Индустрия платежных карт (PCI)
Стандарт безопасности данных

Опросный лист для самостоятельной оценки соответствия стандарту

Инструкции и рекомендации

Версия 3.2.1

Июнь 2018 г.

Изменения в документе

Дата	Версия	Описание
1 октября 2008 г.	1.2	Приведение положений документа в соответствие с новым стандартом PCI DSS версии 1.2 и внесение незначительных изменений с момента публикации исходной версии 1.1.
28 октября 2010 г.	2.0	Приведение положений документа в соответствие с новым стандартом PCI DSS версии 2.0 и уточнение типов среды и критериев соответствия. Введение опросного листа C-VT для ТСП с виртуальными веб-терминалами
Июнь 2012 г.	2.1	Введение опросного листа P2PE-HW для ТСП, которые обрабатывают данные держателей карт только через аппаратные платежные терминалы в рамках проверенного на соответствие стандарту и включенного в список PCI SSC решения PCI Point-to-Point Encryption (P2PE). Данный документ разработан для использования с PCI DSS версии 2.0.
Апрель 2015 г.	3.1	Приведение положений документа в соответствие с PCI DSS v3.1, включая введение A-EP и B-IP, а также уточнение критериев соответствия, указанных в ранее опубликованных опросных листах.
Май 2016 г.	3.2	Обновление для приведения положений документа в соответствие с PCI DSS версии 3.1, а также уточнения критериев, указанных в ранее опубликованных опросных листах.
Июнь 2018 г.	3.2.1	Незначительные обновления для приведения в соответствие со стандартом PCI DSS версии 3.2.1.

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ: Английская версия этого документа, опубликованная на веб-сайте PCI SSC, во всех смыслах, считается официальной версией этих документов и, если есть двусмысленность или несоответствия между настоящим текстом и английским текстом, английская версия, доступная на указанном сайте, будет иметь преимущественную силу.

Оглавление

Изменения в документе ..... **i**

Краткое описание документа **1**

Опросный лист для самостоятельной оценки соответствия стандарту PCI DSS: в чем суть **2**

Обзор опросного листа **3**

Важность PCI DSS **4**

Соответствие требованиям и безопасность: в чем разница 6

Общие советы и стратегии для приведения в соответствие с PCI DSS 6

Выбор опросного листа и свидетельства, оптимальных для вашей организации **10**

Опросный лист A: ТСП, принимающие транзакции без присутствия карты; все функции процессинга данных держателей карт полностью переданы сторонним организациям 12

Опросный лист A-EP: ТСП электронной коммерции, которые частично передали процессинг платежей сайтам сторонних организаций 13

Опросный лист B: ТСП только с импринтерами или только с автономными терминалами с коммутируемым доступом; без хранения данных держателей карт в электронном виде 15

Опросный лист B-IP: ТСП с автономными подключенными через IP платежными терминалами (POI), соответствующими требованиям PTS; без хранения данных держателей карт в электронном виде 16

Опросный лист C-VT: ТСП с виртуальными веб-терминалами; без хранения данных держателей карт в электронном виде 17

Опросный лист C: ТСП с платежными программными системами, подключенными к Интернету; без хранения данных держателей карт в электронном виде 19

Опросный лист P2PE: ТСП, использующие только аппаратные платежные терминалы в рамках решения P2PE; без хранения данных держателей карт в электронном виде 20

Опросный лист D для ТСП: все остальные ТСП, соответствующие критериям 21

Опросный лист D для поставщиков услуг: все остальные поставщики услуг, соответствующие критериям 21

Какой опросный лист оптимален для моей среды? **22**

Краткое описание документа

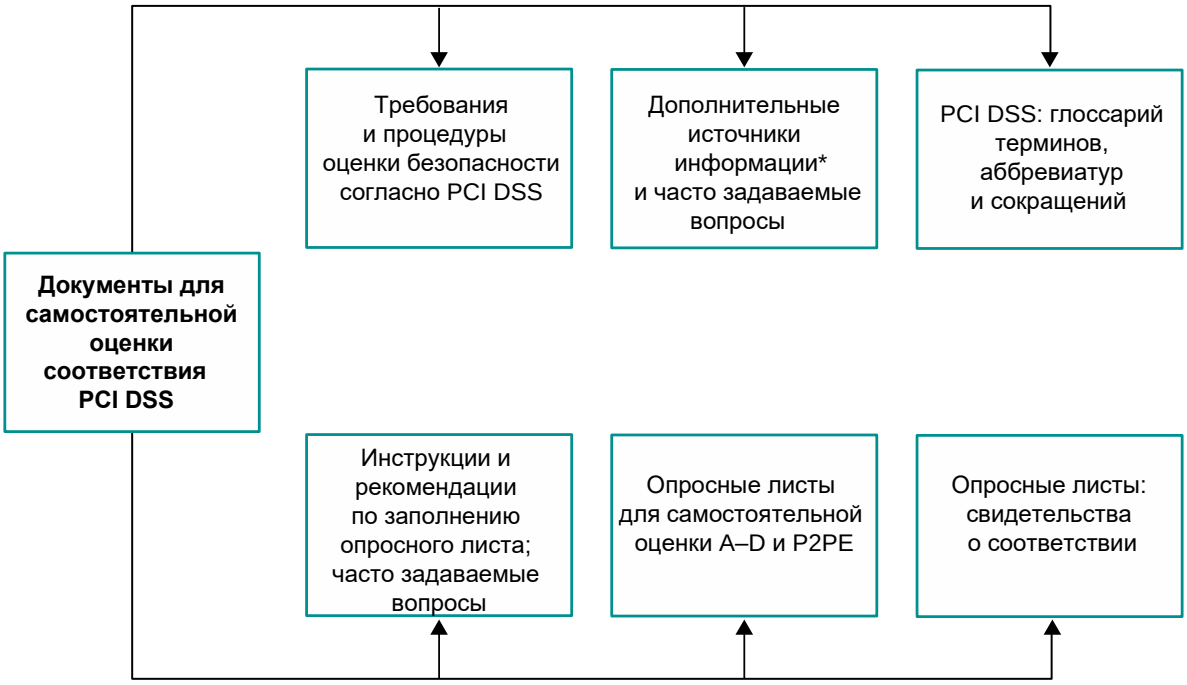
Настоящий документ был разработан, чтобы помочь ТСП и поставщикам услуг разобраться в опросных листах для самостоятельной оценки (SAQ) соответствия требованиям стандарта безопасности данных индустрии платежных карт (PCI DSS). Чтобы понять, почему PCI DSS важен для вашей организации, какие стратегии ваша компания может использовать для упрощения процедуры проверки на соответствие PCI DSS и имеет ли она право на заполнение более короткого варианта SAQ, мы рекомендуем ознакомиться с настоящим документом и указанными в нем инструкциями и рекомендациями.

