УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Настоящий выпуск журнала «Прикладная радиоэлектроника» является тематическим и посвящен проблемным вопросам информационной безопасности и криптографической защиты информации. Представленные в журнале статьи в основном являются заказными, тематика которых определяется практическими приложениями. В основном они подготовлены специалистами по тематике, ориентируясь на задачи, которые решаются спонсором издания журнала – ПАТ «Институт информационных технологий», г. Харьков. Важное внимание уделяется проблемным вопросам создания системы электронных доверительных трансграничных услуг.

В первом разделе представлен ряд статей, посвященных проблемным вопросам синтеза и анализа симметричных криптопреобразований. В основном статьи посвящены симметричным криптографическим преобразованиям типа блочные симметричные шифры (БСШ). В этом направлении остаются актуальными и требующие разрешения задачи доказательства стойкости, оптимизации по критериям криптографическая стойкость – сложность, в первую очередь скорость преобразования. При этом тематика статей носит в основном проблемный теоретический характер, но в тоже время направлены на решение конкретных практических задач – анализа и синтеза перспективных БСШ, а также оценки существующих, в первую очередь закрепленных в стандартах.

Второй раздел посвящен задачам предоставления трансграничных электронных доверительных услуг. В качестве основы рассматриваются решения и требования, которые сегодня закреплены в Регламентах Европейского Союза, соответственно 2012 и 2014 годов. Важными в этом направлении являются задачи и их анализ, которые направлены на выполнение требований «Регламента Европейского Парламента и Совета относительно электронной идентификации трастовых сервисов электронных операций на внутреннем рынке».

В плане решения указанных задач важные результаты получены в научно-техническом проекте EC STORK и STORK 2.0. Поэтому их анализ, на наш взгляд, а также определения задач для Украины, являются актуальными и необходимыми, требующими своего разрешения. Также важными, с точки зрения практики, являются задачи нормализации Европейской нормативной базы в области электронных подписей. В первую очередь относительно схемы нумерации документов ЭЦП, а также предметные области их применения.

В третьем разделе в основном представлены статьи, посвященные криптоанализу асимметричных криптографических систем, построению общесистемных параметров, оценке стойкости многофакторных систем защиты от НСД, а также оценке стойкости систем криптографических преобразований в фактор-кольце. Значительный интерес представляет статья, посвященная необходимости применения кодов аутентификации сообщений (MAC) для обеспечения целостности и достоверности корректирующей информации, формируемой системами дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС.

В четвертом разделе собраны статьи, направленные на решение общих и частных задач защиты информации. Важными и актуальными, на наш взгляд, являются результаты исследования относительно:

– классификации методов обеспечения доверия к безопасности продуктов и систем информационных технологий;

– субъектно-объектной модели доступа и аксиоматически необходимым условиям защищенности информации;

– подходов к созданию и использованию шаблонов для алгоритмов создания и применения услуг безопасности для формальной нотации;

– сравнительного анализа версий криптопротоколов ECIES.

Также на основе достаточно продолжительных обсуждений принята для публикации статья относительно применения в криптографии интегральных уравнений, как альтернативы алгебраическим методам. Надеемся, что по ней пройдут обсуждения и дискуссия в среде специалистов.

С наилучшими пожеланиями,

профессор кафедры БИСТ
Харьковского национального
университета им. В.Н. Каразина,
Главный конструктор ПАТ «ИИТ»

И.Д. Горбенко