

# INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY

## MATERIALS

of IX<sup>th</sup> International Scientific  
and Technical Conference



May 25–26, 2023

**ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА  
ІНФОРМАЦІЙНИХ СИСТЕМ**

**INFORMATION PROTECTION  
AND INFORMATION SYSTEMS SECURITY**

*Ministry of Education and Science of Ukraine*

*National Academy of Sciences of Ukraine*

*Ministry of Science and Higher Education of the Republic of Poland*

*Lviv Polytechnic National University*

*Pidstryhach Institute for Applied Problems of Mechanics and Mathematics National  
Academy of Sciences of Ukraine*

*Odessa National Polytechnic University*

*University of Bielsko-Biala (Poland)*

# **INFORMATION PROTECTION AND INFORMATION SYSTEMS SECURITY**

## **MATERIALS of IX<sup>th</sup> International Scientific and Technical Conference**

May 25–26, 2023

Lviv  
Lviv Polytechnic Publishing House  
2023

*Міністерство освіти і науки України  
Національна Академія наук України  
Міністерство науки та вищої освіти Республіки Польща  
Національний університет “Львівська політехніка”  
Інститут прикладних проблем механіки і  
математики ім. Я. С. Підстригача НАН України  
Одеський національний політехнічний університет  
Університет Бельсько-Бяла (Польща)*

# **ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ**

**МАТЕРІАЛИ**  
**IX Міжнародної**  
**науково-технічної конференції**

25–26 травня, 2023

Львів  
Видавництво Львівської політехніки  
2023

**Conference organizers:**

LVIV POLYTECHNIC NATIONAL UNIVERSITY  
PIDSTRYHACH INSTITUTE FOR APPLIED PROBLEMS  
OF MECHANICS AND MATHEMATICS  
ODESSA NATIONAL POLYTECHNIC UNIVERSITY  
AKADEMIA TECHNICZNO-HUMANISTYCZNA, BIELSKO-BIAŁA (POLSKA)

**Захист** інформації і безпека інформаційних  
3-38 систем: матеріали ІХ Міжнар. наук.-техн. конф. –  
Львів : Видавництво Львівської політехніки, 2023. –  
Режим доступу:  
<https://drive.google.com/drive/folders/1z5BLogqaxwh4xgGk2eMLI8WcVNOXCFX6>, вільний –Заголовок з  
екрана. – Мова укр. і англ.

ISBN 978-966-941-829-6

У збірнику опубліковано матеріали конференції,  
присвяченої проблемам у галузі захисту інформації і безпеки  
інформаційних систем. Видання призначено для науковців,  
аспірантів, студентів.

**УДК 004.056.5**

The collection includes texts of reports and theses of speeches prepared for the IX International Scientific and Technical Conference “Information Security and Information Systems Security”.  
The publication is intended for scientists, postgraduates and students.

*Postal address of the Organizing Committee:*

79005, Lviv, 5, Kn. Romana Str., 1, Information Protection Department, room. No. 204.

*Responsible for the issue – Professor Dudykevych V.B.*

*Computer layout and layout – Oprisky I.R.*

*The materials are presented in the author's wording*

### HONORARY CHAIRMEN

**BOBALO Yu.Ya.** – Rector of Lviv Polytechnic National University, D.Sc., Professor

**KUSHNIR R.M.** – Director of the Pidstryhach Institute for Applied Problems of Mechanics and Mathematics of the National Academy of Sciences of Ukraine, Academician of National Academy of Sciences of Ukraine, D.Sc., Professor

**OBORSKYI H.O.** – Rector of Odessa National Polytechnic University, D.Sc., Professor

### CO-CHAIRMEN

**DEMYDOV I.V.** – Vice-Rector for Research at Lviv Polytechnic National University, D.Sc., Associate Professor

**DUDYKEYVYCH V.B.** – Head of the Information Protection Department, Lviv Polytechnic National University, D.Sc., Professor

**KARPIŃSKI M.** – Head of the Department of Computer Science and Automation, The University of Bielsko-Biala (Poland), D.Sc., Professor

**KOBOZYIEVA A.A.** – Head of the Department of Informatics and Information Systems Security Management, Odessa National Polytechnic University, D.Sc., Professor

### PROGRAM COMMITTEE

**BLINTSOV V.S.** – Vice-Rector for Scientific Work of National University of Shipbuilding, Academician of the Academy of Sciences of Shipbuilding of Ukraine, D.Sc., Professor

**HORBENKO I.D.** – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor

**DIVIZINYUK M.M.** – Head of the Department of Civil Defense and Innovation of the Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine, D.Sc., Professor

**YEVSEYEV S.P.** – Head of the cyber security department of the National Technical University University "Kharkiv Polytechnic Institute", D.Sc., Professor

**ZHURAVEL I.M.** – Professor of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor

**ZADIRAKA V.K.** – Head of Department nr 140, V.M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Academician of the National Academy of Sciences of Ukraine, D.Sc., Professor

**ZAGORODNA N.V.** – Head of the Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ph.D., Associate Professor

**KOVELA S.** – MBA PGCE CIP Senior Lecturer Accounting, Finance and Informatics, Kingston University London, Ph.D. (United Kingdom)

