ABISS
НП «АБИСС»

О взаимодействии Партнерства с PCI Council. Перспективы развития стандарта PCI/PA DSS в 2013 году

Некоммерческое партнерство
«Сообщество пользователей стандартов
по информационной безопасности АБИСС»

V Юбилейный Уральский форум
«Информационная безопасность банков», Республика Башкортостан,
11-16 февраля 2013 г.

ВЗАИМОДЕЙСТВИЕ С PCI COUNCIL

Организация встречи ЦБ РФ и PCI Council (Совет по стандартам безопасности индустрии платежных карт (PCI SSC)

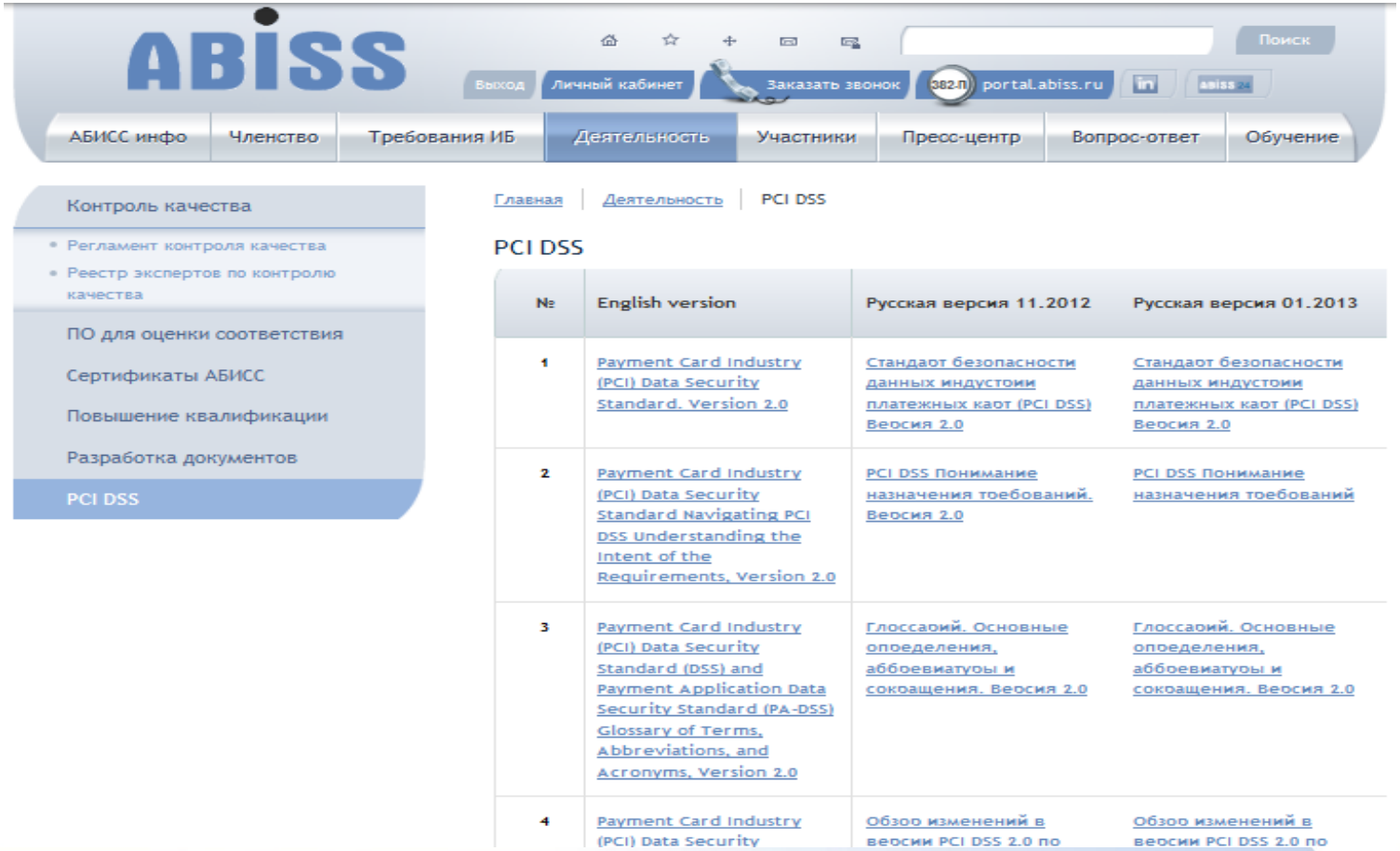
Достигнута договоренность о необходимости официального перевода документов, регламентирующие вопросы информационной безопасности Международных платежных систем

