ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей V Міжнародної науково-практичної конференції ІБІТ 2024

27 листопада 2024 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник доповідей
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с.

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій ІВАНУСА – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Секція 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

насиченістю. Сучасні інформаційні технології у сфері безпеки та оборони. 2019. Т. 34, № 1. С. 115–120.

4. Image disentanglement autoencoder for steganography without embedding / X. Liu et al. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) : conf., New Orleans, LA, USA, 18–24 June 2022. 2022. P. 2293–2302.

5. Rani S., Kurniawardhani A., Rendani Y. A. W. Steganography on digital color image using modulo function and pseudo-random number generator. International Journal on Advanced Science, Engineering and Information Technology. 2021. Vol. 11, no. 6. P. 2470–2475.

6. Горячий О., Максимович В., Шабатура М. Дослідження множини початкових значень генераторів псевдовипадкових чисел на основі арифметики з рухомою комою. Сучасний захист інформації. 2024. Т. 58, № 2. С. 91–102.

УДК 004.932:004.056.55

СТАН ДОСЛІДЖЕНЬ У СФЕРІ ЦИФРОВОГО МАРКУВАННЯ ДЛЯ АУДІОФАЙЛІВ

Остап-Святосла МАЛЕЦЬ
Ольга СМОТР
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper aims to study the current state of the art in the field of digital audio content marking and to outline promising areas of research in the field of digital audio content watermarking. To achieve this goal, the paper uses a systematic review and analysis of scientific articles on the practical implementation of existing digital watermarking methods, a method of comparing results, and a method of synthesizing results. Based on the conducted research, a comprehensive picture of the current state of digital audio content labeling was obtained, the relevance of the research topic was proved, and promising areas of application of these technologies were identified.*

Keywords*: digital watermark, audio content, security, information technology, digital watermarking technologies, neural network.*

Анотація*. У роботі проведено дослідження сучасного стану у сфері цифрового маркування аудіоконтенту та окреслити перспективні напрямки досліджень в галузі цифрового водяного маркування аудіоконтенту. Для досягнення поставленої мети в роботі використано систематичний огляд та аналіз наукових статей, щодо практичних реалізацій існуючих методів цифрового водяного маркування, метод порівняння результатів та метод синтезу результатів. Базуючись на проведених дослідженнях, отримано комплексне уявлення про сучасний стан маркування цифрового аудіоконтенту, доведено актуальність теми дослідження та виділено перспективні напрямки застосування цих технологій.*

***Ключові слова**: цифровий водяний знак, аудіоконтент, безпека, інформаційні технології, технології цифрових водяних знаків, нейронна мережа.*

Цифровізація суттєво спростила створення, розповсюдження та обмін аудіоконтентом. Однак із зростанням доступності цифрових медіа почастішали випадки несанкціонованого копіювання та поширення аудіофайлів, що порушують права інтелектуальної власності. Це створює значні виклики для власників контенту, які прагнуть захистити свої твори від піратства та отримувати справедливу винагороду за їх використання.

Для захисту аудіоконтенту сьогодні застосовують різні методи, такі як шифрування файлів, управління цифровими правами (DRM), технології цифрових водяних знаків і методи аутентифікації. Серед них цифрові водяні знаки мають унікальні переваги, зокрема здатність відстежувати контент і визначати його походження. Ці технології дають змогу ідентифікувати власника та захищати контент навіть після подальшого розповсюдження.

Водночас існують низка невирішених проблем, серед яких забезпечення стійкості водяних знаків до різних видів аудіообробки, таких як стиснення, зміна швидкості відтворення або додавання шуму. Важливим залишається завдання зробити водяні знаки непомітними для слухачів, зберігаючи якість звуку, що є особливо актуальним у сучасних потокових сервісах. Удосконалення надійних і універсальних методів захисту контенту залишається пріоритетним напрямом для наукових досліджень і розробок.

