

Контроль платёжной страницы по PCI DSS 6.4.3 и 11.6.1

Практическая рабочая книга: область применимости, управление скриптами, обнаружение изменений и подмены, тестирование реакции, владельцы и проверяемые доказательства.

PCI DSS v4.0.1

6.4.3

11.6.1

Определить область

Описать платёжные сценарии, состояния браузера, провайдеров и владельцев решений.

Эксплуатировать

Управлять скриптами, утверждать эталоны, находить изменения и реагировать.

Доказать работу

Хранить исходные записи, которые независимый проверяющий найдёт и проследит.

УПРАВЛЕНИЕ ДОКУМЕНТОМ

Основа: PCI DSS v4.0.1 и руководство PCI SSC для e-commerce

Обновлено: 27 июля 2026 г.

Язык: русский

Материал помогает внедрению, но не воспроизводит стандарт, не определяет применимость, не является аудиторским заключением и не гарантирует соответствие. Согласуйте выводы с организацией, управляющей программой соответствия, и с аудитором.

Область применимости и решение

Сначала зафиксируйте архитектуру, затем выбирайте контроль и способ валидации.

Заполняйте раздел для каждого существенно отличающегося платёжного сценария. На одном домене могут одновременно работать редирект, встроенная форма и страница продавца с разными границами ответственности.

01	02	03
Опишите сценарий	Назовите владельца	Приложите основание
URL, локали, мобильные состояния, согласия, менеджеры тегов, CDN и границы провайдера.	Зафиксируйте сторону, отвечающую за вывод: продавца, провайдера, аудитора, эквайера или платёжную систему.	Архитектура, инструкции провайдера, настройки, наблюдаемая страница и согласованное решение.

Запись архитектурного решения

Платёжная схема	Какое решение зафиксировать	Минимальное основание
Серверный редирект	Определить, могут ли скрипты влиять на переход; для ROC аудитор документирует вывод о неприменимости, если он обоснован.	HTTP-поведение, исходная страница, адрес провайдера, владелец изменений, решение аудитора или владельца программы.
Встроенная форма TPSP / iframe	Для SAQ A записать, как выполнен критерий по атакам через скрипты: собственные техники защиты или подтверждение TPSP.	Подтверждение и условия провайдера, настройки внедрения, контроли страницы продавца, протестированные состояния.
Форма продавца / direct post	Подтвердить применимый SAQ или ROC и полную ответственность продавца за контент, доставляемый в браузер.	Архитектура, инвентарь страницы, дизайн контролей, решение по оценке, зависимости от провайдеров.

Не смешивайте контроли

FAQ 1604 указывает: внешнее ASV-сканирование SAQ A относится к страницам продавца и с редиректом, и со встроенным iframe. Оно не заменяет управление скриптами или мониторинг изменений в браузере.

Сценарий / система _____	Рабочий URL или шаблон _____	Владелец архитектуры _____
Способ валидации _____	Владелец программы _____	Решение / дата пересмотра _____

Управление скриптами по требованию 6.4.3

Свяжите исполняемый браузером код с владельцем, авторизацией, необходимостью и целостностью.

Формируйте управляемый реестр по фактически наблюдаемым состояниям платёжной страницы, а не только по репозиторию. Включайте собственные пакеты, сторонние SDK, правила менеджера тегов, виджеты и загрузки.

ID	Результат контроля	Проверочный вопрос	Ожидаемое доказательство
643-01	Полный наблюдаемый инвентарь	Наблюдались ли все скрипты и загрузки во всех значимых сценариях, состояниях и вариантах релиза?	Экспорт браузера, карта URL/состояний, источник, first/last seen, связь с загрузчиком.
643-02	Назначенные владельцы	Есть ли у каждого скрипта ответственные бизнес- и технический владельцы?	Управляемый реестр, сервисная запись, принятие ответственности, путь эскалации.
643-03	Явная авторизация	Можно ли связать каждый активный скрипт с согласованным решением?	Заявка на изменение, дата, согласующий, среда, ссылка на исключение.
643-04	Письменная необходимость	Достаточно ли конкретно описана причина для решения об удалении?	Назначение, сценарий, зависимость, граница данных, дата пересмотра.
643-05	Способ контроля целостности	Задokumentирован и работает ли подход к целостности или подлинности для данного типа скрипта?	SRI/подпись, контролируемая доставка, поддержка CSP, правило мониторинга, тест.
643-06	Сверка жизненного цикла	Сверяется ли фактический состав после релизов и существенных изменений третьих сторон?	Экспорт до/после, релиз, добавления/удаления, решение и проверяющий.

