Стандарт безопасности данных индустрии платежных карт (PCI DSS)

Лист самооценки A и Свидетельство о соответствии стандарту PCI DSS

ТСО, которые не хранят, не обрабатывают или не передают данные платежных карт в электронном виде

Версия 1.2

Октябрь 2008

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

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

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

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

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

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

Оглавление

Стандарт PCI DSS: документы

Следующие документы были созданы для помощи торгово-сервисным организациям (ТСО) и сервис-провайдерам в понимании стандарта PCI DSS и PCI DSS SAQ.

Документ	Организации, которые должны применять документ
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры оценки безопасности *(PCI Data Security Standard: Requirements and Security Assessment Procedures)*	Все ТСО и сервис-провайдеры
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Ориентирование в стандарте PCI DSS: Понимание требований *(PCI Data Security Standard: Navigating PCI DSS: Understanding the Intent of the Requirements)*	Все ТСО и сервис-провайдеры
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки. Инструкции по заполнению *(PCI Data Security Standard: Self-Assessment Questionnaire. Instructions and Guidelines)*	Все ТСО и сервис-провайдеры
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки A и Свидетельство о соответствии стандарту PCI DSS *(PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation of Compliance)*	ТСО[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки B и Свидетельство о соответствии стандарту PCI DSS *(PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation of Compliance)*	ТСО[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки C и Свидетельство о соответствии стандарту PCI DSS *(PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation of Compliance)*	ТСО[1]
Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки D и Свидетельство о соответствии стандарту PCI DSS *(PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation of Compliance)*	ТСО[1] и все сервис-провайдеры
Стандарт безопасности данных индустрии платежных карт (PCI DSS) и PA-DSS. Глоссарий (перечень терминов и сокращений) *(PCI Data Security Standard and Payment Application Data Security Standard: Glossary of Terms, Abbreviations, and Acronyms)*	Все ТСО и сервис-провайдеры

[1] Для определения подходящего для вашей организации листа самооценки см. документ “Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки. Инструкции по заполнению” *(PCI Data Security Standard: Self-Assessment Questionnaire. Instructions and Guidelines)*, раздел “Выбор SAQ и Свидетельства о соответствии стандарту PCI DSS, соответствующих вашей организации”.

Введение

Заполнение листа самооценки

Лист самооценки (SAQ) A предназначен для того, чтобы выделить требования, применимые к ТСО (merchants), которые сохраняют только распечатанные отчеты или чеки, содержащие данные платежных карт, не хранят эти данные в электронном виде, а также не обрабатывают или не передают их в пределах своей территории.

Эти ТСО определены как Validation Type 1 в настоящем документе и в документе “Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки. Инструкции по заполнению” *(PCI Data Security Standard: Self-Assessment Questionnaire. Instructions and Guidelines)*. ТСО категории SAQ Validation Type 1 не хранят данные платежных карт в электронном виде, а также не обрабатывают или не передают их в пределах своей территории. Такие ТСО должны подтверждать соответствие стандарту PCI DSS, заполняя SAQ A и Свидетельство о соответствии стандарту PCI DSS, в которых указывается, что:

- ваша компания производит только транзакции без присутствия платежной карты (card-not-present transactions) (электронная коммерция или заказы по почте/телефону);
- ваша компания не хранит, не обрабатывает или не передает данные платежных карт в пределах своей территории, а полностью передает эти функции стороннему сервис-провайдеру;
- ваша компания подтверждает, что сторонний сервис-провайдер, выполняющий хранение, обработку или передачу данных платежных карт, соответствует стандарту PCI DSS;
- ваша компания сохраняет только распечатанные отчеты или чеки, содержащие данные платежных карт, и эти документы не принимаются в электронном виде;
- ваша компания не хранит данные платежных карт в электронном виде.

Последнее требование не относится к ТСО, осуществляющим транзакции в присутствии держателя платежной карты (face-to-face POS environment).

Порядок оформления подтверждения о соответствии стандарту PCI DSS

1. Заполните SAQ A в соответствии с инструкциями, приведенными в документе “Стандарт безопасности данных индустрии платежных карт (PCI DSS). Лист самооценки. Инструкции по заполнению” *(PCI Data Security Standard: Self-Assessment Questionnaire. Instructions and Guidelines).*
2. Заполните Свидетельство о соответствии стандарту PCI DSS (*Attestation of Compliance*).
3. Отправьте SAQ и Свидетельство о соответствии стандарту PCI DSS вместе с другой необходимой документацией в ваш банк-эквайер.

