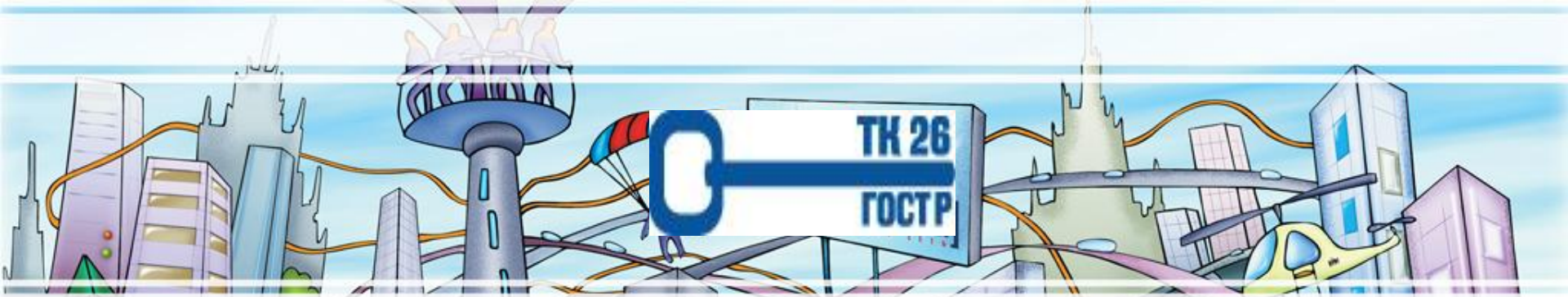
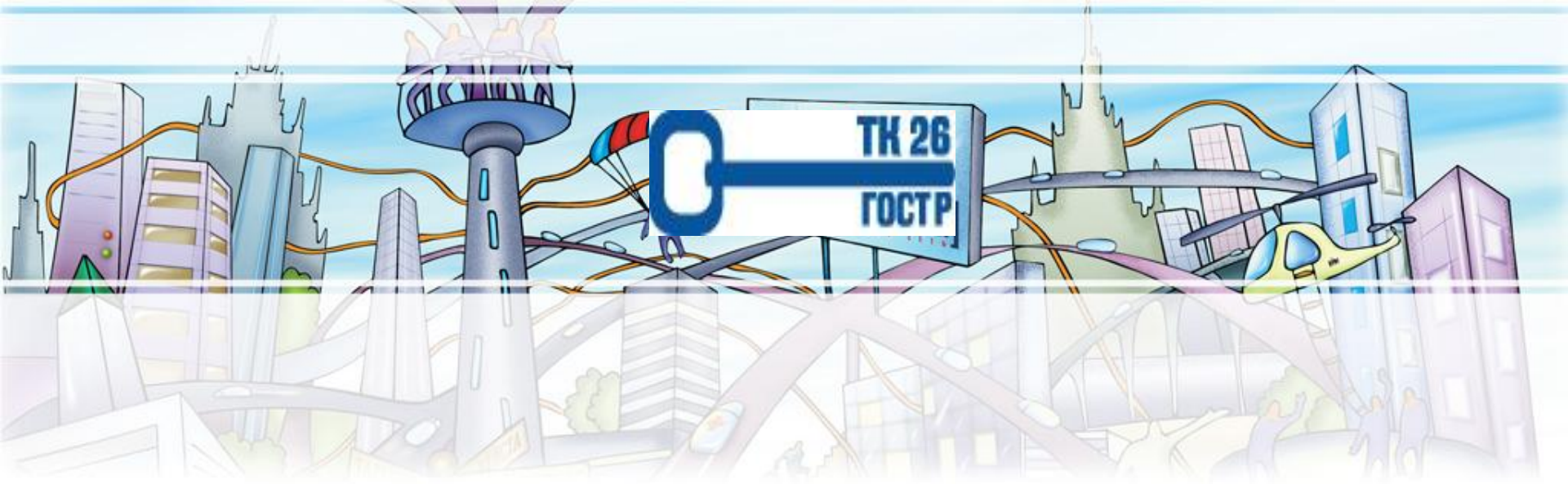