Сучасний розвиток алгоритмів штучного інтелекту та їх доступність сприяли активному використанню нейронних мереж у системах водяного маркування аудіоконтенту [1-6]. Наприклад, у дослідженні Pengcheng Li, Xulong Zhang, Jing Xiao та Jianzong Wang [1] представлено модель подвійного вбудовування водяних знаків, яка покращує ефективність маркування та підвищує стійкість до атак, аналізуючи вплив рівня атак на інвертовану нейронну мережу під час навчання. Однак, як і раніше, залишається актуальним питання забезпечення стійкості до нових типів атак без втрати якості звуку. Інше дослідження [2] пропонує використання глибокої нейронної мережі та перцептивних втрат для вбудовування водяних знаків із врахуванням психоакустичних ефектів.

У роботі [3] наведено огляд сучасних методів водяного маркування з використанням глибоких нейронних мереж, включно з новою таксономією. Водночас автори наголошують на відсутності єдиної методології для оцінки ефективності таких методів, що підкреслює необхідність стандартизації.

Дослідження [4] розглядає застосування згорткових нейронних мереж для підвищення стійкості до атак, а в роботі [5] представлено метод навчання на основі контрзаходів. Втім, ці методи не завжди є ефективними для нових і непередбачуваних атак.

Узагальнену схему системи, що поєднує глибоке навчання з підходом до нанесення водяних знаків на аудіо наведено на рисунку 1. Окреслено основні компоненти системи, включаючи вилучення ознак, класифікацію за допомогою глибоких нейронних мереж (DNN) та процес нанесення водяних знаків.