Минимальные поля реестра скриптов

ID скрипта и наблюдаемый URL _____	Сценарий / состояние _____	Собственный или сторонний _____
Бизнес- и технический владелец _____	Назначение / необходимость _____	Ссылка на авторизацию _____
Способ целостности _____	Первое и последнее наблюдение _____	Пересмотр / дата удаления _____

Примечание

SRI, CSP, подписи, контролируемая доставка и мониторинг помогают разным частям контроля. Не объявляйте одну технику автоматическим соответствием: объясните её уместность для конкретного скрипта и доставки.

Обнаружение изменений по требованию 11.6.1

Утвердите ожидаемые состояния, находите существенные отклонения и сохраняйте реакцию.

Механизм оценивает платёжную страницу и влияющие на безопасность HTTP-заголовки в том виде, в котором их получает браузер пользователя. Нормализация динамики не должна скрывать значимые изменения.

ID	Результат контроля	Проверочный вопрос	Ожидаемое доказательство
1161-01	Утверждённый эталон	Версионированы и согласованы ли состояния, контент, скрипты, источники ресурсов и заголовки?	ID эталона, снимок, релиз, владелец, согласование, дата действия.
1161-02	Содержательное сравнение	Отличает ли механизм ожидаемую динамику от необъяснимого изменения?	Правила сравнения, нормализация, исключения, настройка, отрицательный тест.
1161-03	Требуемая периодичность	Выполняется ли проверка раз в семь дней или с частотой применимого целевого анализа рисков?	Расписание, история запусков, TRA при его использовании, ошибки, повторы, решение по пробелу.
1161-04	Полезное событие	Создаёт ли неавторизованное добавление, удаление или изменение проверяемое событие?	Разница, время, страница/заголовков, источник, критичность, получатель.
1161-05	Реакция и закрытие	Может ли команда назначить, исследовать, сдержать или согласовать, перепроверить и закрыть событие?	Оповещение, временная линия, решение, действие, закрытие, связь с инцидентом или изменением.
1161-06	Доступность контроля	Обнаруживаются ли пропущенные запуски, ошибки сбора и слепые зоны?	Сигнал здоровья, оповещение, история повторов, заявка по отказу, пересмотр покрытия.

Поверхность мониторинга

Поверхность	Что оценивать	Какой контекст сохранять
Контент страницы	Значимый DOM, формы, iframe, ссылки на ресурсы	Сценарий, состояние, снимок, ссылки на сырое и нормализованное сравнение
Скрипты	Добавление, удаление, источник, поведение загрузчика	ID скрипта, источник, владелец, авторизация, способ целостности
HTTP-заголовки	CSP и другие заголовки, влияющие на безопасность страницы и скриптов	Имя/значение, путь ответа, эталон, наблюдаемая разница

Решение о частоте

Если частота определяется целевым анализом рисков, сохраняйте актуальный анализ, согласование, дату пересмотра и подтверждение соответствия расписания. Применимость подтверждает аудитор.

Операционная модель и критерий готовности

Рассматривайте контроль как повторяемый процесс, а не как настроенную панель.

Начните с одного реального сценария, эквивалентного рабочей среде. Расширяйте область после того, как команда объясняет фактическое состояние, обрабатывает контрольное отклонение и извлекает полную цепочку доказательств.

01 Область Сценарии, состояния, зависимости, владельцы и предположения валидации.	02 Наблюдение Скрипты, источники ресурсов, контент страницы и значимые заголовки.	03 Авторизация Владелец, необходимость, согласование, целостность и дата пересмотра.
04 Эталон Ожидаемые состояния и узко описанные правила нормализации.	05 Реакция Маршрутизация, анализ, решение, действие, повторный тест и закрытие.	06 Хранение Исходные записи, независимое извлечение и проверка здоровья контроля.

Сценарий готов только при выполнении всех условий

Область	Реальные варианты и стороны задокументированы; применимость не предполагается.
Управление	Наблюдаемые скрипты связаны с владельцами, целью, авторизацией и целостностью.
Мониторинг	Эталоны утверждены; изменение и отказ контроля создают события.
Реакция	Положительные, отрицательные, маршрутные и отказные тесты имеют фактический результат.
Доказательства	Независимый проверяющий извлекает дизайн и работу без устного восстановления.
Открытые пробелы	Исключение или неудачный тест видимы с владельцем, сроком и эскалацией.

Выход из пилота

Зелёная панель не является критерием. Пилот завершён, когда проверяющий прослеживает штатный релиз, необъяснимое изменение, отказ мониторинга и соответствующие решения от исходной записи до закрытия.

Матрица контролей и доказательств

Заполняйте строку для каждого сценария; связывайте статус с исходной записью.

Перенесите строки в редактируемую CSV-ведомость для управления владельцами, сроками и исключениями. Статус без ссылки на исходную запись остаётся планом, а не доказательством.