**CARLSSON A.** – General Manager of ENGENSEC Tempus Project, lecturer at Blekinge Institute of Technology, Ph.D. (Karlskrona, Sweden)

**JUSTICE C.** – Clinical Associate Professor, CERIAS, Purdue University, CISSP, D.Sc. (USA)

**KORCHENKO O.H.** – Head of the Department of Information Technology Security, National Aviation University, D.Sc., Professor

**ESIN V. I.** – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor

**MARAKOVA-BEGOC I.** – Research Fellow at Bretagne Telecom, D.S (France)

- MATVIYKIV O.M.** – First Vice-Rector of Lviv Polytechnic National University, D.Sc, Professor
- MACHUSKYY Ye.A.** – Head of the Department of Physical and Technical Means for Information Protection, National Technical University of Ukraine "Kyiv Polytechnic Institute", D.Sc., Professor
- MELNYK A.O.** – Head of the Department of Computer Engineering, Lviv Polytechnic National University, D.Sc., Professor
- MELNYK V.A.** – Professor of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor
- MYKYYCHUK M.M.** – Director of the Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, D.Sc., Professor
- MYCHUDA L.Z.** – Professor of Information Technology Security, Lviv Polytechnic National University, D.Sc., Associate Professor
- MOROZ L.V.** – Wydział Mechaniczny Technologiczny, Politechnika Warszawska (Polska), dr hab. inż., profesor uczelni
- NYEMKOVA O.A.** – Associate Professor of the Department of Information Technologies Security, Lviv Polytechnic National University, D.Sc., Professor
- OSTAPOV S.E.** – Head of the Department of Software Computer Systems, Chernivtsi National University, D.Sc., Professor
- PARKHUTS L.T.** – Professor of Information Protection Department, Lviv Polytechnic National University, D.Sc., Professor
- PETROV O.** – Professor AGH, Department of Applied Computer Science, AGH University of Science and Technology Stanisława Staszica, Kraków (Poland), D.Sc..
- POTIY O.V.** – Deputy Head of the State Service for Special Communications and Information Protection of Ukraine, D.Sc., Professor
- RUZHENTSEV V.I.** – Professor of the Department of Information Technology Security, Kharkiv National University of Radio Electronics, Doctor of Technical Sciences, Associate Professor
- RUSYN B.P.** – Head of the Department of Methods and Systems for Images Processing, Analysis and Identification, G.V. Karpenko Physico-Mechanical Institute of the National Academy of Sciences of Ukraine, D.Sc., Professor
- SAMOTYY V.V.** – Professor of the Department of computerized systems of Automation, Lviv Polytechnic University, D.Sc., Professor
- SACHENKO A.O.** – Head of the Department of Information and Computing Systems and Management, Western Ukrainian National University, D.Sc, Professor
- FEDASYUK D.V.** – Head of the Software Department of the Lviv Polytechnic National University, D.Sc., Professor
- KHOMA V.V.** – Professor of the Institute of Automation and Informatics, Opole University of Technology, (Poland), D.Sc., Professor
- KHOROSHKO V.O.** – Professor of the Department of Information Technologies Security, National Aviation University, D.Sc., Professor
- CHAPLYHA V.M.** – Professor of the Department of Automation and Computer-Integrated Technologies of Lviv National Agrarian University, D.Sc, Professor
- CHEVARDIN V.E.** – Head of the Department of Information Protection and Cyber Defense of the Military Institute of Telecommunications and Informatization. Heroes Krut, D.Sc., Senior Researcher
- YAREMCHUK Yu.Ye.** – Director of the Center for Information Technologies and Information Protection, Vinnytsia National Technical University, D.Sc., Professor
- YATSKIV V.V.** – Head of the Department of Cybersecurity, Western Ukrainian National University, D.Sc., Associate Professor

**GUSTAVSSON R.** – Professor at Blekinge Institute of Technology (Karlskrona, Sweden) and at KTH Royal Institute of Technology (Stockholm, Sweden)

**RASMUS J.** – Managing Director of SERIAS (Center of Education and Research in Information Assurance and Security), Purdue University (USA)

**LUZHETSKY V.A.** – Head of the Information Protection Department, Vinnytsia National Technical University, D.Sc., Professor

#### **ORGANIZING COMMITTEE CO-CHAIRMEN**

**MAKSYMОВYCH V.M.** – Head of the Department of Information Technology Security, Lviv Polytechnic National University, D.Sc., Professor

**MARCHUK M.V.** – Head of Department №15, Ya. S. Pidstryhach Institute of Applied Problems of Mechanics and Mathematics of the National Academy of Sciences of Ukraine, D.Sc., Professor

#### **ORGANIZING COMMITTEE**

**BORTNIK L.L.** – Senior lecturer of the Department of Information Protection of Lviv Polytechnic National University, Ph.D.

**VOYTUSIK S.S.** – Associate Professor of the Department of Information Technologies Security, Lviv Polytechnic National University, Ph.D.

