

## СОДЕРЖАНИЕ

### БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ

<i>В.И. Долгов, А.А. Настенко</i> О роли схем разворачивания ключей в атаках на итеративные шифры	7
<i>В. И. Долгов, Е.Д. Мельничук</i> S-блоки для современных шифров	16
<i>А.В. Казимиров, Р.В. Олейников</i> Криптоанализ шифра Mickey на основе анализа внутренних состояний	24
<i>И.В. Лисицкая</i> Вырожденные подстановки	31
<i>В.И. Руженцев</i> Про доказательство отсутствия эффективных байтовых дифференциальных характеристик для Rijndael-подобных шифров	39
<i>А.А. Кузнецов, А.В. Коваленко, С.А. Исаев</i> Формирование нелинейных узлов замен с использованием недвоичных криптографических функций	43

### КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

<i>Е.Г. Качко, Д.С. Балагура, К.А. Погребняк, Ю.И. Горбенко</i> Исследование методов вычисления инверсии в алгоритме NTRU	58
<i>Ю.М. Ленишина, А.В. Ленишин</i> Криптографічна підтримка послуг захисту від несанкціонованого доступу	64
<i>К.А. Погребняк, Д.В. Повтарев</i> Модель використання хмарних обчислень для задач асимметричного криптоанализу на прикладі факторизації чисел методом р-Полларда	72
<i>І.Д. Горбенко, Л.В. Макутоніна</i> Аналіз стійкості обчислювальних задач, що засновані на білінійних відображеннях	79
<i>Д.В. Иваненко</i> Методи протидії атакам спеціального виду на схеми направлено шифрування у кільцях зрізаних поліномів	90
<i>И.Д. Горбенко, Р.И. Мордвинов</i> Сущность и анализ криптографических требований стандарта NISTSP 800-90B	99
<i>Е.В. Котух</i> Универсальное хеширование с ограничением функционального поля алгебраических кривых	109
<i>І. Д. Горбенко, М. В. Єсіна</i> Алгоритм решета числового поля	116
<i>В.Ю.Ковтун, А.А.Охрименко</i> Подходы к распараллеливанию программной реализации операции умножения целых чисел	123
<i>О.А. Шевчук, Ю.І. Горбенко</i> Автентифікація апаратних засобів КЗІ	132
<i>О.Г. Халимов, А.Н. Герцог</i> Универсальное хеширование по обобщенным кривым Гурвица	140
<i>А.П. Бубир, І.Д. Горбенко</i> Оцінка стійкості направлено шифру NTRU до атаки з адаптивно підібраними шифротекстами	147
<i>Х.А. Бугаєнко, І.Д. Горбенко</i> Аналіз двох методів автентифікації особи для застосування в електронному біометричному паспорті	152

### ПЕРЕДАЧА И ОБРАБОТКА ИНФОРМАЦИИ

<i>Ю.І. Горбенко, О.С. Тоцький, В.А. Пономар</i> Аналіз методів знеособлення персональних даних	159
<i>А.В. Потий, Д.Ю. Пилипенко</i> Модель институционального управления деятельностью по защите информации	164
<i>А.А. Замула, С.А. Сирота, Н.И. Косиковская</i> Количественная оценка уязвимостей информационно-телекоммуникационных систем	171
<i>А.А. Замула</i> Предложения по построению широкополосных систем передачи со сложными сигналами	177
<i>Б.О. Бабич, А.В. Сагун, О.А. Кожуховская, А.Д. Кожуховский</i> Синтез системы многоуровневой защиты корпоративных порталов на платформе MS SHARE POINT	185
<i>А.А. Смирнов</i> Критерии и показатели эффективности стеганографических систем защиты информации	189
<i>И.В. Олешко, И.Д. Горбенко</i> Сравнительный анализ протоколов строгой аутентификации	198

### РАДИОЛОКАЦИЯ

<i>О.В. Сытник, В.М. Карташов, А.А. Супрун</i> Пространственная селекция широкополосных источников по собственным числам ковариационной матрицы	210
<i>О.О. Байздренко, В.Б. Лубський</i> Розрахунок характеристик виявлення сигналів, відбитих об'єктами, розташованими на морській поверхні, полуактивною бістатичною РЛС з цифровим телевізійним сигналом освітлення	216

<i>А.А. Буланый, Г.В. Майстренко, А.А. Стрельницкий, В.М. Шокало</i> Сравнительный анализ помехозащищенности и спектральной эффективности Wi-Fi каналов связи с линейными и двумерными адаптивными антенными решетками при воздействии нескольких помех и одного сигнала	222
<i>С.В. Марченко, В.М. Морозов., А.М. Съянов</i> Исследование ФАР с диэлектрическим заполнением и согласующей периодической структурой	229
<i>В.М. Карташов, Д.Н. Куля</i> Синтез и анализ дискриминатора следающего устройства систем радиоакустического зондирования атмосферы	234
<i>Б.В. Жуков, А.В. Одновол</i> Контроль уровня легкоиспаряющихся жидкостей методом акустической локации	239
<i>Г.М. Чекалин, Г.Н. Чекалина</i> Об аналитических методах синтеза поляризационного эллипса	245
<i>Ю.В. Лыков</i> Результаты экспериментального исследования телефонных радиозакладных устройств методом нелинейной локации	252
<i>В.И. Леонидов</i> Модельно-структурный анализ эхосигналов акустического зондирования атмосферы	258