Об основных направлениях деятельности Технического комитета по стандартизации «Криптографическая защита информации

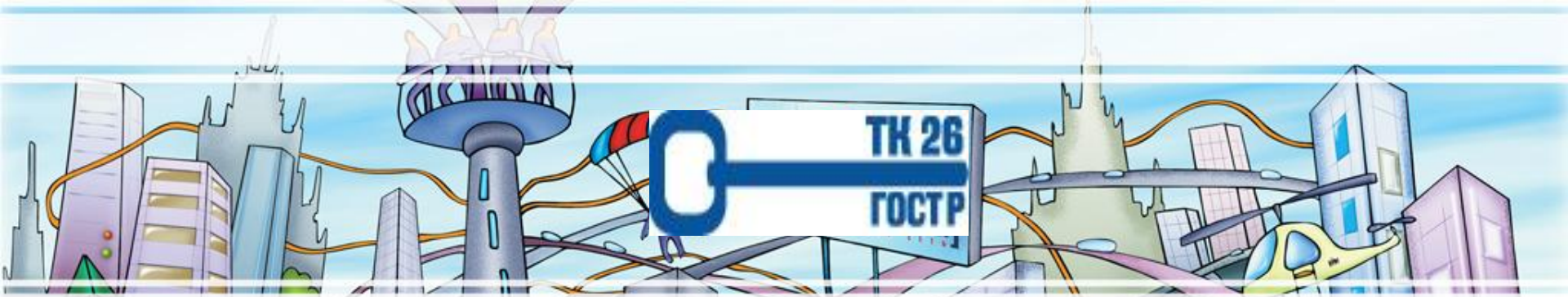
Лунин Анатолий Васильевич

GOST R Expert

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



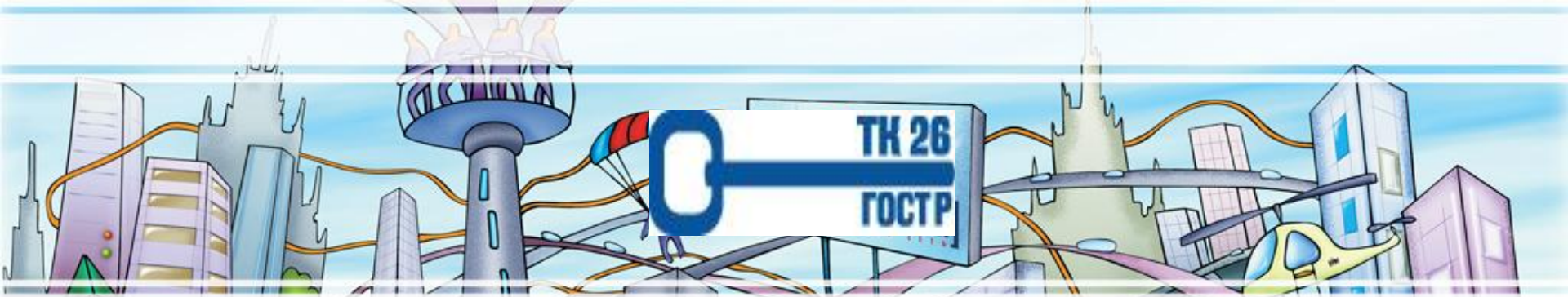
Национальная система стандартизации



Ростехрегулирование GOST R

Федеральное агентство по техническому регулированию и метрологии

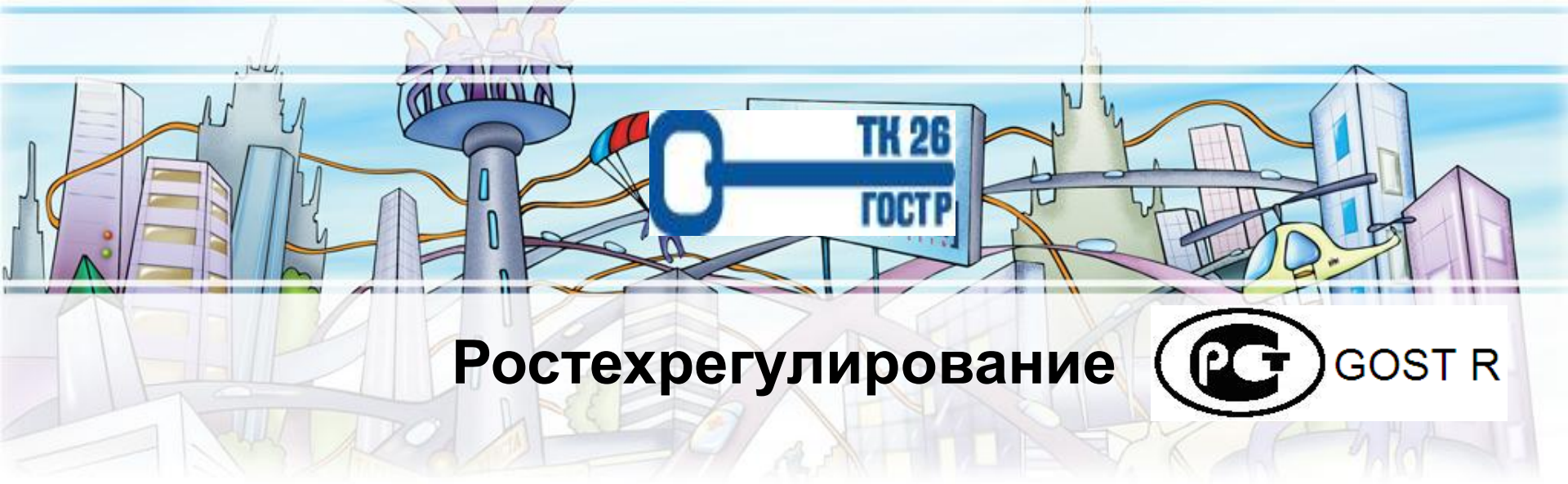
