

СОДЕРЖАНИЕ

МЕТОДЫ И МЕХАНИЗМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

<i>Е.Г. Качко, Ю.И. Горбенко, М.В. Есина, О.С. Акользина</i> Оптимизация алгоритма направленного шифрования NTRU Prime	5
<i>І.Д. Горбенко, О.Г. Качко, М.В. Єсіна</i> Аналіз алгоритму направлено шифрування NTRU PRIME ІТ UKRAINE з урахуванням відомих атак	11
<i>Ю.І. Горбенко, К.В. Ісірова</i> Удосконалений механізм одноразових ключів для постквантового періоду на основі геш-функцій	24
<i>Н.Е. Иванов, Р.В. Олейников</i> Оценка пропускной способности платформы Ethereum на основе математической модели смарт-контракта	40
<i>М.Ю. Родінко, Р.В. Олійников</i> Методи пошуку диференційних характеристик циклової функції симетричного блокового шифру «Кипарис»	47
<i>О.О. Кузнецов, Д.В. Иваненко, М.С. Луценко, В.А. Тимченко, О.М. Мелкозерова, М.О. Осадчук, Є.В. Острианська</i> Порівняльні дослідження алгоритмів потокового криптографічного перетворення	52

СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

<i>И.Д. Горбенко, А.А. Замула</i> Аналитическая оценка значений максимальных боковых лепестков функций корреляции сложных нелинейных дискретных сигналов	76
<i>А.В. Бессалов, О.В. Цыганкова</i> Суперсингулярные полные кривые Эдвардса над простым полем	88
<i>В.И. Есин</i> Выразительные средства модели данных «объект-событие»	99
<i>В.А. Горбачев, К.Б. Абдулрахман</i> Обзор проблем безопасности и проектирования защищенных электронных систем	113
<i>Д.В. Мялковский, З.А. Орешко, А.В. Потій</i> Аналіз предметної області ідентифікації та автентифікації	120
<i>В.А. Краснобаев, А.А. Замула, В.Н. Шлокин</i> Методы определения вычетов чисел в комплексной числовой области	128

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

<i>В.К. Волосюк, С. С. Жила, В.В. Павликов, А.Д. Абрамов, В.Г. Яковлев</i> Оптимальный алгоритм оценки радиояркости в пространственно-распределенных радиометрических системах	143
<i>И.В. Барышев, К.А. Щербина, Е.П. Мсаллам, М.А. Вонсович, А.В. Одокиенко</i> Анализ по показателям качества работы схем узкополосной фильтрации непрерывного доплеровского сигнала	150
<i>В.Е. Кудряшов, С. М. Тамаш, Д. С. Шмаков</i> Рознесена двохпозиційна радіометрична система картографування об'єктів	158
<i>В.М. Безрук, С.А. Иваненко</i> Исследования методов обнаружения неизвестных сигналов	167
<i>Б.В. Перельгин, А.М. Лужбин</i> Построение сплошного радиолокационного поля системы гидрометеорологического мониторинга на основе геометрического подхода	173
<i>В.М. Карташов, В.Н. Олейников., С.А. Шейко, С.И. Бабкин, И.В. Корытцев, О.В. Зубков, М.А. Анохин</i> Информационные характеристики звукового излучения малых беспилотных летательных аппаратов	181
<i>Хассан Мохамед Мухи-Алдин, Е.Б. Ткачева</i> Адаптивный алгоритм перераспределения сетевых ресурсов в сетях с поддержкой технологии NFV	188
<i>А.В. Осадчук, В.С. Осадчук, Я.А. Осадчук, Е.А. Селецкая</i> Частотный преобразователь концентрации газа на основе транзисторной структуры с негативным сопротивлением	195
<i>В.В. Усик, И.Г. Мягкий</i> Особенности проведения акустического моделирования как завершающего этапа акустической экспертизы помещений зрительных залов на примере драматического театра на 500 мест	203
РЕФЕРАТЫ	212