**HORPENYUK A.Ya.** – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

**ESINA M.V.** – Professor of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, D.Sc., Professor.

**KOROBAYNIKOVA T.I.** – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

**KOSTIV Yu.M.** – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

**KUTEN R.B.** – Assistant of the Department of Information Protection, Lviv Polytechnic National University

**CHUBYK R.V.** – Associate Professor of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

**LAH Yu.V.** – Associate Professor of Information Protection, Lviv Polytechnic National University, Ph.D.

**SHABATURA M.M.** – Associate Professor of the Department of Information Technology Security, Lviv Polytechnic National University, Ph.D., Associate Professor

**SOVYN Ya.R.** – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D., Associate Professor

**STAKHIV M.Yu.** – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D.

**TYSHYK I.Ya.** – Associate Professor of the Department of Information Protection, Lviv Polytechnic National University, Ph.D.

#### **SECRETARY**

**OPIRSKYI I.R.** – Professor of the Department of Information Protection, Lviv Polytechnic National University, D.Sc., Professor



## CONTENT

<b>SECTION I ADMINISTRATION AND MANAGEMENT OF INFORMATION AND CYBER SECURITY</b>	<b>13</b>
<b>Andrii SHPILKIN, Vadym VOLOTKA. COMPARATIVE ANALYSIS OF UKRAINIAN AND US CYBER STRATEGIES</b>	13
<b>Yevhenii KURII, Ivan OPIRSKYI, Leonid BORTNIK. ISO/IEC 27001:2022 – ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD</b>	15
<b>Валерія БАЛАЦЬКА, Іван ОПІРСЬКИЙ. МЕХАНІЗМИ ДОСЯГНЕННЯ НАДІЙНОСТІ В БЛОКЧЕЙНІ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ</b>	17
<b>Lidiia VLASENKO, Tetiana SAVCHENKO. ANALYSIS OF IoT SECURITY LEVELS</b>	19
<b>Serhii BUCHYK, Anastasiia SHABANOVA, Oleksandr BUCHYK. DEVELOPMENT OF AN ENTERPRISE INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON IT-GRUNDSCHUTZ TECHNOLOGIES</b>	21
<b>Андрій ГІЗУН, Владислав ГРІГА. ВИЗНАЧЕННЯ БАЗОВИХ ПАРАМЕТРІВ ДЛЯ ОЦІНЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ</b>	23
<b>Олена САМОЙЛЕНКО. ДОСЛІДЖЕННЯ ТА АНАЛІЗ ДІЯЛЬНОСТІ ETSI TC CYBER</b>	25
<b>Ілля ТАЧЕНКО, Тетяна КОРОБЕЙНИКОВА, Наталя ЛУЖЕЦЬКА. МЕТОД РОЗРОБЛЕННЯ ЗАГАЛЬНИХ МЕТРИК ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ</b>	27
<b>Дмитро ЧИНЧИК, Тетяна КОРОБЕЙНИКОВА, Наталя ЛУЖЕЦЬКА. МЕТОД КОМПЛЕКСНОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ</b>	29
<b>Єлизавета ПОПОВСЬКА, Юлія КУЛЯ. АНАЛІЗ СУЧАСНИХ ЗАГРОЗ БЕЗПЕЦІ БЕЗПРОВОДОВИХ МЕРЕЖ</b>	31
<b>Наталя ПЕТЛЯК, Юрій КЛЬОЦ, Віра ТІТОВА, Віктор ЧЕШУН. ВИЯВЛЕННЯ ЗЛОВМИСНОГО ВИХІДНОГО ТРАФІКУ МЕРЕЖІ НА ОСНОВІ НЕЧІТКОГО ЛОГІЧНОГО ВИСНОВКУ</b>	33
<b>Сергій ШОЛОХОВ, Богдан НІКОЛАЄНКО, Юрій ГОЛОВІН, Євген САМБОРСЬКИЙ. МЕТОДИКА ОПТИМІЗАЦІЇ РЕСУРСУ ЗАСОБІВ ДЕСТРУКТИВНОГО ПРОГРАМНОГО ВПЛИВУ ТА РАДІОПРИГНІЧЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ</b>	35
<b>Антон ЗАГІНЕЙ, Олег КУРЧЕНКО, Юрій ЩЕБЛАНІН. РИЗИКИ ВИКОРИСТАННЯ ТУМАННИХ ОБЧИСЛЕНЬ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ</b>	37
<b>Олена НЕМКОВА, Моріка РУСИНКО, Юрій ЛАХ. АВТЕНТИФІКАЦІЯ НОУТБУКІВ З ВИКОРИСТАННЯМ НЕПАРАМЕТРИЧНОГО КРИТЕРІЮ КОЛМОГОРОВА-СМИРНОВА</b>	39
<b>Ілля КОСТЕРЕВ. ЗАСТОСУВАННЯ СКАНЕРУ МЕРЕЖІ ТА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ СЕРВЕРА З ВИКОРИСТАННЯМ NFTABLES</b>	41
<b>Анатолій ШИЯН, Яна ЯРЕМЧУК, В'ячеслав САВРАЦЬКИЙ. МЕТОД ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ВІД ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ АТАК У СОЦІАЛЬНИХ МЕРЕЖАХ</b>	43
<b>SECTION II INFORMATION PROTECTION IN INFORMATION AND COMMUNICATION SYSTEMS. CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION</b>	<b>45</b>
<b>Василь ПОБЕРЕЖНИК, Іван ОПІРСЬКИЙ, Тарас КРЕТ. АНАЛІЗ ПРИДАТНОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПОБУДОВИ СЕРВІСІВ ОБМІНУ ПОВІДОМЛЕННЯМИ</b>	45