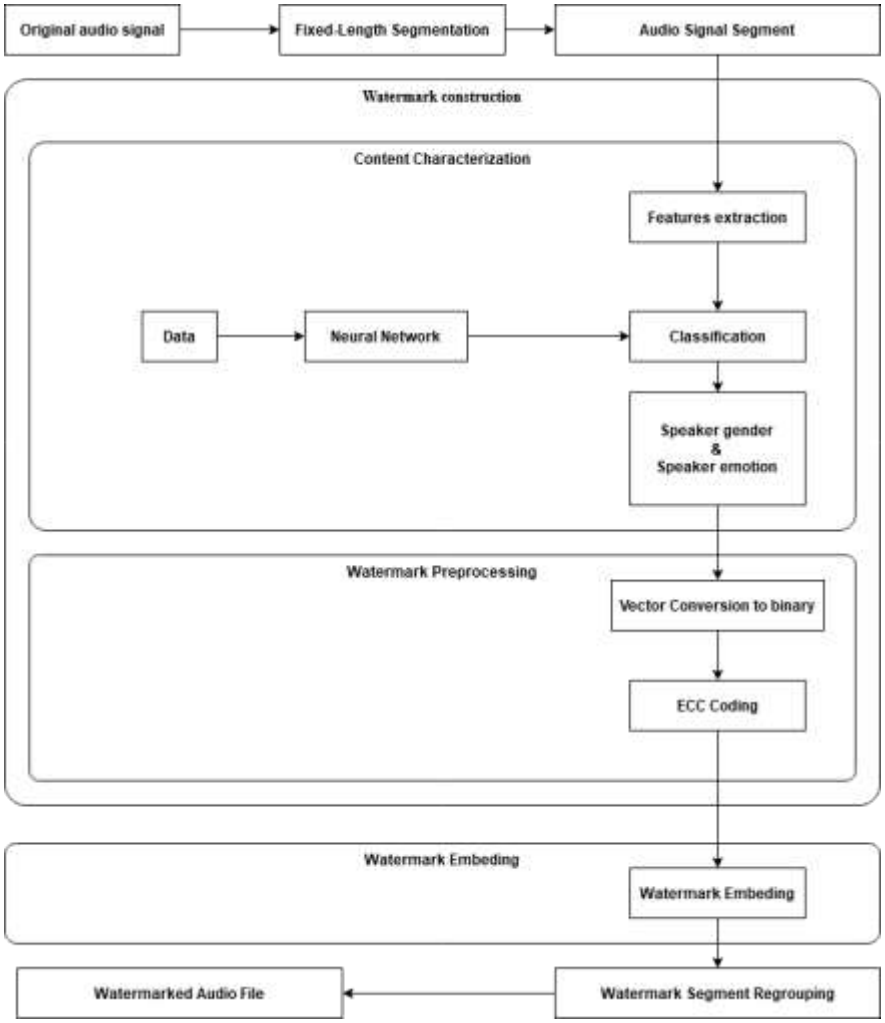

Рисунок 1. Узагальнена схема нанесення водяних маркерів на аудіоконтент

Запропонована система вбудовує водяний знак за допомогою методу DCT-MLP-LSB, призначеного для характеризації та класифікації аудіо за такими категоріями, як музика, мова, стать та емоції. Експериментальні результати демонструють ефективність системи як на відкритих наборах даних, так і стійкість водяних знаків. Для додатків, що не пов'язані з безпекою, стійкість до навмисних атак не є критичною, але стійкість до обробки сигналу, наприклад, стиснення, є необхідною. У цьому випадку водяний знак містить метадані, такі як інформація про виконавця або місце реєстрації, що допомагає індексувати сигнал.

Попри значний прогрес у використанні нейронних мереж для водяного маркування аудіоконтенту, залишається багато питань для подальших досліджень, зокрема забезпечення стійкості до атак, оптимізація якості звуку та створення єдиних стандартів оцінки ефективності методів.

Інформаційні джерела

1. M. Charfeddine, E. Mezghani, S. Masmoudi, C. B. Amar and H. Alhumyani, "Audio Watermarking for Security and Non-Security Applications," in IEEE Access, vol. 10, pp. 12654-12677, 2022, doi: 10.1109/ACCESS.2022.3145950.

2. J. Zhou and P. Chen, "Generalized Discrete Cosine Transform," 2009 Pacific-Asia Conference on Circuits, Communications and Systems, Chengdu, China, 2009, pp. 449-452, doi: 10.1109/PACCS.2009.62.

3. M. M. Kurdi, I. A. Elzein and A. M. Zeki, "Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in digital watermarking," 2016 12th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2016, pp. 111-116, doi: 10.1109/ICENCO.2016.7856454.

4. Gupta, A., & Yilmaz, A. (2018). Social network inference in videos. In Elsevier eBooks (pp. 395–424).

5. A. D. P. Ramirez, J. I. de la Rosa Vargas, R. R. Valdez and A. Becerra, "A comparative between Mel Frequency Cepstral Coefficients (MFCC) and Inverse Mel Frequency Cepstral Coefficients (IMFCC) features for an Automatic Bird Species Recognition System," 2018 IEEE Latin American Conference on Computational Intelligence (LA-CCI), Gudalajara, Mexico, 2018, pp. 1-4, doi: 10.1109/LA-CCI.2018.8625230.

6. Y. Martyn, O. Smotr, N. Burak, N. Prydatko and I. Malets, Informational graphic technologies for fire safety level determination in special purpose buildings, in: Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 398-403. doi: 10.1109/DSMP47368.2020.9204180.

З М І С Т

СЕКЦІЯ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

НАПРЯМ 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ

Балацька В., Побережник В. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА NFT ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДЕРЖАВНИХ РЕЄСТРІВ 6

Федінець Н., Синиця О. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В СУЧАСНИХ РЕАЛІЯХ 9

Полотай О. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ БАНКІВСЬКОЇ УСТАНОВИ 12

Ткаченко А. ВІРУСИ-ДРОППЕРИ: ТЕХНІКИ ДОСТАВКИ ШКІДЛИВОГО ПЗ ТА ОБХІД ЗАХИСНИХ СИСТЕМ 16

Ящук В., Ошурко Б. СУЧАСНІ ВИКЛИКИ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УМОВАХ ВІЙНИ 17

Ящук В., Столярчук В. ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМУ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ 20

Виглазов В. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ВОЄННИЙ ЧАС 23

Паньків А-М-І., Хлевной О. КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ: ТАКТИКИ, МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ 27

Бик Е., Бурак Н. ДОСЛІДЖЕННЯ СУЧАСНИХ КОМУНІКАЦІЙНИХ ПЛАТФОРМ ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПОВСЯКДЕННОЇ ДІЯЛЬНОСТІ ДСНС УКРАЇНИ 29