Опросный лист для самостоятельной оценки соответствия стандарту PCI DSS: в чем суть

PCI DSS и сопроводительные документы представляют собой общий набор отраслевых инструментов, помогающих обезопасить обработку данных держателей карт. Сам стандарт формирует основу для разработки процесса обеспечения надежности и безопасности, включая предотвращение, обнаружение и реагирование на инциденты. Чтобы снизить риск компрометации данных и смягчить последствия, если это произойдет, важно, чтобы все организации, которые хранят, обрабатывают или передают данные держателей карт, соответствовали установленным требованиям.

В таблице ниже представлены инструменты, которые помогут организациям разобраться в критериях соответствия PCI DSS и заполнить опросные листы для самостоятельной оценки.

Эти и другие документы по теме можно найти на сайте www.pcisecuritystandards.org.



**В дополнительных источниках информации содержатся вспомогательные данные и рекомендации, которые не заменяют требования PCI DSS.*

**Примечание. Внесенные дополнения несут информативный и рекомендательный характер; они не заменяют и не отменяют какие-либо требования PCI DSS.*

Обзор опросного листа

Данные *опросные листы для самостоятельной оценки* (SAQ) — это инструменты проверки для ТСП и поставщиков услуг, которые помогают им самостоятельно определить, насколько они соответствуют требованиям PCI DSS. Существует несколько версий PCI DSS, предназначенных для различных типов оценки. Этот документ был разработан, чтобы помочь вам понять, какие опросные листы лучше всего подходят для среды, используемой в вашей организации.

Опросный лист PCI DSS — это инструмент самостоятельной проверки на соответствие стандарту для ТСП и поставщиков услуг. Представление отчета о соответствии требованиям (ROC) стандарта PCI DSS эквайерам или операторам платежных систем не требуется.Детальные требования к проверке на соответствие PCI DSS можно выяснить у своего эквайера или оператора платежной системы.

Все опросные листы PCI DSS состоят из следующих компонентов:

1. Вопросы, относящиеся к требованиям PCI DSS в зависимости от различных сред: см. раздел настоящего документа "Выбор опросного листа и свидетельства, оптимального для вашей организации". В этот раздел также входит столбец "Предстоящее тестирование" с процедурами проверки на соответствие стандартам PCI DSS.
2. Свидетельство о соответствии. Свидетельство включает ваше заявление на право заполнения опросного листа самостоятельной оценки для проверки на соответствие стандарту PCI DSS и результаты оценки.

Важность PCI DSS

Учредители Совета по стандартам безопасности PCI (American Express, Discover, JCB, Mastercard и Visa) постоянно отслеживают случаи компрометации данных банковских счетов. Проверяется деятельность организаций любого масштаба, а именно малых и крупных ТСП и поставщиков услуг.

Нарушение безопасности и последующая компрометация данных платежных карт имеют серьезные последствия для причастных организаций, в том числе:

1. Оповещение регулирующих органов.
2. Ущерб репутации.
3. Потеря клиентов.
4. Возможные финансовые обязательства (например, регуляторные и другие сборы и штрафы).
5. Судебные разбирательства.

Ретроспективный анализ случаев компрометации показывает, что распространенные уязвимости в области безопасности, предотвращение и устранение которых являются целью PCI DSS, в большинстве случаев возникают по причине отсутствия контроля по стандарту PCI DSS или ненадлежащего принятия предусмотренных мер в момент компрометации. Целью создания PCI DSS была разработка детальных требований для сведения к минимуму вероятность возникновения подобных ситуаций и нейтрализации их последствий, если они все же произошли.

