УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Выпуск журнала «Прикладная радиоэлектроника» является тематическим и посвящен проблемным вопросам защиты информации. Представленные в журнале статьи в основном являются заказными. Они подготовлены специалистами по тематике, ориентируясь на задачи, которые решаются нашим спонсором – ПАТ «Институт информационных технологий.

Сегодня можно утверждать, что наша цивилизация стоит на рубеже создания электронного цифрового общества. В Европейском Союзе (ЕС) и в некоторой степени в Украине признано, что укрепление доверия в электронной онлайн среде является ключом к экономическому развитию. Отсутствие доверия заставляет потребителей, бизнес и руководство, при осуществлении трансграничных доверительных операций в электронном виде быть в некоторой степени неопределенности и принимать новые услуги с осторожностью. Также признано, что основополагающим принципом осуществления внутреннего рынка в ЕС должно быть отсутствие на территории государства-члена ограничений относительно предоставления доверительных услуг провайдерами доверительных услуг, расположенных в других государствах-членах ЕС.

Для Украины, на наш взгляд, очень важным является изучение и анализ возможностей использования европейского опыта с целью предоставления безопасных электронных услуг по электронной идентификации, электронной аутентификации электронной подписи, электронных печатей, электронных меток времени, электронных документов, услуг электронной доставки и проверки подлинности веб-сайта. Поэтому в первом разделе журнала представлены, на наш взгляд, методологические статьи, которые посвящены концептуальным положениям реализации доверительных услуг и безопасности облачных вычислений.

Во втором разделе журнала представлены статьи, которые посвящены теории и практике симметричных криптографических преобразований, в основном блочным симметричным шифрам, функциям хеширования и генераторам случайных последовательностей. По-прежнему актуальными являются исследования, связанные с исследованием криптографической стойкости симметричных шифров, функций хеширования и генераторов случайных последовательностей. На наш взгляд, серия статей в этом направлении позволяет получить уточненные оценки свойств симметричных шифров, функций хеширования и генераторов случайных последовательностей в части создания первоначальной неопределенности.

Серия статей третьего раздела посвящена асимметричным криптопреобразованиям. Прежде всего рассматриваются асимметричные преобразования в фактор-кольцах, которые получили название «преобразования в кольцах срезанных полиномов». Относительно этих преобразований важными есть задачи доказательства их стойкости, учитывая аппарат алгебраических решеток. Приводится фундаментальное решение задачи оптимизации процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Применение предложенного подхода открывает принципиально новую область возможностей для комплексного решения проблемы повышения стойкости защиты информации.

Серия из трех статей: «Параметры криптосистемы на кривой Эдвардса над расширениями малых простых полей», «Деление точки на два для кривой Эдвардса над простым полем» и «Криптостойкие кривые Эдвардса над простыми полями» написаны их авторами под руководством профессора А.В. Бессалова. Также мы считаем возможным публикацию статьи, автор М.В. Есина, которая посвящена анализу сложности преобразований на эллиптических кривых в различных базисах. Важными являются исследования, которые посвящены атакам специального вида и методам защиты от этих атак. Они представлены в статьях авторов Д.С. Балагуры и Д.В. Иваненко.

В четвертом разделе представлены статьи, которые можно отнести к сфере информационной безопасности. Так, в статье авторов В.В. Котенко, С.В. Котенко, К.Е. Румянцева и Горбенко Ю.И. приводится фундаментальное обоснование стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей.

В статье А.Н. Алексейчука и А.Ю. Грязнухина представлено решение задачи восстановления систематического линейного кода набора искаженных кодовых слов, наблюдаемых на выходе двоичного симметричного канала связи. Получены оценки сложности решения систем уравнений. В статье И.В. Олешко представлены предложения по совершенствованию протокола нулевых знаний. В статье А.А. Кузнецова, С.И. Приходько, Билал Хамзе представлены результаты исследования линейных блоковых кодов в частотной области. В статье А.А. Смирнова представлен алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции, который основан на сечении циклических орбит групповых кодов. В статье В.А. Краснобаева, М.А. Маврина и А.А. Замулы, предложен метод повышения достоверности контроля данных, представленных в классе вычетов. В статье С.В. Николаенко представлен способ усиления безопасности пинг-понг протокола с парами перепутанных кубитов. Статья В.И. Заболотного и Е.В. Задорожной посвящена обоснованию способов защиты информации от конкурентной разведки с учетом возможности применения средств технических разведок. Исследования Т.А. Гриненко и А.П. Нарежного представлены работами по обоснованию необходимости применения кодов аутентификации сообщений (MAC) для обеспечения целостности и достоверности корректирующей информации в системе GPS/ГЛОНАСС. В статье А.В. Леншина предлагается комплексный метод проектирования и верификации комплексов средств защиты информации от несанкционированного доступа. Анализируется подход к созданию и использованию шаблонов для алгоритмов реализации услуг безопасности в формальной нотации Паронджанова.

Ректор ХНУРЭ,
член-корреспондент НАНУ,
профессор

М.Ф. Бондаренко

Заведующий кафедрой
БИТ ХНУРЭ, профессор

И.Д. Горбенко