ТК26 – в авангарде стандартизации. Уже 10 лет

Алексей Уривский, *ТК 26*

Технический комитет 26 «Криптографическая защита информации»

Приказ о создании – 28 декабря 2007

Основная решаемая задача - организация разработки и экспертизы проектов национальных, межгосударственных и международных **стандартов** шифровальных (криптографических) средств защиты информации

Организаций-членов – более 70

Подкомитетов – 4, рабочих групп – 9

Заседания 2 раза в год – апрель и ноябрь

Национальная стандартизация

ГОСТ Р 34.10-2012
Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11-2012
Функция хэширования

ГОСТ Р 34.12-2015
Блочные шифры

ГОСТ Р 34.13-2015
Режимы работы блочных шифров

Национальная стандартизация

Р 50.1.110-2016
Контейнер хранения ключей

Р 50.1.111-2016
Парольная защита ключевой информации

Р 50.1.112-2016
Транспортный ключевой контейнер

Р 50.1.113-2016
Сопутствующие криптографические алгоритмы

Р 50.1.114-2016
Параметры эллиптических кривых

Р 50.1.115-2016
Протокол выработки общего ключа с аутентификацией на основе пароля

Национальная стандартизация

Особенности

- ❑ уникальные разработки: не переиздания, не перевод;
- ❑ последовательное повышение статуса:

методические рекомендации ТК ->
рекомендации по стандартизации ->
национальный стандарт;

- ❑ криптографическая экспертиза

Планы 2017:

- ❑ 11 рекомендаций по стандартизации

Международная стандартизация

ISO/IEC JTC1/SC27/WG2

Cryptography and security mechanisms

ISO TC307

Blockchain and distributed ledger technologies

IETF

Crypto Forum Research Group

Международная стандартизация

ISO/IEC 14888-3 – EC-RDSA
ISO/IEC 10118-1 – Hash-function – General
ISO/IEC 10118-3 – Streebog (FDIS)
ISO/IEC 18033-3 – Kuznyechik (PDAM)

RFC 7791 – Cloning IKE v2 SA
RFC 7836 – Guidelines
RFC 8019 – IKE v2 protection vs. DDOS
RFC 8133 – SESPAKE
draft RFC – ACPKM

Научная деятельность

CTCrypt – ежегодный (с 2012 г.) симпозиум «Современные тенденции в криптографии»

Открытый конкурс научно-исследовательских работ Streebog (2013-2015 гг.):
18 работ, 20 рецензентов, 48 рецензий


Спасибо!