

СОДЕРЖАНИЕ

СИНТЕЗ И АНАЛИЗ СИММЕТРИЧНЫХ КРИПТОПРИМИТИВОВ

<i>Р.В. Олейников, Д.В. Мурин, С.В. Килипко</i> Моделирование атак на отказ в обслуживании для web-приложений с применением бот-сетей	7
<i>А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук</i> Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной	13
<i>О.Г. Халимов, Е.В. Алекси, Г.З. Халимов</i> Построение нетривиальных кривых Гурвица	21
<i>І.Д. Горбенко, К.Е. Лисицкий</i> О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным	27
<i>І.Д. Горбенко, О.О. Кузнецов, А.В. Самойлова</i> Статистичні властивості блокових симетричних шифрів з міжнародного стандарту ISO/IEC 29192-2	40
<i>О.О. Кузнецов, Р.І. Мордвінов, Є.П. Колованова, А.В. Самойлова</i> Дослідження режимів застосування блокових симетричних шифрів відповідно до ISO/IEC 10116-2006	45
<i>В.И. Руженцев</i> Об условиях отсутствия эффективных усеченных байтовых дифференциалов для блочных симметричных шифров	55

СИНТЕЗ И АНАЛИЗ АСИММЕТРИЧНЫХ КРИПТОПРИМИТИВОВ

<i>Е. А. Винокурова</i> Генератор псевдослучайных последовательностей на основе модифицированной рекуррентной нейронной сети	62
<i>А.П. Бубырь, І.Д. Горбенко</i> Оценка стойкости направленного шифра NTRU к атаке, основанной на изменениях времени расшифрования	68
<i>А. О. Бойко, Ю. О. Сергійчук, А. В. Трипілка</i> Аналіз умов імплементації електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку	74
<i>А.В. Бессалов, А.А. Дихтенко</i> Изоморфизм несуперсингулярных кривых над полями характеристики 2 и кривых Эдвардса с одним параметром	88
<i>С.С. Тімохін, І.Д. Горбенко</i> Кодування інформації точками на еліптичній кривій	93

МЕХАНИЗМЫ И СРЕДСТВА ЗАЩИТЫ СЕТЕЙ СВЯЗИ

<i>А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко, А. Березовский</i> Статистический анализ сетевого трафика для систем обнаружения и предотвращения вторжений	97
<i>І.Д. Горбенко, М.І. Харламб</i> Механізми захищеного обміну інформацією при обчисленнях в хмарі	111
<i>В.І. Заболотний, Є.В. Герасименко, В.І. Перепадя</i> Дослідження зміни форми сигналу у каналі побічних електромагнітних випромінювань монітору	116
<i>А.А. Замула, В.Л. Морозов</i> Системы обнаружения и предотвращения вторжения	122
<i>И.А. Громыко</i> Влияние качества интернет-услуг на риски собственника компьютерной сети	127

СОВЕРШЕНСТВОВАНИЕ И РАЗВИТИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

<i>І.Ф. Аулов, І.Д. Горбенко</i> Аналіз формальної моделі безпеки хмари NIST	131
<i>Ю.І. Горбенко, Ю.В. Гончарова</i> Електронна ідентифікація: поняття, визначення, вимоги	138
<i>Ю.І. Горбенко</i> Сутність та необхідність виконання додаткових вимог відносно надання довірчих послуг в ЄС та Україні в період 2015 – 2030 рр.	145
<i>І.Д. Горбенко, М.І. Харламб</i> Створення та аналіз моделі загроз при обчисленнях в хмарі	153
<i>Ю.Є. Яремчук</i> Спеціалізовані процесори реалізації цифрового підписування на основі рекуррентних послідовностей	159

<i>Д.А. Зайцев, Т.Р. Шмелева, В. Ретчитзеггер, Б. Пролл</i> Оценка влияния злонамеренного трафика на функционирование вычислительных решеток	164
--	-----

ФИЗИКА ПРИБОРОВ И СИСТЕМ

<i>Д.Н. Татьянако, Ю.П. Мачехин, К.А. Лукин</i> Влияние поляризации оптического излучения на фототок различных моделей трап-детекторов	172
<i>Ю. П. Мачехин, Е. Г. Меркулов</i> Оптические частотные реперы на основе холодных атомов в дефектах фотонных кристаллов	181
<i>А. С. Вакула, С. В. Недух, С. И. Тарапов, С. Ю. Полевой</i> Комплекс для исследования наноразмерных магнетиков методом сверхвысокочастотного электронного парамагнитного резонанса	187
<i>О.А. Сушко, И.В. Мукановская</i> Квантово-механический подход к определению параметров нанофотонного сенсора при детектировании 3,4-бензпирена	191