Неприменимость отдельных требований стандарта PCI DSS

Неприменимость требований: Требования, которые неприменимы к вашей среде данных платежных карт, должны быть отмечены как “N/A” в столбце “Комментарий” листа самооценки. Для каждого такого требования заполните форму “Причины неприменимости требований”, приведенную в приложении настоящего документа.

Свидетельство о соответствии стандарту PCI DSS (Attestation of Compliance), SAQ A

Инструкции по предоставлению документа

ТСО должна заполнить это Свидетельство о соответствии стандарту PCI DSS для подтверждения статуса соответствия ТСО Стандарту безопасности данных индустрии платежных карт (PCI DSS). Заполните все применимые поля и следуйте инструкциям в разделе “Порядок оформления подтверждения о соответствии стандарту PCI DSS”.

Раздел 1. Информация о компании, имеющей статус Qualified Security Assessor (если применимо)

Название компании:					
Имя ведущего аудитора QSA:		Должность:			
Телефон:		Адрес электронной почты:			
Адрес компании:		Город:			
Регион/область:		Страна:		Почтовый индекс:	
URL-адрес:					

Раздел 2. Информация о ТСО

Название компании:		DBA(S):			
Имя контактного лица:		Должность:			
Телефон:		Адрес электронной почты:			
Адрес компании:		Город:			
Регион/область:		Страна:		Почтовый индекс:	
URL-адрес:					

Раздел 2a. Тип деятельности ТСО (отметьте все, что применимо):

☐ Предприятие розничной торговли ☐ Телекоммуникационная компания
☐ Продовольственный магазин или супермаркет

☐ АЗС ☐ Предприятие электронной коммерции ☐ Заказы по почте/телефону
☐ Другое (укажите):

Перечень помещений и других объектов, включенных в область оценки соответствия стандарту PCI DSS:

Раздел 2b. Договорные отношения

Связана ли деятельность вашей компании с одним или более сторонними сервис-провайдерами (например, платежные шлюзы, компании, предоставляющие услуги веб-хостинга, агентства по бронированию авиабилетов, агентства по привлечению клиентов и т. д.)? ☐ Да ☐ Нет

Сотрудничает ли ваша компания более чем с одним банком-эквайером? ☐ Да ☐ Нет

Раздел 2c. Право на заполнение SAQ A

ТСО подтверждает право на заполнение этой сокращенной версии SAQ, поскольку:

☐	ТСО не хранит, не обрабатывает или не передает данные платежных карт в пределах своей территории, а полностью передает эти функции стороннему сервис-провайдеру
☐	Сторонний сервис-провайдер, выполняющий хранение, обработку и/или передачу данных платежных карт, соответствует стандарту PCI DSS (имеется подтверждающий документ)
☐	ТСО не хранит какие-либо данные платежных карт в электронном виде
☐	При необходимости хранения данных платежных карт ТСО хранит такие данные только в распечатанных отчетах или в копиях чеков и не хранит их в электронном виде

Раздел 3. Проверка соответствия стандарту PCI DSS

На основании информации, указанной в SAQ A, на *(дата завершения оценки) (название ТСО)* имеет следующий статус соответствия стандарту PCI DSS (выберите один):

☐ **Соответствует:** Все разделы PCI DSS SAQ заполнены и на все вопросы дан ответ “Да” – это позволяет дать оценку **СООТВЕТСТВУЕТ**, тем самым *(название ТСО)* полностью соответствует стандарту PCI DSS

☐ **Не соответствует:** Не все разделы PCI DSS SAQ заполнены либо на некоторые вопросы дан ответ “Нет” – это позволяет дать оценку **НЕ СООТВЕТСТВУЕТ**, тем самым *(название ТСО)* не соответствует стандарту PCI DSS

Дата устранения несоответствий:

Организация, предоставляющая эту форму со статусом “Не соответствует”, должна заполнить План устранения несоответствий, приведенный в разделе 4 настоящего документа. *Проконсультируйтесь с вашим банком-эквайером или платежной системой, нужно ли заполнять раздел 4, поскольку не все платежные системы требуют его заполнения.*