ID	Результат	Фокус проверки	Основной владелец	Статус / ссылка
SCOPE-01	Область сценария	Все варианты и влияющие страницы нанесены на карту.	PCI / архитектура	Статус: Ссылка:
VAL-01	Путь валидации	SAQ/ROC и решение о применимости задокументированы.	PCI / аудитор	Статус: Ссылка:
643-01	Инвентарь	Наблюдаемые скрипты соответствуют реестру.	AppSec / приложение	Статус: Ссылка:
643-02	Авторизация	У каждого скрипта есть согласование и обоснование.	Бизнес / технический владелец	Статус: Ссылка:
643-03	Целостность	Работает подходящий способ целостности или подлинности.	Разработка / AppSec	Статус: Ссылка:
1161-01	Эталон	Ожидаемые состояния страницы и заголовков утверждены.	Владелец приложения	Статус: Ссылка:
1161-02	Обнаружение	Существенное изменение создаёт проверяемое событие.	Операции ИБ	Статус: Ссылка:
1161-03	Частота и пробелы	Расписание, ошибки, повторы и риск-решения подтверждены.	Владелец контроля / платформы	Статус: Ссылка:
1161-04	Реакция	События назначаются, разбираются, обрабатываются и закрываются.	SOC / реагирование	Статус: Ссылка:
EVID-01	Извлечение	Выборка воспроизводится без восстановления истории.	Аудит / владелец контроля	Статус: Ссылка:
GOV-01	Управление	Приняты RACI, хранение, исключения и пересмотр.	Владелец контроля	Статус: Ссылка:

ID сценария / области

Период проверки

Владелец ведомости

Независимый проверяющий

Открытые исключения

Следующий пересмотр

Приёмочные и операционные тесты

Сохраняйте ожидаемый и фактический результат; не превращайте неудачу в общее принятие.

Проводите набор тестов в контролируемой среде, достоверно повторяющей рабочее поведение. Используйте синтетические значения и не включайте карточные данные в доказательства.

Тест	Сценарий	Ожидаемый результат	Что сохранить
T-01	Согласованный релиз меняет скрипт.	Изменение связано с релизом; эталон обновлён через согласование.	До/после, заявка, согласующий, версия эталона.
T-02	Добавлен неожиданный скрипт или загрузчик.	Событие содержит страницу, источник, разницу и маршрут.	Условие, оповещение, время, владелец, разбор.
T-03	Изменён или удалён защитный заголовок.	Разница обнаружена с сырым и нормализованным контекстом.	Заголовки, эталон, разница, решение.
T-04	Меняется легитимное динамическое значение.	Шум нормализуется без сокрытия значимого изменения.	Правило, пример, причина, проверяющий, отрицательный тест.
T-05	Сбор или плановая проверка завершилась ошибкой.	Видимы сигнал здоровья, повтор, владелец и решение по пробелу.	Ошибка, повторы, заявка по отказу или пробелу.
T-06	Критичное событие маршрутизируется.	Дежурный путь получает и подтверждает событие в целевой срок.	Уведомление, подтверждение, временная линия эскалации.
T-07	Проверяющий запрашивает выборку.	Цепочка извлечена по сценарию, дате и требованию.	Запрос, экспорт, исходные ссылки, запись доступа.

Среда / версия _____	Окно теста _____	Исполнитель _____
Независимый проверяющий _____	Неудачные тесты / заявки _____	Согласование повтора _____

Граница данных

Доказательства объясняют контроль, но не должны хранить PAN, чувствительные аутентификационные данные, секреты, токены сессий или лишние данные клиентов. Опишите редактирование и доступ.

Владельцы, RACI и обработка события

Разделяйте ответственность, эксплуатацию, проверку и оценку.

Замените названия ролей на реальные команды и дежурные каналы. Участие QSA или внутреннего аудита не передаёт им ответственность организации за работу контроля.

Действие	Владелец PCI	Прил. / Dev	AppSec	SOC / IR	Аудит / QSA
Область и путь валидации	A	C	C	I	C
Ведение реестра скриптов	C	R	A	I	I
Согласование целостности	I	R	A	C	I
Эталон / релиз	I	A/R	C	I	I
Разбор и сдерживание	I	C	C	A/R	I
Хранение / исключения	A	R	R	R	C
Независимый тест / выборка	C	I	C	C	A/R

A = accountable, R = responsible, C = consulted, I = informed. Исполнителей может быть несколько, но подотчётность должна быть явной.

Минимальная временная линия события

01 Получить Время, сценарий, источник, критичность и канал уведомления.	02 Разобрать Релиз, эталон, инвентарь, владелец и признаки компрометации.	03 Решить Согласовать, сдержать, удалить, эскалировать или открыть инцидент.
04 Восстановить Вернуть состояние, проверить страницу и закрыть пробел наблюдения.	05 Закрыть Повторный тест, полная цепочка, последующие задачи и согласование.	06 Улучшить Обновить реестр, эталон, инструкцию, настройку и риск-предположения.