<b>Андрій ТЕРЕЩЕНКО, Валерій ЗАДРАКА. БАГАТОРАЗРЯДНА АРИФМЕТИКА ДЛЯ КВАНТОВОЇ МОДЕЛІ ОБЧИСЛЕНЬ</b>	47
<b>Іван БОБОК, Алла КОБОЗЄВА. ОСНОВИ ЗАГАЛЬНОГО ПІДХОДУ ДО ВИЯВЛЕННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ</b>	49
<b>Yehor BOROVYI, Maryna YESINA. RESEARCH AND ANALYSIS OF METHODS FOR ENSURING THE SECURITY OF ARTIFICIAL INTELLIGENCE SYSTEMS</b>	51
<b>Роман БАНАХ, Андріян ПІСКОЗУБ. ВИМІРЮВАННЯ ПОТУЖНОСТІ СИГНАЛУ ВІД КЛІЄНТСЬКИХ ПРИСТРОЇВ В МЕРЕЖАХ IEEE 802.11 ДЛЯ ТРЕНУВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ЗАДЛЯ ВИЯВЛЕННЯ АТАК</b>	53
<b>Іван ГОРБЕНКО, Марина ЄСІНА, Володимир ПОНОМАР. СТАН ТА ПРОБЛЕМИ РОЗРОБКИ ТА ПРИЙНЯТТЯ ПОСТКВАНТОВИХ СТАНДАРТІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ РІВНЯХ</b>	55
<b>Ярослав ДЕРЕВ'ЯНКО, Іван ГОРБЕНКО. ПРАКТИЧНА ОЦІНКА КОНТРЗАХОДІВ ПРОТИ АТАК СТОРОННІМИ КАНАЛАМИ ТА ПОМИЛКАМИ НА DILITHIUM</b>	57
<b>Леонов МИКИТА. СТАН АЛГОРИТМІВ ПОСТКВАНТОВОГО ШИФРУВАННЯ ЗА ДОПОМОГОЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ РІВНЯХ</b>	59
<b>Ігор САВЧЕНКО. ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ</b>	61
<b>Іванов ДЕНИС. ЗАХИСТ ШЛЯХОМ ПОДВІЙНОГО ХЕШУВАННЯ ДАНИХ</b>	63
<b>Злата ПОТАПОВА, Володимир ПОНОМАР. ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСОБІВ БЕЗПЕКИ В УКРАЇНСЬКИХ СИСТЕМАХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ</b>	65
<b>Євгеній КАПТЬОЛ. KEY ENCAPSULATION MECHANISMS SECURITY IN THE RANDOM ORACLE MODEL / БЕЗПЕКА МЕХАНІЗМІВ ІНКАПСУЛЯЦІЇ КЛЮЧІВ У МОДЕЛІ ВИПАДКОВОГО ОРАКУЛА</b>	67
<b>Валерій ДУДИКЕВИЧ, Галина МИКИТИН, Володимир ФІГУРНЯК. ДО ПИТАННЯ БЕЗПЕКИ КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ ДІМ»</b>	69
<b>Сергій КУЛИНА. МЕТОД ЗАХИЩЕНОГО ЗБЕРІГАННЯ ДАНИХ НА ОСНОВІ НАДЛИШКОВОЇ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ТА ХЕШ ФУНКЦІЇ</b>	71
<b>Наталія КУХАРСЬКА, Дем'ян МОРОЗ. ПРИХОВУВАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В АУДИОФАЙЛАХ З ВИКОРИСТАННЯМ K-SHUFFLE ПІДХОДУ</b>	73
<b>Єлизавета ЛАЗАРЄВА, Юрій ГОРБЕНКО. КРИПТОГРАФІЧНІ МЕТОДИ У ХМАРНИХ СЕРВІСАХ</b>	75
<b>Сергій ЛІЛКОВИЧ, Віталій ЄСІН. ПІДХІД ДО ШИФРУВАННЯ З МОЖЛИВІСТЮ ПОШУКУ ЧИСЛОВИХ ДАНИХ</b>	77
<b>Єлизавета ЛОГАЧОВА, Марина ЄСІНА. КОНТРОЛЬ ЗАХИСТУ ДАНИХ НА ПІДПРИЄМСТВАХ</b>	79
<b>Володимир ЛУЖЕЦЬКИЙ, Галина КРАЙНІЧУК, Євгеній РАДЧЕНКО, Ігор ПИЛЯВЕЦЬ. АЛГОРИТМ ШИФРУВАННЯ НА ОСНОВІ СІР-КВАЗІГРУП</b>	81
<b>Володимир ЛУЖЕЦЬКИЙ, Юрій БАРИШЕВ. ПІДХІД ДО ПАРАЛЕЛЬНОГО ГЕШУВАННЯ ДАНИХ НА ОСНОВІ МОДЕЛІ КВАТЕРНІОНА</b>	83

