

# СОДЕРЖАНИЕ

## МЕТОДЫ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ, ОБРАБОТКИ И АНАЛИЗА ДАННЫХ

<i>И.Д. Горбенко, А.А. Замула, В.Л. Морозов</i> Информационная безопасность и помехозащищенность телекоммуникационных систем в условиях различных внутренних и внешних воздействии	5
<i>В. И. Есин</i> Кибернетический подход к решению задачи реинжиниринга баз данных	15
<i>В. І. Заболотний, А.В. Єрмолович</i> Методика організації заходів захисту від технічних засобів конкурентної розвідки	23
<i>В. А. Краснобаев, С. А. Кошман, А. С. Янко</i> Усовершенствованный метод определения альтернативной совокупности чисел в системе остаточных классов	29

## МЕХАНИЗМЫ И МЕТОДЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

<i>А.Н. Алексейчук, А.А. Матийко</i> Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU	38
<i>О.О. Кузнецов, Ю.І. Горбенко, І.М. Білозерцев, А.В. Андрушкевич, О.П. Наріжний</i> Алгебраїчний імунітет нелінійних вузлів симетричних шифрів	47
<i>А.А. Кузнецов, А.И. Пушкарев, А.С. Киян</i> Алгоритмы электронной цифровой подписи на основе алгебраического кодирования	59
<i>Е.Г. Качко, Д.К. Телевний</i> Исследование применимости SMT/SAT доказательств в криптоанализе хеш-функций семейства Кессак	75
<i>К.Е. Лисицкий</i> Закон распределения вероятностей смещений таблиц линейных аппроксимаций случайных подстановок	81
<i>П.И. Стеценко, Г.З. Халимов</i> Проблема совершения условных транзакций в закрытых Blockchain-системах	90
<i>М.Ю. Родінко, Р.В. Олійников</i> Постквантовый малоресурсный симметричный блочный шифр «Кипарис»	100
<i>Н.А. Полуяненко, А.В. Потий</i> Использование технологий параллельных вычислений в графических процессорах для генераторов потокового шифрования	108
<i>Ю.І. Горбенко, Т.В. Мельник, І.Д. Горбенко</i> Аналіз потенційних постквантових механізмів електронних підписів на основі геш-функцій	115

## РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

<i>И.И. Обод, И.В. Свид, И.А. Штых</i> Синтез и анализ оптимального обнаружителя сигналов запроса в самолетных ответчиках вторичных систем наблюдения	132
<i>В.М.Карташов, С.И.Бабкин, Е.Г Толстых</i> Методические погрешности измерения метеовеличин при корреляционной обработке сигналов систем радиоакустического зондирования. Сообщение 2	136
<i>В.Н. Олейников, С.В. Дорошенко, В.Д. Пшеничный</i> Оценка параметров спектров рассеянных сигналов в РЛС вертикального зондирования атмосферы	141
<i>Ю.Ю. Коляденко, И.Г. Лукинов</i> Модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов	148
<i>А.А. Глуценко, Е.А. Медведев, Д.Ю. Горелов</i> О проблеме астероидно-кометной опасности	155

## ФИЗИКА ПРИБОРОВ, ЭЛЕМЕНТОВ И СИСТЕМ

<i>А.В. Безуглый, А.М. Петченко</i> Распределение плотности потока фотонов в дифракционной картине от одной и двух параллельных щелей	162
<i>А.И. Филипенко, А.Н. Донсков</i> Определение зависимости характеристик фотонной запрещенной зоны от показателя преломления материала	166
<i>О.Ю. Бабыченко</i> Многокомпонентные полупроводниковые структуры в конструкциях солнечных элементов	172
<i>Ли Хе-Пинг</i> Применение наземной многопозиционной технологии в управлении воздушным движением	179

## СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

<i>А.Н. Олейников, А.В. Бородавка</i> Основные направления совершенствования средств акустической разведки	189
<i>В.А. Алексеев, Д.В. Маслий, Д.Ю. Горелов</i> Сравнительный анализ перспективных технологий аутентификации пользователей ПК по клавиатурному почерку	195