Водоніс Я., Полотай О. ПРОЦЕСНИЙ ПІДХІД В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВАХ, ЯКІ НАДАЮТЬ ІТ-ПОСЛУГИ 32

Литвиненко Р., Лучик В. ЦИФРОВА КРИМІНАЛІСТИКА 36

Мукан І., Котовська О. КРИМІНАЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У КІБЕРПРОСТОРІ ТА ЕКСПЕРТНА РОЛЬ ГРОМАДСЬКИХ (НЕУРЯДОВИХ) ОРГАНІЗАЦІЙ 40

Ящук В., Водніцька О., Sharadze A. АНАЛІЗ СВІТОВИХ ПРАКТИК УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 44

Дем'янчук Ю. МОДЕЛЬ ПОВЕДІНКИ «АГЕНТІВ» ВОЄННОЇ КОМУНІКАЦІЇ: ФОРМАЛЬНО-СИНТАКСИЧНА ІЄРАРХІЯ 48

Харчук А.І., Харчук А.А. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ 52

Бундус В., Лучик В. РОЗСЛІДУВАННЯ КІБЕРАТАК У ВОЄННИХ УМОВАХ 54

НАПРЯМ 2.
ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ

Борматов Р. ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ 57

Пилипенко В., Тимчишин О., Федець Н. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ 60

НАПРЯМ 3.
БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Savchuk K. AI IN ACTION: DEFENDING AGAINST EVOLVING CYBER THREATS 64

Орощук Х., Маслова Н., Любименко О. ЗАГРОЗИ CLOUD COMPUTING: ВИКЛИКИ ТА МЕТОДИ ЗАХИСТУ 68

Івануса А., Ткаченко А., Петрович А. ВДОСКОНАЛЕННЯ АРХІТЕКТУРИ ЗАСОБІВ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ 73

Кондратюк М. ЗАХИСТ КРИПТОВАЛЮТНИХ ГАМАНЦІВ 76

Івануса А., Брич Т., Ткач М. РОЗРОБКА МОДУЛІВ І ФУНКЦІОНАЛЬНОСТІ ЗАСОБУ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ 79

Грабченков Б., Лучик В. СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЇХ ЗАСТОСУВАННЯ 83

Івануса А., Сорока А., Ланчевич А. АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ У WEB-ДОДАТКАХ 86

НАПРЯМ 4.
ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Сабадах І., Лучик В. РОЛЬ ШИФРУВАННЯ У ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ 91

Гордієнко Т. АНАЛІЗ ЗАГРОЗ У КАНАЛАХ ЗВ'ЯЗКУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОПЕРАТИВНОЇ ПОЛІГРАФІЇ 94

Світличний В., Шестаков В. МЕТОДИ ЗАХИСТУ IoT-ПРИСТРОЇВ ВІД КІБЕРЗАГРОЗ 98

Клименко Т. АКТУАЛЬНІСТЬ ЗАХИСТУ Й БЕЗПЕКИ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ І МЕСЕНДЖЕРАХ В УМОВАХ ВІЙСЬКОВОГО СТАНУ 103

Ящук В., Кутник Н. ОЦІНЮВАННЯ ВРАЗЛИВОСТЕЙ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ З ВИКОРИСТАННЯМ ПЛАТФОРМИ TRYHACKME 106

Любімов О., Іовенко І. РОЗУМІННЯ МАЙБУТНІМИ ОФІЦЕРАМИ ЗАХИЩЕНОГО ЗВ'ЯЗКУ З ОРБІТАЛЬНИМИ НАНОСУПУТНИКАМИ 109

Остапець Д., Сухомлин О. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ 117

Остапець Д., Мотиленко В. МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОКАЗІВ НУЛЬОВОГО РОЗГОЛОШЕННЯ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ 120

Курінний І., Світличний В. АНТИВІРУСНІ ПРОГРАМИ:ЇХ ЗНАЧЕННЯ ТА ЕФЕКТИВНІСТЬ У ЗАХИСТІ ДАНИХ 123

