

## ЗМІСТ

### МЕТОДИ ТА МЕХАНІЗМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

<i>В.В. Семенець, О.С. Марухненко, І.Д. Горбенко, Г.З. Халімов</i> Порівняльний аналіз одноразових підписів на базі геш-функцій	5
<i>М.В. Єсіна, Б.С. Шахов</i> Аналіз та дослідження алгоритму цифрового підпису Рісніс	19
<i>М.А. Полуяненко, Ю.І. Горбенко, В.Е. Сафоненко, О.О. Кузнецов</i> Уточнення оцінок ймовірності успіху атаки подвійної витрати на блокчейн системи, з урахуванням моделі незалежних гравців (рос.)	25
<i>О.О. Кузнецов, О.А. Смирнов, А.С. Киян, Т.Ю. Кузнецова</i> Приховування даних на основі адресації шумоподібних сигналів (рос.)	38
<i>А.В. Бессалов, Л.В. Ковальчук, Н.В. Кучинська</i> Оцінка ефективності диференціального додавання точок кривих в узагальненої формі Едвардса (рос.)	50
<i>М.С. Луценко</i> Постквантовий алгоритм інкапсуляції ключів Classic McEliece (рос.)	60
<i>Д.В. Гармаш, Г.А. Малєєва, С.О. Кандій</i> Проект стандарту електронного підпису Rainbow та його основні властивості і можливості щодо застосування	82

### МЕТОДИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ

<i>Р.Ю. Гвоздьов, Р.В. Олійников</i> Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах	91
<i>І.Д. Горбенко, Д.О. Фесенко</i> Використання BLOCKCHAIN в автомобільній безпеці	97
<i>К.Ю. Шеханін, Ю.І. Горбенко, Л.О. Горбачова, О.О. Кузнецов</i> Дослідження властивостей носіїв інформації для стеганографічного приховування даних в кластерних файлових системах	109
<i>В.О. Поддубний, О.В. Северінов</i> Менеджмент вразливостей з використанням формалізованого опису	121

### МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ СИГНАЛІВ

<i>І.Д. Горбенко, О.А. Замула, Хо Чі Лик</i> Методи синтезу і формування систем нелінійних дискретних сигналів для сучасних інформаційно - комунікаційних систем	126
<i>С.Г. Рассомахін, О.А. Замула, І.Д. Горбенко, Хо Чі Лик</i> Порівняльний аналіз завадостійкості прийому нелінійних складних дискретних сигналів зі стандартними сигналами АФМ-16 BPSK	133
<i>О.А. Замула, І.Д. Горбенко, Хо Чі Лик</i> Статистичні властивості похідних систем сигналів	141

### РАДІОТЕХНІЧНІ СИСТЕМИ

<i>В.М. Карташов, В.Н. Олейніков, В.І. Леонідов, В.В. Воронін, А.І. Капуста, І.С. Селєзнев, Є.В. Першин</i> Комплексна обробка сигналів інтегрованої системи спостереження безпілотних літальних апаратів з використанням цілевказівки (рос.)	148
<i>І.В. Свід, І.І. Обод, Г.Е. Заволодько</i> Оптимізація обробки даних в літакових відповідачах системи ідентифікації «свій-чужий»	162

### ЕЛЕКТРОДИНАМІКА, ОПТИКА, ТЕХНІКА, НВЧ

<i>М.І. Дзюбенко, В.А. Маслов, В.П. Радіонов, А.А. Фомін</i> Способи регулювання зворотного зв'язку в лазерах терагерцового діапазону (рос.)	170
<i>Б.В. Жуков, С.І. Борбульов</i> Однорезонаторний НВЧ пристрій для контролю комплексної діелектричної проникності рідких паливно-мастильних матеріалів (рос.)	176
<i>А.І. Козар</i> Розсіювання електромагнітних хвиль дискретним октаедром з резонансних сфер (рос.)	181

### ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

<i>В.В. Семенець, В.І. Леонідов</i> Дослідження частотних характеристик імпедансу біологічних тканин (рос.)	186
---	-----

### ОБРОБКА СИГНАЛІВ

<i>В.А. Душена, Є.А. Тягнирядно, І.В. Барішев</i> Порівняльний аналіз алгоритмів суміщення зображень: нормована кореляція проти суміщення на основі SIFT (англ.)	191
<i>В.В. Жирнов, С.В. Солонська</i> Семантичний аналіз флуктуацій радіолокаційної пачки для ідентифікації повітряних об'єктів (рос.)	197