### **СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ**

<i>И.С. Шостко, Ю.Э. Соседки, Алмакадма Таха</i> Разработка рекомендаций по регулированию пропускной способности в WPAN	262
<i>И.В. Ковтун</i> Особенности передачи данных по блокам в транкинговой системе стандарта ARCO 25	270
<i>Ю.Г. Лега</i> Завадостійкість m-позиційного автокореляційного приймача шумових сигналів в гауссовому каналі	275
<i>С.А. Шейко</i> Особенности межкадрового сжатия видеoinформации в устройствах видеонаблюдения и видеорегистрации	283
<i>В.Г. Котух, М.А. Мирошник, С.Н. Селевко</i> Методы планирования ресурсов в распределенных компьютерных системах	290

### **РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА**

<i>Л.М. Карпуков, Р.Ю. Корольков</i> Прямой метод синтеза полосно-пропускающих шлейфовых фильтров с чебышевской характеристикой	300
<i>П.Ф. Лебедев, В.П. Дробышев</i> Схемы замещения конденсаторов и катушек индуктивности	306
<i>Д.Ю. Пенкин, Л.П. Яцук</i> Анализ энергетических характеристик поперечной щели в широкой стенке прямоугольного волновода с локальным диэлектрическим включением	313
<i>С. Л. Бердник</i> Излучение электромагнитных волн электрически длинной щелью с диэлектрическим заполнением в узкой стенке многомодового прямоугольного волновода	322
<i>О.І. Филипенко, О.В. Сичова</i> Моделювання впливу структури фотонно-кристалічних волокон на розподіл модового поля та втрати оптичного сигналу в їх з'єднаннях	327
<i>Н.И. Слипченко, В.А. Письменецкий, А.В. Фролов, Н.В. Герасименко, М.Ю. Гуртовой, Е.С. Глушко, Т.Е. Стыценко</i> Исследование и оптимизация пленочных кремниевых аморфных фотопреобразователей на p-i-n-структурах	332
<i>А.А. Жалило</i> Разработка и тестирование новых эффективных методов и алгоритмов обнаружения и устранения фазовых скачков статических и кинематических ГНСС-наблюдений	340
<b>ABSTRACTS</b>	372

*От редколлегии*

В сборнике «Радиотехника» №170 были опубликованы три статьи П.П.Лезова. Редколлегия считает эти статьи ошибочными и приносит извинения за их публикацию.

*Редколлегия*

## CONTENT

### BLOCK AND SYMMETRIC CYPHERS

<i>V.I. Dolgov, A.A. Nastenko</i> On the role of key schedules in attacks on iterated ciphers	7
<i>V.I. Dolgov, E.D. Melnichuk</i> S-blocks for modern ciphers	16
<i>O.V. Kazymyrov, R.V. Oliynykov</i> Mickey cipher cryptanalysis based on internal states analysis	24
<i>I.V. Lisitskaya</i> Degenerated substitutions	31
<i>V.I. Ruzhentsev</i> About the proof of effective byte differential characteristics absence for Rijndael-like ciphers	39
<i>A.A. Kuznetsov, A.V. Kovalenko, S.A. Isaev</i> Synthesis of nonlinear substitution components with the use of non-binary cryptographic functions	43

### CRYPTOGRAPHIC TRANSFORMATION

<i>E.G. Kachko, D.S. Balagura, K.A. Pogrebnyak, Y.I. Gorbenko</i> Investigation of methods for calculation of the inversion algorithm, NTRU	58
<i>I.M. Lyenshyna, A.V. Lyenshyn</i> Cryptographic support of unauthorized access protection services	64
<i>K.A. Pogrebnyak, D.V. Povtariev</i> Model of using cloud computing for problems of asymmetric cryptanalysis illustrated by the example of factorization of numbers by $\rho$ -Pollard algorithm	72
<i>I.D. Gorbenko, L.V. Makutonina</i> Resistance analysis computational problems based on the bilinear maps	79
<i>D.V. Ivanenko</i> Methods to counteract side channel attacks to the schemes in rings of truncated polynomials	90
<i>U.I. Gorbenko, R.I. Mordvinov</i> Essence and analysis of cryptographic requirements from NIST SP 800-90B	99
<i>Ye. Kotukh</i> Universal hashing with limited functional field of algebraic curves	109
<i>I. D. Gorbenko, M. V. Yesina</i> Number field sieve algorithm	116
<i>V.Y. Kovtun, A.O. Okhrimenko</i> Approaches to parallelization of software implementation of integer multiplication	123
<i>O.A. Shevchuk, U.I. Gorbenko</i> HSM Authentication	132
<i>O.G. Khalimov, A.N. Guetzog</i> Universal hashing by generalized Hurwitz curves	140
<i>A.P. Buby, I.D. Gorbenko</i> Evaluation of lattice-based public key algorithm NTRU resistance against adaptive chosen cipher texts attack	147
<i>A.P. Buby, I.D. Gorbenko</i> Evaluation of lattice-based public key algorithm NTRU resistance against adaptive chosen ciphertexts attack	152

