐	
12.8		В случае, когда данные о держателях карт становятся доступны поставщикам услуг, разработаны ли политики и процедуры взаимодействия с ними?			
	12.8.1	Поддерживается ли перечень поставщиков услуг?	☐	☐	
	12.8.2	Составляются ли письменные соглашения о том, что поставщики услуг ответственны за безопасность переданных им данных о держателях карт?	☐	☐	
	12.8.3	Применяется ли установленный процесс тщательной проверки поставщика услуг перед началом взаимодействия с ним?	☐	☐	
	12.8.4	Поддерживается ли программа проверки соответствия поставщика услуг требованиям PCI DSS?	☐	☐	
12.9		Используется ли план расследования инцидентов для немедленного реагирования на нарушение безопасности систем?			
	12.9.1	(a) Разработан ли план реагирования на инциденты, применяемый в случае нарушения безопасности систем?	☐	☐	
		(b) 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;	☐	☐	

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
		описание процессов резервного копирования данных;	☐	☐	
		анализ требований законодательства об оповещении о фактах компрометации;	☐	☐	
		описание всех критичных системных компонентов;	☐	☐	
		ссылки или включение процедур реагирования на инциденты международных платежных систем.	☐	☐	
12.9.2	Проверка плана производится не реже одного раза в год?		☐	☐	
12.9.3	Назначен ли соответствующий персонал, готовый реагировать на сигналы тревоги в режиме 24/7?		☐	☐	
12.9.4	Персонал, ответственный за реагирование на нарушения безопасности, обучен соответствующим образом?		☐	☐	
12.9.5	План включает в себя процедуры реагирования на сигналы тревоги систем обнаружения и предупреждения вторжений, а также систем мониторинга целостности файлов?		☐	☐	
12.9.6	Разработан ли процесс изменения и развития плана реагирования на инциденты в соответствии с полученным опытом и разработками в данной отрасли?		☐	☐	

Приложение A. Дополнительные требования PCI DSS для поставщиков услуг хостинга

Требование A.1. Поставщики услуг хостинга должны защищать среду данных платежных карт

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
A.1	Обеспечена ли защита данных каждого клиента (т.е. торгово-сервисных компаний, поставщиков услуг и других клиентов), согласно требованиям с A.1.1 по A.1.4: *Хостинг-провайдер должен удовлетворять всем этим требованиям, помимо требований PCI DSS.* *Примечание. Даже если хостинг-провайдер соответствует требованиям PCI DSS, это не значит, что каждая организация, которая пользуется его услугами, соответствует этим требованиям. Поэтому каждая организация должна проходить аудит на соответствие требованиям PCI DSS.*				
	A.1.1 Процессы каждого клиента имеют доступ только к среде данных о держателях карт этого клиента? При этом приложения используют уникальный идентификатор данного клиента? Например: • ни одно приложение и ни один пользователь не может использовать имя пользователя, от которого работает разделяемый веб-сервер. • Все CGI-сценарии, используемые клиентом, должны быть созданы и запущены от имени идентификатора клиента.		☐	☐	
	A.1.2 Доступ клиенту предоставляется только к своей среде данных о держателях карт?				
		(a) Ни один из клиентов не обладает правами администратора/суперпользователя?	☐	☐	

* *"Неприменимо" (Н/п) или "Использованы компенсирующие меры". Организации, заполняющие этот раздел, должны заполнить таблицу компенсирующих мер или указать причины неприменимости требований (см. приложение).*

	Вопрос PCI DSS	Ответ:	Да	Нет	Комментарии*
	(б) Каждый клиент имеет права чтения, записи и выполнения только своих утилит и данных? (Для ограничения могут применяться права доступа к файловой системе, списки контроля доступа, средства chroot, jailshell и т.п.) *Важно. Файлы клиента не должны быть доступны группе пользователей.*		☐	☐	
	(в) У клиента отсутствует доступ с правом записи к общим системным двоичным файлам?		☐	☐	
	(г) Просмотр журналов протоколирования доступен только владельцу?		☐	☐	
	(д) Применяются ли ограничения на использование следующих сетевых ресурсов? • Дисковое пространство • Сетевые подключения • Память • ЦП *Это позволяет избежать ситуации, когда один клиент монопольно использует все ресурсы сервера для эксплуатации уязвимостей (таких как ошибки, конфликты и условия перезапуска, результатом которых может стать переполнение буфера).*		☐	☐	
A.1.3	Включено ли протоколирование действий и событий включено для каждого клиента согласно требованию 10 стандарта PCI DSS? Протоколирование событий удовлетворяет следующим критериям (для среды торгово-сервисных организаций и поставщиков услуг):		☐	☐	
	• Протоколирование настроено для всех типичных используемых на сервере приложений сторонних производителей?		☐	☐	
	• Протоколирование включено по умолчанию?		☐	☐	
	• Журналы доступны для просмотра администратору и клиенту, для которого выполняется протоколирование?		☐	☐	
	• Расположение журналов известно клиенту?		☐	☐	
A.1.4	Есть ли в в наличии политика и процессы, позволяющие проводить расследование инцидентов по каждому клиенту?		☐	☐	

Приложение Б. Компенсирующие меры

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

Компенсирующие меры должны удовлетворять следующим требованиям:

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

   При анализе избыточности следует руководствоваться следующими моментами:

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

   a) Существующее требование PCI DSS НЕ МОЖЕТ рассматриваться как компенсирующая мера, если она уже описана в отчете. Например, пароли на административный удаленный доступ должны передаваться в зашифрованном виде, для защиты от перехвата. Организация не может использовать другие меры относительно паролей PCI DSS, такие как блокировка нарушителя, сложные пароли и т. д., для компенсации отсутствия зашифрованных паролей, поскольку эти меры не способствуют снижению риска перехвата паролей. Кроме того, другие меры уже являются требованиями PCI DSS для объекта, подлежащего проверке (пароли).

   b) Существующее требование PCI DSS МОЖЕТ рассматриваться как компенсирующая мера, если оно снижает существующий риск. Например, двухфакторная аутентификация, являющаяся требованием при удаленном доступе. Она также может использоваться *и внутри сети* для защиты административного доступа, если шифрование аутентификационных данных невозможно. Двухфакторная аутентификация может считаться допустимой компенсирующей мерой в следующих случаях: 1) если она соответствует цели изначального требования и обеспечивает защиту от перехвата паролей администраторов; и 2) если она настроена надлежащим образом и выполняется в защищенной среде.

   c) Существующие требования PCI DSS могут использоваться совместно с другими мерами как компенсирующие. Например, если компания не может реализовать нечитаемое хранение карточных данных в соответствии с требованием 3.4 (например, путем шифрования), компенсирующей мерой может считаться использование устройства или комбинации устройств, приложений и мер, направленных на 1) сегментацию сети; 2) фильтрацию по IP- или MAC-адресам; 3) использование двухфакторной аутентификации во внутренней сети.

4. Компенсирующие меры должны быть соизмеримыми с дополнительным риском, вызванным невозможностью выполнить требование PCI DSS;

Руководствуясь вышеперечисленными пунктами, аудитор должен проверить каждую компенсирующую меру, чтобы убедиться, что она адекватно соотносится с риском, который

призвано уменьшить исходное требование PCI DSS. Следует также иметь установленные процедуры и использовать определенные меры по соответствию требованиям, чтобы гарантировать, что компенсирующие меры остаются эффективными после выполнения оценки.

Приложение B. Компенсирующие меры – форма для заполнения

Укажите в этой форме компенсирующие меры для всех требований, где был выбран ответ "Да" и в столбце "Комментарии" были упомянуты компенсирующие меры.

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

Номер и определение требования:

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	
2. Цель	Определите цель исходного требования и компенсирующей меры.	
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением исходного требования.	
4. Определение компенсирующих мер	Опишите компенсирующую меру и то, как она соответствует требованию, создает дополнительные риски (если создает).	
5. Проверка компенсирующих мер	Опишите, как компенсирующие меры были проверены и протестированы.	
6. Соблюдение	Опишите, как контролируется процесс соблюдения компенсирующей меры.	

Перечень компенсирующих мер – пример заполнения

Укажите в этой форме компенсирующие меры для всех требований, где был выбран ответ "Да" и в столбце "Комментарии" были упомянуты компенсирующие меры.

Номер требования: *8.1 — Все ли пользователи имеют уникальный идентификатор для получения доступа к системным компонентам среды данных держателя карты?*

	Требуемая информация	Объяснение
1. Ограничения	Перечислите ограничения, препятствующие выполнению исходного требования стандарта.	*Компания XYZ использует отдельно стоящие Unix-серверы без LDAP-авторизации. Таким образом, на каждый из них требуется заходить с учетной записью суперпользователя ("root"). Компания не может управлять входом "root" и следить за использованием этой учетной записи каждым пользователем.*
2. Цель	Определите цель исходного требования и компенсирующей меры.	*Использование уникального идентификатора преследует две цели. Во-первых, с точки зрения безопасности недопустимо использовать общие учетные записи. Во-вторых, в таком случае невозможно определить, какой администратор ответственен за определенные действия.*
3. Определение риска	Опишите дополнительный риск, связанный с невыполнением исходного требования.	*Дополнительный риск связан с тем, что не всем пользователям назначен уникальный идентификатор и их действия не могут быть отслежены.*
4. Определение компенсирующих мер	Опишите компенсирующую меру и то, как она соответствует требованию, создает дополнительные риски (если создает).	*Пользователям предписано использовать команду SU для получения доступа с правами суперпользователя. Все действия, связанные с запуском этой команды, записываются в отдельный файл журнала. Таким образом, действия каждого пользователя можно отслеживать через учетную запись SU.*
5. Проверка компенсирующих мер	Опишите, как компенсирующие меры были проверены и протестированы.	*Компания XYZ продемонстрировала аудиторам, что команда SU выполняется и что действия тех пользователей, которые используют эту команду, записываются с целью определения того, что пользователь выполняет действия с правами доступа root.*
6. Соблюдение	Опишите, как контролируется процесс соблюдения	*Компания XYZ имеет процессы и процедуры, которые обеспечивают неизменность конфигурации SU и*

	компенсирующей меры.	*возможность для пользователей выполнять команды root без отслеживания и протоколирования.*

Приложение Г. Причины неприменимости требований

Если в столбце “Комментарии” был указан ответ “Н/д” или “Неприменимо”, поясните в этой таблице, почему соответствующее требование неприменимо к вашей организации.

Требование	Причина, в силу которой требование неприменимо
Пример. 9.3.1	*Посетителям запрещен вход в помещения, где обрабатываются или находятся данные о держателях карт.*