	10
<b>Сніжана НОВОСЬОЛОВА, Юрій ГОРБЕНКО. АНАЛІЗ ТА ДОСЛІДЖЕННЯ ВИМОГ ДО КІБЕРЗАХИСТУ ПРИ ВИКОРИСТАННІ ХМАРНИХ ОБЧИСЛЕНЬ</b>	85
<b>Андрій ПАРТИКА, Денис ШЕВЧУК. ПОБУДОВА ЗАХИЩЕНОГО СЕРВІСУ ДЛЯ АВТЕНТИФІКАЦІЇ, АВТОРИЗАЦІЇ ТА ОБЛІКУ КОРИСТУВАЧІВ У ХМАРНОМУ СЕРЕДОВИЩІ AZURE</b>	87
<b>Юрій ЯРЕМЧУК, Василь КАРПІНЕЦЬ, Ірина ЗОРЯ. ПІДВИЩЕННЯ СТІЙКОСТІ ЦВЗ У ПОТОКОВИХ ВІДЕОЗАПИСАХ</b>	89
<b>Юрій СОРОКАТИЙ, Юрій ДОБРОВОЛЬСЬКИЙ. МОДЕЛЬ ФОТОПРИЙМАЧА ДЛЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ОПТИЧНИХ ЦИФРОВИХ КАНАЛАХ ЗВ'ЯЗКУ</b>	91
<b>Марія ШАБАТУРА. ПОРІВНЯННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ</b>	93
<b>Дмитрій ТИХОЛАЗ, Роман БАНАХ. ЗАХИСТ ОБЛІКОВОГО ЗАПИСУ В AWS ЗА ДОПОМОГОЮ DETECTIVE CONTROLS</b>	95
<b>Михайло КІХ, Марія ШАБАТУРА, Володимир МАКСИМОВИЧ. ПОКРАЩЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ LFSR</b>	97
<b>Любов ЗАГОРУЙКО, Людмила ПОЛОВЕНКО, Дмитро ЧЕРНОВ. СТРУКТУРУВАННЯ НЕЙРОПОДІБНОЇ МЕРЕЖІ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ</b>	99
<b>Сергій БУЧИК, Сергій ТОЛЮПА, Олександр БУЧИК. МЕТОДИ ДЕТЕКТУВАННЯ ФІШИНГОВИХ САЙТІВ</b>	101
<b>Pavlo HLUSHCHENKO, Valeriy DUDYKEYUCH. ADVANTAGES OF ZERO TRUST ARCHITECTURE FOR SECURITY OF CI/CD PIPELINES AND INFRASTRUCTURE</b>	103
<b>Vladyslav HAMOLIA, Viktor MELNYK. CRYPTOGRAPHIC ALGORITHMS EXECUTION FEATURES IN HETEROGENEOUS COMPUTER SYSTEMS</b>	105
<b>Roman KARPIUK, Petro VENHERSKYI. USING MACHINE LEARNING (ML) TO DETECT CYBERSECURITY ANOMALIES</b>	107
<b>Galyna MYKYTYN, Khrystyna RUDA, Yuriy KHOMA. CATEGORIZATION OF DEERFAKE METHODS: A COMPARISON OF SINGLE-SHOT AND MULTI-SHOT TRANSFER APPROACHES</b>	109
<b>Elena NYEMKOVA, Nazar CHURA. HIERARCHICAL BIT TEMPLATE MODEL FOR DYNAMIC AUTHENTICATION OF ELECTRONIC DEVICES</b>	111
<b>Любомир РОМАНЧУК, Олег ГАРАСИМЧУК, Анастасія ГАРАСИМЧУК, Михайло ПРИГАРА. ПРОБЛЕМИ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ</b>	113
<b>Юрій ДАНИК, Валерій ШЕСТАКОВ. ПРОБЛЕМНІ ПИТАННЯ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНТЕРЕСАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ</b>	115
<b>SECTION III SOFTWARE AND TECHNICAL METHODS OF INFORMATION PROTECTION</b>	118
<b>Vadym VOLOTKA. EXAMPLE USE'S OF "OUTGUESS" SOFTWARE PRODUCT</b>	118
<b>Vitalii SUSUKAILO, Ivan OPIRSKYI, Sviatoslav VASYLYSHYN. ANALYSIS OF THE POSSIBILITY OF USING CHATBOTS WITH ARTIFICIAL INTELLIGENCE TO DETECT INFORMATION SECURITY INCIDENTS</b>	120

