Стандарт безопасности данных платежных приложений (PA-DSS) индустрии платежных карт (PCI)

Обзор изменений в PA-DSS версии 3.0 по сравнению с версией 2.0

Ноябрь 2013 г.

Введение

В этом документе представлен обзор изменений в PA-DSS версии 3.0 по сравнению с PA-DSS версии 2.0. В таблице 1 представлен обзор типов изменений в PA-DSS версии 3.0. В таблице 2 на следующих страницах представлен обзор важных изменений в PA-DSS версии 3.0.

Таблица 1: Типы изменений

Тип изменений	Определение
Пояснение	Пояснение назначения требования. Обеспечивает соответствие лаконичной формулировки назначению требования.
Дополнительные рекомендации	Объяснения, определения и (или) инструкции для разъяснения или предоставления дополнительной информации или рекомендаций по определенной теме.
Изменение требований	Изменения для обеспечения актуальности стандартов и их соответствия новым угрозам и изменениям на рынке.

Таблица 2: Обзор изменений

Раздел		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
Введение	Введение	**Назначение документа** Объяснено назначение и применение данного документа и добавлены ссылки на бланк отчета (ROV) о проверке PA-DSS.	Пояснение
		Связь между стандартами PCI DSS и PA-DSS Добавлено пояснение, что для областей применения стандарта PA-DSS также производится проверка на соответствие стандарту PCI DSS.	Пояснение
Область применения стандарта PCI DSS	Область применения стандарта PCI DSS	Раздел перемещен и обновлен для соответствия изменениям в стандарте PCI DSS. Удалены некоторые формулировки стандарта PCI DSS, не применимые к PA-DSS.	Пояснение
Область действия стандарта PA-DSS	Область действия стандарта PA-DSS	Удалена информация о том, какие платежные приложения соответствуют требованиям стандарта PA-DSS. Информацию о требованиях стандарта PA-DSS можно найти в *Руководстве по программе PA-DSS*.	Пояснение
Должности и обязанности		Информация о соответствующих заинтересованных лицах и их должностях и обязанностях в разработке PA-DSS была удалена в связи с включением этой информации в *Руководство по программе PA-DSS*.	Пояснение
Руководство по внедрению стандарта PA-DSS	Руководство по внедрению стандарта PA-DSS	Добавлена новая информация о *Руководстве по внедрению стандарта PA-DSS* и разъяснены обязанности PA-QSA.	Дополнительные рекомендации
Инструкции по заполнению и требования к содержанию отчета о проверке	Инструкции по заполнению и требования к содержанию отчета о проверке	Материал был перемещен, чтобы отделить *бланк отчета о проверке (ROV)*.	Пояснение

Шаги создания отчета о проверке PA-DSS	Шаги создания отчета о проверке PA-DSS	Раздел был обновлен, чтобы сконцентрироваться на процессе оценки, а не на документации (сведения о документации перемещены в *бланк отчета о проверке (ROV)*).	Пояснение
Руководство по программе PA-DSS	Руководство по программе PA-DSS	Удалена ссылка о переходе на PABP, поскольку переходного процесса больше не существует.	Пояснение
Стандарт безопасности данных платежных приложений (PA-DSS). Требования и процедуры аудита безопасности	Стандарт безопасности данных платежных приложений (PA-DSS). Требования и процедуры аудита безопасности	Добавлены формулировки для определения заголовков столбцов и удалены ссылки на столбцы "Выполнено", "Не выполнено" и "Целевая дата/комментарии"	Пояснение

Общие изменения в требованиях стандарта PA-DSS	Тип
Добавлен новый столбец "Информация", описывающий назначение и функцию безопасности каждого требования. Информация в этом столбце предназначена для разъяснения требований и не заменяет и не дополняет требования и процедуры проверки на соответствие стандарту PA-DSS.	Дополнительные рекомендации
Обновлены требования и (или) процедуры проведения проверки с целью отражения изменений в стандарте PCI DSS и соответствия требований стандарта PA-DSS требованиям стандарта PCI DSS.	Согласно определению в PCI DSS
Обновлена формулировка требований и (или) соответствующих процедур проведения проверки для обеспечения соответствия между ними.	Пояснение
Для ясности сложные требования отделены от процедур проведения проверки и удалены лишние и пересекающиеся процедуры проведения проверки.	Пояснение
Улучшены процедуры проведения проверки: разъяснены ожидаемые уровни соответствия каждому требованию, включая: ▪ необходимую информацию о Руководстве по внедрению стандарта PA-DSS; ▪ установку приложения согласно *Руководству по внедрению стандарта PA-DSS* для проверки точности инструкций *Руководства по внедрению*.	Пояснение
Другие общие редакторские правки, в том числе: ▪ удалены следующие столбцы: "Выполнено", "Не выполнено" и "Целевая дата/комментарии"; ▪ перенумерованы требования и процедуры проведения проверки для соответствия изменениям; ▪ изменен формат требований и процедур проведения проверки для повышения удобочитаемости: например, абзац преобразован в маркированный список и т. д.; ▪ внесены незначительные изменения в формулировки для повышения удобочитаемости; ▪ исправлены типографские ошибки.	Пояснение