CONTENT

METHODS AND MECHANISMS OF CRYPTOGRAPHIC INFORMATION PROTECTION

<i>O.G. Kachko, Yu. I. Gorbenko, M.V. Esina, O.S. Akolzina</i> Optimization of NTRU Prime asymmetric encryption algorithm	5
<i>I.D. Gorbenko, O.G. Kachko, M.V. Yesina</i> Analysis of the end-to-end encryption algorithm NTRU PRIME IIT UKRAINE taking into account known attacks	11
<i>Yu.I. Gorbenko, K.V. Isirova</i> Improved Post-quantum Hash Based One-Time Key Mechanism	24
<i>M. Ivanov, R. Oliynykov</i> Estimating the capacity of the Ethereum platform based on the mathematical model of the smart contract	40
<i>M.Yu. Rodinko, R.V. Oliynykov</i> Methods for finding differential characteristics of block cipher “Cypress”	47
<i>O.O. Kuznetsov, D.V. Ivanenko, M.S. Lutsenko, V.A. Timchenko, OM Melkozerova, M.O. Osadchuk, C.V. Ostrianska</i> Comparative studies of flow cryptographic transformation algorithms	52

SYSTEMS OF INFORMATION PROCESSING AND PROTECTION

<i>I.D. Gorbenko, A.A. Zamula</i> Analytical estimation of the values of the maximum side lobes of correlation functions of complex nonlinear discrete signals	76
<i>A.V. Bessalov, O.V. Tsygankova</i> Supersingular complete Edwards curves over a prime field	88
<i>V.I. Yesin</i> Expressive means of the «object-event» data model	99
<i>V.A. Gorbachov, K.B. Abdulrahman</i> Overview of security problems and the design of secure electronic systems	113
<i>D.V. Mylkovsky, Z.A. Oreshko, A.V. Potii</i> Analysis of domain identification and authentication	120
<i>V.A. Krasnobayev, A.A. Zamula, V.N. Shlokin</i> Methods of determining the remnants of numbers in a complex numerical domain	128

RADIO ENGINEERING AND TELECOMMUNICATIONS NETWORKS AND SYSTEMS

<i>V.K. Volosyuk, S.S. Zhyla, V.V. Pavlikov, A.D. Abramov, V.G. Yakovlev</i> Optimal algorithm of radio brightness estimation in the spatial distributed radiometric systems	143
<i>I.V. Baryshev, K.A. Scherbina, E.P. Msallam, M.A. Vonsovitch, A.V. Odokienko</i> The experimental research of filtration quality of doppler signal spectral structure by modulated filter	150
<i>V.E. Kudriashov, S.M. Tamash, D.S. Shmakov</i> Diversified bi-static radiometric system for object mapping	158
<i>V.M. Bezruk, S.A. Ivanenko</i> Research methods for detecting unknown signals	167
<i>B.V. Perehygin, A.M. Luzbin</i> Construction of a continuous radar field of a hydrometeorological monitoring system based on a geometric approach	173
<i>V.M. Kartashov, V.N. Oleynikov, S.A. Sheyko, S.I. Babkin, I.V. Koryttsev, O.V. Zubkov, A.M. Anokhin</i> Information characteristics of sound emission from small unmanned aerial vehicles	181
<i>Hassan Mohamed Muhi-Aldeen, O.B. Tkachova</i> Adaptive algorithm reallocation of network resources in a network that supports NFV technology	188
<i>A.V. Osadchuk, V.S. Osadchuk, I.A. Osadchuk, O.O. Seletska</i> Frequency converter of gas concentration in transistor structure with negative resistance	195
<i>V. Usik, I. Myagkiy</i> Features of acoustic modeling as the final stage of acoustic examination of premises of auditoriums exemplified by a drama theater for 500 seats	203
ABSTRACTS	212