<b>Anatolii DAVYDENKO, Olena VYSOTSKA, Oleksandr POTENKO.</b> DEVELOPING A SOFTWARE APPLICATION FOR THE PROTECTION OF INFORMATION SYSTEMS BASED ON THE ANALYSIS OF GRAPHIC IMAGES	122
<b>Ярослав ПОПОВ, Валерій ДУДИКЕВИЧ, Андрій ГОРПЕНЮК.</b> ЯК ВИКОРИСТАННЯ ШІ МОЖЕ ВПЛИнути НА ПРАКТИКИ КОНТРОЛЮ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	124
<b>Serhiy SEMENYUK.</b> CONSTRUCTION OF MARKOV MODULATED POISSON PROCESS MODELS FOR NETWORK INTRUSION DETECTION	126
<b>Volodymyr КНОМА, Halyna KENYO.</b> MACHINE LEARNING APPLICATIONS IN CYBERSECURITY: STATE OF ART AND TRENDS	128
<b>Dmytro MORHUL, Oleksiy NARIEZHNI.</b> SECURITY REASONS OF IMPLEMENTATION OUTBOUND TRAFFIC FILTERING FOR WEB SERVICE QRNG	130
<b>Андрій ВАЛЬЧУК, Валерій ДУДИКЕВИЧ.</b> РОЗРОБКА АВТОМАТИЗОВАНОГО ПІДХОДУ ДО РОЗГОРТАННЯ СИСТЕМ ПРИМАНОК	131
<b>Володимир ВИШНЯКОВ, Олег КОМАРНИЦЬКИЙ.</b> ПРИНЦИПИ ПОБУДОВИ СИСТЕМ ІоТ ЗАХИЩЕНИХ ВІД КІБЕРАТАК	133
<b>Володимир ДЖУЛІЙ, Віктор ЧЕШУН, Сергій МОСТОВИЙ, Євген МАЙОР.</b> ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	135
<b>Володимир КРИЖАНОВСЬКИЙ, Юлія РАССОХІНА, Василь КОМАРОВ,</b> <b>Михайло Прокоф'єв.</b> ЗАХИСТ NFC ЗВ'ЯЗКУ ВІД ПІДСЛУХОВУВАННЯ НА ЧАСТОТАХ ВИЩИХ ГАРМОНІК	137
<b>Максим ОПАНОВИЧ, Андріян ПІСКОЗУБ.</b> ДОСЛІДЖЕННЯ ЗАКОНОМІРНОСТЕЙ ТА ТЕНДЕНЦІЙ СУЧАСНИХ КІБЕРАТАК	139
<b>Даниїл ЖУРАВЧАК, Валерій ДУДИКЕВИЧ.</b> ВИКЛИКИ ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ	141
<b>Віталій БРИДІНСЬКИЙ, Дмитро САБОДАШКО.</b> ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ДІАРИЗАЦІЇ АУДІОЗАПИСІВ	143
<b>Юрій КАСЬЯНОВ, Анастасія МИХАЙЛИЧЕНКО.</b> ВИБІР ТЕКСТОВОГО МАТЕРІАЛУ ДЛЯ ДОСЛІДЖЕНЬ СПЕКТРУ УКРАЇНСЬКИХ ДОВГОТРИВАЛИХ МОВНИХ СИГНАЛІВ	145
<b>Анастасія КРАВЧЕНКО, Софія КРАВЧЕНКО, Всеволод БОБУХ.</b> ЗАГРОЗИ ЦІЛІСНОСТІ ДАНИХ ТА ПРОПОНОВАНІ РІШЕННЯ У ХМАРНИХ ОБЧИСЛЕННЯХ	147
<b>Kateryna KUPYRO, Yurii GORBENKO.</b> USING CLOUD SERVICES IN THE BANKING SECTOR	149
<b>Андрій ПАРТИКА, Владислав Д'ЯКОНОВ.</b> РЕАЛІЗАЦІЯ ЗАХИЩЕНОГО ВЕБ-ПРОЕКТУ З ВИКОРИСТАННЯМ ВБУДОВАНИХ ІНСТРУМЕНТІВ БЕЗПЕКИ AWS	151
<b>Сергій АРТЕМУК, Ігор МИКИТИН.</b> ПОРІВНЯННЯ МЕТОДІВ ВИЗНАЧЕННЯ КООРДИНАТ ДЖЕРЕЛА АКУСТИЧНОГО СИГНАЛУ	153
<b>Віталій БРИДІНСЬКИЙ, Соломія МАРКО, Дмитро САБОДАШКО, Юрій ХОМА.</b> ПОРІВНЯННЯ СУЧАСНИХ МОДЕЛЕЙ ГЛИБИННОГО НАВЧАННЯ У ЗАДАЧАХ РОЗПІЗНАВАННЯ ЛЮДИНИ ЗА ГОЛОСОМ	155

