Ассоциация Российских Банков

О системе требований к информационной безопасности Национальной системы платежных карт

Велигура Александр Николаевич

председатель комитета по банковской безопасности АРБ

«Информационная безопасность платежных систем. PCI DSS Russia 2016» 1 июня 2016 г.

Ассоциация Российских Банков

Общий взгляд

Стандарты обеспечения ИБ НСПК должны охватывать **не только вопросы обращения с платежными картами** и относящейся к ним информацией, но и регламентировать **процедуры и механизмы, обеспечивающие безопасность использования всей инфраструктуры**, включая меры обеспечения доверия к безопасности применяемых автоматизированных систем и приложений. Кроме того, иерархия требований стандартов должна охватывать и **технические меры защиты информации**.

Ассоциация Российских Банков

Область применения

- Инфраструктура НСПК
- Объекты среды
- Процессы, происходящие у участников НСПК: у разработчиков, в ТСП, у аудиторов, в органах по сертификации…
- Меры и средства защиты информации в НСПК
- Меры обеспечения доверия к безопасности, включая сертификацию, аудит, тестирование, мониторинг.

Ассоциация Российских Банков

Субъекты

Все участники НСПК, сервис-провайдеры, эквайеры, эмитенты, торгово-сервисные предприятия, разработчики автоматизированных систем и приложений, интеграторы, аудиторы, органы по сертификации и испытательные лаборатории (центры).

Ассоциация Российских Банков

Структура комплекса стандартов

1. Стандарт безопасности национальной системы платежных карт
2. Модель (модели) угроз
3. Стандарт безопасности обработки платежных карт и использования платежных приложений
4. Пакеты требований к объектам
5. Стандарт обеспечения доверия.

Ассоциация Российских Банков

Стандарт безопасности национальной системы платежных карт

Концептуально-организационный (как СТО БР 1.0, разделы 1-6.). Область действия. Структура системы стандартов. Их назначение и как применять. Общие принципы обеспечения ИБ в НСПК. Процессный подход, ролевая модель. Описание процессов. Использование пакетов требований по ИБ к объектам как основа для проведения их сертификации. Применение мер контроля, в т.ч. аудитов, их периодичность, какая для кого и т.п...

Ассоциация Российских Банков

Модель (модели) угроз

Утвержденная модель угроз НСПК (далее – Главная модель угроз, ГМУ).

Частные модели для объектов (типов объектов) как проекции угроз из ГМУ плюс детализация и их актуальность на разных стадиях жизненного цикла.

Ассоциация Российских Банков

Стандарт безопасности обработки платежных карт и использования платежных приложений

Обеспечение ИБ при обработке платежей в НСПК, в том числе с использованием карт МИР. Его прототипы – PCI DSS и PA DSS. Вопросы контроля (аудит, пен-тесты и т.п.) предлагается вынести в отдельный документ (стандарт).

Ассоциация Российских Банков

Состав пакета требований к объектам

1. Идентификатор объекта и его доменов (сегментов).
2. Описание объекта, его предназначения и основных характеристик безопасности.
3. Требования соответствия (ссылки на действующие нормативные требования, положения, организационно-распорядительные документы, ГМУ и т.п.).
4. Частная модель угроз (для объекта).
5. Функциональные цели безопасности и цели доверия к безопасности. Обоснование целей безопасности.
6. Требования безопасности:
   а) функциональные требования – применительно к угрозам на некотором стандартизированном языке, для стадий ЖЦ
   б) требования доверия – описание того, каким образом должно быть получена уверенность в том, что объект удовлетворяет функциональным требованиям (здесь, например, пен-тесты, аудит и мониторинг) – также на стадиях ЖЦ.
7. Метрики степени выполнения требований.
8. Меры и механизмы безопасности (управленческие, организационные и технические).
9. Описание того, каким образом объект на практике удовлетворяет требованиям
10. Для доменов – подпакет сходной структуры.

Ассоциация Российских Банков

Состав типового пакета требований к объектам

1. Идентификатор объекта и его доменов (сегментов).
2. Описание объекта, его предназначения и основных характеристик безопасности.
3. Требования соответствия (ссылки на действующие нормативные требования, положения, организационно-распорядительные документы, ГМУ и т.п.).
4. Частная модель угроз (для объекта).
5. Функциональные цели безопасности и цели доверия к безопасности. Обоснование целей безопасности.
6. Требования безопасности:
   а) функциональные требования – применительно к угрозам на некотором стандартизированном языке,
   б) требования доверия – описание того, каким образом должно быть получена уверенность в том, что объект удовлетворяет функциональным требованиям (здесь, например, пен-тесты, аудит и мониторинг).
7. Метрики степени выполнения требований.
8. Меры и механизмы безопасности (управленческие, организационные и технические).
9. Для доменов – подпакет сходной структуры.