Действует на основании Положения о Ростехрегулировании, утвержденного Постановлением Правительства Российской Федерации от 17 июня 2004 г. № 294



Ростехрегулирование GOST R

Среди его основных функций:

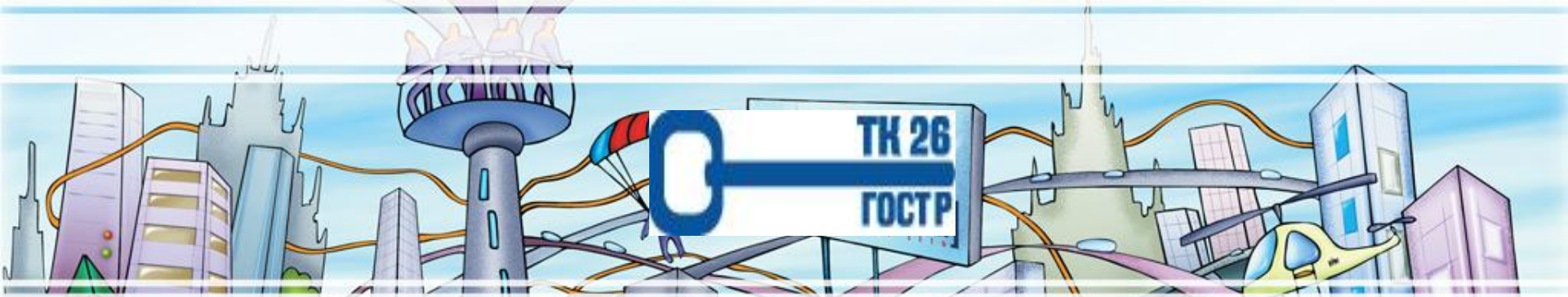
- реализация функций национального органа по стандартизации;
- осуществление госконтроля (надзора) за соблюдение обязательных требований стандартов;
- оказание государственных услуг в сфере стандартизации.