<b>Василь КОМАРОВ, Дмитро ЧЕРНОВ, Михайло ПРОКОФЬЄВ, Володимир КРИЖАНОВСЬКИЙ. ДЕКОДУВАННЯ КОДУ ВІД RFID ПРИСТРОЮ ПРИ СКІМІНГУ НА ЧАСТОТІ ТРЕТЬОЇ ГАРМОНІКИ</b>	157
<b>Ярослав СВЕТЛІЧНИЙ. ПРОБЛЕМА ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПРОТОКОЛ ARP</b>	159
<b>Juliy VOIKO, Oleksiy POLIKAROVSKYKH, Vitalii TKACHUK. DIRECTION FINDER ANTENNA FOR THE TERRITORY PROTECTION SYSTEM AGAINST UNMANNED AERIAL VEHICLES</b>	161
<b>Дмитро ЄВГРАФОВ, Юрій ЯРЕМЧУК. МОЖЛИВОСТІ СУЧАСНОЇ ШУМОВОЇ ГЕНЕРАЦІЇ СИГНАЛІВ ДЛЯ ПРИДУШЕННЯ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ З ЕКРАНІВ МОНІТОРІВ</b>	163
<b>Олександр ІСАКОВ, Степан ВОЙТУСІК. ТЕХНІКИ АКТИВНОГО ПРИДУШЕННЯ ШУМУ</b>	165
<b>Анастасія ТОЛКАЧОВА. РЕАЛІЗАЦІЯ БЕЗПЕКИ У ХМАРНОМУ СЕРЕДОВИЩІ</b>	167
<b>Дмитро ЄВЕНКО. МЕТОДИ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ МІКРОСЕРВІСІВ НА ПРИКЛАДІ KUBERNETES</b>	169
<b>Михайло МАРЧУК, Богдан ДРОБЕНКО, Віра ПАКОШ, Володимир ХАРЧЕНКО, Микола ХОМ'ЯК. ІНФОРМАЦІЙНА БЕЗПЕКА ЗА ВИКОРИСТАННЯ КОМЕРЦІЙНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОЄКТНИХ РОЗРАХУНКІВ У ГАЛУЗІ РАКЕТНО-КОСМІЧНОЇ ТЕХНІКИ</b>	171
<b>Ілля СЕМЕНЕНКО. СТВОРЕННЯ ЗАСТОСУНКУ ДОСЛІДЖЕННЯ МОДЕЛЕЙ БОЙОВИХ ДІЙ ТИПУ ЛАНЧЕСТЕРА</b>	173
<b>Володимир МАДЖА, Володимир ПОНОМАР. МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ</b>	175
<b>Дмитро ДАРІЄНКО, Юрій ШИШКІН, Любомир ПАРХУЦЬ. ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБРАЗІВ КОНТЕЙНЕРА ПІД ЧАС ЗБЕРІГАННЯ ТА ЗБІРКИ</b>	177
<b>Дмитро ПОНАЙДА, Назарій КОГУТ, Любомир ПАРХУЦЬ. ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОНТЕЙНЕРИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ</b>	179
<b>Орест СИНЯВСЬКИЙ, Марина КОСТЯК. ОГЛЯД ОСНОВНИХ КАНАЛІВ ЗВ'ЯЗКУ ДЛЯ УПРАВЛІННЯ БЕЗПЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ</b>	181

## ПІДВИЩЕННЯ СТІЙКОСТІ ЦВЗ У ПОТОКОВИХ ВІДЕОЗАПИСАХ

Юрій ЯРЕМЧУК<sup>a</sup>, Василь КАРПНЕЦЬ<sup>a</sup>,  
Ірина ЗОРЯ<sup>a</sup>

<sup>a</sup> *Вінницький національний технічний університет,  
вул. Хмельницьке шосе, 95, м. Вінниця, Україна*

**Анотація.** У роботі представлено аналіз можливості підвищення стійкості вбудованого ЦВЗ у потоковий відеозапис на основі вдосконаленого алгоритму DEW із його подальшою програмною реалізацією. Вдосконалення методу здійснюється за рахунок вбудовування ЦВЗ у низькочастотні коефіцієнти ДКП та застосування методу сегментації Канні, який використовує багаторівневий обчислювальний підхід виявлення меж сегментів, сприяє зменшенню візуальних змін контейнера.

**Ключові слова.** Цифровий водяний знак, Differential Energy Watermarking, метод Канні, стійкість ЦВЗ, онлайн-сервіс, потокове відео.

### Вступ

Сьогодні дослідження проблеми захисту інтелектуальної власності не тільки не втрачає своєї актуальності, проте стає ще більш затребуваним, оскільки безперервне зростання обсягів цифрової інформації використання Інтернету збільшується з кожним днем. Активне застосування цифрових водяних знаків [1] у цифрові файли (стегоконтейнери) для захисту права власності призводить до необхідності розробки методів, більш стійких до активних атак та природних спотворень у каналі обробки та передавання. Вище згаданий засіб захисту авторського права на основі ЦВЗ успішно використовується для вирішення завдань підтвердження авторського права по відношенню до цифрових файлів, контролю їх використання авторизованими користувачами та іншими особами, підтвердження справжності та надійності копій програмних засобів та мультимедіа об'єктів, що використовуються. Проведено аналіз існуючих методів вбудовування ЦВЗ у відеофайли. Зокрема, виявлено недоліки оригінального алгоритму DEW [2] такі як вразливість високочастотних коефіцієнтів контейнера до певних видів атак (оскільки застосовувані у алгоритмі DEW високочастотні коефіцієнти ДКП легко відкидаються фільтрами), а також можливість суттєвих візуальних змін (оскільки алгоритм DEW не враховує, який вплив на вихідне зображення має відкидання коефіцієнтів ДКП). Отримані результати дослідження свідчать, що

подальше вдосконалення таких методів є необхідним, оскільки проблеми стійкості до атак залишаються актуальними. Враховуючи дані фактори, в роботі для дослідження обраний алгоритм вбудовування цифрового водяного знаку, що базується на ідеї диференціального енергетичного водяного знаку та є методом вбудовування ЦВЗ, що заснований на вибіркового відкиданні частини високочастотних коефіцієнтів ДКП стислих зображень і відеозображень.

### Основна частина

Розглянемо вдосконалення стенографічного методу на основі алгоритму DEW та запропонуємо можливе його застосування для розробки відповідного програмного засобу. Запропоноване вдосконалення дозволить усунути виявлені недоліки, здійснити програмну розробку засобу для вбудовування ЦВЗ у потоковий відеозапис та у подальшому здійснити тестування отриманих результатів роботи вдосконаленого алгоритму.