Ассоциация Российских Банков

Стандарт обеспечения доверия

Процедуры аудита, оценки соответствия, формы аудита, пен-тесты, сканирование.

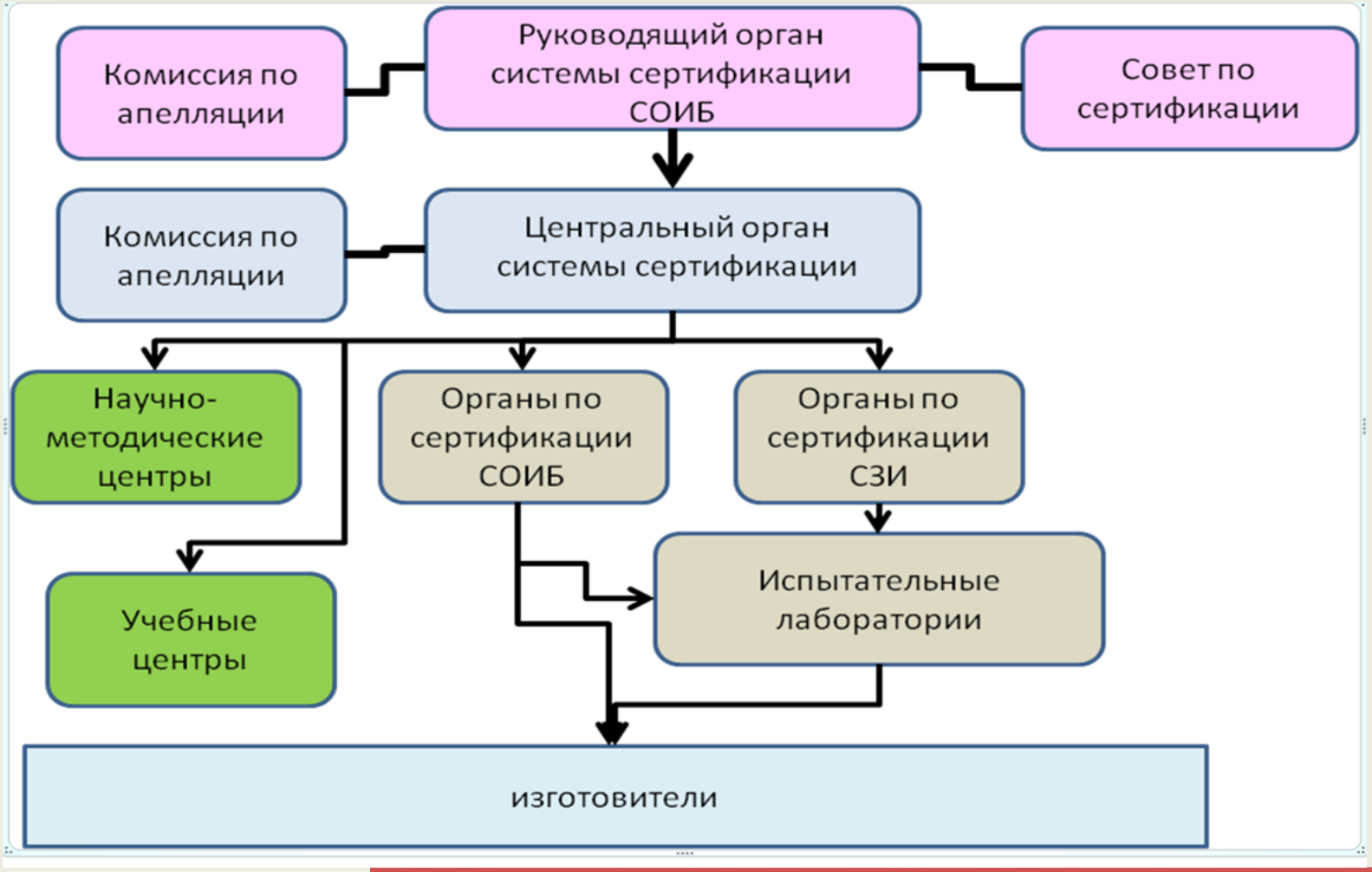
Вид и форма результатов. Использование результатов в дальнейшем.

Процедуры и частота их проведения включается в пакеты требований как требования доверия

Требования к компании-аудитору и к лицам-аудиторам. Процедуры контроля аудиторов (Возможно, это лучше включить в основной Стандарт).

Ассоциация Российских Банков

Система подтверждения соответствия (сертификации)



Спасибо за внимание!

Велигура Александр Николаевич

Председатель комитета
по банковской безопасности
Ассоциации российских банков

Заместитель генерального директора
ООО Андэк Консалтинг

Москва, ул.Городская, д.8
Телефон:+7 (495) 984-60-40
E-mail: a.veligura@andekconsult.ru

«Информационная безопасность платежных систем.
PCI DSS Russia 2016» 1 июня 2016 г.