ТК 26
ГОСТ Р

Памяти Алексея Сергеевича Кузьмина посвящается

Стандартизация российских криптографических алгоритмов и протоколов на национальном, региональном и международном уровнях

Лунин Анатолий Васильевич

заместитель ответственного секретаря ТК26

Технический комитет по стандартизации (ТК26) «Криптографическая защита информации»

PKI-FORUM РОССИЯ

ПРИКАЗ

12 августа 2011 г. № 4402

г. Москва

О внесении изменений в приказ Федерального агентства по техническому регулированию и метрологии от 28 декабря 2007 г. № 3825дсп «О создании технического комитета по стандартизации «Криптографическая защита информации»

утвердить председателем ТК № 026 заместителя начальника Центра ФСБ России Кузьмина Алексея Сергеевича.

Руководитель
Федерального агентства Г.И. Элькин

ГОСТ – международные стандарты ИСО/МЭК

- **ISO/IEC 14888-3:2016** Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms

  (**ГОСТ 34.10-2012** Процессы формирования и проверки электронной цифровой подписи)
- **ISO/IEC DIS 10118-3** Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

  (**ГОСТ 34.11-2012** Функция хэширования)
- **Call for contribution** to the SC27/WG2 Study Period on “Inclusion of the block cipher Kuznyechik in ISO/IEC 18033-3”

  (**ГОСТ 34.12-2015** Блочные шифры)
- **ISO/IEC DIS 10116** Information technology -- Security techniques -- Modes of operation for an n-bit block cipher

  (**ГОСТ 34.13-2015** Режимы работы блочных шифров)

ГОСТ – международные стандарты

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

PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40 OASIS* Standard 14 April 2015

*OASIS (Organization for the Advancement of Structured Information Standards)

https://www.oasis-open.org/

ГОСТ – международные стандарты

PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40

2 Mechanisms

…

2.44 GOST 28147-89

2.45 GOST R 34.10-2001

2.44.9 GOST R 34.11-94

ГОСТ – международные рекомендации

IETF

RFC 5830 **GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms** Errata	2010-03	Informational RFC
RFC 6986 **GOST R 34.11-2012: Hash Function**	2013-08	Informational RFC
RFC 7091 **GOST R 34.10-2012: Digital Signature Algorithm**	2013-12	Informational RFC
RFC 7801 **GOST R 34.12-2015: Block Cipher "Kuznyechik"** Errata	2016-03	Informational RFC
RFC 7836 **Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012**	2016-03	Informational RFC

ГОСТ - Региональные стандарты стран СНГ

- ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
- ГОСТ 34.310-2004 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ 34.311-95 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ - национальные стандарты России

- ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
- ГОСТ 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования
- ГОСТ 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры
- ГОСТ 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(Росстандарт)

ПРИКАЗ

29 июня 2016 г. № 813

Москва

О внесении изменений в Программу национальной стандартизации на 2016 год, утвержденную приказом Федерального агентства по техническому регулированию и метрологии от 18 января 2016 г. № 18

11.	Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. Разработка Р
12.	Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов. Разработка Р
13.	Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля. Разработка Р
14.	Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации. Разработка Р
15.	Информационная технология. Криптографическая защита информации. Транспортный ключевой контейнер. Разработка Р
16.	Информационная технология. Криптографическая защита информации. Контейнер хранения ключей. Разработка Р

Предлагаемые сроки завершения этапов работ (месяц, год), установленные ПНС на 2016 год			
направление уведомления о начале разработки	представление окончательной редакции	направление в МГС	утверждение документа
11.2014	08.2016	-	11.2016

ГОСТ – методические документы ТК26

- Идентификаторы объектов (OID) технического комитета по стандартизации "Криптографическая защита информации" (ТК 26)
- Ключевой контейнер (дополнение к PKCS#15) версия 1.0
- Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89
- Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012
- Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)
- Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 И ГОСТ Р 34.10 в криптографических сообщениях формата CMS