ЭЛЕКТРОДИНАМИКА

<i>А.В. Безуглий, О.М. Петченко</i> Дифракция электронов при похилому падінні на гратку нескінченно тонких металевих стрічок	200
<i>Л.И. Кожара, С.Ю.Полевой, Д.С.Филонов, С.И. Тарапов</i> Передача субволнового изображения проволочной линзой с фазовой компенсацией в миллиметровом диапазоне длин волн	205
<i>А. А. Харченко</i> Поверхностные электромагнитные состояния и левосторонние свойства в структуре фотонный кристалл – феррит – плазмopodobная среда	210

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

<i>О.Ю. Евсеева, Э. М. Аль-Аззави</i> Модель маршрутизации и распределения канальных ресурсов WiMaxmesh-сети	214
<i>С.В. Гаркуша, Е.В. Гаркуша</i> Модель выделения требуемой скорости передачи в нисходящем канале связи технологии LTE	221
<i>Фуад Вехбе, С.А.Заводов</i> Исследование влияния самоподобного трафика на показатели качества передачи речи в информационно-телекоммуникационных системах	229

ОБРАБОТКА СИГНАЛОВ

<i>С.К. Мещанинов</i> Задача построения адекватного математического описания процесса преобразования сигнала в электронно-измерительной системе	235
<i>А.И.Литвин-Попович</i> Системы обработки сигналов в режиме реального времени	242

РАДИОТЕХНИЧЕСКИЕ УСТРОЙСТВА И СРЕДСТВА ТЕЛЕКОММУНИКАЦИИ

<i>О.Б. Зайченко, И.И. Ключник, М.А. Мирошник, Р.И. Цехмистро</i> Сравнительный анализ погрешности многозондовых микроволновых мультиметров с обработкой методами фильтра Калмана и наименьших квадратов, учитывающий переотражения зондов	247
<i>И.С. Шостко, Ю.Э. Соседка</i> Анализ энергопотребления модулей для беспроводных сенсорных сетей стандарта IEEE 802.15.4	253
<i>С.А. Макаров, О.М. Чекунова, С.А. Юхновський</i> Математична модель швидкодіючої самонастроювальної нелінійної системи фазового автопідстроювання частоти	258

РЕФЕРАТЫ	262
-----------------	-----

CONTENT

SYNTHESIS AND ANALYSIS OF SYMMETRIC CRYPTOPRIMITIVES

<i>R.V. Oliynykov, D.V. Murin, S.V. Kylypko</i> Modelling of botnet based DDoS attacks targeted to web applications	7
<i>A.N. Alekseychuk, S.N. Konushok, A.Y. Storozhuk</i> Statistical attack on key-stream generator with linear re-initialization mechanism and output function close to an algebraic degenerate one	13
<i>O.G. Khalimov, E.V. Alexi, G.Z. Khalimov</i> Nontrivial Hurwitz curves construction	21
<i>I.D. Gorbenko, K.E. Lisitskiy</i> The dynamics of the parish to a random permutation ciphers using S-boxes with exponents of nonlinearity close to the limit	27
<i>I.D. Gorbenko, O.O. Kuznetsov, A.V. Samoilo</i> Statistical properties of symmetric block cipher of the ISO / IEC 29192-2 international standard	40
<i>O.O. Kuznetsov, R.I. Mordvinov, E.P. Kolovanova, A.V. Samoilo</i> Investigation into symmetric block cipher modes application in accordance with ISO/IEC 10116-2006	45
<i>V.I. Ruzhentsev</i> About conditions of effective truncated byte differential absence for block ciphers	55

SYNTHESIS AND ANALYSIS OF ASYMMETRIC CRYPTOPRIMITIVES

<i>O. A. Vynokurova</i> Pseudorandom number generator based on modified neural network	62
<i>A.P. Buby, I.D. Gorbenko</i> Evaluation of lattice-based public key algorithm NTRU resistance against timing attack	68
<i>A. Boiko, Y. Sergiichuk, A. Trypilka</i> Analysis of conditions for implementation of electronic identification and trusted services for electronic transactions in the domestic market	74
<i>A.V. Bessalov, A.A. Dihtenko</i> Birational equivalence between canonical elliptic curves over fields of characteristics 2 and Edwards curves	88
<i>S.S. Timohin, I.D. Gorbenko</i> Encoding of information using points on elliptic curves	93