Ростехрегулирование GOST R

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

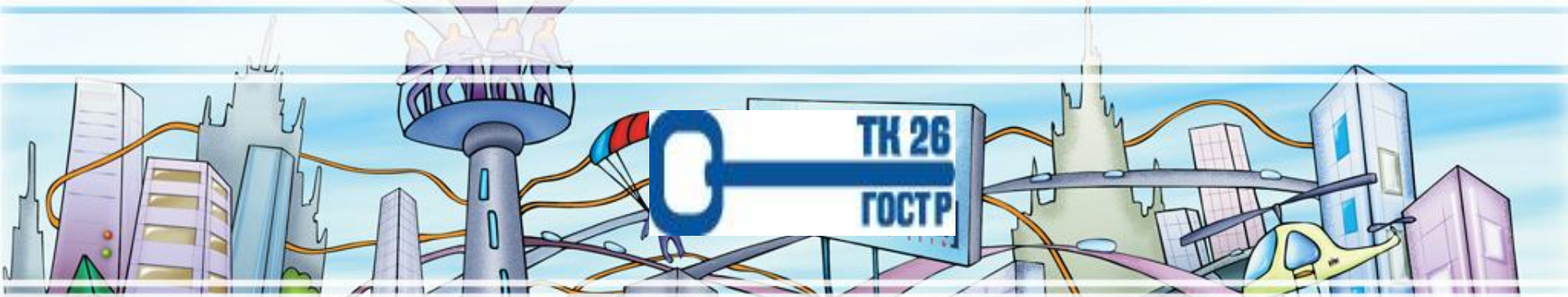
Создан приказом Ростехрегулирования
28 декабря 2007 г.



Ростехрегулирование GOST R

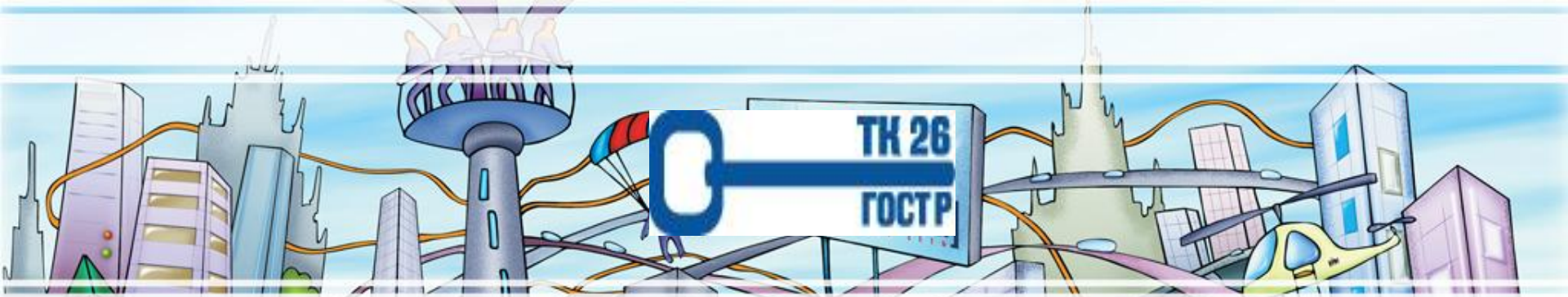
Организация, которой поручено ведение секретариата ТК 26 «Криптографическая защита информации» и его подкомитетов

Открытое акционерное общество «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)



Ростехрегулирование GOST R

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.

