УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Выпуск настоящего журнала является тематическим и посвящен проблемным вопросам криптологии и ряду аспектов защиты информации. Статьи в основном являются заказными и подготовлены специалистами по соответствующим направлениям. Большинство статей посвящено новым и уже ставшим традиционными криптографическим преобразованиям. Однако, при заказе статей мы руководствовались в основном практическими аспектами криптологии, ориентируясь на задачи, которые решаются нашим спонсором – ПАТ «Институт информационных технологий».

В первом разделе журнала представлены статьи, которые посвящены теории и практике симметричных криптографических преобразований, в основном блочным симметричным шифрам (БСШ). По-прежнему актуальными являются исследования, связанные с решением систем линейных булевых уравнений с искаженными частями. На наш взгляд, интересные результаты в этом направлении получены профессором Алексейчуком А.Н, которые представлены в первой статье журнала. В статье профессора Долгова В.И. и доцента Лисицкой И.В. излагается уточнённый подход к определению Марковских шифров, основывающийся на стохастических уравнениях Марковских процессов. Такой подход является дискуссионным и требует обсуждения. Определенное внимание заслуживает статья, подготовленная под руководством профессора Долгова В.И., посвященная вопросам практической оценки максимальных значений дифференциалов и линейных корпусов марковских шифров. Также в связи с признанием направления, связанного с развитием БСШ на основе применения схемы Лея – Массея, представлены исследования по оценке сложности различения схемы Лея – Массея и случайной1 перестановки, авторы доцент Олейников Р.В. и аспирант Кайдалов Д.С. Статья доцента Руженцева В.И. посвящена исследованию особенностей организации интегральных атак на различные варианты шифров с rijndael-подобными преобразованиями. Существенного внимания заслуживает и статья доцента Халимова Г.З. и аспиранта Бойко А.А., в которой предлагается метод универсального хеширования по рациональным функциям алгебраических кривых над кольцами векторов. В первом разделе также представлены статьи. Посвященные генерации и исследованию псевдослучайных последовательностей битов и функций хеширования.

Во втором разделе представлены статьи по вопросам анализа и синтеза асимметрических криптопреобразований. Не умаляя статьи раздела, прежде всего, отметим статью авторов Качко Е.Г., Балагура Д.С. и Горбенко Ю.И., посвященную обоснование и исследованию практической реализации улучшенного алгоритма цифровой подписи NTRUSign. Полученные авторами результаты имеют важное практическое значение, так как позволяют повысить скорость преобразований с одновременным обеспечением экспоненциальной сложности реализации атаки «полное раскрытие». Заслуживают внимания, скорее теоретического, результаты сравнительного анализа алгоритмов криптографических преобразований основных алгоритмов преобразований на идентификаторах, в которых также применяются алгебраические решетки, авторы профессор Горбенко И.Д. и аспирант Макутонина Л.В. Определенный интерес имеет, скорее теоретический обобщающая статья, Д.А. Паршиной, И.А. Митяевой и И.Д. Горбенко, в которой представлены результаты анализа возможностей применения групп КОС в криптографии. Также во втором разделе публикуются статьи, написанные под руководством профессора Бессалова А.В., тематика которых связанна с приложениями эллиптических кривых. Практическую ценность имеют и остальные статьи второго раздела.

В третьем разделе представлены результаты исследований, связанные с обработкой данных большого объема в условиях неопределенности и практическими исследованиями различных источников биометрической информации.

В четвертом разделе представлены ряд статей, посвященных, различным аспектам защиты информации, в том числе формальные основы методов блокировки аппаратных закладных устройств профессора Горбачева В.А, метод оперативного контроля данных в классе вычетов профессора Краснобаева В.А, рассматривается задача синтеза дискретных сигналов с заданными корреляционными, структурными и ансамблевыми свойствами профессоров Замулы А.А. и Горбенко И.Д, результаты исследований свойств деятельного аспекта защиты информации как системной категории, полученные под руководством профессора Потия А.В., и другие статьи.

С уважением и наилучшими пожеланиями, с благодарностью авторам за подготовленные статьи и будущим читателям. Мы надеемся, что опубликованные в этом журнале статьи послужат решению вопросов развития национальной криптологии.

Ректор ХНУРЭ,
член-корреспондент НАНУ,
профессор

Бондаренко М.Ф.

Заведующий
кафедрой БИТ ХНУРЕ,
профессор

Горбенко И.Д.