

ЗМІСТ

ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

<i>І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій</i> Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки	5
<i>Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, М.В. Єсіна, Г.А. Малєєва</i> Основні положення щодо моделі безпеки для асиметричних перетворень типу ЕП з урахуванням вимог та загроз постквантового періоду	29
<i>Є.Ю. Каптьол, І.Д. Горбенко</i> Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері	37
<i>Ю.І. Горбенко, О.С. Дроздова</i> Аналіз стійкості постквантового електронного підпису Dilithium до атак на помилки	49
<i>І.Д. Горбенко, С.О. Кандій, М.В. Єсіна, Є.В. Остряньська</i> Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки	57
<i>В.А. Кулібаба</i> Процеси та методи вибору загальносистемних параметрів перспективного алгоритму електронного підпису на основі алгебраїчних решіток	64
<i>Ю.І. Горбенко, М.В. Єсіна, В.В. Онопрієнко, Г.А. Малєєва</i> Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису	72
<i>В.І. Руженцев</i> Порівняльний аналіз ARX схем шифрування	79

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

<i>І.Д. Горбенко, Є.А. Семенко, О.А. Замула</i> Методи та засоби синтезу і генерації сигналів – фізичних переносників даних у сучасних інформаційно-комунікаційних системах	87
<i>В.Р. Воронов, В.І. Заболотний, В.І. Лиско</i> Врахування інтерференційної складової в технічному каналі витоку інформації побічного електромагнітного випромінювання відеотракту при рознесеному прийомі	99
<i>І.Д. Горбенко, О.А. Замула, Хо Чі Лик</i> Комплексне вирішення проблеми електромагнітної сумісності сучасних інформаційно-комунікаційних систем	106
<i>К.Є. Лисицький, І.В. Лисицька</i> Математична модель випадкової підстановки (рос.)	116

ОБРОБКА СИГНАЛІВ В РАДІОТЕХНІЧНИХ СИСТЕМАХ

<i>І.В. Корытцев, С.О. Шейко, В.М. Карташов, О.В. Зубков, В.М. Олейніков, С.І. Бабкін, І.С. Селезньов</i> Обробка сигналів при пеленгації і визначенні дальності до малорозмірних БПЛА в оптичному і інфрачервоному діапазонах (рос.)	125
<i>О.В. Зубков, С.О. Шейко, В.М. Олейніков, В.М. Карташов, І.В. Корытцев, С.І. Бабкін</i> Дослідження ефективності детектування та розпізнавання зображень дронів за відеопотоком (рос.)	136
<i>В.І. Леонідов, В.В. Семенець</i> Аналіз частотно-часової структури акустичних шумів малих автоматичних аеросистем (рос.)	147
<i>В.М. Карташов, І.В. Корытцев, С. О. Шейко, В.М. Олейніков, О.В. Зубков, С.І. Бабкін</i> Оптико-електронні методи виявлення повітряних об'єктів та вимірювання їхніх координат (рос.)	153
<i>Є.В. Рогожкін, Ю.І. Под'ячий, Л.Я. Ємельянов</i> Особливості застосування теореми відліків при обробці вузькосмугових радіосигналів з відомою центральною частотою спектра (рос.)	160
<i>С.В. Солонська, В.В. Журнов</i> Предикатна модель процесних знань при виявленні і розпізнаванні протяжних об'єктів типу хмари, «ангел-луна» в оглядових РЛС (рос.)	164
<i>В.М. Карташов, В.Н. Олейніков, В.П. Рябуха, С.И. Бабкин, В.В. Воронин, А.И. Капуста, И.С. Селезнев</i> Методы комплексной обработки и интерпретации радиолокационных, акустических, оптических и инфракрасных сигналов беспилотных летательных аппаратов (рос.)	173

ПРИСТРОЇ РАДІОТЕХНІКИ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

<i>В.Г. Крижановський</i> Фазові характеристики підсилювача класу Е з різними вихідними ланками	183
---	-----

ФІЗИКА ПРИСТРОЇВ ТА СИСТЕМ

<i>О.М. Андреев, О.М. Андреева</i> Дослідження інерційних характеристик фоторезисторів у фізичному практикумі (рос.)	189
--	-----