Наиболее распространенные случаи, возникающие в результате недостаточного контроля по стандарту PCI DSS:

- Хранение конфиденциальных аутентификационных данных (SAD), таких как данные треков, после авторизации (требование 3.2). Большинство партнеров, у которых происходила компрометация данных, не знали, что данные сохраняются в их системах.
- Недостаточные меры ограничения доступа из-за неправильно установленных систем точек продажи (POS), в результате чего злоумышленники могут проникать в них, воспользовавшись методами, предназначенными для вендоров POS (требования 7.1, 7.2, 8.2 и 8.3).
- Системные настройки и пароли по умолчанию не были изменены при установке системы (требование 2.1).
- Ненужные и небезопасные службы не были удалены (или не была обеспечена их надлежащая защита) при установке системы (требования 2.2.2 и 2.2.3).
- Веб-приложения с неподходящим программным кодом, приводящие к SQL-инъекции и другим уязвимостям, которые позволяют получить доступ к базе данных держателей карт непосредственно с сайта (требование 6.5).
- Исправления системы безопасности отсутствуют или устарели (требование 6.2).
- Ведение журнала не выполняется (требование 10).
- Мониторинг проводится в неполной мере (проверка журналов, отслеживание/предотвращение вторжений, ежеквартальное сканирование уязвимостей и механизмов обнаружения изменений) (требования 10.6, 11.2, 11.4 и 11.5).

- Неправильные решения по определению области оценки: например, часть сети не была включена в проверку на соответствие PCI DSS из-за ненадлежащей сегментации (которая предварительно не была оценена) (требование 11.3.4). Это приводит к тому, что среда хранения данных держателей карт непреднамеренно подвергается воздействию уязвимостей в других частях сети, которые не были защищены в соответствии со стандартом PCI DSS (например, из-за незащищенных точек беспроводного доступа и уязвимостей, возникших при использовании электронной почты сотрудников и просмотре веб-страниц) (требования 1.2, 1.3 и 1.4).

Соответствие требованиям и безопасность: в чем разница

Необходимо понимать разницу между соответствием требованиям и безопасностью. Соответствие требованиям стандарта PCI DSS в определенный момент времени не гарантирует, что ваша среда не будет подвергаться изменениям в дальнейшем. Если не будут приняты надлежащие меры контроля, эти изменения могут снизить безопасность системы. Поэтому вы должны быть уверены, что инструменты контроля PCI DSS продолжают надлежащим образом применяться в рамках обычной деловой активности (BAU) и реализации общей стратегии безопасности. Выполнение данных условий позволит постоянно отслеживать эффективность инструментов контроля безопасности, применяемых в вашей организации, и сохранять соответствие среды стандартам PCI DSS между проверками. Примеры оптимальной интеграции требований PCI DSS в обычную деловую активность приведены в разделе "Как оптимально внедрять PCI DSS в обычные бизнес-процессы" стандарта PCI DSS.

Кроме того, требования безопасности PCI DSS предусматривают меры защиты данных платежных карт, а в вашей организации могут содержаться и другие конфиденциальные данные и элементы, которые нуждаются в защите, но могут выходить за рамки критериев PCI DSS. Таким образом, несмотря на то, что соответствие стандартам PCI DSS при правильном соблюдении требований, безусловно, способствует общей безопасности, оно не является альтернативой надежной общекорпоративной программе защиты данных.

Общие советы и стратегии для приведения в соответствие с PCI DSS

Ниже приведены некоторые общие рекомендации и стратегии обеспечения соответствия стандарту PCI DSS на начальном этапе. Эти рекомендации помогут вам избежать хранения ненужных данных держателей карт, уменьшить уязвимость действительно необходимых данных, централизованно разместив их в определенных и контролируемых местах, и снизить трудозатраты во время проверки на соответствие PCI DSS. Например, удалив данные держателей карт, которые вам не нужны, и/или снизив уязвимость тех, которые вам действительно необходимы, разместив их в определенных и контролируемых местах, вы можете удалить системы и сети, которые не хранят, не обрабатывают и не передают данные держателей карт и не подключаются к системам, которые выполняют эти функции — и всё это в рамках самостоятельной проверки.

1. **Конфиденциальные данные аутентификации (включая полные данные треков на магнитной полосе или эквивалентные данные на чипе, коды и значения проверки подлинности карты, ПИН-коды и ПИН-блоки):**

   Убедитесь, что у вас ***эти данные никогда не сохраняются*** после авторизации:

2. **Узнайте о степени безопасности вашей системы, задав следующие вопросы вашему POS-вендору:**

   a. Были ли изменены настройки и пароли по умолчанию в системах и базах данных в POS-системе?

   b. Есть ли у вас удаленный доступ к моей POS-системе? Если да, были ли приняты соответствующие меры защиты для предотвращения случаев доступа иных лиц к моей POS-системе, например, путем внедрения безопасных методов удаленного доступа и исключения использования общих паролей или паролей по умолчанию? Как часто вы подключаетесь к моему POS-устройству удаленно и с какой целью? Кому разрешен удаленный доступ к моему POS?

c. Были ли удалены все ненужные и небезопасные службы из систем и баз данных в POS-системе?

d. Проверено ли мое программное обеспечение POS на соответствие стандарту безопасности данных платежных приложений (PA-DSS)? См. список проверенных платежных приложений PCI SSC.

e. Сохраняются ли в моем программном обеспечении POS конфиденциальные данные аутентификации, такие как данные треков или ПИН-блоки? Если да, то хранение таких данных запрещено. Вы поможете мне их оперативно удалить?

f. Сохраняются ли в моем программном обеспечении POS основные номера платежных карт (PAN)? Если да, то такое хранение должно быть защищено. Как защищаются эти данные в POS?

g. Будет ли сформирован список файлов, созданных приложением, с кратким описанием содержимого каждого файла, чтобы можно было убедиться, что вышеуказанные запрещенные данные не сохранены?

h. Требует ли мое программное обеспечение POS создания сложных и уникальных паролей для всех пользователей?

i. Можете ли вы подтвердить, что не используете простые пароли и пароли по умолчанию для доступа к моей системе и системам других ТСП, с которыми сотрудничаете?

j. Все ли системы и базы данных в составе POS-системы содержат последние обновления инструментов безопасности?

k. Включена ли функция ведения журнала для систем и баз данных, которые являются частью POS-системы?

l. Если в предыдущих версиях моего программного обеспечения POS хранились конфиденциальные аутентификационные данные, были ли эти данные удалены после установки последних обновлений? Использовалась ли специальная программа для безопасного удаления этих данных?