ГОСТ – проекты методических документов ТК26

- Парольная защита с использованием алгоритмов ГОСТ (дополнения к PKCS#5) версия 2.1
- Транспортный ключевой контейнер (дополнения к PKCS#8 и PKCS#12) версия 2.1
- Ключевой контейнер (дополнение к PKCS#15) версия 2.0
- Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012
- Техническая спецификация Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 3411 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509

ГОСТ – проекты методических документов ТК26

- Техническая спецификация Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPSEC ESP
- Техническая спецификация Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE и ISAKMP
- Техническая спецификация Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP
- Техническая спецификация Использование ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPSEC и ESP
- Техническая спецификация Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015

ГОСТ – национальная ветка объектных идентификаторов

Value	*Name*	*Comment*
1.2.643.7.1	id-tc26	корень ТК 26 в российском сегменте мирового пространства идентификаторов объектов
1.2.643.7.1.0	modules	Asn.1 модули ТК 26
1.2.643.7.1.0.1	gostR3410-2012-ParamSetSyntax	Asn.1 модуль синтаксиса параметров
1.2.643.7.1.0.2	gostR3410-2012-PKISyntax	Asn.1 модуль синтаксиса ключей
1.2.643.7.1.0.3	gostR3410-2012-SignatureSyntax	Asn.1 модуль синтаксиса подписи
…	…	…

Анкетные данные

- **ФИО:**
  Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)
- **Дата и место рождения:**
  28 декабря 2007 года, город Москва
- **Родители:**
  Росстандарт, ФСБ России
- **Статус:**
  форма сотрудничества физических и юридических лиц на добровольной основе
- **Адрес:**
  tc26.ru, 127287, Москва, Старый Петровско-Разумовский проезд, 1/23, стр. 1, офис ОАО «ИнфоТеКС», тел./факс: (495)737-6192/7278

- секретариат ТК 26:
  tc26@tc26.ru
- авторы:
  matyukhin_dv@tc26.ru, serikov_ia@tc26.ru

Анкетные данные (продолжение)

- Род занятий:
  - организация разработки и экспертизы проектов национальных, межгосударственных и международных стандартов
  - участие в работе ТК международных (межгосударственных) организаций по стандартизации, в том числе в целях принятия национальных стандартов РФ в качестве международных (межгосударственных)
  - подготовка предложений по разработке международных и межгосударственных стандартов и предложений относительно позиции РФ для голосования по проектам международных и межгосударственных организаций по стандартизации
- Место в рейтинге ТК (2015): 47 (из 265)

- секретариат ТК 26: tc26@tc26.ru
- авторы: matyukhin_dv@tc26.ru, serikov_ia@tc26.ru

ТК 26 в деталях: состав и структура

- председатель ( ), заместитель (И.Ф. Качалин), заместитель - ответственный секретарь (А.А. Чапчаев)
- 66 членов (20 государственных предприятий и организаций, 46 частных компаний), 2 компании в процессе вступления
- секретариат (ОАО «ИнфоТеКС»)
- 4 подкомитета
- временные рабочие группы (5 активно действующих в настоящее время)

В настоящее время готовятся приказы Росстандарта по структурной реорганизации ТК26 (в части руководства технического комитета и состава подкомитетов ТК).

ТК 26 в деталях: подкомитеты

- ПК 1 - криптографические механизмы для применения в поставляемых для федеральных государственных нужд шифровальных (криптографических) средствах защиты информации, содержащей сведения, составляющие государственную тайну
- ПК 2 - то же для сведений, относимых к охраняемой в соответствии с законодательством информации ограниченного доступа
- ПК 3 - криптографические механизмы в национальной платежной системе (новая планируемая сфера деятельности)
- ПК 4 - российские СКЗИ, не попадающие в сферу деятельности ПК 1 и ПК 2, а также зарубежные СКЗИ на территории Российской Федерации (новая планируемая сфера деятельности)

ТК 26
ГОСТ Р

Спасибо за внимание!
Вопросы?

Лунин Анатолий Васильевич
заместитель ответственного секретаря ТК26
заместитель генерального директора ОАО «ИнфоТеКС»
www.tc26.ru
lunin_av@tc26.ru
www.infotecs.ru
lunin@infotecs.ru

PKI-FORUM РОССИЯ