ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ НАЦИОНАЛЬНОЙ СТАНДАРТИЗАЦИИ В ОБЛАСТИ КРИПТОГРАФИИ

Владимир Бельский, НПК «Криптонит»

Иван Чижов, МГУ имени М.В. Ломоносова, НПК «Криптонит»

Василий Шишкин, НПК «Криптонит»

КРИПТОНИТ

ЭВОЛЮЦИЯ СИСТЕМЫ НАЦИОНАЛЬНЫХ СТАНДАРТОВ

КРИПТОНИТ

1

2011 год

- 3 криптографических стандарта

2

2012-2015 года

- 4 основных криптографических стандарта

3

2022 год

- около четырёх десятков утверждённых документов, более сотни механизмов

ЭВОЛЮЦИЯ СИСТЕМЫ НАЦИОНАЛЬНЫХ СТАНДАРТОВ

КРИПТОНИТ

1

2011 год

- 3 криптографических стандарта

2

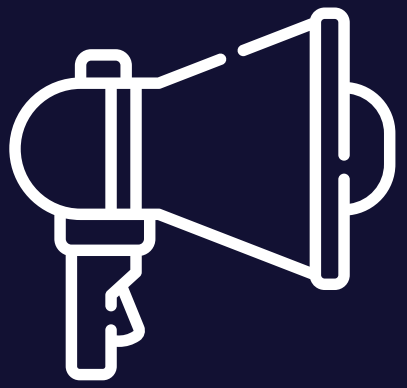
2012-2015 года

- 4 основных криптографических стандарта

3

2022 год

- около четырёх десятков утверждённых документов, более сотни механизмов



Конец истории?

КУДА ДВИГАТЬСЯ ДАЛЬШЕ?

КРИПТОНИТ

Национальные задачи

Электронное голосование

Цифровые валюты и РР

Мобильная связь

Защита персональных данных

Международные тенденции

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

IETF

ITU

3GPP

GSMA

МЕЖДУНАРОДНЫЕ ТЕНДЕНЦИИ

КРИПТОНИТ

Постквантовые механизмы на основе
- функций хэширования
- теории кодов, исправляющих ошибки
- теории решёток
- изогений

Блочные шифры с параметром
- собственно шифры
- режимы работы
- механизмы аутентификации

Низкоресурсные механизмы
- блочные шифры
- функции хэширования
- механизмы аутентификации (включая AEAD)

Различные виды подписи
- анонимная подпись
- слепая подпись
- групповая подпись
- редактируемая подпись

И многое другое
- разделение секрета
- совместные вычисления (MPC)
- шифрование, сохраняющее формат
- гомоморфное шифрование

НАЦИОНАЛЬНЫЕ ЗАДАЧИ

КРИПТОНИТ

Электронное голосование

- гомоморфное шифрование (частичное)
- доказательства знания без разглашения
- слепая подпись

Цифровые валюты и PP

- гомоморфное шифрование
- доказательства знания без разглашения
- групповая подпись
- гомоморфная подпись

Мобильная связь

- низкоресурсные механизмы
- блочные шифры с параметром
- механизмы аутентификации (включая AEAD)

Защита персональных данных

- гомоморфные шифрование
- гомоморфная подпись
- механизмы аутентификации

Постквантовые механизмы

- подпись
- выработка общего ключа по незащищённому каналу
- гомоморфные механизмы

ИТАК…

Останавливаться нельзя, но нужно расставить приоритеты

- слепая подпись
- гомоморфное шифрование
- доказательства знания без разглашения
- низкоресурсные блочные шифры, функции хэширования, механизмы аутентификации
- постквантовые механизмы

КРИПТОНИТ

ОСТАНОВИТЬСЯ/ ПРОДОЛЖАТЬ/ УСКОРЯТЬСЯ ?

ВЫСОКАЯ ТРУДОЁМКОСТЬ ЭКСПЕРТИЗЫ

делегирование части полномочий

«ОПЕРЕЖАЮЩАЯ» СТАНДАРТИЗАЦИЯ

ускорение внедрения новых технологий

ФОРМИРОВАНИЕ ОБЩЕЙ ТЕРМИНОЛОГИ