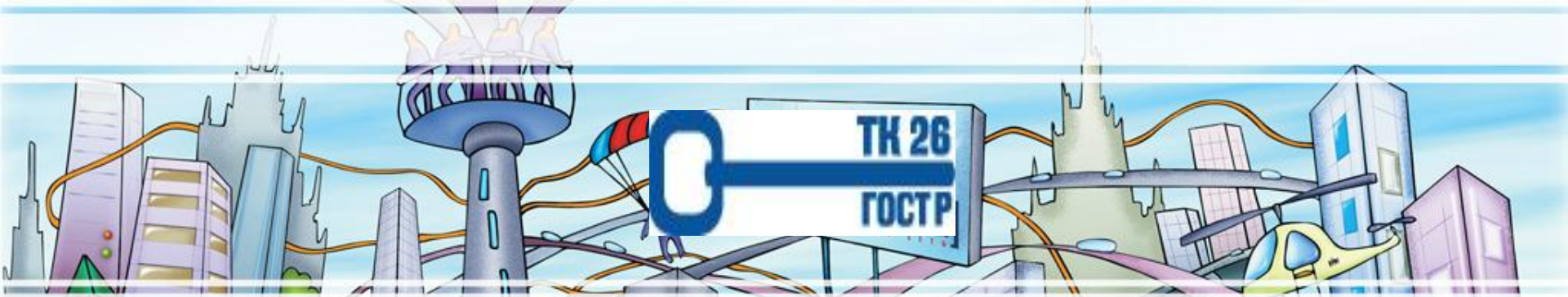


Ростехрегулирование

GOST R

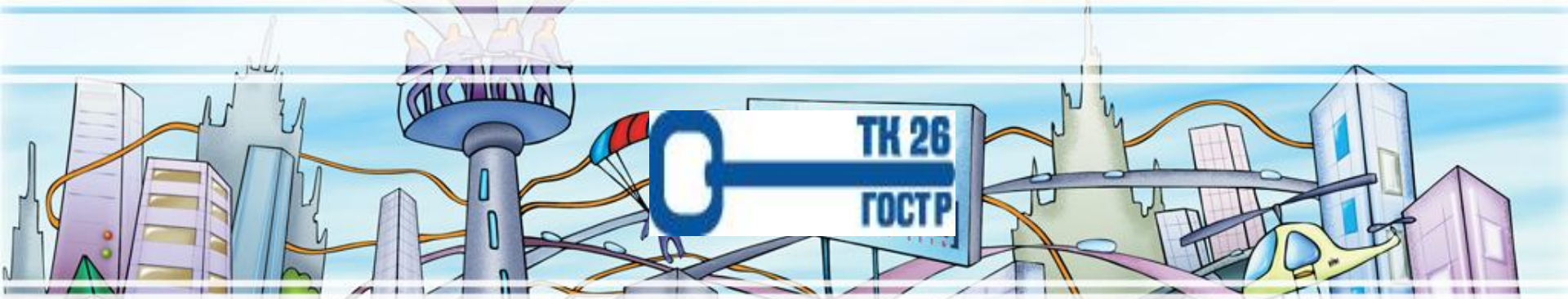
ТК26 уполномочен рассматривать вопросы стандартизации продукции и услуг, относящиеся к:

- 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.



