

СОДЕРЖАНИЕ

ЗАЩИЩЕННЫЕ ТЕЛЕКОМУНИКАЦИОННЫЕ СИСТЕМЫ И ПЕРЕДАЧА ДАННЫХ

<i>И.Д. Горбенко, А.А. Замула</i> Криптографические сигналы: требования, методы синтеза, свойства, применение в телекоммуникационных системах	7
<i>А.А. Замула, В.Л. Морозов</i> Информационные технологии передачи данных в современных телекоммуникационных системах	24

ПРОБЛЕМЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ И ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ ИХ РАЗРЕШЕНИЯ В БУДУЩЕМ

<i>И.Д. Горбенко, О.О. Кузнецов, О.В. Потий, Ю.И. Горбенко, Р.С. Ганзя, В.А. Пономар</i> Постквантовая криптография та механізми її реалізації	32
<i>Ю.И. Горбенко, О.В. Шевцов, Т.Ю. Кузнецова</i> Модель порушника систем электронных цифровых підписів в умовах квантового криптоаналізу	53
<i>А.А. Кузнецов, А.И. Пушкарёв, И.И. Сватовский, А.В. Шевцов</i> Несимметричные криптосистемы на алгебраических кодах для постквантового периода	70
<i>А.В. Потий, А.С. Карпенко</i> Реализация постквантового алгоритма электронно-цифровой подписи	91
<i>В.А. Пономар</i> Особливості та проблематика створення криптосистем, заснованих на використанні ізогеній еліптичних кривих	96

МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

<i>И.Д. Горбенко, О.Г. Качко, К.А. Погребняк, Л.В. Макутоніна</i> Аналіз, оцінки та пропозиції відносно методу генерації системних параметрів у NTRU-подібних асиметричних системах	103
<i>А.В. Бессалов</i> Метод нахождения порядка точки скрученной кривой Эдвардса	110
<i>В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий</i> Усовершенствованный блочный симметричный шифр Калина	119
<i>В.И. Долгов, И.В. Лисицкая, К.Е. Лисицкий</i> Новая концепция проектирования блочных симметричных шифров	132
<i>Н.А. Полуяненко, А.В. Потий</i> Сравнение объема ансамбля М-РСЛОС и М-РСНОС, скорости генерации на их основе для $GF(2)$ и в расширениях поля $GF(2^2)$	153
<i>М.В. Єсіна, Н.В. Ковальова, І.Д. Горбенко</i> Порівняльний аналіз властивостей електронного підпису згідно з ДСТУ ISO/IEC 9796-3:2014	160
<i>Т.О. Грінченко, О.П. Нарєжній, І.Д. Горбенко</i> Методика вимірювання спектральної щільності потужності шуму квантової радіооптичної системи генератора випадкових чисел	172

РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОМУНИКАЦИОННЫЕ СИСТЕМЫ И УСТРОЙСТВА

<i>В.М. Карташов, В.А. Тихонов, В.В. Воронин</i> Особенности построения и применения комплексных систем дистанционного зондирования атмосферы	184
<i>В.В. Семенец, В.И. Леонидов</i> Координатный метод оценки радиальной скорости в системах акустического зондирования атмосферы	189
<i>О.Ю. Евсеева, Е. Н. Ильяшенко</i> Координационный метод управления ресурсами многоуровневой транспортной оптической сети по критерию минимума энергопотребления	194

<i>Е. В. Дуравкин, Е.Б. Ткачева, Салим Мухамед Джамал</i> Применение теории формальных грамматик и аппарата Е-сетей для анализа корректности распределения сетевых ресурсов инфраструктуры NFV	202
<i>Н.А. Штомпель</i> Оптимизация нерегулярных кодов с малой плотностью проверок на четность на основе природных вычислений	207
<i>В.В. Печенин, К.А. Щербина, М.А. Вонсович, Ю.В. Съедина</i> Синтез модулированного фильтра с самосинфазированием для слеящего приема и обработки частотно-модулированного сигнала методом имитационного моделирования	211
<i>Т.А. Цалиев, К.В.Куцук</i> Широкополосная двухкольцевая планарная антенна	217
РЕФЕРАТЫ	223

