infotecs®

ТК 26 ГОСТР

GOST R

Вопросы организации экспертизы проектов документов в области стандартизации в техническом комитете «Криптографическая защита информации» (ТК 26)

Сериков Игорь Анатольевич
(секретариат ТК 26)

26 марта 2014 г.

Международная научно-практическая конференция «РусКрипто»

Организационно-функциональная структура национальной системы стандартизации

- национальный орган по стандартизации (Федеральное агентство по техническому регулированию и метрологии);
- федеральные органы исполнительной власти, а также организации, осуществляющие функции государственных заказчиков при выполнении работ по стандартизации;
- технические комитеты по стандартизации;
- совещательные органы по стандартизации;
- межотраслевые советы по стандартизации;
- службы стандартизации юридических лиц;
- организации (в том числе научные), деятельность которых связана с работами в области стандартизации.

ТК 26 ГОСТР

GOST R

Деятельность технического комитета осуществляется для решения следующих задач:

- организация разработки и экспертизы проектов национальных, межгосударственных и международных стандартов в закрепленной области деятельности;
- участие в формировании (ПРНС) в области 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;
- анализ стандартов в составе Федерального информационного фонда технических регламентов и стандартов на предмет их обновления и дальнейшего использования;

ТК 26 ГОСТР

GOST R

- участие в работе ТК международных (региональных) организаций по стандартизации (в закрепленной области деятельности), в том числе в целях принятия национальных стандартов Российской Федерации в качестве международных (региональных), а также в ведении их секретариатов в соответствии с соглашениями между национальным органом по стандартизации Российской Федерации и международными (региональными) организациями по стандартизации;
- подготовка предложений по разработке международных и межгосударственных стандартов и предложений относительно позиции Российской Федерации для голосования по проектам международных и региональных организаций по стандартизации;
- подготовка официальных переводов международных стандартов для передачи их в Федеральный информационный фонд технических регламентов и стандартов.

ТК 26 ГОСТР

GOST R

Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" определяет, что в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу; **продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа**; продукции (работ, услуг), сведения о которой составляют государственную тайну; продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии; **процессов проектирования (включая изыскания), производства,** строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения соответственно **указанной продукции обязательными требованиями наряду с требованиями технических регламентов являются требования,** установленные государственными заказчиками, **федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности**, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии, государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами).

ТК 26 ГОСТР

GOST R

Требования в качеству представляемых на экспертизу проектов документов по стандартизации:

- название, дату представления документа, номер версии;
- строгое формальное описание целевых криптографических функций, условий анализа и требований к стойкости для предлагаемого синтезного решения (примитива/конструкции/схемы/механизма/протокола/алгоритма);
- описание возможных сфер применения предлагаемого синтезного решения;
- обоснование целесообразности стандартизации предлагаемого синтезного решения;
- строгое формальное описание спецификации предлагаемого синтезного решения;
- обоснование синтезных решений (по каким критериям/причинам выбран каждый структурный элемент, константа и т.д.);
- криптографический анализ по отношению к известным методам, обоснование стойкости;

ТК 26 ГОСТР

GOST R

- доказательство стойкости (желательно);
- краткая экспертная оценка результатов независимых криптографических исследований предлагаемого синтезного решения;
- аналитическое сравнение предлагаемого синтезного решения с существующими аналогами (преимущества и возможные ограничения);
- контрольные примеры;
- результаты сравнения эксплуатационных характеристик (в условиях предлагаемых сфер применения) предлагаемого синтезного решения с существующими аналогами;
- сведения о наличии патентных ограничений;
- исчерпывающий библиографический список, охватывающий работы содержащие описание, принципы синтеза, вопросы применения, криптографического анализа, реализации предлагаемого синтезного решения и его аналогов.

ТК 26 ГОСТР

GOST R

Минимальные требования, предъявляемые к предлагаемому к стандартизации синтезному решению:

- наличие независимых криптографических исследований, результаты которых опубликованы в ведущих рецензируемых изданиях;
- отсутствие эффективных методов криптографического анализа;
- приемлемые (т.е. не ухудшающие функциональные характеристики) эксплуатационные качества предлагаемого решения в рамках рассматриваемых сфер применения;
- соответствие предлагаемого синтезного решения современным тенденциям развития информационных технологий и методов обеспечения защиты информации.

ТК 26 ГОСТР

GOST R