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
Требование 1			

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
Требование 1 – общее		Заголовок изменен для достижения единообразия; "магнитная лента" заменена на "полоска данных"	Пояснение
1.1.c	1.1.1 – 1.1.3	Удалена процедура проведения тестирования 1.1.c и добавлены инструкции к аналогичным процедурам проведения тестирования для требований 1.1.1–1.1.3.	Пояснение
Требование 2			
2.x	2.x	К процедурам проведения тестирования в этом разделе добавлены компоненты *Руководства по внедрению стандарта PA-DSS*.	Изменение требований
2.1	2.1	Изменена формулировка для описания безопасного удаления данных, а не очистки.	Пояснение
2.2	2.2	Улучшены процедуры проведения тестирования: добавлено обязательное подтверждение наличия функций маскировки основного номера держателя карты.	Пояснение
2.4		Удалено требование по использованию решений для полного шифрования диска. Последующие требования соответствующим образом перенумерованы.	Изменение требований
2.6.x	2.5.x	Обновлены процедуры проведения тестирования: разъяснено, что методики управления ключами должны тестироваться надлежащим образом.	Пояснение
2.7	2.6	Разъяснено, что поставщик приложения должен предоставлять механизм удаления криптографических ключей, если в текущей или предыдущей версии использовались криптографические ключи или криптограммы.	Пояснение
Требование 3			
3.1	3.1	Примечание перемещено из процедуры проведения тестирования 3.1.d в требование 3.1.	Пояснение
3.1.b – 3.1.c	3.1.1 – 3.1.2	Процедуры проведения тестирования 3.1.b – 3.1.c преобразованы в новые требования, чтобы гарантировать, что приложение требует изменения паролей, установленных по умолчанию, и надлежащим образом проверяет это.	Пояснение
3.1.4	3.1.7	Требование перемещено в пункт 3.1.7 для улучшения группировки требований.	Пояснение

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
3.1.6 – 3.1.7	3.1.6	Требования к сложности пароля объединены для соответствия стандартам PCI DSS версии 3.0 и обеспечения возможности использования альтернативных средств составления паролей, соответствующих минимальным требованиям к надежности.	Пояснение
3.3	3.3.1 – 3.3.2	Требование 3.3 разделено на два требования, затрагивающие *передачу* паролей (3.3.1) и *хранение* паролей (3.3.2). Требование 3.3.2 обновлено: добавлено требование использования надежного одностороннего криптографического алгоритма с уникальной входной переменной, делающей пароли нечитаемыми.	Изменение требований
	3.4	От приложений теперь требуется ограничивать доступ к необходимым функциям и ресурсам и назначать встроенным учетным записям приложения наименьший приоритет.	Изменение требований
Требование 4			
4.2.5	4.2.5	Требование обновлено: разъяснены типы механизмов идентификации и аутентификации, которые должны регистрироваться, включая создание новых учетных записей.	Пояснение
Требование 5			
5.1	5.1	Требование улучшено: проверка безопасности включена в процесс разработки.	Изменение требований
	5.1.5	Разработчики платежных приложений теперь должны проверять целостность исходного кода в процессе разработки.	Изменение требований

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
	5.1.6	Добавлено требование разрабатывать платежные приложения с использованием передовых методов безопасного программирования, включая: ▪ разработку с наименьшими привилегиями для среды; ▪ разработку с отказоустойчивыми значениями по умолчанию – например, по умолчанию запрещено исполнение любого кода, кроме указанного изначально; ▪ разработку для всех видов точек доступа, включая такие разновидности ввода, как многоканальный ввод в приложение; ▪ документирование способов хранения основных номеров держателей карт и критичных аутентификационных данных в памяти.	Изменение требований
	5.1.7	Процедуры проведения тестирования 5.2.a и 5.2.b были преобразованы в требование обучать разработчиков платежных приложений методам безопасной разработки.	Пояснение
5.2	5.2	Требование обновлено: акцент сделан на предотвращении распространенных программных уязвимостей.	Пояснение
	5.2.10	Новое требование по противодействию взлому механизмов аутентификации и управления сеансами.	Изменение требований
5.4	8.2	Требование перемещено в пункт 8.2 для объединения с другими требованиями к безопасности среды PCI DSS и посвящения требований 5.x методам разработки приложений.	Пояснение
	5.4	Новое требование: поставщик платежного приложения теперь обязан определять и внедрять методологию назначения версии в соответствии с *Руководством по программе PA-DSS*.	Изменение требований
	5.5	Новое требование: поставщики платежных приложений теперь обязаны включать технологии оценки рисков в процесс разработки ПО.	Изменение требований
	5.6	Поставщики платежных приложений теперь обязаны внедрять процесс формальной аутентификации до финального выпуска.	Изменение требований