Раздел 3a. Подтверждение статуса соответствия стандарту PCI DSS

ТСО подтверждает, что:

☐	Лист самооценки A версии *(версия SAQ)* заполнен в соответствии с приведенными в нем инструкциями
☐	Все сведения, содержащиеся в упомянутом выше SAQ и в данном свидетельстве, представляют собой объективные результаты самооценки
☐	Я прочитал стандарт PCI DSS и обязуюсь постоянно поддерживать полное соответствие ему

Раздел 3b. Подтверждение ТСО

Подпись исполнительного директора ТСО ↑	*Дата ↑*
Имя исполнительного директора ТСО ↑	*Должность ↑*

ТСО представлена↑

Раздел 4. План устранения несоответствий (Action Plan) при статусе “Не соответствует”

Для каждого требования выберите нужный статус соответствия. Если для какого-либо требования вы выберете “Нет”, то необходимо указать дату, когда ваша компания будет соответствовать этому требованию, и привести краткое описание действий, предпринимаемых для того, чтобы она соответствовала ему.
Проконсультируйтесь с вашим банком-эквайером или платежной системой, нужно ли заполнять раздел 4, поскольку не все платежные системы требуют его заполнения.

Требование стандарта PCI DSS	Описание требования	Статус соответствия требованию (выберите один вариант)		Дата устранения несоответствий и меры по их устранению (заполняется при ответе “НЕТ”)
		ДА	НЕТ	
9	Физический доступ к данным платежных карт должен быть ограничен	☐	☐	
12	Должна поддерживаться политика информационной безопасности, регламентирующая деятельность сотрудников и контрагентов	☐	☐	

Дата заполнения:

Реализация мер по строгому контролю доступа

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

	Вопрос	Ответ:	Да	Нет	Комментарий*
9.6	Обеспечивается ли физическая защита всех бумажных и электронных носителей, содержащих данные платежных карт?		☐	☐	
9.7	(a) Обеспечивается ли строгий контроль за внутренним или внешним перемещением носителей всех видов, содержащих данные платежных карт?		☐	☐	
	(b) Включает ли эта мера следующее:				
9.7.1	Маркировку носителей, чтобы они могли быть идентифицированы как содержащие конфиденциальную информацию		☐	☐	
9.7.2	Отправку носителей с доверенным курьером или с помощью другого способа доставки, который можно проконтролировать		☐	☐	
9.8	Утверждает ли руководство перемещение всех носителей, содержащих данные платежных карт, за пределы защищенной территории (в особенности если носители передаются отдельным лицам)?		☐	☐	
9.9	Обеспечивается ли строгий контроль хранения и доступности носителей, содержащих данные платежных карт?		☐	☐	
9.10	Уничтожаются ли носители, содержащие данные платежных карт, если их хранение больше не обосновано с точки зрения соблюдения требований законодательства или выполнения бизнес-задач? Уничтожаются ли носители следующими способами:		☐	☐	
9.10.1	Перекрестное измельчение, сожжение или преобразование в целлюлозную массу печатных документов, чтобы данные платежных карт невозможно было восстановить		☐	☐	

* “Неприменимо” (N/A) или “Применяемая компенсационная мера”. Организации, заполняющие этот столбец, должны также заполнить форму “Компенсационные меры. Форма для заполнения (Compensating Controls Worksheet)” или форму “Причины неприменимости требований”, приведенные в приложении настоящего документа.

Поддержание политики информационной безопасности

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

	Вопрос	Ответ:	Да	Нет	Комментарий*
12.8	Если данные платежных карт доступны нескольким сервис-провайдерам, реализованы ли и выполняются ли политики и процедуры управления сервис-провайдерами, включающие следующее:		☐	☐	
12.8.1	Поддержание перечня сервис-провайдеров		☐	☐	
12.8.2	Составление соглашения, подтверждающего признание сервис-провайдерами обязанностей по обеспечению безопасности данных платежных карт, к которым они получают доступ		☐	☐	
12.8.3	Должна существовать определенная процедура подключения сервис-провайдеров, включающая необходимость выполнения проверок до подключения		☐	☐	
12.8.4	Должна быть разработана программа для отслеживания статуса соответствия сервис-провайдера стандарту PCI DSS		☐	☐	

* “Неприменимо” (N/A) или “Применяемая компенсационная мера”. Организации, заполняющие этот столбец, должны также заполнить форму “Компенсационные меры. Форма для заполнения (Compensating Controls Worksheet)” или форму “Причины неприменимости требований”, приведенные в приложении настоящего документа.

