ABISS
НП «АБИСС»

Официальный перевод PCI DSS на русский язык

Некоммерческое партнерство
«Сообщество пользователей стандартов
по информационной безопасности АБИСС»

Москва, 10 июня 2015 г.

В чем новость?

PCI DSS на русском языке	
Неофициальные переводы существуют	с 2006 года
Официальный перевод опубликован	в 2012 году
Годен к употреблению	**с июня 2015 года**

ABISS
НП «АБИСС»

Зачем это нужно?

- Исполнение заказа Банка России от 2012 года
- Понимание требований стандарта русскоязычными пользователями
- Избежание споров о толковании требований
- Заполнение листов самооценки русскоязычными ТСП
- Интеграция с существующими нормативными документами, такими как 382-П, СТО БР ИББС и 152-ФЗ
- Применение при разработке национальных нормативных документов по безопасности индустрии платежных карт, в том числе, стандартов НСПК

ABISS
НП «АБИСС»

Перспективы

- Разработка национальных стандартов безопасности платежных карт на основе мировой практики, в том числе для торгово-сервисных предприятий

«Пока от меня ЦБ РФ не потребует, я не буду защищать номера карт»
(с) CISO одной крупной сети супермаркетов

- Гармонизация российских и международных требований в области безопасности индустрии платежных карт

Несколько стандартов – одни правила

ABISS
НП «АБИСС»

Состояние документов

PCI DSS 3.0	**Есть официальный перевод. Можно использовать.**
Глоссарий	**Есть официальный перевод. Можно использовать.**
PCI DSS 3.1	**Планируется работа по переводу на основе имеющегося PCI DSS 3.0.**
Опросные листы самооценки	**Есть официальный перевод. Качество плохое. Планируется работа по исправлению.**
PCI PA-DSS	**Есть официальный перевод. Качество плохое. Недоступен публично. Планируется работа по исправлению.**
Прочие документы Совета PCI SSC	**Планируется работа по переводу.**

ABISS
НП «АБИСС»

Что сделано?

- Построены взаимоотношения с Советом PCI SSC
- Инициирован совместный проект по созданию русскоязычных документов
- Обработано **50 610** слов на **203** страницах
- Исправления составили более **50%** текста
- Опубликованы финальные версии **двух** основных документов
- Сформированы рекомендации по переводу следующих документов
- Работа продолжается

ABISS
НП «АБИСС»

Как это выглядит?

5	prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	запрещают копирование, перемещение и хранение ~~данных о держателях карт~~ДДК на локальных жестких дисках и ~~иных~~ съемных электронных носителях ~~при удаленном доступе~~, если доступ к этим данным ~~осуществляется через~~ технологии удаленного доступа;
2106	[1]To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computers or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so.	[1]~~Для обеспечения осведомленности персонала~~Чтобы работники знали о ~~запрете хранения и копирования данных о держателях карт~~своем обязательстве не хранить или не копировать ДДК на свои персональные компьютеры или другие носители информации, политика ~~компании~~организации должна явно запрещать действия такого рода, ~~за исключением сотрудников~~исключая работников, которым ~~на выполнение такого действия дано специальное разрешение~~ так делать явно разрешено.
2107	Storing or copying cardholder data onto a local hard drive or other media must be in accordance with all applicable PCI DSS requirements.	Хранение или копирование ~~данных о держателях карт~~ДДК на локальный жесткий диск или ~~другой~~иной носитель должно осуществляться в соответствии со всеми ~~действующими~~применимыми требованиями стандарта PCI DSS.
2108	[1]12.3.10.b[2] For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	~~[1]12.3.10.b[2] Для авторизованных сотрудников убедиться, что правила эксплуатации предписывают обеспечение защиты данных о держателях карт в соответствии с требованиями стандарта PCI DSS.~~[1]12.3.10.b[2] требуют от должным образом уполномоченных работников, чтобы они защищали ДДК в соответствии с требованиями PCI DSS.
2109	[1]12.4 [2]Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	[1]12.4 ~~[2]Политика~~ Гарантировать, что политика и процедуры ~~обеспечения~~ безопасности ~~должны однозначно определять~~четко определяют обязанности ~~всего персонала организации, относящиеся к~~по обеспечению информационной безопасности для всех работников.

АБИСС
НП «АБИСС»

Что мы исправляем?

Например, это:

Оригинал	Как было	Как стало
Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created	Данные обновления могут быть дополнительно зашифрованы симметричным ключом и списками контроля доступа	Как вариант, данные обновления можно зашифровать с помощью симметричного ключа, а также можно создать списки контроля доступа
Organizations should contact their acquirer or the individual payment brands directly	Организации должны напрямую связаться со своими эквайерами или отделениями, отвечающими за отдельные торговые марки	Организациям следует связаться со своими эквайерами или напрямую с конкретными международными платежными системами

ABISS
НП «АБИСС»

Кто участвует в работе?

Участник	Выполняемая роль
Совет PCI SSC	Управляет стандартами, предоставляет первую версию перевода, принимает правки, утверждает финальную версию.
НП «АБИСС»	Контролирует качество перевода, руководит процессом исправления. Обладает статусом Participating Organization в Совете PCI SSC.
Рабочая группа экспертов по ИБ	Формировалась из членов АБИСС, ТК122 и QSA-аудиторов. Согласовала терминологию, подготовила первый пакет правок. Работа группы завершена.
Существенную часть правок выполнило Бюро переводов **ГК «Альянс ПРО»**	
Особая благодарность члену АБИСС - Компании **Deiteriy** за активную работу и спонсорскую поддержку проекта.	

Где найти утвержденные документы PCI DSS на русском языке?

На официальных сайтах:

- Глобальный сайт Совета PCI SSC:
  - https://www.pcisecuritystandards.org/
- Русскоязычный сайт Совета PCI SSC:
  - https://ru.pcisecuritystandards.org/

ABISS
НП «АБИСС»

СПАСИБО ЗА ВНИМАНИЕ!

Некоммерческое партнерство
«Сообщество пользователей стандартов
по информационной безопасности АБИСС»