Технический комитет по стандартизации
«Криптографическая защита информации» ТК 26

Национальная и международная стандартизация российских криптографических алгоритмов

Маршалко Г.Б.

ТК 26: направления деятельности

- **Национальная стандартизация**
  - **Криптографические стандарты**
  - **Методические рекомендации**
- **Международная стандартизация**
  - **Участие в работе ISO/IEC JTC 1/SC 27/WG 2**
- **Научное сопровождение работ по стандартизации**
  - **мини-симпозиум CTCrypt**

ТК 26: Национальная стандартизация. Стандарты

- **2012 год. Обновление стандартов:**
  - **ГОСТ Р 34.11-2012**
  - **ГОСТ Р 34.10-2012**

- **2014 год: Открытое обсуждение**
  - **проекта обновленного стандарта, определяющего блочный шифр: ГОСТ 28147-89 + «Кузнечик»**
  - **проекта стандарта, определяющего режимы работы блочных шифров:**

ECB+CTR+OFB+CBC+CFB+MAC

ТК 26: Национальная стандартизация. Рекомендации

- **Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11**
- **в профиле сертификата и списке отзыва сертификатов (CRL)**
- **инфраструктуры открытых ключей X.509**
- **Криптографические алгоритмы, сопутствующие применению**
- **стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012**
- **Задание узлов замены блока подстановок**
- **алгоритма шифрования ГОСТ 28147-89**
- **Задание параметров эллиптических кривых в**
- **соответствии с ГОСТ Р 34.10-2012**
- **Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11**
- **и ГОСТ Р 34.10 в криптографических сообщениях формата CMS**
- **Использование наборов алгоритмов шифрования на основе**
- **ГОСТ 28147-89 для протокола безопасности транспортного**
- **уровня (TLS)**
- **Использование ГОСТ 28147-89 при шифровании вложений в**
- **протоколе IPSEC ESP**

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Российские алгоритмы

- **2010 год: Российский стандарт ЭП включен в соответствующий международный стандарт ГОСТ Р 34.10-2012 = > ISO/IEC 14888-3**

- **2014 год:**
  - **Проходит процедура обновления международного стандарта ЭП: ГОСТ Р 34.10-2012 = > ISO/IEC 14888-3**
  - **Начата процедура обновления стандарта, определяющего функции хэширования ГОСТ Р 34.11-2012 = > ISO/IEC 10118-3**

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Экспертная деятельность

- **Анализ решений, предлагаемых зарубежными коллегами:**
- **– 2010 год: показана возможность выработки «слабых» вариантов датчика случайных чисел MQ_DRBG, предложенного французскими специалистами для включения в ISO/IEC 18031**
- **– 2013 год: показано наличие классов «слабых» модулей модулярной функции хэширования MASH-1 из ISO/IEC 10118-4**
- **– Постоянно: экспертиза стандартов при их разработке и ревизии**

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Экспертная деятельность

Участие в разработке базовых нормативных документов, регламентирующих оценку безопасности Криптографических алгоритмов. В частности:

– ISO/IEC 18033-1. Симметричные алгоритмы Шифрования. Общие положения

– ISO/IEC 10118-1(разрабатывается). Функции хэширования. Общие положения

– SD 5. Процесс включения и исключения криптографических механизмов

– SD 6 (разрабатывается). Руководство по реагированию на возможные угрозы безопасности криптографических алгоритмов

– SD 12. Криптографические алгоритмы и длины ключей (www.jtc1sc27.din.de)

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Методика деятельности

- **Анализ и выбор наиболее критичных с точки зрения обеспечения безопасности направлений исследований алгоритмов**
- **Поиск и подбор специалистов для проведения исследований в требуемых областях**
- **Активная работа на всех этапах разработки международных стандартов, включая подготовку и обоснование собственных предложений, экспертиза соответствующих предложений партнеров по вопросам стандартизации, а также их обсуждение на и между заседаниями рабочей группы**
- **Общее научное обеспечение деятельности по стандартизации**

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Научное обеспечение

- **С 2012 года: мини-симпозиум «Современные тенденции в криптографии» CTCrypt**
  - **Теоретическая криптография**
  - **Анализ стандартизированных механизмов**
  - **Круглые столы по актуальным вопросам применения СКЗИ**
- **Единственная российская рецензируемая конференция по криптографии, чьи труды издаются на английском языке**
- **За три года иностранное представительство увеличилось с 0 до 7 стран**

ТК 26: Международная стандартизация. ISO/IEC JTC 1/SC 27/WG 2. Много или мало?

- **Российская делегация стала полноправным членом 2-й группы рабочей**
- **Но таких групп 5 + несколько временных исследовательских групп!**
- **Постоянное представительство только во 2-й рабочей группе. На всех остальные РГ – представитель из ТК 22 (на весеннем заседании не было никого)**
- **Зарубежные эксперты заинтересованы в участии наших специалистов (где они?)**

Международная стандартизация. Перспективы

- **Что:**
  – Разработка новых информационных технологий сопровождается разработкой соответствующих международных, отраслевых стандартов
  – Включение в такие стандарты отечественных механизмов облегчит обеспечение трансграничного обмена данными, выход на новые рынки, сертификацию устройств
  – Анализ разрабатываемых стандартов позволит заранее выявлять возможные «слабости»

- **Когда:**
  – На этапе разработки новых технологий и стандартов, до их непосредственного внедрения на территории Российской Федерации

Международная стандартизация. Перспективы

- **Кто:**
  – Коммерческие организации, заинтересованные во внедрении и использовании таких технологий, развитии бизнеса, продвижении на новые рынки, уменьшении издержек, должны брать на себя работу по продвижению отечественных механизмов безопасности

  – ТК 26 в рамках своих полномочий и с учетом накопленного опыта (первоочередной) деятельности в ISO готов оказывать методическое и научное обеспечение такой деятельности

Спасибо за внимание