Всё, что вы хотели знать о ТК 26, но боялись спросить

Дмитрий Матюхин (ФСБ России),
Игорь Сериков (ТК 26)

РусКрипто’2016,
24 марта 2016 г.

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

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)

ТК 26 в деталях: состав и структура

- председатель (с 12.08.2011 - А.С. Кузьмин), 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)

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 в деталях: результаты

- обновлены все 4 национальных стандарта в области криптографической защиты информации
- 11 методических рекомендаций ТК: OID; ГОСТы в TLS, CMS, PKCS#5,8,12,15; подстановки ГОСТ 28147; эллиптические кривые ГОСТ Р 34.10; сопутствующие алгоритмы; протокол SESPAKE (тексты - tc26.ru/methods/recommendation/)
- схема ГОСТ Р 34.10-2012 - в ISO/IEC 14888-3
- вклад в пересмотр и экспертизу ещё 6 действующих стандартов ISO/IEC (10118-4,11770-3,15946-1,18031,18033-1,29192-5) и 1 постоянного документа (JTC 1/SC 27 SD12)
- ГОСТ 28147, Р 34.10, Р 34.11-94 - в PKCS#11
- 4 симпозиума CTCrypt (2012-2015)
- открытый конкурс работ по анализу хэш-функций ГОСТ Р 34.11-2012

ТК 26 в деталях: текущие проекты

- 1 проект рекомендаций по стандартизации (в завершающей стадии)
- 4 проекта методических рекомендаций ТК
- 6 проектов технических спецификаций ТК
- 2 проекта стандартов ISO/IEC (10118-1 - в завершающей стадии, 10118-3 - включение хэш-функций ГОСТ Р 34.11-2012)
- 2 проекта IETF RFC на основе методических рекомендаций ТК (1 в стадии RFC-EDITOR) и ещё 1 при участии (RFC-to-be 7801 - ГОСТ Р 34.12-2015 «Кузнечик»)
- V симпозиум «Современные тенденции в криптографии» (CTCrypt 2016, Ярославль, 6-8 июня)

Проекты методических рекомендаций-2016

- использование блочных шифров и их режимов
- алгоритмы выработки псевдослучайных последовательностей
- схемы аутентифицированной выработки общего ключа двумя абонентами по открытому каналу

Проекты методических рекомендаций-2017+

- алгоритмы выработки производных ключей
- режимы блочных шифров, обеспечивающие одновременно шифрование и аутентификацию
- древовидное хэширование
- режимы блочных шифров, обеспечивающие шифрование статических данных

Также в планах на 2016-2017 гг. - начать процесс включения ГОСТ Р 34.12-2015 «Кузнечик» в ISO/IEC 18033-3

ТК 26 в деталях: как представить проект

«Порядок оформления документов, содержащих проекты методических рекомендаций по вопросам, относящимся к стандартизации в области криптографической защиты информации»

- утверждён председателем ТК 12 октября 2014 г.
- опубликован на сайте ТК (tc26.ru/methods/)
- основные положения:
  - в качестве проекта национального стандарта могут быть рассмотрены только соответствующие методические рекомендации ТК 26 по истечении не менее 6 месяцев с момента ввода их в действие
  - заявка на рассмотрение проекта методических рекомендаций должна содержать результаты криптографических исследований и обоснование криптографических качеств предлагаемого решения

ТК 26 в деталях: как вступить

На паритетных началах и добровольной основе включаются полномочные представители соответствующих подразделений организаций:

- к компетенции которых отнесена защита информации с использованием криптографических методов
- имеющих опыт в организации разработок образцов шифровальных (криптографических) средств, прошедших сертификацию по требованиям ФСБ России
- имеющих лицензию ФСБ России на право:
  - проведения работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации
  - занятия одним из видов деятельности, связанных с шифровальными (криптографическими) средствами

Остались вопросы?

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