3. Данные держателя карты. Если они вам не нужны, не храните их.

a. Правила платежной системы позволяют хранить основной номер счета (PAN), срок действия, имя держателя карты и сервисный код.

b. Пересмотрите цели и места хранения этих данных. Если данные не служат законной коммерческой цели, следует их удалить.

c. Помните, что хранение этих данных и соответствующие бизнес-процессы могут повлечь за собой следующее:

   i. Риск компрометации данных.

   ii. Принятие дополнительных мер согласно PCI DSS для защиты этих данных.

   iii. Регулярное обеспечение соответствия стандарту PCI DSS.

4. Данные держателя карты. Если они вам нужны, консолидируйте и изолируйте их.

Вы можете уменьшить область оценки соответствия PCI DSS, консолидировав хранимые данные в определенной среде и изолировав данные с помощью надлежащей сегментации сети. Например, если ваши сотрудники выходят в Интернет и получают электронную почту на том же компьютере или сегменте сети, где содержатся данные держателей карт,

рассмотрите возможность сегментации (изоляции) данных держателей карт на отдельном компьютере или сегменте сети (например, через маршрутизаторы или брандмауэры). Если вы сможете эффективно изолировать данные держателей карт, вы сможете сосредоточить свои усилия на соответствии PCI DSS только изолированной части, а не всех ваших устройств.

5. Компенсационные меры

В целях соответствия большинству требований PCI DSS следует также рассмотреть компенсационные меры, когда организация не может выполнить требование PCI DSS в силу обоснованных технических ограничений, но при этом успешно снизила риск, связанный с данным требованием, за счет выполнения других действий. Если в вашей организации не принимаются меры, указанные в PCI DSS, но принимаются другие аналогичные меры, которые подходят в качестве "компенсационных" согласно PCI DSS (см. раздел "Компенсационные меры" Приложения B к PCI DSS, а также *"Глоссарий. Основные определения, аббревиатуры и сокращения"*), вашей организации следует:

a. Выполнять процедуру применения компенсационных мер, описанную в Приложении B.

b. Для всех требований, которые были выполнены с помощью компенсационных мер, отметьте в опросном листе графу "Да, с КМФ" (КМФ = компенсационные меры: форма для заполнения).

c. Укажите все компенсационные меры в форме КМФ Приложения B опросного листа.

> КМФ должна быть заполнена для каждого требования, выполненного с помощью компенсационных мер.

d. Отправьте все заполненные КМФ вместе с заполненным опросным листом и/или сертификатом о соответствии согласно инструкциям вашего эквайера или платежной системы.

6. Профессиональная поддержка и обучение

a. Если вы хотите привлечь специалиста по безопасности для помощи в выполнении самостоятельной оценки, рекомендуем обратиться к сертифицированному аудитору безопасности (QSA). Аудиторы QSA сертифицированы Советом PCI SSC для проведения оценки на соответствие стандарту PCI DSS. Список аудиторов размещен на сайте PCI SSC.

b. Сайт PCI SSC является основным источником дополнительных ресурсов, включая:

- *Глоссарий PCI DSS. Основные определения, аббревиатуры и сокращения*
- Часто задаваемые вопросы (FAQ)
- Вебинары
- Вспомогательные материалы и рекомендации
- Формы опросных листов и свидетельства о соответствии

Примечание. *Вспомогательные материалы содержат дополнительные рекомендации по соблюдению требований PCI DSS; они не заменяют и не отменяют стандарт PCI DSS.*

c. PCI SSC также предлагает ряд обучающих программ для повышения уровня осведомленности персонала организации. К примеру, программы PCI Awareness, PCI Professional (PCIP) и Internal Security Assessor (ISA).

   Подробнее — на сайте www.pcisecuritystandards.org.

d. Учебные программы и ресурсы по платежным системам также доступны у платежных операторов и/или вашего эквайера ТСП.

Выбор опросного листа и свидетельства, оптимальных для вашей организации

Все ТСП и поставщики услуг должны всегда соответствовать стандарту PCI DSS применительно к их средам. Есть несколько типов опросных листов, краткие сведения о которых приведены в таблице ниже, более подробное описание — на следующих страницах. Воспользуйтесь таблицей, чтобы определить, какой из опросных листов подходит для вашей организации, затем ознакомьтесь с подробным описанием, чтобы убедиться, что вы соответствуете всем требованиям этого опросного листа.

Примечание для всех типов опросных листов, кроме типа D. Данные опросные листы содержат вопросы, которые относятся к определенной среде ТСП согласно требованиям опросного листа. Если существуют требования PCI DSS, применимые к вашей среде, которые не охвачены данным опросным листом, это может указывать на то, что опросный лист не подходит для вашей среды. Кроме того, чтобы получить положительную оценку, вы должны соответствовать всем применимым требованиям PCI DSS.