РЕФЕРАТЫ	202
----------	-----

# CONTENT

## METHODS FOR PROTECTED TRANSMISSION, PROCESSING AND ANALYSIS OF DATA

<i>I.D. Gorbenko, A.A. Zamula, V.L. Morozov</i> Information security and interference immunity of telecommunication systems under conditions of various internal and external impacts	5
<i>V. I. Yesin</i> Cybernetic approach to solving the task of database reengineering	15
<i>V.I. Zabolotniy, A.V. Yermolovych</i> Methodology for organization of protection measures against technical means of competitive intelligence	23
<i>V. A. Krasnobayev, S. A. Koshman, A. S. Yanko</i> Improved method for determining an alternative set of numbers in a system of residual classes	29

## MECHANISMS AND METHODS OF CRYSTALLOGRAPHIC TRANSFORMATIONS

<i>A.N. Alekseychuk, A.A. Matiyko</i> Estimates of the probability of reversibility of random polynomials used in the modified version of NTRU cryptosystem	38
<i>AA Kuznetsov, Yu.I. Gorbenko, I.N. Bilozertsev, A.V. Andrushkevych, A.P. Narezhny</i> Algebraic immunity of non-linear components of symmetric ciphers	47
<i>A.A. Kuznetsov, A.I. Pushkarev, A.S. Kiyan</i> Algorithms of electronic digital signature based on algebraic coding	59
<i>O.Kachko, D.Televnyi</i> A study of the applicability of the SMT/SAT-based theorem proves for Keccak hash functions cryptanalysis	75
<i>K.E Lisitzky</i> Law of probability distribution of displacements tables of random substitution linear approximations	81
<i>P.I. Stetsenko, G.Z. Khalimov</i> The problem of performing conditional transactions in private Blockchain-systems	90
<i>M.Yu. Rodinko, R.V. Oliynykov</i> Post- quantum lightweight symmetric block cipher “Cypress”	100
<i>N. Poluyanenko, O. Potii</i> Using parallel computing technologies in graphics processors for stream cipher generators	108
<i>Yu.I. Gorbenko, T.V. Melnik., I.D. Gorbenko</i> Analysis of potential post-quantum mechanisms of electronic signatures based on hash functions	115

## RADIO ENGINEERING AND TELECOMMUNICATION SYSTEMS AND NETWORKS

<i>I.I. Obod, I.V. Svyd, I.A. Shtyh</i> Synthesis and analysis of request signals optimal detector in aircraft responders of secondary observation systems	132
<i>V.M. Kartashov, S.I. Babkin, E.G. Tolstykh</i> Methodical errors in meteorological measurements during correlation processing of signals from radio acoustic sensing systems. Communication 2	136
<i>V.M. Oleynikov, S.V. Dorochenko, V.D. Pshenichniy</i> Estimation of parameters of the scattered signals spectra in the radar of vertical sounding of atmosphere	141
<i>Y. Kolyadenko, I. Lukinov</i> Model for identifying and eliminating vulnerabilities in software-configurable communication networks based on the apparatus of Markov processes	148
<i>A.A. Glushenko, E.A. Medvedev, D.Y. Gorelov</i> On the problem of asteroid-comet hazard	155

## PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

<i>A.V. Besougly, A.M. Petchenko</i> Distribution of the flux of fotons in the diffraction pattern from one and two parallel slits	162
<i>A. I. Filipenko, A.N. Donskov</i> Investigation of the characteristics of the band gap on a refractive index of materials	166
<i>O. Babychenko</i> Multicomponent semiconductor structures in the construction of solar cells	172
<i>Li He-Ping</i> The application of multilateration technology in air traffic control	179

## SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

<i>A. N. Oleynikov, A. V. Borodavka</i> The main directions of improving acoustic intelligence devices	189
<i>V.A. Alekseev, D.V. Masliy, D.Y. Gorelov</i> Comparative analysis of advanced technologies for authenticating users by keystroke dynamics	195

ABSTRACTS	202
-----------	-----