РЕФЕРАТИ	204
СПИСОК РЕЦЕНЗЕНТІВ У 2020р.	230

# CONTENT

## METHODS AND MECHANISMS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

<i>V.V. Semenetz, O.S. Marukhnenko, I.D. Gorbenko, G.Z. Khalimov</i> Comparative analysis of one-time hash-based signatures	5
<i>M.V. Yesina, B.S. Shahov</i> Analysis and research of digital signature algorithm Picnic	19
<i>N.A. Poluyanenko, Yu.I. Gorbenko, V.E. Safonenko, A.A. Kuznetsov</i> Refinement of estimates of the success probability of a double-spend attack on the Blockchain System, Based on the Independent Players Model	25
<i>A.A. Kuznetsov, O.A. Smirnov, A.S. Kiian, T.Y. Kuznetsova</i> Data hiding based on noise-like signal addressing	38
<i>A.V. Bessalov, L.V. Kovalchuk, N.V. Kuchynska</i> Evaluation of the efficiency of differential addition of points of curves in the generalized Edwards form	50
<i>M.S. Lutsenko</i> Post-quantum algorithm of Classic McEliece key encapsulation	60
<i>D.V. Garmash, G.A. Maleeva, S.O. Kandy</i> Draft of Rainbow electronic signature standard and its main properties and application possibilities	82

## INFORMATION PROTECTION METHODS AND MECHANISMS

<i>R.Y. Gvozдов, R.V. Oliynykov</i> Method and technique of formal design of complex information security system in information and telecommunication systems	91
<i>I.D. Gorbenko, D. Fesenko</i> Using BLOCKCHAIN in automotive security	97
<i>K.Yu. Shekhanin, Yu.I. Gorbenko, L.O. Gorbachova, A.A. Kuznetsov</i> Study of storage devices properties for steganographic data hiding in cluster file systems	109
<i>V.O. Poddubnyi, O.B. Severinov</i> Vulnerability management using a formalized description	121

## METHODS OF SYNTHESIS AND ANALYSIS OF SIGNALS

<i>I.D. Gorbenko, A.A. Zamula, Ho Tri Luc</i> Methods of synthesis and formation of a system of nonlinear discrete signals for modern information and communication systems	126
<i>S.G. Rassomakhin, A.A. Zamula, I.D. Gorbenko, Ho Tri Luc</i> Comparative analysis of noise immunity of reception of nonlinear complex discrete signals with standard signals AFM-16 BPSK	133
<i>A.A. Zamula, I.D. Gorbenko, Ho Tri Luc</i> Statistical properties of derived signal systems	141

## RADIO ENGINEERING SYSTEMS

<i>V.M. Kartashov, V.M. Oleinikov, V.P. Ryabukha, V.I. Leonidov, V.V. Voronin, A.I. Kapusta, I.S. Seleznirov, I.V. Pershyn</i> Complex processing of signals of integrated unmanned aerial vehicles surveillance system with the use of target designation	148
<i>I.V. Svyd, I.I. Obod, G.E. Zavalodko</i> Optimization of data processing in aircraft transponder of the "friend or foe" identification system	162

## ELECTRODYNAMICS, OPTICS, MICROWAVE TECHNOLOGY

<i>M.I. Dzyubenko, V.A. Maslov, V.P. Radionov, A.A. Fomin</i> Methods for adjusting feedback in terahertz lasers	170
<i>B.V. Zhukov, S.I. Borbulev</i> Single resonator microwave device for monitoring the complex dielectric constant of liquid fuels and lubricants	176
<i>A.I. Kozar</i> Scattering of electromagnetic waves by a discrete octahedron from resonant spheres	181

## APPLICATION OF METHODS OF RADIO ENGINEERING

<i>V.V. Semenetz, V.I. Leonidov</i> Investigation of frequency characteristics of biological tissues impedance	186
--	-----

## SIGNAL PROCESSING

<i>V.A. Dushhepa, Y.A. Tiahnyriadno, I.V. Baryshev</i> Comparative analysis of algorithms for images fusion: normalized correlation versus fusion based on SIFT	191
<i>V. Zhyrnov, S. Solonskaya</i> Semantic analysis of fluctuations of a radar pack for identification of air objects	197

ABSTRACTS	204
LIST OF REVIEWERS IN 2020	230