Опросный лист	Описание
A	ТСП, принимающие транзакции без присутствия карты (транзакции электронной коммерции или заказы по эл. почте/телефону), которые полностью передали процессинг данных держателей карт сторонним поставщикам услуг, подтвердившим свое соответствие требованиям стандарта PCI DSS. Такие ТСП не хранят, не обрабатывают и не передают какие-либо данные держателей карт в электронном виде в своих системах или локальных средах. *Не применяется к каналам очного взаимодействия.*
A-EP	ТСП, выполняющие транзакции электронной коммерции, которые полностью передали процессинг данных держателей карт сторонним организациям, подтвердившим свое соответствие требованиям стандарта PCI DSS, с сайтом (сайтами), который самостоятельно не получает данные держателей карт, но который влияет на безопасность транзакции. Такие ТСП не хранят, не обрабатывают и не передают в электронном виде данные держателей карт в своих системах или локальной среде. *Применяется исключительно к каналам электронной коммерции.*
B	ТСП, использующие исключительно: ▪ Импринтеры без электронного хранения данных держателей карт и/или ▪ Автономные терминалы с коммутируемым доступом без хранения данных держателей карт в электронном виде. *Не применяется к каналам электронной коммерции.*
B-IP	ТСП с автономными терминалами, соответствующими требованиям PTS, с IP-подключением, без хранения данных держателей карт в электронном виде. *Не применяется к каналам электронной коммерции.*
C-VT	ТСП, которые вводят вручную данные отдельной транзакции с помощью клавиатуры виртуального платежного терминала, подключенного к Интернету, который предоставлен сторонним поставщиком услуг, подтвердившим свое

Опросный лист	Описание
	соответствие требованиям стандарта PCI DSS, и который размещен у этого поставщика. Без хранения данных держателей карт в электронном виде. *Не применяется к каналам электронной коммерции.*
C	ТСП с платежными программными системами, подключенными к Интернету; без хранения данных держателей карт в электронном виде. *Не применяется к каналам электронной коммерции.*
P2PE	ТСП, использующие аппаратные платежные терминалы, в составе решений Point-to-Point Encryption (P2PE), включенных в список Совета PCI SSC, без хранения данных держателей карт в электронном виде. *Не применяется к каналам электронной коммерции.*
D	***Опросный лист D для остальных ТСП***, к которым не подходит ни одно из вышеперечисленных описаний.
	Опросный лист D для поставщиков услуг, имеющих право, по определению платежного оператора, на заполнение опросного листа.

Опросный лист A: ТСП, принимающие транзакции без присутствия карты; все функции процессинга данных держателей карт полностью переданы сторонним организациям

В опросном листе A учтены требования к ТСП, которые полностью передали хранение, обработку или передачу каких-либо данных держателей карт проверенным сторонним организациям, а самостоятельно хранят только бумажные отчеты или квитанции с данными держателей карт.

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист A, могут включать предприятия электронной коммерции, или компании, принимающие заказы по почте или телефону (без присутствия карты); такие ТСП не хранят, не обрабатывают и не передают какие-либо данные держателей карт в электронном виде в своих системах или локальных средах.

ТСП, использующие опросный лист A, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Ваша компания принимает исключительно транзакции без присутствия карты (транзакции электронной коммерции или посредством почты/телефонной связи).
- Весь процесс обработки данных держателей карт полностью передан сторонним организациям, подтвердившим свое соответствие требованиям стандарта PCI DSS.
- Ваша компания не хранит, не обрабатывает и не передает данные держателей карт в ваших системах или локальной среде в электронном виде, но привлекает для выполнения всех этих функций сторонние организации.
- Ваша компания подтверждает, что все сторонние организации, выполняющие хранение, обработку и/или передачу данных держателей карт, соответствуют требованиям стандарта PCI DSS.
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.

Дополнительно для каналов электронной коммерции:

- Все элементы страниц оплаты, отображаемые в браузере клиента, создаются исключительно сторонними организациями, соответствующими требованиям стандарта PCI DSS.

Данный опросный лист не распространяется на каналы очного взаимодействия.

Опросный лист A-EP: ТСП электронной коммерции, которые частично передали процессинг платежей сайтам сторонних организаций

В опросном листе A-EP учтены требования к ТСП сферы электронной коммерции с сайтом (сайтами), который самостоятельно не получает данные держателей карт, но который влияет на безопасность платежной транзакции и/или состояние страницы, которая принимает данные держателей карт клиентов.

ТСП, использующие опросный лист A-EP, — это ТСП, проводящие транзакции электронной коммерции, которые частично передали свои платежные каналы электронной коммерции сторонним организациям, подтвердившим свое соответствие требованиям стандарта PCI DSS, и которые не хранят, не обрабатывают и не передают в электронном виде данные держателей карт в своих системах или локальной среде.