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
Требование 6			
6.1 – 6.2	6.1 – 6.3	Требования перегруппированы для разъяснения механизмов контроля, которые относятся ко всем приложениям, и механизмов контроля, которые относятся только к платежным приложениям, предназначенным для использования с беспроводными точками доступа. Процедура проведения тестирования 6.2.b преобразована в новое требование 6.3.	Пояснение
Требование 7			
Требование 7 – общее		Заголовок обновлен, чтобы лучше отражать назначение требования (исправление уязвимостей *и регулярное обновление приложения).*	Пояснение
7.1	7.1.1 – 7.1.3	Разделено на несколько требований и добавлено требование использования авторитетных источников информации об уязвимостях.	Пояснение
7.2	7.2.1 – 7.2.2	Разделено на несколько требований.	Пояснение
	7.3	Поставщики приложений теперь обязаны предоставлять сведения о выпуске для каждого обновления приложения.	Изменение требований
Требование 8			
8.1	8.1	Пример расширен: разъяснено назначение требования.	Пояснение
5.4	8.2	Требование перемещено из пункта 5.4 для объединения с другими требованиями к безопасности среды PCI DSS.	Пояснение
10.1	8.3	Требование перемещено из пункта 10.1 для объединения с другими требованиями к безопасности среды PCI DSS.	Пояснение
Требование 9			
9.1	9.1	Добавлена формулировка, разъясняющая назначение требования о том, что веб-серверы и компоненты системы хранения данных держателя карты не обязательно должны находиться в одной сетевой зоне. Базы данных теперь представлены как пример компонентов системы хранения данных держателя карты, а демилитаризованная зона (DMZ) – как пример сетевой зоны.	Пояснение
Требование 10			

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
10.1	8.3	Требование перемещено в пункт 8.3 для объединения с другими требованиями к безопасности среды PCI DSS. Последующие требования перенумерованы.	Пояснение
10.2	10.1	Разъяснено требование к удаленному доступу, осуществляемому извне сети клиента.	Пояснение
	10.2.2	Поставщики, предоставляющие услуги поддержки/техобслуживания клиентам, обязаны предоставлять каждому клиенту уникальные учетные данные для проверки подлинности.	Изменение требований
10.3.2	10.2.3	Разъяснено, что требование относится ко всем видам удаленного доступа.	Пояснение
Требование 11			
11.1	11.1	Незначительные изменения с целью дальнейшего разъяснения и соответствия стандарту PCI DSS.	Пояснение
Требование 12			
12.1	12.1 12.2	Требования перегруппированы для разъяснения механизмов контроля, которые относятся ко всем приложениям, и механизмов контроля, которые относятся только к платежным приложениям, упрощающим административный доступ без использования консоли.	Пояснение
Требование 13			
Требование 13 – общее		Заголовок изменен: сделан акцент на требованиях в *Руководстве по внедрению стандарта PA-DSS*. Требования к обучающей документации и программам обучения перемещены в новое требование 14.	Пояснение
	13.1.1	Добавлено требование проверять, что *Руководство по внедрению стандарта PA-DSS* относится к оцениваемому приложению и версии (версиям).	Пояснение
13.1.3	13.1.3	Разъяснено, что *Руководство по внедрению стандарта PA-DSS* следует пересматривать и обновлять при каждом изменении требований к приложению или в стандарте PA-DSS.	Пояснение
Требование 14			

Требование		Изменение	Тип
PA-DSS, версия 2.0	**PA-DSS, версия 3.0**		
Требование 14 – общее		См. "Требование 13 – общее" выше. Новое требование, посвященное обучающей документации и программам обучения, включая внутреннее обучение сотрудников поставщика обязанностям по стандарту PA-DSS.	Пояснение
	14.1	Обучение сотрудников поставщика по вопросам информационной безопасности и требованиям стандарта PA-DSS должно проходить не реже, чем раз в год.	Изменение требований
	14.2	Новое требование о назначении обязанностей сотрудникам поставщика по стандарту PA-DSS.	Изменение требований
13.2	14.3	Улучшены требования к программам обучения реселлеров/интеграторов, ранее входившие в требование 13. Разъяснено, что обучающие материалы следует пересматривать и обновлять при каждом изменении требований к приложению или в стандарте PA-DSS.	Пояснение
Приложение B			
Подтверждение конфигурации лаборатории по тестированию, предназначенной для проведения оценки на соответствие требованиям PA-DSS	Конфигурация лаборатории по тестированию для проведения оценки соответствия требованиям PA-DSS	В приложение добавлена информация о требованиях и оснащении лаборатории, предназначенной для проведения оценки соответствия требованиям PA-DSS. Сведения и бланк для записи конфигурации лаборатории по тестированию выделены в отдельный *бланк отчета (ROV) о проверки стандарта PA-DSS*.	Пояснение