MECHANISMS AND MEANS OF COMMUNICATION NETWORK PROTECTION

<i>O.O. Kuznetsov, A.A. Smirnov, D.A. Danilenko, A. Berezovskiy</i> Statistical analysis of network traffic detection systems and intrusion prevention	97
<i>I.D. Gorbenko, M.I. Kharlamb</i> Mechanisms for secure communication in cloud computing	111
<i>V.I. Zabolotny, E.V. Gerasimenko, V.I. Perepadya</i> Studies on changes in the signal waveform in the channel of the monitor side electromagnetic radiation	116
<i>A.A. Zamula, V.L. Morozov</i> Intrusion detection and prevention systems	122
<i>I.A. Gromyko</i> Influence of internet service quality on risks of a computer network owner	127

IMPROVEMENT AND DEVELOPMENT OF INFORMATION-TELECOMMUNICATION SYSTEM

<i>I.F. Aulov, I.D. Gorbenko</i> Analysis of NIST formal cloud security model	131
<i>Yu.I. Gorbenko, Yu.V. Goncharova</i> Electronic identification: concept, definition, requirements	138
<i>Yu. I. Gorbenko</i> The essence and the need to fulfill additional requirements for the provision of trustee services in the EU and Ukraine in the period of 2015 - 2030	145
<i>I.D. Gorbenko, M.I. Kharlamb</i> Creation and analysis of the threats model in cloud computing	153
<i>Iu. Iaremchuk</i> Specialized processors realization of digital signature based on recurrent sequences	159
<i>D.A. Zaitsev, T.R. Shmeleva, W. Retschitzegger, B. Proll</i> Evaluation of ill-intended traffic influence on computing grids functioning	164

PHYSICS OF DEVICES AND SYSTEMS

<i>D. N. Tatyanko, Y. P. Machekhin, K. A. Lukin</i> Influence of optical radiation polarization on photocurrent of different trap detectors models	172
<i>Y. P. Machekhin, E. G. Merkulov</i> Generation of optical frequency bench mark based on photonic crystals with defects and trapped cold atoms	181
<i>A. S. Vakula, S. V. Nedukh, S. I. Tarapov, S. Yu. Polevoy</i> Complex of nanoscale magnetic materials study by microwave electron spin resonance method	187
<i>O.A. Sushko, I.V. Mukanovska</i> Quantum-mechanical approach to determination of nanophotonic sensor parameters during 3,4-benzpyrene detection	191

ELECTRODYNAMICS

<i>A.V. Besougly, A.M.Petchenco</i> Diffraction of electrons on the grating of infinitely thin metallic strips at the inclined incidence	200
<i>L. Kozhara, S. Polevoy, D. Filonov, S. Tarapov</i> Transmission of subwavelength image by wire lens with phase compensation in the millimeter wavelength range	205
<i>G.O.Kharchenko</i> Surface electromagnetic states and left-hand properties of the photonic crystal – ferrite – plasma-like media structure	210

TELECOMMUNICATIONS SYSTEMS AND NETWORKS

<i>O.Yu. Yevsyeyeva, E.M. Al-Azzawi</i> Model of routing and scheduling in WiMaxmesh-network	214
<i>S.V. Garkusha, O.V. Garkusha</i> Model for the desired transmission rate selection in the downlink technology LTE	221
<i>Fouad Wehbe, S.A.Zavodov</i> Investigation of self-similar traffic influence on the voice transmission quality in information and telecommunication systems	229

SIGNAL PROCESSING

<i>S.K.Meshaninov</i> Problem of constructing an adequate mathematical description of the signal shaping process in the electronic-measuring system	235
<i>A.I.Lytvyn-Popovych</i> Signal processing systems in real-time mode	242

RADIO ENGINEERING DEVICES AND TELECOMMUNICATIONS MEANS

<i>O.B. Zaychenko, I. I. Klyuchnyk, M.A. Miroshnik, R.I. Tsekhmistro</i> Comparative analysis of the multiprobe microwave multimeters errors with methods of Kalman filter and least squares processing, taking into account the multireflection of probes	247
<i>I.S. Shostko, J.E. Sosedka</i> Power analysis modules for wireless sensor networking standard	253
<i>S. A. Makarov, O.N. Chekunova, S.A. Yukhnovsky</i> Mathematical model of high-speed self-adaptive nonlinear system of phase lock	258

ABSTRACTS	262
-----------	-----