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист A-EP, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Ваша компания принимает исключительно транзакции электронной коммерции.
- Весь процесс обработки данных держателей карт (за исключением платежной страницы) полностью передан сторонним процессинговым компаниям, подтвердившим свое соответствие требованиям стандарта PCI DSS.
- Ваш сайт электронной коммерции не получает данные держателей карт, но контролирует процесс перенаправления клиентов или их данных к сторонним процессинговым компаниям, подтвердившим свое соответствие требованиям стандарта PCI DSS.
- Если сайт ТСП размещен у стороннего провайдера, такой провайдер проверен на соответствие всем применимым требованиям стандарта PCI DSS (включая, например Приложение A к стандарту PCI DSS, если провайдер является поставщиком услуг виртуального хостинга).
- Каждый элемент страницы (страниц) оплаты, отображаемый в браузере клиента, создается либо на сайте ТСП, либо сторонними организациями, соответствующими требованиям стандарта PCI DSS.
- Ваша компания не хранит, не обрабатывает и не передает данные держателей карт в ваших системах или локальной среде в электронном виде, но привлекает для выполнения всех этих функций сторонние организации.
- Ваша компания подтверждает, что все сторонние организации, выполняющие хранение, обработку и/или передачу данных держателей карт соответствуют требованиям стандарта PCI DSS.
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.

Этот опросный лист распространяется исключительно на каналы электронной коммерции.

Примечание.*В рамках настоящего опросного листа A-EP требования стандарта PCI DSS, относящиеся к "среде данных держателей карт" применимы к сайту (сайтам) ТСП. Это обусловлено тем, что сайт ТСП непосредственно влияет на то, как происходит передача данных держателей карт, несмотря на то, что сам сайт не получает такие данные.*

Опросный лист B: ТСП только с импринтерами или только с автономными терминалами с коммутируемым доступом; без хранения данных держателей карт в электронном виде

В опросном листе B учтены требования к ТСП, которые обрабатывают данные держателей карт исключительно через импринтеры или автономные терминалы с коммутируемым доступом.

ТСП, использующие опросный лист B, могут быть как традиционными магазинами (проводящими транзакции с присутствием карты), так и предприятиями, принимающими заказы по почте/телефону (без присутствия карты), которые не хранят данные о держателях карт в какой-либо компьютерной системе. ТСП, использующие опросный лист B, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

- Для получения информации о платежных картах клиентов ваша компания использует только импринтер и/или только автономные терминалы с коммутируемым доступом (подключенные через телефонную линию к процессинговой системе).
- Автономные терминалы с коммутируемым доступом не подключены к каким-либо другим системам в вашей среде.
- Автономные терминалы с коммутируемым доступом не подключены к Интернету.
- Ваша компания не передает данные о держателях карт по сети (внутренней сети или через Интернет).
- Любые данные о держателях карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.
- Ваша компания не хранит данные о держателях карт в электронном формате.

Этот опросный лист не распространяется на каналы электронной коммерции.

Опросный лист B-IP: ТСП с автономными подключенными через IP платежными терминалами (POI), соответствующими требованиям PTS; без хранения данных держателей карт в электронном виде

В опросном листе B-IP учтены требования к ТСП, которые обрабатывают данные держателей карт исключительно через автономные платежные терминалы (POI), одобренные PTS, которые подключены к платежной системе по IP.

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист B-IP, могут быть как традиционными магазинами (проводящими транзакции с присутствием карты), так и предприятиями, принимающими заказы по почте/телефону (без присутствия карты), которые не хранят данные о держателях карт в какой-либо компьютерной системе.

ТСП, использующие опросный лист B-IP, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Для получения информации о платежных картах клиентов ваша компания использует только автономные платежные терминалы (POI) (кроме SCR), одобренные PTS и подключенные к процессинговой системе по IP.
- Автономные терминалы POI, подключенные по IP, проверяются программой POI PTS согласно перечню, указанному на сайте PCI SSC (за исключением SCR).
- Автономные терминалы POI, подключенные по IP, не подключены к каким-либо другим системам в вашей среде (например за счет сегментации сети для изоляции терминалов POI от других систем).
- Передача данных держателей карт осуществляется исключительно с терминалов POI, соответствующих требованиям PTS, в процессинговую систему.
- Для подключения к платежной системе в терминале POI не используется какое-либо другое устройство (например, компьютер, мобильный телефон, планшет и пр.).
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.
- Ваша компания не хранит данные держателей карт в электронном формате.

Этот опросный лист не распространяется на каналы электронной коммерции.

Опросный лист C-VT: ТСП с виртуальными веб-терминалами; без хранения данных держателей карт в электронном виде

В опросном листе C-VT учтены требования к ТСП, которые обрабатывают данные держателей карт исключительно через изолированные виртуальные платежные терминалы, установленные на персональном компьютере, подключенном к Интернету.

Виртуальный платежный терминал — это система доступа через браузер к эквайеру, процессинговой системе или сайту стороннего поставщика услуг для авторизации транзакций по платежным картам, в которой ТСП вручную вводит данные платежной карты через браузер с защищенным подключением. В отличие от физических терминалов, виртуальные платежные терминалы не считывают данные непосредственно с платежной карты. Данные для проведения транзакций с платежной картой вводятся вручную.

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист SAQ C-VT, обрабатывают данные держателей карт только через виртуальный платежный терминал и не хранят данные держателей карт в какой-либо компьютерной системе. Виртуальные терминалы подключаются к Интернету для доступа к ресурсам стороннего поставщика услуг, который предлагает функцию обработки платежей через виртуальный терминал. В качестве стороннего поставщика услуг может выступать процессинговая система, эквайер или другой сторонний поставщик услуг, который хранит, обрабатывает и/или передает данные держателей карт для авторизации и/или проведения платежных транзакций, поступающих с виртуальных терминалов ТСП.

