

## СОДЕРЖАНИЕ      ЗМІСТ

### МЕТОДЫ, МЕХАНИЗМЫ И АЛГОРИТМЫ КРИПТОГРАФИЧЕСКИХ ПЕРСПЕКТИВНЫХ ПРЕОБРАЗОВАНИЙ

#### МЕТОДИ, МЕХАНІЗМИ ТА АЛГОРИТМИ КРИПТОГРАФІЧНИХ ПЕРСПЕКТИВНИХ ПЕРЕТВОРЕНЬ

<i>И.Д. Горбенко, О.Г. Качко, М.В. Есина</i> Общие положения и анализ алгоритма направленного шифрования NTRU Prime ПТ Ukraine	5
<i>О.О. Кузнецов, И.Д. Горбенко, Ю.И. Горбенко, А.М. Олексійчук, В.А. Тимченко</i> Математична структура потокового шифру Струмук	17
<i>А.М. Олексійчук, С.М. Ігнатенко</i> Алгоритми оцінювання стійкості SNOW 2.0-подібних поточкових шифрів над кільцями лишків відносно кореляційних атак	28
<i>О.Г. Качко, Ю.І. Горбенко, О.С. Акользіна</i> Аналіз атак спеціального типу щодо NTRU-подібного алгоритму	35
<i>А.С. Киян, М.С. Луценко, А.А. Кузнецов</i> Первичный анализ и исследование кодовых схем электронной цифровой подписи и направленного шифрования с NIST PQC	41
<i>М.С. Луценко, А.С. Киян, Т.Ю. Кузнецова, А.А. Кузнецов</i> Анализ и сравнительные исследования кодовых схем инкапсуляции ключей, представленных на конкурс NIST PQC	53
<i>М.О. Полуянченко, О.В. Потій</i> Дослідження реєстрів зсуву з нелінійними зворотними зв'язками в якості комбінуючих та фільтруючих функцій	67
<i>Г.З. Халімов, Є.В. Котух, Ю.О. Сергійчук, О.С. Марухненко</i> Аналіз складності реалізації криптосистеми на групі Судзукі	75
<i>Е.В. Исирова, А.В. Потий, В.В. Семенец</i> Принципы построения децентрализованной инфраструктуры открытых ключей	82
<i>О.О. Кузнецов, В.О. Фроленко, Є.С. Єрьомін, Д.В. Іваненко</i> Дослідження кросплатформних реалізацій потокових симетричних шифрів	94
<i>В.Н. Шлокин, С.Г. Рассомахин</i> Вероятностная модель дактилоскопических образов компьютерной биометрической аутентификации	107

### МЕТОДЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

#### МЕТОДИ БУДУВАННЯ ЗАХИЩЕНИХ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

<i>О.П. Нарезній, В.В. Семенец, Т.О. Гріненко</i> Метод вимірювання квантового фазового шуму та ширини лінії робочого переходу радіооптичної системи генератора випадкових чисел	118
<i>В.И. Есин</i> Инвариантная к предметным областям схема базы данных и ее отличительные особенности	133
<i>В.А. Краснобаев, А.А. Замула, А.С. Янко</i> Примеры определения ранга числа, представленного в непозиционной системе счисления остаточных классов	143
<i>О.А. Замула</i> Технології формування OFDM сигналів в сучасних інформаційно-комунікаційних системах	152
<i>В.І. Заболотний, А.В. Єрмолович</i> Доцільний розподіл витрат на впровадження заходів захисту від технічних засобів розвідки	159
<i>В.І. Заболотний, В.І. Перепадя</i> Особливості моделювання параметрів відеоімпульсу для дослідження спектрів побічних електромагнітних випромінювань	164
<i>К.Ю. Шеханін, А.О. Колгатін, Є.Є. Деменко, О.О. Кузнецов</i> Приховування даних у структуру файлової системи сімейства FAT	169
<i>Є.В. Брошеван, О.В. Потій</i> Особливості реалізації EDELIVERY в контексті електронних довірчих послуг. Досвід Євросоюзу	179
<i>А.В. Потий, А.С. Карпенко</i> Реализация механизма контроля целостности программного обеспечения в постквантовый период	186
<i>И.Д. Горбенко, О.А. Замула</i> Дослідження структури спектрів сигналів з лінійною частотною модуляцією	192
РЕФЕРАТЫ	199