Взаимодействие с ЦБРФ по переводу Стандарта PCI DSS

23 ноября 2012 г. между НП «АБИСС» и Центральным банком Российской Федерации был заключен договор на оказание услуг по переводу на русский язык документов, входящих в состав Стандарта PCI DSS, с последующим размещением их на официальном сайте Совета по стандартам безопасности индустрии платежных карт (PCI SSC). В рамках договора были разработаны первые русскоязычные версии документов, все они размещены на сайте www.abiss.ru в закрытом разделе PCI DSS.

ABISS
НП «АБИСС»

РАЗДЕЛ PCI DSS НА САЙТЕ ПАРТНЕРСТВА



№	English version	Русская версия 11.2012	Русская версия 01.2013
1	Payment Card Industry (PCI) Data Security Standard. Version 2.0	Стандаот безопасности данных индустоии платежных каот (PCI DSS) Веосия 2.0	Стандаот безопасности данных индустоии платежных каот (PCI DSS) Веосия 2.0
2	Payment Card Industry (PCI) Data Security Standard Navigating PCI DSS Understanding the Intent of the Requirements, Version 2.0	PCI DSS Понимание назначения тоебований. Веосия 2.0	PCI DSS Понимание назначения тоебований
3	Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms, Version 2.0	Глоссаоий. Основные опоеделения, аббоевиатуоы и сокоащения. Веосия 2.0	Глоссаоий. Основные опоеделения, аббоевиатуоы и сокоащения. Веосия 2.0
4	Payment Card Industry (PCI) Data Security	Обзоо изменений в веосии PCI DSS 2.0 по	Обзоо изменений в веосии PCI DSS 2.0 по

ABISS
НП «АБИСС»

РАБОТА ПО ПЕРЕВОДУ PCI DSS НА РУССКИЙ ЯЗЫК

Комментарии по первой версии перевода документов PCI DSS были получены от следующих специалистов:

Дроздов Андрей Валентинович - НП «АБИСС», Гончаров Игорь Васильевич - ЗАО «НПО «Инфобезопасность», Евтушенко Кирилл - ЗАО НИП «ИНФОРМЗАЩИТА», Сергей Шустиков - ООО «Дейтерий», Федор Янович Дзержинский - ОАО «Промсвязьбанк», Максимов Вячеслав - ЗАО «Андэк», Гриценко Андрей Александрович - банк «Возрождение» (ОАО), Лукацкий Алексей Викторович – Cisco Systems, Inc., Никитин Александр Владимирович - ООО «Линс-М», Бутенко Валерий Владимирович - ОАО «АЛЬФА-БАНК».

ABISS
НП «АБИСС»

ЗАСЕДАНИЕ РАБОЧЕЙ ГРУППЫ

11 декабря 2012 г. в офисе НП «АБИСС» состоялось заседание рабочей группы

по переводу Стандарта безопасности данных индустрии платежных карт (PCI DSS) и сопутствующих документов на русский язык, в котором приняли участие эксперты НП «АБИСС», Банка России, участники ТК №122, QSA-аудиторы из QSA-компаний, работающих на российском рынке, а также представители банков-эквайеров.

В результате был определен состав Рабочей группы, а также систематизированы полученные комментарии и правки.

ABISS
НП «АБИСС»

СОСТАВ РАБОЧЕЙ ГРУППЫ

В рабочую группу вошли эксперты из следующих организаций:

- Банк России;
- НП «АБИСС»;
- ЗАО НИП «ИНФОРМЗАЩИТА»;
- Trustwave Holdings, Inc.;
- ООО «Дейтерий»;
- ЗАО «Андэк»;
- ОАО «Промсвязьбанк»;
- ОАО Банк «Возрождение».