Ростехрегулирование GOST R

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

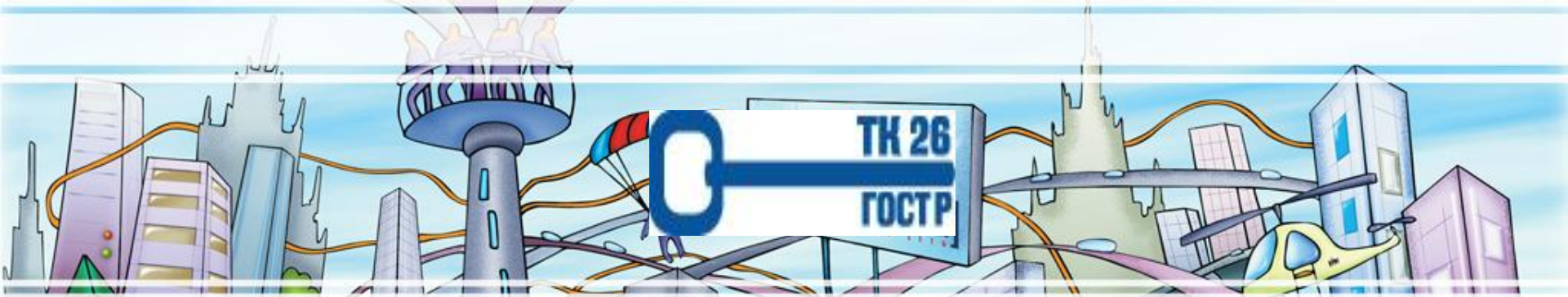


ГОСТ Р

GOST R

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

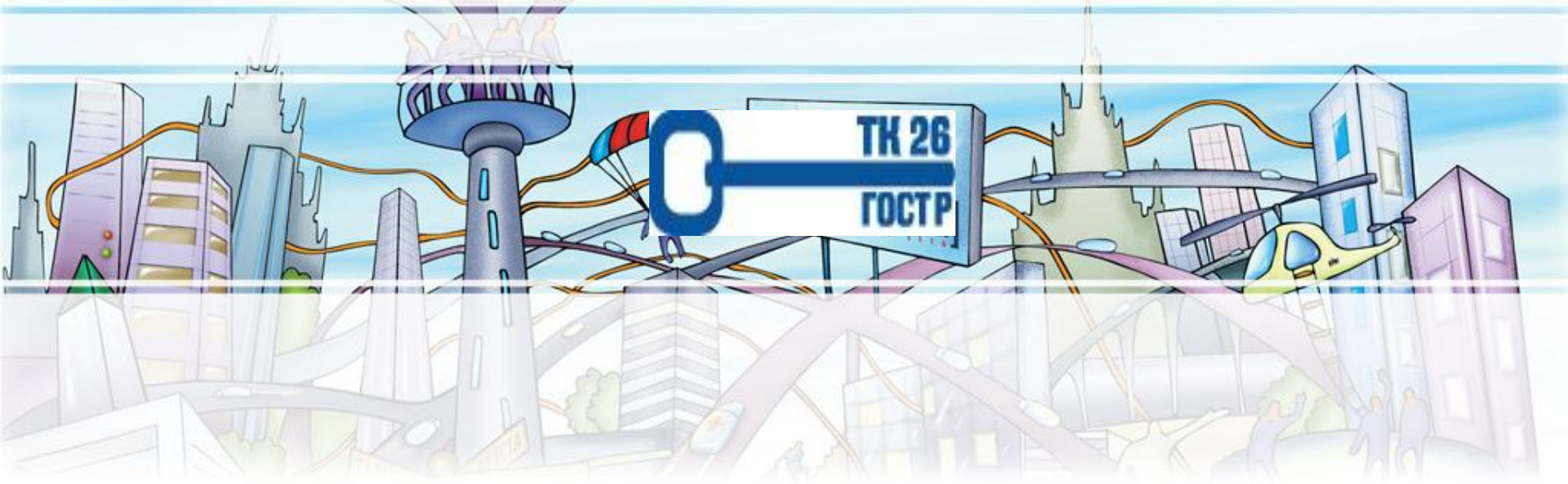
GOST R

Российские (национальные) криптографические стандарты

Пример неудачной попытки гармонизации

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

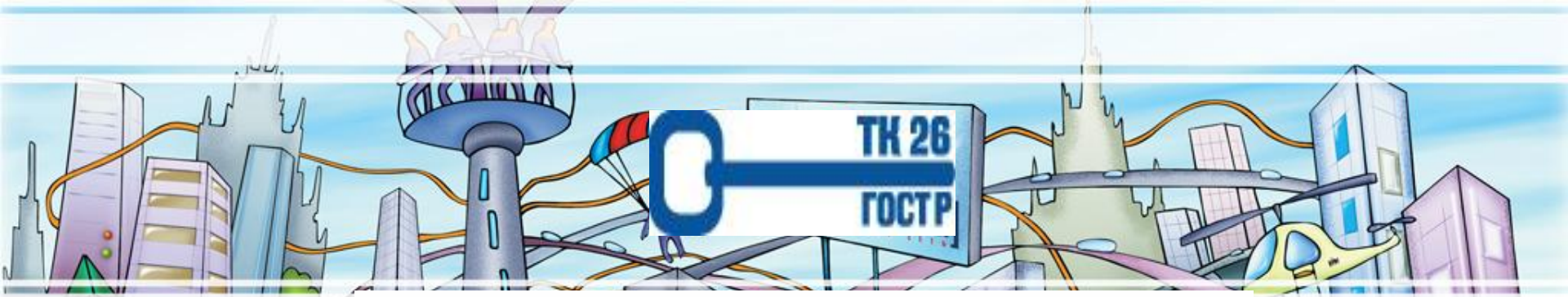
ISO/IEC 10116: 2006, Modes of operation for an n-bit block cipher (3rd edition)