# CONTENT

## METHODS, MECHANISMS AND ALGORITHMSC OF CRYPTOGRAPHIC PERSPECTIVE TRANSFORMATIONS

<i>I.D. Gorbenko, O.G. Kachko, M.V. Yesina</i> General statements and analysis of the end-to-end encryption algorithm NTRU Prime IIT Ukraine	5
<i>O.O. Kuznetsov, I.D. Gorbenko, Y.I. Gorbenko, A.M. Alekseychuk, V.A. Tymchenko</i> Mathematical structure of the Strumok stream cipher	17
<i>A.N. Alekseychuk, S.M. Ignatenko</i> Algorithms for evaluation of the SNOW 2.0-like stream ciphers security over residue rings against correlation attacks	28
<i>O.G. Kachko, Yu. I. Gorbenko, O.S. Akolzina</i> Side-channel attacks analisys against NTRU-similar algorithm	35
<i>A.S. Kiian, M.S. Lutsenko, A.A. Kuznetsov</i> Primary analysis and research on code-based schemes of electronic digital signature and public-key cryptosystems from NIST PQC	41
<i>M.S. Lutsenko, A.S. Kiian, T.Y. Kuznetsova, A.A. Kuznetsov</i> Analysis and comparative studies of code-based key encapsulation mechanisms submitted to the NIST PQC competition	53
<i>N. Poluyanenko, O. Potii</i> Investigation of shift registers with nonlinear feedbacks as combining and filtering functions	67
<i>G.Z. Khalimov, Y.V. Kotukh, Yu.A. Sergiychuk, A.S.</i> Analysis of the implementation complexity of the cryptosystem on the Suzuki group	75
<i>K.V. Isirova, O.V. Potii, V.V. Semenez</i> Principles of decentralized public key infrastructure building	82
<i>A.A. Kuznetsov, V.O. Frolenko, E.S. Eremin, D.V. Ivanenko</i> Investigation of cross-platform realizations of stream symmetric ciphers	94
<i>V.M. Shlokin, S.G. Rasomakhin</i> Probabilistic model of fingerprint images of computer biometric authentication	107

## METHODS FOR CONSTRUCTION OF PROTECTED TELECOMMUNICATIONS AND INFORMATION TECHNOLOGIES

<i>O.P. Nariezhnii, V.V. Semenets, T.O. Grinenko</i> Method for measuring quantum phase noise and working transition line width of radio-optical system of random number generator	118
<i>V.I. Yesin</i> Database schema invariant to subject domains and its distinctive features	133
<i>V.A. Krasnobayev, A.A. Zamula, A.S. Yanko</i> Examples of determining the rank of a number represented in the non-position system of residual classes	143
<i>A.A. Zamula</i> Technologies of forming OFDM signals in modern information and communication systems	152
<i>V.I. Zabolotniy, A.V. Yermolovych</i> Expedient allocation of costs for implementation of protection measures against technical reconnaissance means	159
<i>V.I. Zabolotny, V.I. Perepadia</i> Features of video-pulse parameters simulation for studying spectra of secondary electromagnetic radiation	164
<i>K.Yu. Shekhanin, A.O. Kolhatin, E.E. Demenko, A.A. Kuznetsov</i> Data hiding in the FAT family file system structure	169
<i>E.V. Brochevan, A.V. Poty</i> Features of the EDELIVERY implementation in the context of electronic trust services. The experience of the Euro-Union	179
<i>O. Potii, A. Karpenko</i> Realization of the mechanism of control software integrity in post quantum period	186
<i>I.D. Gorbenko, A.A. Zamula</i> Investigation into the structure of spectra of signals with linear frequency modulation	192
ABSTRACTS	199