Приложение A. (не используется)

Эта страница намеренно оставлена пустой

Приложение B. Компенсационные меры

Компенсационные меры могут применяться для большинства требований стандарта PCI DSS, если указано, что организация не соответствует требованию стандарта PCI DSS в явном виде по причине технической невозможности или бизнес-ограничений, однако риск, связанный с этим требованием, может быть значительно снижен путем принятия других мер.

Компенсационные меры должны удовлетворять следующим критериям:

1. Соответствовать цели и строгости исходного требования стандарта PCI DSS.
2. Предоставлять уровень защиты относительно рассматриваемой угрозы, близкий к тому, который обеспечивает исходное требование стандарта PCI DSS, чтобы компенсационная мера могла в достаточной степени нейтрализовать риск компрометации данных платежных карт, от которого должно защищать соответствующее исходное требование. (Цель каждого требования стандарта PCI DSS приведена в документе “Ориентирование в стандарте PCI DSS: Понимание требований”.)
3. Не только соответствовать другим требованиям стандарта PCI DSS, но и быть “сверх требуемого”. (Буквально: только лишь соответствие другим требованиям стандарта PCI DSS не является компенсационной мерой.)

   При оценке того, удовлетворяет ли компенсационная мера критерию “сверх требуемого”, необходимо учитывать следующее:

   Примечание. Пункты a), b) и c) приведены лишь в качестве примера. Все компенсационные меры должны оцениваться и проверяться аудитором, проводящим оценку соответствия стандарту PCI DSS, на то, достаточно ли они снижают риск компрометации данных платежных карт. Эффективность компенсационной меры зависит от конкретной среды, в которой реализуется эта мера, смежных защитных мер и конфигурации меры. Компании должны отдавать себе отчет в том, что какая-то конкретная компенсационная мера не будет эффективной во всех средах.

   a) Существующие требования стандарта PCI DSS НЕ МОГУТ рассматриваться как компенсационная мера, если они уже указаны в проверяемом пункте как требование. Например, пароли для неконсольного административного доступа должны пересылаться в зашифрованном виде с целью снижения риска перехвата незашифрованных паролей администратора. Организация не должна применять другие требования стандарта PCI DSS к паролям (блокирование паролей злоумышленника, сложные пароли и т. д.), чтобы компенсировать отсутствие зашифрованных паролей, поскольку эти требования не снижают риск перехвата незашифрованных паролей. Кроме того, другие меры по защите паролей уже являются требованиями стандарта PCI DSS для проверяемого пункта (пароли).

   b) Существующие требования стандарта PCI DSS МОГУТ рассматриваться как компенсационные меры, если их соблюдение необходимо в другой области и не требуется в проверяемом пункте. Например, для устройств удаленного доступа двухфакторная аутентификация является требованием стандарта PCI DSS. Применение двухфакторной аутентификации во внутренней сети также может рассматриваться как компенсационная мера для неконсольного административного доступа, если не поддерживается передача зашифрованных паролей. Двухфакторная аутентификация может рассматриваться как приемлемая компенсационная мера, если она: (1) соответствует цели исходного требования, состоящей в снижении риска перехвата незашифрованных административных паролей; (2) правильно применяется в защищенной среде.

   c) Существующие требования стандарта PCI DSS можно объединять с новыми мерами, в результате чего они становятся компенсационными мерами. Например, если компания не может привести данные платежных карт к нечитаемому виду в соответствии с требованием 3.4 (например, путем шифрования), компенсационная мера может включать в себя применение устройства или комбинации устройств, приложений и мер для реализации всех следующих мер: (1) сегментации внутренней сети; (2) фильтрации IP-адресов или MAC-адресов; (3) двухфакторной аутентификации во внутренней сети.

4. При этом следует учитывать дополнительный риск, связанный с несоответствием организации стандарту PCI DSS.

При каждой ежегодной оценке соответствия организации стандарту PCI DSS аудитор должен тщательно оценивать компенсационные меры, чтобы проверить, что каждая мера позволяет адекватно снизить риск, который должно снижать исходное требование стандарта (см. пп. 1–4 выше). Чтобы поддерживать соответствие стандарту PCI DSS, должны существовать процессы и меры, обеспечивающие эффективное действие компенсационных мер после завершения оценки.