### Розробка алгоритму роботи методу для вбудовування ЦВЗ

В основі даного методу лежить диференціальне вбудовування енергії (DEW). Під енергією розуміється значення коефіцієнтів ДКП аналізованої області зображення. За методом DEW здійснюється впровадження ЦВЗ, яке складається з біт  $b_j (j = 0, 1, 2, \dots, l - 1)$ . Кожен біт ЦВЗ вбудовується в обрану область, що складається з блоків  $n$  по  $8 \times 8$  коефіцієнтів ДКП каналу яскравості зображення кожен. Розмір обраної області визначає швидкість вбудовування – що вище  $n$ , то нижча швидкість. Кожен біт ЦВЗ впроваджується в обрану область модифікацією різниці енергій між високочастотними коефіцієнтами ДКП верхньої частини цієї області (субобласть А) та її нижньої частини (субобласть В). Підмножина високочастотних коефіцієнтів позначається  $S(c)$ . Центральну роль, як у процесі вбудовування, й у процесі вилучення вбудованої інформації грають енергії субобластей А і В, величина яких визначається чотирма чинниками: характером субобластей А та В; кількістю блоків  $n$  на одну обрану область; кроком квантувача; розміром підмножини  $S(c)$ .

Вдосконалення методу вбудовування ЦВЗ у відео-файли

Враховуючи, що однією із проблем стійкості методу до атак є вразливість високочастотних коефіцієнтів контейнера, в запропонованому методі пропонується враховувати лише низькочастотні коефіцієнти ДКП. Для усунення недо-

ліку суттєвої помітності візуальних змін контейнера застосуємо метод сегментації Канні [3], який використовує багаторівневий обчислювальний підхід виявлення меж сегментів на зображенні. У більшості випадків, особливо при аналізі зашумлених зображень, цей метод має певні переваги перед іншими. Регульованим параметром методу Канні є поріг чутливості: двоелементний вектор, у якому перший елемент нижній поріг, а другий елемент верхній поріг. Оскільки, низькочастотні коефіцієнти ДКП модифікувати небажано, так як це може погіршити візуальну якість зображення, поріг повинен бути не менше за певне значення  $c_{min}$ . Для визначення відповідного  $c$  використаємо формулу:

$$c(n, Q, c_{min}) = \max\{c_{min}, \max\left\{g \in \{1, 63\} \mid E_A(g, n, Q) > D\right\} \cap \left(E_B(g, n, Q) > D\right)\}.$$

Для отримання вбудованого біта одержувачу необхідно знайти поріг  $c$ . Але тепер береться вже максимум за всіма порогами для субобластей А і В. Робота методу перевіряється на моделях зображень із різними дефектами. Результати зображення є бінарними, де одиницею відображається наявність кордонів, а нулем її відсутність.

Розробка додатку за вдосконаленим методом вбудовування ЦВЗ у відео-файли

На основі запропонованого вдосконаленого методу вбудовування ЦВЗ здійснимо реалізацію програмного засобу, що являє собою онлайн-сервіс для публікації відео. Оскільки передбачається, що вдосконалений метод буде застосовуватись для вбудовування у потоковий відеозапис, мультимедійний файл, що слугуватиме стенографічним контейнером, будемо розглядати як послідовність кадрів (фреймів), де кожен з них обробляється як незалежне зображення і ЦВЗ вбудовується у кожний фрейм окремо. В роботі використовуватимуться формати відео .mp4 та .avi. Розроблено онлайн-сервіс, доступ до роботи з

яким мають лише авторизовані користувачі. Авторизувавшись на сервісі, користувач має можливість переглядати та додавати відео, захищені цифровим водяним знаком, ставити відповідні реакції на відео, залишати коментарі. Застосувавши вдосконалений алгоритм для розробки програмного продукту, було здійснено тестування розробки. Було обрано десять відео із вбудованим ЦВЗ, що являє собою тестове повідомлення «Дане відео захищене авторським правом» (повідомлення представлено у вигляді стрічки ASCII, кількість символів 37, кожен символ по 8 біт, розмір повідомлення 296 біт).

#### Висновки

Проведений аналіз запропонованого методу вбудовування ЦВЗ та результатів його тестування за показниками візуального впливу (SSIM, SNR, PSNR, AD, NAD, IF) та стійкості до атак показав, що у цілому застосування вдосконаленого методу дозволяє підвищити показники орієнтовно на 12%, зокрема, усувається недолік візуальної помітності змін у відео та має підвищену стійкість до атак перекодування та стиснення. ЦВЗ, що вбудовується у файл, не здійснює на нього суттєвого впливу, а вбудовування даних у низькочастотні коефіцієнти дозволяє підвищити стійкість до атак.

#### Список літератури

- [1] Захист авторського права. Helpx: веб-сайт. URL: <https://helpx.adobe.com/ua/> (дата звернення: 14.10.2022).
- [2] Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії: Навч. посібник для студентів і аспірантів. – Вінниця: ВДТУ, 2003. – 143с.
- [3] Canny J.A Computational Approach to Edge Detection / J.Canny // IEEE Transactions on Pattern Analysis and Machine Intelligence, 1986. – Pp. 679-698.