Этот опросный лист предназначен только для ТСП, которые вручную вводят данные отдельной транзакции с помощью клавиатуры виртуального платежного терминала, подключенного к Интернету. ТСП, использующие опросный лист C-VT, могут быть как традиционными магазинами (проводящими транзакции с присутствием карты), так и предприятиями, принимающими заказы по почте/телефону (без присутствия карты).

ТСП, использующие опросный лист C-VT, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Единственной системой процессинга платежей вашей компании является виртуальный платежный терминал, доступ к которому осуществляется через подключенный к Интернету браузер.
- Виртуальный платежный терминал вашей компании предоставлен сторонним поставщиком услуг, подтвердившим свое соответствие требованиям стандарта PCI DSS, и размещен у этого поставщика.
- Ваша компания получает доступ к виртуальному платежному терминалу, соответствующему стандарту PCI DSS, через изолированный на одном объекте компьютер, который не подключен к каким-либо другим объектам или системам в вашей среде (такое решение можно реализовать, например, с помощью брандмауэра или сегментации сети для изоляции компьютера от других систем).
- На компьютере вашей компании не установлено программное обеспечение, которое позволяет хранить данные держателей карт (например, нет программы для пакетной обработки или хранения и передачи).
- К компьютеру вашей компании не подключены устройства, которые используются для сбора или хранения данных держателей карт (например, считыватели карт).

- Ваша компания не получает и не передает данные держателей карт в электронном виде по каким-либо другим каналам (например, через внутреннюю сеть или Интернет).
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.
- Ваша компания не хранит данные держателей карт в электронном формате.

Этот опросный лист не распространяется на каналы электронной коммерции.

Опросный лист C: ТСП с платежными программными системами, подключенными к Интернету; без хранения данных держателей карт в электронном виде

В опросном листе C учтены требования, предъявляемые к ТСП, чьи платежные программные системы (например, системы точек продажи) подключены к Интернету (например, через DSL, кабельный модем и т. д.).

ТСП, использующие опросный лист C, обрабатывают данные держателей карт через систему точек продажи (POS) или другие платежные программные системы, подключенные к Интернету, не хранят данные держателей карт в какой-либо компьютерной системе и могут быть как традиционными магазинами (проводящими транзакции с присутствием карты), так и предприятиями, принимающими заказы по почте/телефону (без присутствия карты).

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист C, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Ваша компания имеет платежную программную систему и подключение к Интернету на том же устройстве и/или в той же локальной сети (LAN).
- Платежная программная система/интернет-устройство не подключено к каким-либо другим системам в вашей среде (например за счет сегментации сети для изоляции платежной системы/интернет-устройства от всех других систем).
- Физическое место расположения среды POS не связано с другими локальными средами или местами, и любая локальная сеть предназначена только для внутреннего хранения данных.
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.
- Ваша компания не хранит данные держателей карт в электронном формате.

Этот опросный лист не распространяется на каналы электронной коммерции.

Опросный лист P2PE: ТСП, использующие только аппаратные платежные терминалы в рамках решения P2PE; без хранения данных держателей карт в электронном виде

В опросном листе P2PE учтены требования, предъявляемые к ТСП, которые обрабатывают данные держателей карт только через платежные терминалы в рамках проверенного на соответствие стандарту и включенного в список PCI SSC решения Point-to-Point Encryption (P2PE).

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

ТСП, использующие опросный лист P2PE, не имеют доступа к незашифрованным данным банковских счетов в какой-либо компьютерной системе; они вводят данные счетов только через аппаратные платежные терминалы в рамках соответствующего стандарту PCI SSC решения P2PE. ТСП, использующие опросный лист P2PE, могут быть как традиционными магазинами (проводящими транзакции с присутствием карты), так и предприятиями, принимающими заказы по почте/телефону (без присутствия карты). Например, ТСП, принимающие заказы по почте/телефону, могут воспользоваться опросным листом P2PE, если получают данные держателей карт в бумажном виде или по телефону и вводят их непосредственно в проверенное аппаратное устройство P2PE.

ТСП, использующие опросный лист P2PE, подтверждают, что соответствуют следующим требованиям к данному платежному каналу:

- Весь процессинг платежей осуществляется с помощью утвержденного решения PCI P2PE, проверенного на соответствие стандарту и включенного в список PCI SSC.
- Единственными системами в среде ТСП, которые хранят, обрабатывают или передают данные банковского счета, являются автономные платежные терминалы (POI), одобренные для использования с включенным в список PCI решением P2PE.
- Ваша компания не получает и не передает данные держателей карт в электронном виде.
- В среде компании нет устаревшей системы хранения электронных данных держателей карт.
- Любые данные держателей карт, которые хранит ваша компания, хранятся на бумаге (например, в распечатанных отчетах или квитанциях), и соответствующие документы не принимаются в электронном виде.
- Ваша компания внедрила все элементы управления из *руководства по эксплуатации P2PE*, которое предоставил поставщик решения P2PE.

Этот опросный лист не распространяется на каналы электронной коммерции.

Опросный лист D для ТСП: все остальные ТСП, соответствующие критериям

Опросный лист D применяется к ТСП, соответствующим требованиям, к которым не подходят другие типы опросных листов.

Примеры ТСП, которые могут использовать опросный лист D (список не является исчерпывающим):

- ТСП электронной коммерции, которые принимают данные держателей карт на своем сайте.
- ТСП, хранящие данные держателей карт в электронном виде.
- ТСП, которые не хранят данные держателей карт в электронном виде, но не соответствуют критериям других типов опросных листов.
- ТСП со средами, которые могут соответствовать критериям других типов опросных листов, но в отношении которых действуют дополнительные требования PCI DSS.