Региональная система стандартизации

Об организации

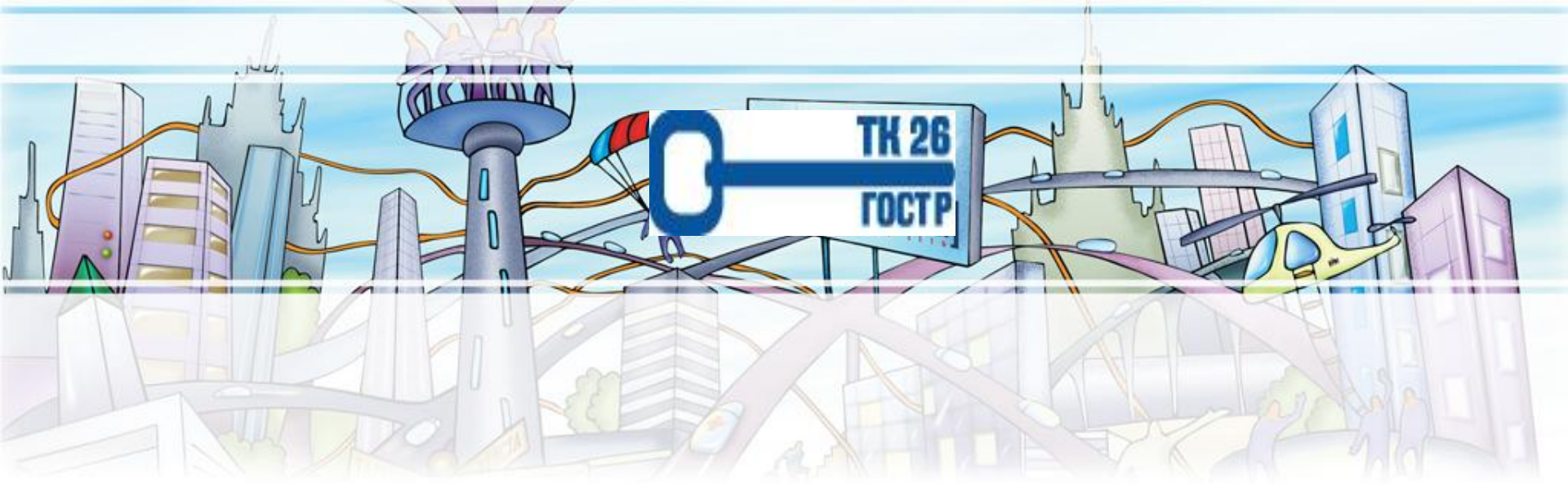
Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) Содружества Независимых Государств (СНГ) является межправительственным органом СНГ по формированию и проведению согласованной политики по стандартизации, метрологии и сертификации.



Межгосударственный Совет
по стандартизации, метрологии и сертификации

Международные (региональные) криптографические стандарты

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ 34.310-2002. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.



Международная система стандартизации

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

Объединяет национальные системы стандартизации 157 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»*

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

Идет финальное голосование

(до 10 мая 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 обсуждение

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

Подготовка дополнения к стандарту **ISO 10118-3:2004** «Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions»
на основе российского стандарта ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»