### INFORMATION TRANSMISSION AND PROCESSING

<i>Y.I. Gorbenko, A.S. Totsky, V.A. Ponomar</i> Analysis of the methods of personal data anonymization	59
<i>A.V. Potiy, D.Y. Pilipenko</i> Institutional model of information security activities management	164
<i>O.A. Zamula, S.O. Syrota, N.I. Kosikovskaia</i> Quantitative assessment of information technology systems vulnerabilities	171
<i>O.A. Zamula</i> Proposal for construction of the wide-band transmission systems with complex signals	177
<i>B.A. Babich, A.V. Sagun, O.A. Kozhukhovska, A.D. Kozhukhovskiy</i> Synthesis of system of multilevel protection of corporate portals on the base of Share Point Platform	185
<i>A.A. Smirnov</i> Criteria and indexes of efficiency of the steganography systems of priv	189
<i>I.V. Oleshko, I.D. Gorbenko</i> Comparative analysis of strong authentication protocols	198

### RADAR

<i>O.V. Sytnik, V.M. Kartashov, O.O. Suprun</i> Spatial selection of wide-band sources using eigenvalue of the covariance matrix	210
<i>A.A. Baizdrenko, V.B. Lubsky</i> Calculation of detection characteristics of signals, reflected by objects located on the sea surface, in semi-active bistatic radar with digital TV signal illumination	216
<i>A.A. Bulany, G.V. Maistrenko, A.A. Strelnitsky, V.M. Shokalo</i> Comparative analysis of immunity and spectral efficiency of Wi-Fi channels with linear and two-dimensional adaptive antenna array under the influence of several interferences and a signal	222

<i>S.V. Marchenko, V.M. Morozov, A.M. Syanov</i> Investigation of PAA with dielectrical inclusion and matching periodical structure	229
<i>V.M. Kartashov, D.M. Kulia</i> Synthesis and analysis of the tracker device discriminator of the atmosphere radio acoustic sensing systems	234
<i>B.V. Zhukov, A.V. Odnovol</i> Control over the level of easily evaporated liquids by the acoustic location method	239
<i>G.M. Chekalin, G.N. Chekalina</i> About analytical methods for synthesis of the polarization ellipse	245
<i>Y.V. Lykov</i> Results of experimental study of telephone radio bugs using nonlinear locations method	252
<i>V.I. Leonidov</i> Model-structural analysis of echo signals of atmospheric acoustic sounding	258

### INFORMATION PROCESSING SYSTEMS

<i>I.S. Shostka, J.E. Sosedka, Almakadma Taha</i> Development of recommendations concerning adjusting of carrying capacity in WPAN	262
<i>I.V. Kovtun</i> Particularities of data transmission to the blocks in the trunking system of APCO 25 standard	270
<i>Yu.G. Lega</i> Noise-immunity of m-positional autocorrelation receiver of noise signals in Gaussian channel	275
<i>S. O. Sheiko</i> Particularities of inter frame coding of video information in the video monitoring and video recording devices	283
<i>V.G. Kotuh, M.A. Miroshnik, S.N. Selevko</i> Methods of resources planning in the distributed computer systems	290

### RADIO ENGINEERING DEVICES

<i>L.M. Karpukov, R.Y. Korolkov</i> The direct method of synthesis bandpass stub filters with Chebyshev characteristic	300
<i>P.F. Lebedev, V.P. Drobyshev</i> Equivalent circuits of condensers and inductance coils	306
<i>D.Yu. Penkin, L.P. Yatsuk</i> Analysis of power characteristics of the transversal slot in the wide wall of the rectangular waveguide with a local dielectric including	313
<i>S. L. Berdnik</i> Radiation of electromagnetic waves by electrically long slot with dielectric filling in the narrow wall of the multimode rectangular waveguide	322
<i>A. I. Filipenko, O.V. Sychova</i> Modeling of the photonic crystal fiber structure impact on the mode field distribution and on the optical signal loss in their connections	327
<i>N.I. Slipchenko, V.A. Pismenetskiy, A.V. Frolov, N.V. Gerasimenko, M.Y. Gurtovoy, L.G. Glushko, T.E. Stytsenko</i> Research and optimization of p-i-n structure based on the amorphous silicon films	332
<i>A.A. Zhalilo</i> Development and testing of new methods and algorithms for detecting and correction the carrier-phase slips of static and kinematic GNSS observations	340

ABSTRACTS	365
-----------	-----