РЕФЕРАТИ	196
----------	-----

CONTENT

PROSPECTIVE METHODS AND MEANS OF CRYPTOGRAPHIC TRANSFORMATIONS

<i>I.D. Gorbenko, A.M. Alekseychuk, O.G. Kachko, Yu.I. Gorbenko, M.V. Yesina, S.O. Kandy</i> Methods for calculating system parameters for electronic signature "Crystals-Dilithium" 128, 256, 384 and 512 bits of security levels	5
<i>Yu.I. Gorbenko, O.V. Potii, V.V. Onoprienko, M.V. Yesina, G.A. Maleeva</i> Basic statements on the security model for asymmetric transformations of the ES type taking into account the requirements and threats of the post-quantum period	29
<i>Ye.Yu. Kaptol, I.D. Gorbenko</i> Analysis of the possibilities and peculiarities of programming cryptology problems on a quantum computer	37
<i>U.I. Gorbenko, O.S. Drozdova</i> Analysis of Dilithium post-quantum electronic signature resistance to fault attacks	49
<i>I.D. Gorbenko, S.O. Kandy, M.V. Yesina, E.V. Ostryanska</i> Generation of system-wide parameters for Falcon cryptosystem for 256, 384, 512 bits of security	57
<i>V.A. Kulibaba</i> Processes and methods of selection of system-wide parameters of perspective algorithm of electronic signature based on algebraic lattices	64
<i>Yu.I. Gorbenko, M.V. Yesina, V.V. Onoprienko, G.A. Maleeva</i> Threat models for asymmetric cryptotransformations of the promising electronic signature	72
<i>V.I. Ruzhentsev</i> Comparative analysis of ARX encryption schemes	79

PROTECTION OF INFORMATION IN INFORMATION AND COMMUNICATION SYSTEMS

<i>I.D. Gorbenko, E.A. Semenko, A.A. Zamula</i> Methods and means of synthesis and generation of signals – physical carriers of data in modern information and communication systems	87
<i>V.R. Voronov, V.I. Zabolotny, V.I. Lysko</i> Accounting for the interference component in the technical channel of information leakage of spurious electromagnetic radiation in the video path with diversity reception	99
<i>I.D. Gorbenko, A.A. Zamula, Ho Tri Luc</i> Comprehensive solution to the problem of electromagnetic compatibility of modern information and communication systems	106
<i>K. Lisitsky, I.V. Lysitskya</i> Mathematical model of random substitution	116

SIGNAL PROCESSING IN RADIO ENGINEERING SYSTEMS

<i>I.V. Koryttsev, S.O. Sheiko, V.M. Kartashov, O.V. Zubkov, V.M. Oleynikov, S.I. Babkin, I.S. Selieznov</i> Signal processing for direction finding and range determining to small UAVs in the optical and infrared ranges	125
<i>O.V. Zubkov, S.A. Sheyko, V.N. Oleynikov, V.M. Kartashov, I.V. Koryttsev, S.I. Babkin</i> Study of the efficiency of detecting and recognizing drone images from a video stream	136
<i>V.I. Leonidov, V.V. Semenetz</i> Analysis of frequency-time structure of acoustic noise of small automatic air systems	147
<i>V.M. Kartashov, I.V. Koryttsev, S.A. Sheyko, V.N. Oleynikov, O.V. Zubkov, S.I. Babkin</i> Optoelectronic methods for detecting air objects and measuring their coordinates	153
<i>E.V. Rogozhkin, Yu.I. Podyachiy, L.Ya. Emelyanov</i> Features of application of the sampling theorem when processing narrow-band radio signals with known center frequency of the spectrum	160
<i>S. Solonskaya, V. Zhyrnov</i> Predicate model of process knowledge when detecting and recognizing extended objects such as clouds, angel-echoes in surveillance radars	164
<i>V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, S.I. Babkin, V.V. Voronin, A.I. Kapusta, I.S. Seleznirov</i> Methods for complex processing and interpretation of radar, acoustic, optical and infrared signals from unmanned aerial vehicles	173

RADIO ENGINEERING DEVICES AND MEANS OF TELECOMMUNICATIONS

<i>V.G. Krizhanovski</i> Phase characteristics of E class amplifier with various output networks	183
--	-----

PHYSICS OF DEVICES AND SYSTEMS

<i>O.M. Andreiev, O.M. Andreieva</i> Study on inertial characteristics of photoresistors in a physical workshop	189
---	-----

ABSTRACTS	196
-----------	-----