Приложение C. Компенсационные меры. Форма для заполнения (Compensating Controls Worksheet)

Эта форма используется для определения компенсационных мер для каждого требования, для которого в столбце о соответствии указано "ДА", а в столбце "Комментарий" сделана отметка.

***Примечание.** Использовать компенсационные меры для достижения соответствия стандарту PCI DSS могут лишь компании, выполнившие анализ рисков и имеющие технические или документированные бизнес-ограничения.*

Номер и описание требования:

	Необходимые сведения	Описание
1. Ограничения	Перечислить ограничения, препятствующие соответствию исходному требованию	
2. Цель	Определить цель компенсационных мер	
3. Риск	Описать дополнительные риски, возникающие вследствие невыполнения исходного требования	
4. Определение компенсационных мер	Определить компенсационные меры и объяснить, как они способствуют достижению целей применения изначальных (некомпенсационных) мер, а также описать присутствующий повышенный риск в результате использования компенсационных, а не изначальных мер (если таковой имеется)	
5. Проверка компенсационных мер	Описать, как проверялись и тестировались компенсационные меры	
6. Техническая поддержка компенсационных мер	Определить процессы и меры по технической поддержке компенсационных мер	

Компенсационные меры. Пример

Эта форма используется для определения компенсационных мер для каждого требования, для которого в столбце о соответствии указано "ДА", а в столбце "Комментарий" сделана отметка.

Номер требования: *8.1. Идентифицируется ли каждый пользователь по уникальному имени пользователя до предоставления доступа к системным компонентам или данным платежных карт?*

	Необходимые сведения	Описание
1. Ограничения	Перечислить ограничения, препятствующие соответствию исходному требованию	*Организация XYZ использует изолированные серверы UNIX без LDAP. Таким образом, для каждого сервера необходима регистрация с помощью учетной записи 'root'. При этом невозможна реализация как управления учетными записями 'root', так и регистрации событий, связанных с любой активностью этой учетной записи, осуществляемой индивидуальным пользователем*
2. Цель	Определить цель компенсационных мер	*Цель требования уникальных учетных записей двояка. Во-первых, с точки зрения обеспечения безопасности разделение учетных данных неприемлемо. Во-вторых, при использовании разделяемых учетных записей невозможно точно выяснить лицо, ответственное за совершение определенного действия*
3. Риск	Описать дополнительные риски, возникающие вследствие невыполнения исходного требования	*При отсутствии уникального идентификатора у каждого пользователя дополнительный риск в системе контроля доступа связан с отсутствием возможности отслеживания их действий*
4. Определение компенсационных мер	Определить компенсационные меры и объяснить, как они способствуют достижению целей применения изначальных (некомпенсационных) мер, а также описать присутствующий повышенный риск в результате использования компенсационных, а не изначальных мер (если таковой имеется)	*Организация XYZ планирует реализацию обязательной регистрации всех пользователей на серверах со своих персональных компьютеров с использованием команды SU. Использование этой команды предоставит пользователям возможность доступа к учетной записи 'root' и выполнения действий с привилегиями 'root', при этом будет выполняться регистрация событий в директорию SU-log, что позволит отслеживать действия каждого пользователя*
7. Проверка компенсационных	Описать, как проверялись и тестировались компенсационные	*Организация XYZ демонстрирует аудитору, что команда SU*

	Необходимые сведения	Описание
мер	меры	*выполняется и что пользователи, использующие ее, зарегистрированы в системе и выполняют операции с привилегией root*
8. Техническая поддержка компенсационных мер	Определить процессы и меры по технической поддержке компенсационных мер	*Организация XYZ документирует процессы и процедуры, запрещающие изменение или удаление конфигураций SU, чтобы разрешить индивидуальным пользователям выполнение команд root без необходимости их отслеживания или регистрации*

Приложение D. Причины неприменимости требований

Эта форма используется для обоснования причин неприменимости к вашей организации требований, для которых в столбце "Комментарий" указано "Неприменимо" (N/A).

Требование	Причина неприменимости требования
Пример: 12.8	*Запрет доступа к данным платежных карт сервис-провайдерам*