ABISS
НП «АБИСС»

ИТОГИ ЗАСЕДАНИЯ РАБОЧЕЙ ГРУППЫ

По итогам заседания были сформулированы общие комментарии и правки ко всему комплекту документов (PCI DSS), а также детальный перечень замечаний к файлам:

- Стандарт безопасности данных индустрии платежных карт (PCI DSS) Версия 2.0;
- Стандарт безопасности данных индустрии платежных карт (DSS).Стандарт безопасности данных платежных приложений (PA-DSS) Глоссарий. Основные определения, аббревиатуры и сокращения. Версия 2.0.

В завершении заседания рабочей группой был принят дальнейший план по проведению процедур согласования перевода Стандарта безопасности данных индустрии платежных карт (PCI DSS) и сопутствующих документов на русский язык и взаимодействия с PCI Council. Протокол заседания рабочей группы, а также сводные таблицы с правками и комментариями были направлены на рассмотрение в PCI Council, который внес соответствующие изменения в перевод всех документов.

ABISS
НП «АБИСС»

ПЛАНЫ РАЗВИТИЯ СТАНДАРТОВ (по информации PCI Council)

В 2012 году PCI Council получил более 200 комментариев по следующим направлениям (в порядке убывания):

- Изменения текущих требований и тестовых процедур;
- Прояснение положений стандартов;
- Необходимость разработки дополнительных руководств с рекомендациями;
- Только комментарии без требований изменений стандартов;
- Необходимость разработки новых требований/тестовых процедур.

PCI Council учитывает поступающие комментарии в процессе разработки новых версий стандартов.

ABISS
НП «АБИСС»

ДЕТАЛЬНЫЕ КОММЕНТАРИИ ПО РАЗВИТИЮ СТАНДАРТОВ (по информации PCI Council)

Предметная область	Предложения
Требование 11.2	Обязать ASV-компании проводить внутреннее сканирование. Привести перечень конкретного ПО, а также дать определение понятию “существенного изменения сети”
Scope of Assessment	Дать детальное руководству по определению и сегментации области оценки
Требование 12.8	Прояснить термины “service provider” и “shared” и дать более конкретные требования в отношении договоров с поставщиками услуг
SAQs	Рассмотреть возможность обновления SAQs; они или слишком сложны для понимания, или недостаточно детализированы

ABISS
НП «АБИСС»

ДЕТАЛЬНЫЕ КОММЕНТАРИИ ПО РАЗВИТИЮ СТАНДАРТОВ (по информации PCI Council)

Предметная область	Предложения
Требование 3.4	Вопросы управления ключами и криптозащиты - достаточно сложны. Дать больше разъяснений и рекомендаций
Требование 8.5	Обновить требования в отношении парольной защиты
Требования PA-DSS	Разработать дополнительные требования PA-DSS для различных технологий (mobile, EMV, tokenization)
PA-DSS Program	Усовершенствовать процедуры в отношении PA-QSA
PA-DSS scope/eligibility	Расширить применимость PA-DSS в отношение неплатежных приложений, приложений разработанных на заказ, платежных терминалов и т.п.

ABISS
НП «АБИСС»

ПЛАНЫ РЕАГИРОВАНИЯ НА КОММЕНТАРИИ (по информации PCI Council)

1. Комментарии проанализированы и категорированы (апрель-август 2012)
2. Полученные комментарии доведены до Сообщества PCI (сентябрь 2012)
3. Комментарии презентованы на Конференциях Сообщества PCI (сентябрь-октябрь 2012)
4. Подготовка проектов обновлений стандартов PCI-DSS и PA-DSS (ноябрь 2012-апрель 2013)
5. Подготовка финальных версий (май-июль 2013)
6. Публикация новых версий стандартов (октябрь 2013)

ABISS
НП «АБИСС»

РЕЗЮМЕ ПО ОБНОВЛЕНИЯМ СТАНДАРТОВ (по информации PCI Council)

- Техническая рабочая группа PCI Council анализирует полученные комментарии и определяет, что будет включено в новые версии стандартов
- Большинство специалистов в целом удовлетворены стандартами
- Большая часть рекомендаций - в отношении необходимости дополнительных разъяснений и руководств
- Когда тексты стандартов будут готовы, они будут доступны для окончательного анализа
- Публикация новых версий стандартов (октябрь 2013)

ABISS
НП «АБИСС»

ABISS
НП «АБИСС»

СПАСИБО ЗА ВНИМАНИЕ!

Некоммерческое партнерство
«Сообщество пользователей стандартов
по информационной безопасности АБИСС»

www.abiss.ru