CONTENT

PROTECTED TELECOMMUNICATION SYSTEMS AND DATA TRANSFER

<i>I.D. Gorbenko, A.A. Zamula</i> Cryptographic signals: requirements, synthesis methods, properties, application in telecommunication systems	7
<i>A.A. Zamula, V.L. Morozov</i> Information transmission technology in modern telecommunications systems	24

PROBLEMS OF POST-QUANTUM CRYPTOGRAPHY AND POSSIBLE DIRECTIONS FOR THEIR RESOLUTION IN THE FUTURE

<i>I.D. Gorbenko, O. Kuznetsov, O.V. Potii, Y.I. Gorbenko, R.S. Ganzya, V.A. Ponomar</i> Post quantum cryptography and mechanisms for its implementation	32
<i>Y. I. Gorbenko, O.V. Shevtsov, T.U. Kuznetsova</i> Adversary model of digital signatures schemes in terms of quantum cryptanalysis	53
<i>A.A. Kuznetsov, A.I. Pushkarev, I.I. Svatovskiy, O.V. Shevtsov</i> Asymmetric cryptosystems on algebraic codes for post quantum period Public-key Code-Based Cryptography for the post-quantum period	70
<i>O.V. Potii, A.S. Karpenko</i> Implementation of post-quantum algorithm of electronic-digital signature	91
<i>V.A. Ponomar</i> Features and problems of creating cryptosystems based on using isogenies of elliptic curves	96

METHODS, MECHANISMS AND TOOLS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

<i>I.D. Gorbenko, O.G. Kachko, K.A. Pogrebnyak, L.V. Makutonina</i> Analysis, assessment and proposals regarding the method of the system parameters generation in the NTRU-similar asymmetric systems	103
<i>A.V. Bessalov</i> Method for finding of the point's order of the Edwards twisted curve	110
<i>V.I. Dolgov, I.V. Lysytskaya, K.E. Lysytsky</i> Improved Kalina symmetric block cipher	119
<i>V.I. Dolgov, I.V. Lysytskaya, K.E. Lysytsky</i> A new concept for designing of block symmetric ciphers	132
<i>N.A. Poluyanenko, O.V. Potii</i> Comparison of the M-LSFR and M-NLSFR ensembles' volume, the rate of generation on their basis for the $GF(2)$ and in expansions of the $GF(2^2)$ field	153
<i>M.V. Yesina, N.V. Kovaleva, I.D. Gorbenko</i> Comparative analysis of electronic signature properties according to the DSTU ISO IEC 9796-3:2014	160
<i>T.A. Grinenko, O.P. Nariezhnii, I.D. Gorbenko</i> Methods for spectral density noise power measurement of quantum radio-optical system of random number generator	172

RADIO ENGINEERING AND TELECOMMUNICATIONS SYSTEMS AND DEVICES

<i>V.M. Kartashov, V.A. Tikhonov, V.V. Voronin</i> Features of construction and application of complex systems for the atmosphere remote sounding	184
<i>V.V. Semenetz, V.I. Leonidov</i> Coordinate method for estimation of radial velocity in systems of acoustic sounding of the atmosphere	189
<i>O. Yu. Yevsieieva, Y. N. Ilyashenko</i> Coordination method for resources management in multilevel transport optical network according to minimum energy consumption criterion	194

<i>E.V. Duravkin, O.B. Tkachova, Mohammed Jamal Salim</i> Application of the theory of formal grammars and the E-nets tools for analysis of correctness of network resources distribution in the NFV infrastructure	202
<i>M.A. Shtompel</i> Optimization of irregular low-density parity-check codes based on natural computing	207
<i>V.V. Pechenin, K.A. Scherbina, M.A. Vonsovitch, J. V. Syedina</i> Synthesis of the modulated filter with self-cophasing for tracking and processing of frequency-modulated signal by means of simulation method	211
<i>T.A. Tsaliev, K.V.Kutsuk</i> Broadband double-ring planar antenna	217
ABSTRACTS	223