СТБ 34.101.27++: обновление требований к СКЗИ

IT Security Conference

[Минск, 31.03.2017]

1: Криптографическая инфраструктура

ГосСУОК

(единая система управления открытыми ключами)

МСИ, Id-карта

(универсальная идентификация и аутентификация)

СТБ 34.101.bias: топология, объекты, протоколы, интерфейсы, форматы

форматы криптографических данных	службы	общие требования	прикладные протоколы
сертификаты открытых ключей, CMS, OCSP, **идентификаторы**, **XML DSig/Enc**, атрибутные сертификаты, **расширенные ЭЦП**	**штампов времени, заверения данных**	СКЗИ (в т.ч. аппаратные)	протокол TLS 1.2 с дополнительными криптонаборами
СТБ 34.101.17,19,23,26,**50**,67, **ades**	**СТБ 34.101.ts** **СТБ 34.101.dvcs**	СТБ 34.101.27	СТБ 34.101.65

криптографические алгоритмы и протоколы											
шифрование (формат, дисковое)	имитозащита	хэширование	ЭЦП	транспорт	HMAC	PRNG	**OTP**	разделение секрета	формирование общего ключа, аутентификация	хэширование	древовидное хэш-ие шифрование имитозащита защита сеансов
СТБ 34.101.31			СТБ 34.101.45		СТБ 34.**101.47**			СТБ 34.101.60	СТБ 34.101.66	СТБ 34.101.77	

2: Требования к СКЗИ

СТБ 34.101.27	СТБ П 34.101.43
программные средства	аппаратные средства
просто требования	профиль защиты
стандарт	предстандарт
ФС	ЗБ
испытания	оценка

3: Требование как компромисс

Требование — это компромисс между заказчиком, разработчиком и экспертом

Заказчик заинтересован в ужесточении требований

Разработчик заинтересован в реализуемости требований

Эксперту важна проверяемость требований

Потребитель?

4: Требование (пример)

Требование 1. ГСЧ, который используется для построения ключей, должен выдавать непредсказуемые последовательности битов.

Требование 1а. ГСЧ должен выдавать реализации независимых случайных величин с равномерным распределением на $\{0, 1\}$.

Требование 2. ГСЧ должен строить выходные последовательности по данным от источников случайности, для которых построена физическая модель и теоретически оценена удельная энтропия (уровень непредсказуемости).

Требование 3. ГСЧ должен строить выходные последовательности по данным от источников случайности, для которых оценена (теоретически или экспериментально) удельная энтропия. Уровень накопленной энтропии должен соответствовать длине выходной последовательности. При обработке данных от источников случайности должны использоваться криптографические преобразования.

5: Общий план

- СТБ 34.101.27 += аппаратные СКЗИ
- СТБ 34.101.27 += новые уровни (классы)
- СТБ 34.101.27 += новые требования (пакеты)
- СТБ 34.101.27 $\rightarrow$ корректировка требований

6: Разработка

https://github.com/bcrypto/stb/34.101.27

7: Сколько должно быть уровней?

Уровень 1: базовый

Уровень 2: усиленный

Уровень 3: аппаратная защита

Уровень 4: повышенные гарантии

8: Нужны ли нам пакеты?

Пакет = набор консолидированных требований

- аудит
- обновление программ
- очистка перед выводом из эксплуатации
- защита каналов

9: Самотестирование: можно ли упростить?

Проблема: алгоритмов может быть много, аппаратных компонент может быть много

Нужно тестировать все алгоритмы на всех компонентах?

10: Защита ключей верхнего уровня

Проблема: КШД можно защитить на КШК, КШК на МК, но как защитить МК?

Текущие требования: аппаратная защита (смарт-карта) или разделение секрета

Вопрос: можно ли разрешить защиту МК оргмерами? («сам виноват»)

11: Требования к криптографическим программам?

- не должно быть бесконечных циклов
- не должно быть недостижимых участков кода
- не должно быть сравнений операндов с плавающей точкой

Статические анализаторы?

12: Считать программу управления аппаратным СКЗИ частью СКЗИ или нет?

Стандартный сценарий: аппаратный токен + программа управления

13: Как оценивать ключевые системы?

Ключевая система – часть ФС?

Или ключевая система оценивается отдельно?

Нужно ли ввести требования к ключевым системам (напр., защита от «чтения назад»)?

14: Атрибуты средства

Вопрос: программа хэширует документ и передает его средству ЭЦП на подпись. Является ли программа средством КЗИ?

С одной стороны, в программе реализован криптографический алгоритм хэширования. С другой стороны, программа не работает с ключами, выполняет, по сути, функции посредника.

15: Полнота покрытия тестами?

Автоматические инструменты?

100%?

Fuzzy для форматов?