Об основных направлениях деятельности Технического комитета по стандартизации «Криптографическая защита информации

Лунин Анатолий Васильевич

GOST R Expert

зам. ответственного секретаря технического комитета по стандартизации «Криптографическая защита информации»

Национальная система стандартизации

Росстандарт

GOST R

Федеральное агентство по техническому регулированию и метрологии

Действует на основании Положения о Росстандарте, утвержденного Постановлением Правительства Российской Федерации от 17 июня 2004 г. № 294

Росстандарт

Среди его основных функций:

- реализация функций национального органа по стандартизации;
- осуществление госконтроля (надзора) за соблюдение обязательных требований стандартов;
- оказание государственных услуг в сфере стандартизации.

Росстандарт

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

Создан приказом Росстандарта
28 декабря 2007 г.

Росстандарт

Основная цель ТК26 – организация и проведение работ в области национальной, региональной и международной стандартизации шифровальных (криптографических) средств защиты информации, а также технических решений по их применению в информационно-телекоммуникационных системах и системах шифрованной, засекреченной и иных видов специальной связи.

Росстандарт

ТК26 уполномочен рассматривать вопросы стандартизации продукции и услуг, относящиеся к:

- методам шифрования (криптографического преобразования) информации;
- способам их реализации;
- методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись.

Росстандарт

В ТК 26 представлены органы и организации, к компетенции которых отнесена защита информации с использованием криптографических методов, имеющих опыт в организации разработок образцов шифровальных (криптографических) средств

ГОСТ Р

Российские (национальные) криптографические стандарты

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р

GOST R

Российские (национальные) криптографические стандарты

Пример неудачной попытки гармонизации

ГОСТ Р ИСО/МЭК 10116-93. Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования

ISO/IEC 10116: 2006, Modes of operation for an n-bit block cipher (3rd edition)

Международная система стандартизации

ISO (International Organization for Standardization)
ИСО (Международная организация по стандартизации)

Объединяет национальные системы стандартизации более 150 стран.

Каждая из стран представлена одним голосом.

Центральный Секретариат, координирующий деятельность в ИСО, расположен в Женеве, Швейцария.

Место в иерархии ИСО

JTC 1 - Information technology

JTC 1/SC 27 - IT Security techniques

JTC 1/SC 27/WG 2 - Cryptography and security mechanisms

ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

В 2007 г. компанией «**ИнфоТеКС**» было предложено подготовить **дополнение к стандарту *ISO/IEC 14888-3:2006(E)*** *«Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms»* **на основе *ГОСТ Р 34.10-2001*** *«Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»*

ISO International Organization for Standardization

ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

ISO/IEC 14888-3/Amd.1 Information technology – Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms. Amendment 1. Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm

Вступил в силу в июне 2010 г.

ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

Подготовка дополнения к стандарту **ISO 18033-3:2005** «Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers»
на основе ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

Проект внесен в ИСО в мае 2009 года
Идет работа

infotecs®

ТК 26 ГОСТ Р

Неправительственные системы стандартизации

ITU International Telecommunication Union

IETF®

RSA The Security Division of EMC

RSA
The Security Division of EMC

Расширение стандарта PKCS#11

Расширение стандарта *RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)* российскими криптографическими алгоритмами.

В 2009 г. опубликована новая версия PKCS #11 v2.30, включающая ГОСТ 28147-89 и другие российские алгоритмы.

RSA
The Security Division of EMC

Использование стандарта PKCS#15

Использование стандарта *RSA Security Inc. PKCS #15 Cryptographic Token Information Format Standard совместно с* российскими криптографическими алгоритмами.

Позволяет создать т.н. контейнер хранения ключей пользователя для получения госуслуг, например, при помощи универсальной электронной карты.

Документ уже проходит экспертизу в в/ч 43753.

Использование стандарта PKCS#12

Использование стандарта *RSA Security Inc. PKCS #12 Personal Information Exchange Syntax Standard совместно с* российскими криптографическими алгоритмами.

Позволяет создать т.н. транспортный контейнер ключей пользователя для организации получения госуслуг, например, при помощи универсальной электронной карты.

GOST R

Планы ТК26

Развитие системы криптографических стандартов

Предмет стандартизации	2010	2011-2012
Криптографическая функция хэширования, в том числе с длиной хэш-кода 512 бит	1 кв. – решение о стандартизации одной хэш-функции или семейства хэш-функций с переменной длиной хэш-кода 4 кв. – содержательная часть проекта стандарта	Разработка и утверждение нового стандарта ГОСТ Р 34.11 взамен ГОСТ Р 34.11-94
Схема электронной цифровой подписи с длиной подписи больше 512 бит	1 кв. – решение о стандартизации одной схемы или семейства схем с переменной длиной подписи 4 кв. – содержательная часть проекта дополнения к стандарту ГОСТ Р 34.10-2001	Разработка и утверждение изменений стандарта ГОСТ Р 34.10-2001

Развитие системы криптографических стандартов

Предмет стандартизации	2010	2011	2012	2013
Схема блочного шифрования с длиной блока 128 бит	Проект схемы	Независимые исследования проекта, разработка режимов шифрования	Содержательная часть проекта стандарта	
Рекомендации по выработке общего ключа		Проект рекомендаций	Независимые исследования проекта	Содержательная часть проекта стандарта
Алгоритм выработки псевдослучайной двоичной последователь-ности		Проект алгоритма	Независимые исследования проекта	Содержательная часть проекта стандарта

GOST R

Благодарю за внимание!

Лунин Анатолий Васильевич
ОАО «ИнфоТеКС»
GOST R Expert,
зам. ответственного секретаря технического комитета по стандартизации «Криптографическая защита информации»
Тел. +7 (495) 737 61 92
tc26@infotecs.ru
www.tc26.ru