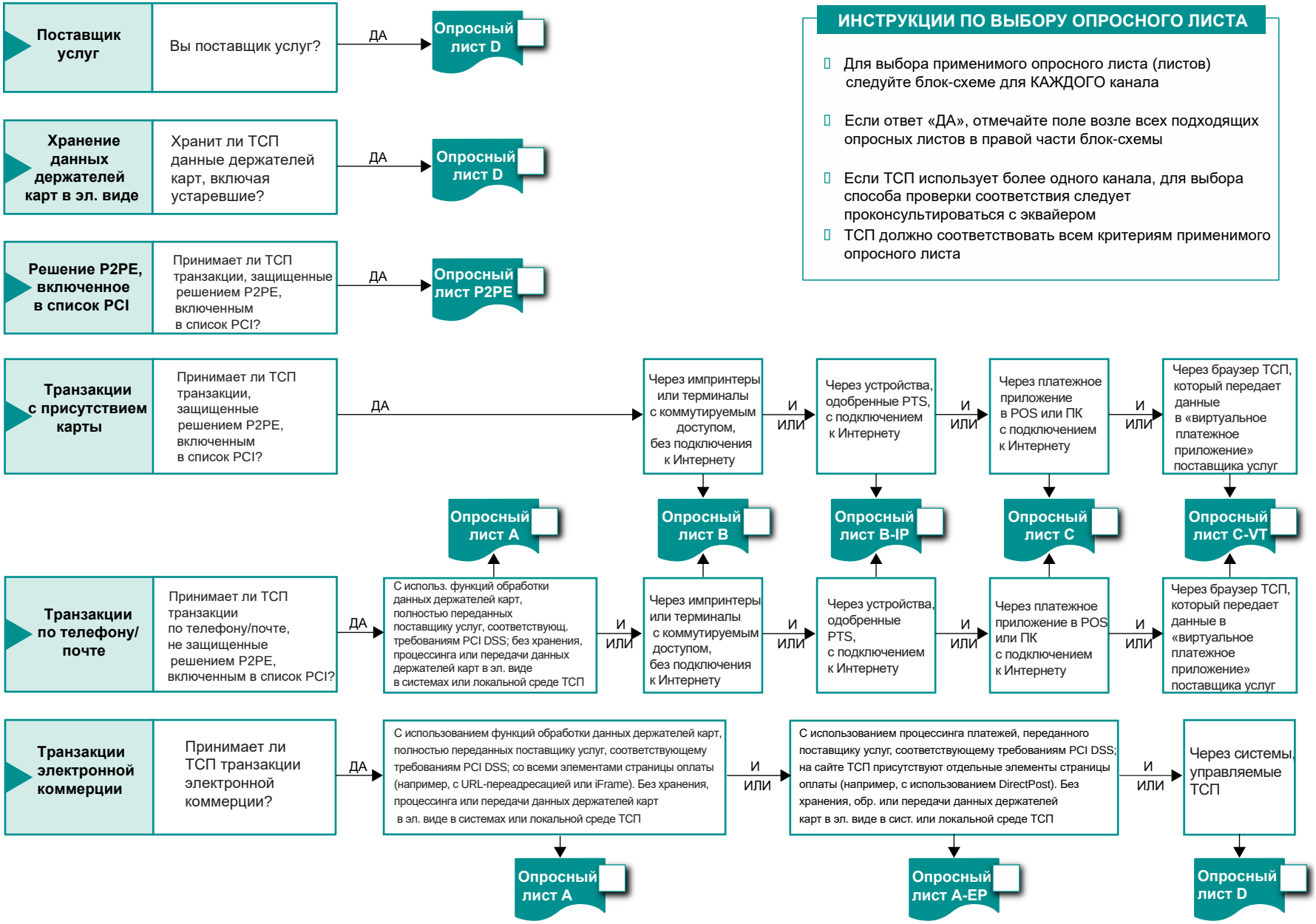
Опросный лист D для поставщиков услуг: все остальные поставщики услуг, соответствующие критериям

Опросный лист D для поставщиков услуг применяется ко всем поставщикам услуг, которые по определению платежного оператора имеют право на заполнение опросного листа.

Примечание к опросному листу D для поставщиков услуг. Большинство организаций, заполняющих опросный лист D, должны подтвердить соответствие всем требованиям PCI DSS, однако к отдельным организациям с очень специфическими бизнес-моделями некоторые требования неприменимы. Например, если компания вообще не использует беспроводные технологии, она не должна подтверждать соответствие разделам PCI DSS, относящимся к управлению такими технологиями. Подробную информацию об исключении других специфических требований см. в руководстве к опросному листу D.

Графическое руководство по выбору типа опросного листа см. в разделе «Какой опросный лист лучше всего подходит для моей среды?» на странице 22.

Какой опросный лист оптимален для моей среды?



ИНСТРУКЦИИ ПО ВЫБОРУ ОПРОСНОГО ЛИСТА

- Для выбора применимого опросного листа (листов) следуйте блок-схеме для КАЖДОГО канала
- Если ответ «ДА», отмечайте поле возле всех подходящих опросных листов в правой части блок-схемы
- Если ТСП использует более одного канала, для выбора способа проверки соответствия следует проконсультироваться с эквайером
- ТСП должно соответствовать всем критериям применимого опросного листа