Принцип хранения	Определяйте сроки по периоду оценки, применимым требованиям PCI, внутренней политике, правовым основаниям и ожиданиям аудитора. Не назначайте один универсальный срок всем артефактам.
-------------------------	--

Профессиональный пакет доказательств

Обеспечьте независимую трассируемость дизайна и работы.

Используйте устойчивые идентификаторы в архитектуре, реестре скриптов, событиях, заявках и экспортах. Проверяющий должен пройти от требования к контролю, событию, владельцу, действию и исходной записи.

Раздел пакета	Минимальный контекст	Примеры артефактов
01 Область и архитектура	Сценарий, состояния, граница, владелец, путь валидации.	Схема, карта URL, поток данных, решение об области.
02 Управление скриптами	Источник, назначение, владелец, согласование, целостность, жизненный цикл.	Экспорт реестра, заявки, исключения, удаление.
03 Дизайн мониторинга	Эталон, сравнение, нормализация, частота, маршрутизация.	Конфигурация, манифест, TRA при его использовании, инструкция.
04 Рабочие выборки	Штатный запуск, релиз, необъяснимое изменение, отказ.	История, разницы, оповещения, заявки, решения.
05 Реакция и инциденты	Критичность, назначение, анализ, действие, восстановление, закрытие.	Временная линия, инцидент, повторный тест, согласование.
06 Управление	RACI, доступ, хранение, исключения, периодический пересмотр.	Процедура, пересмотр доступа, реестр исключений, протокол.
07 Независимое извлечение	Способ выборки, исходные ссылки, пробелы, вывод.	Индекс доказательств, журнал извлечения, задачи.

Повестка рабочей проверки

20м Архитектура Один реальный сценарий: область, влияние браузера и решение о валидации.	25м Работа контроля Штатный релиз, неожиданное изменение и отказ наблюдения.	15м Извлечение Проверяющий выбирает дату, сценарий, скрипт и событие без подготовки.
---	---	---

Критерий качества

Скриншоты дают контекст, но не должны быть единственной исходной записью. Предпочитайте экспорты, неизменяемые ID событий, версии конфигурации, заявки и оригиналы с контролируемым доступом.

09

Официальные источники и ограничения

Авторитетный источник - актуальные публикации PCI SSC.

Ссылки проверены при выпуске рабочей книги. Следите за обновлениями в библиотеке PCI SSC и уточняйте у владельца программы соответствия последующие редакции, региональные правила и способ валидации.

Основные материалы PCI SSC

01	Библиотека документов PCI SSC - PCI DSS v4.0.1 и актуальные сопроводительные материалы	www.pcisecuritystandards.org/document_library/
02	PCI SSC - защита платёжных страниц и предотвращение e-skimming	blog.pcisecuritystandards.org/new-information-supplement-payment-page-security-and-preventing-e-skimming
03	PCI SSC - изменения 2025 года для организаций, использующих SAQ A	blog.pcisecuritystandards.org/important-updates-announced-for-merchant-s-validating-to-self-assessment-questionnaire-a
04	PCI SSC FAQ 1588 - критерий SAQ A по атакам через скрипты	www.pcisecuritystandards.org/faqs/1588/
05	PCI SSC FAQ 1331 - критерии SAQ и применимость требований в ROC	www.pcisecuritystandards.org/faqs/1331/
06	PCI SSC FAQ 1604 - ASV-сканирование SAQ A для редиректа и iframe	www.pcisecuritystandards.org/faqs/1604/

Чего рабочая книга не делает

01	Не воспроизводит и не заменяет PCI DSS, SAQ, шаблон ROC или руководство PCI SSC.
02	Не определяет применимость, область, выборку, компенсирующие меры, customized approach или достаточность оценки.
03	Не сертифицирует Cartelta, другой продукт или конкретное внедрение как соответствующее стандарту.
04	Не заменяет безопасную архитектуру, управление уязвимостями, ASV-сканирование, реагирование и контроль провайдеров.
05	Должна быть адаптирована, версионирована, согласована и сохранена с исходными доказательствами среды.

Продолжение рабочего комплекта

Локализованное HTML-руководство и редактируемая CSV-ведомость доступны по адресу cartelta.com/ru/resources/pci-dss-6-4-3-11-6-1-checklist. Cartelta JSIR помогает строить инвентарь скриптов, мониторинг изменений платёжной страницы и поток проверяемых доказательств.

Владелец документа

Среда / сценарий

Согласующий

Следующий пересмотр