Проект внесен в ИСО в мае 2009 года

Проект отклонен

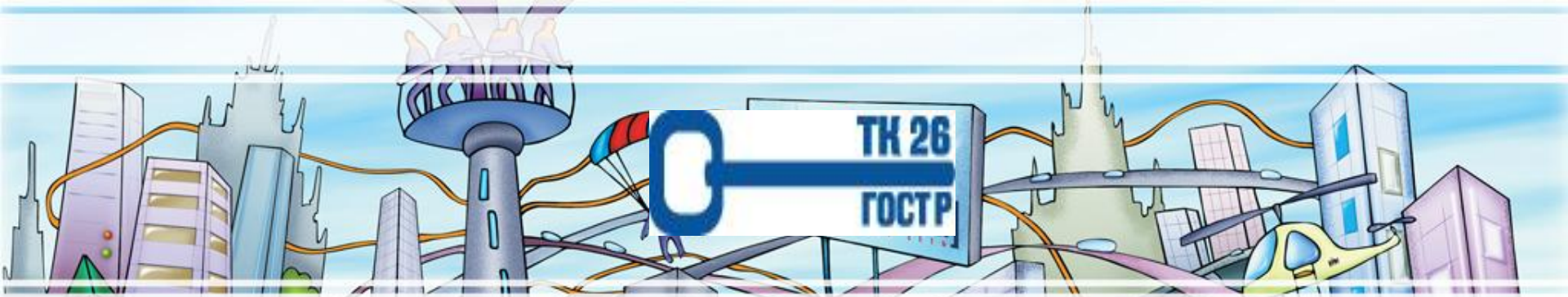
RSA Laboratories

Рабочая группа ТК26 завершила работы по расширению спецификации базового стандарта

•*PKCS#11: RSA Laboratories. Cryptographic Token Interface Standard*

механизмами и атрибутами российских криптографических алгоритмов.

Работа проводилась с согласия и в координации с RSA Security Lab (Magnus Nyström).



RSA

RSA Laboratories

PKCS #11 Mechanisms v2.30: Cryptoki – Draft 7

RSA Laboratories

29 July 2009

The draft Version 2.30 of the PKCS #11 specification is now available for 30-day public review.

В 2010 г. в IETF опубликованы документы

RFC 5830 «GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms»

RFC 5831 «GOST R 34.11-94: Hash Function Algorithm»

RFC 5832 «GOST R 34.10-2001: Digital Signature Algorithm»

в статусе *Informational*

These documents are intended to be a source of information about the Russian Federal standards.

Планы ТК26

GOST R

- Развитие системы криптографических стандартов.
- Применение российских криптографических алгоритмов:
  - в протоколах IPsec etc;
  - в TCG (Trusted Computing Group);
  - в DNSSec;
  - в схемах с одноразовыми паролями (OTP).

-Унификация форматов закрытых ключей в системах открытого распределения ключей.

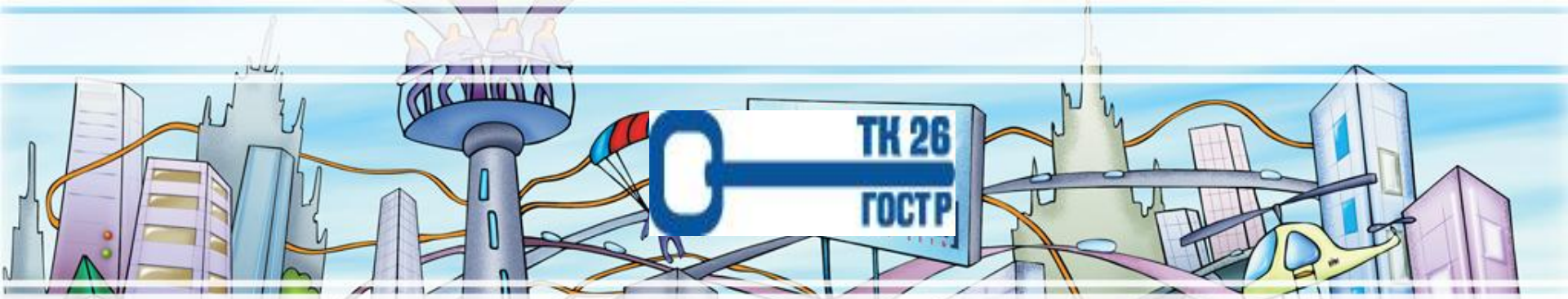
-Стандартизация криптографической защиты персональных данных.

Развитие системы криптографических стандартов

Предмет стандартизации	2008	2009	2010
Криптографическая функция хэширования, в том числе с длиной хэш-кода 512 бит	Проект хэш-функции с длиной хэш-кода 512 бит	Независимые исследования проекта	1 кв. – решение о стандартизации одной хэш-функции или семейства хэш-функций с переменной длиной хэш-кода 4 кв. – содержательная часть проекта стандарта
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

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