Об открытом конкурсе научно-исследовательских работ по ГОСТ Р 34.11-2012

Алексей Уривский

секретариат ТК26 «Криптографическая защита информации»

urivskiy@infotecs.ru

Участие в международной стандартизации

Российские эксперты участвуют в работе

GOST R

ISO International Organization for Standardization

ISO/IEC JTC1 SC27 WG2 –

Information Technology - Security Techniques - Cryptography and security mechanisms

Стандартизация российской криптографии: состояние и задачи

ISO/IEC 14888-3:2006/Amd 1:2010

Digital signatures with appendix — Part 3: Discrete logarithms based mechanisms — Amendment 1: **Elliptic Curve Russian Digital Signature Algorithm**

соответствует **ГОСТ Р 34.10-2001** и **ГОСТ Р 34.10-2012**

Задача

Провести алгоритм из **ГОСТ Р 34.11-2012** в состав **ISO/IEC 10118-3**

Hash-functions – Part 3: Dedicated hash-functions

Необходимые условия стандартизации в ISO

Для стандартов

- **доступность** описания алгоритма для анализа **не менее 3-х лет**;
- публикация **на английском языке** официальным органом по стандартизации.

Положительная оценка свойств алгоритма экспертами ISO – **публикации**:

- исследование криптографических качеств;
- ведущие профильные конференции, симпозиумы и журналы.

Открытый конкурс научных работ по исследованию хэш-функции ГОСТ Р 34.11-2012

Организатор – ОАО «ИнфоТеКС»
при поддержке **ТК26**
и **Академии криптографии РФ**

Цель: поощрение исследований по оценке криптографических качеств ГОСТ Р 34.11-2012

Сроки: с **21 октября 2013** по **15 декабря 2014**

Языки: русский и английский

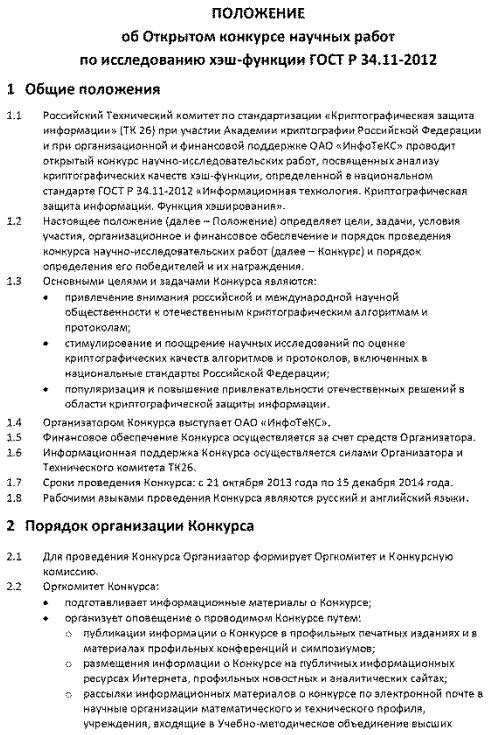
Гражданство участников не имеет значения

Условия Конкурса

- **1-ый этап** – с **21.10.2013** по **28.02.2014**
  - **не публиковавшиеся** ранее **работы**;
  - «слепое» рецензирование;
  - до 8 победителей;
  - призы – **70000 рублей** для организации публикации.
- **2-ой этап** – с **01.04.2014** по **30.11.2014**
  - **опубликованные** (принятые к публикации) **не ранее 2010 года работы**;
  - 2 первые премии по **500000** рублей и 2 вторые премии по **300000** рублей.
- Интеллектуальные права остаются за авторами.

Информация и контакты

- Интернет-адреса:
  - www.infotecs.ru;
  - www.tc26.
- Контактное лицо:
  Сериков Игорь Анатольевич
  serikov@infotecs.ru
- Проект положения о конкурсе
  http://tc26.ru/research/streebog/thesis/thesis.php



ПОЛОЖЕНИЕ
об Открытом конкурсе научных работ
по исследованию хэш-функции ГОСТ Р 34.11-2012

1 Общие положения

1.1 Российский Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) при участии Академии криптографии Российской Федерации и при организационной и финансовой поддержке ОАО «ИнфоТеКС» проводит открытый конкурс научно-исследовательских работ, посвященных анализу криптографических качеств хэш-функции, определенной в национальном стандарте ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

1.2 Настоящее положение (далее – Положение) определяет цели, задачи, условия участия, организационное и финансовое обеспечение и порядок проведения конкурса научно-исследовательских работ (далее – Конкурс) и порядок определения его победителей и их награждения.

1.3 Основными целями и задачами Конкурса являются:
- привлечение внимания российской и международной научной общественности к отечественным криптографическим алгоритмам и протоколам;
- стимулирование и поощрение научных исследований по оценке криптографических качеств алгоритмов и протоколов, включенных в национальные стандарты Российской Федерации;
- популяризация и повышение привлекательности отечественных решений в области криптографической защиты информации.

1.4 Организатором Конкурса выступает ОАО «ИнфоТеКС».

1.5 Финансовое обеспечение Конкурса осуществляется за счет средств Организатора.

1.6 Информационная поддержка Конкурса осуществляется силами Организатора и Технического комитета ТК26.

1.7 Сроки проведения Конкурса: с 21 октября 2013 года по 15 декабря 2014 года.

1.8 Рабочими языками проведения Конкурса являются русский и английский языки.

2 Порядок организации Конкурса

2.1 Для проведения Конкурса Организатор формирует Оргкомитет и Конкурсную комиссию.

2.2 Оргкомитет Конкурса:
- подготавливает информационные материалы о Конкурсе;
- организует оповещение о проводимом Конкурсе путем:
  - публикации информации о Конкурсе в профильных печатных изданиях и в материалах профильных конференций и симпозиумов;
  - размещения информации о Конкурсе на публичных информационных ресурсах Интернета, профильных новостных и аналитических сайтах;
  - рассылки информационных материалов о конкурсе по электронной почте в научные организации математического и технического профиля, учреждения, входящие в Учебно-методическое объединение высших

infotecs

Спасибо за внимание!
Вопросы?

Алексей Уривский
секретариат ТК26 «Криптографическая защита информации»
urivskiy@infotecs.ru