Лучик В., Прокопчук Н. ЗАХИСТ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМИ ПРОЦЕСАМИ (SCADA) 127

Полотай О. ДОСЛІДЖЕННЯ СПОСОБІВ ЗАХИСТУ WEB-САЙТІВ ВІД МЕРЕЖЕВИХ АТАК 129

Одерій Н., Світличний В. ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ: МОТИВАЦІЯ ЗЛОВМИСНИКІВ 133

Федоренко А. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВУ ЕПОХУ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ 135

Полотай О., Гуменюк М. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN 138

Пільов К. ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ 142

Лучик В., Гончаров Д. ОСНОВНІ ПРОТОКОЛИ МЕРЕЖЕВОЇ БЕЗПЕКИ 144

Рошинець І., Полотай О. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ VPN 148
Лучик В., Гуменюк І. БРАНДМАУЕРИ ТА ЇХ ВИКОРИСТАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ 152
Світличний В., Колода Я. БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ: МЕТОДИ ЗАХИСТУ ВІД СПАМУ ТА ШКІДЛИВИХ ВКЛАДЕНЬ 156
Ориник С., Полотай О. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД АТАК VLAN HOPPING 159
Курило Д., Світличний В. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІЇ ІНТЕРНЕТ ПІРАТСТВУ 162
Назаров В. ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІЖНАРОДНОЇ РЕКЛАМНОЇ АГЕНЦІЇ В УМОВАХ ДЕЦЕНТРАЛІЗОВАНОГО СЕРЕДОВИЩА 164
Panovyk U., Panovyk R., Rajesh N., Fedyna B. SECURE DOCUMENT MANAGEMENT VIA VPN IN CORPORATE INFORMATION SYSTEMS 170
Філіпчук Б., Ткачук Р. ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАХИЩЕНИХ КАНАЛІВ, ПОБУДОВАНИХ НА ПРОТОКОЛАХ WireGuard ТА OpenVPN 175
Світличний В., Ковтун І. СУЧАСНІ МЕТОДИ БОРОТЬБИ З АТАКАМИ ТИПУ SQL-ІН'ЄКЦІЙ 179
Кугот В., Сабат В. ОПЕРАТИВНЕ УПРАВЛІННЯ В ІЄРАРХІЧНО-СТРУКТУРОВАНИХ СИСТЕМАХ ТА ВИБІР МОДЕЛЕЙ СТРАТЕГІЙ ЦІЛЕОРІЄНТОВАНИХ ДІЙ В УМОВАХ ЗАГРОЗ 182
Гончарук І., Манжай О. ЗАХИСТ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ПРАКТИКИ ТА ПЕРСПЕКТИВИ В УКРАЇНІ 186
Руденко М. ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ 188
Нечипорук В., Лучик В. АНАЛІЗ ВРАЗЛИВОСТЕЙ В ПОПУЛЯРНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ТА ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ 191

НАПРЯМ 5.
ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Яхно Н., Лучик В. ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 195
Шевців Ю., Костишин Е. ВПЛИВ ВІЙНИ НА ГЕНДЕРНУ ПАРИТЕТНІСТЬ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ 198
Яремко Р., Ткачик О. ПОНЯТТЯ ПРО ГЕНДЕРНІ СТЕРЕОТИПИ ТА ЇХ ВПЛИВ НА ПОВСЯКДЕННЕ ЖИТТЯ ЛЮДЕЙ 200
Коваль І., Лакіш В. ГЕНДЕРНІ ВІДМІННОСТІ У ПІДГОТОВЦІ РЯТУВАЛЬНИКІВ 203

НАПРЯМ 6.
КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Grytsiuk P., Sikora L. THE MECHANISM OF GENERATING FIBONACCI AND LUCAS POLYNOMIALS 206

Чорненька С., Манжай О. КРИПТОГРАФІЧНІ МЕТОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ 211

Кобилкіна О., Ровецький І. СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ 215

Остапець Д., Дзюба В. АПАРАТНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ 218

Галицький І., Лаврик Т. ІНТЕГРАЦІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: АНАЛІЗ ПРОГРАМНИХ РІШЕНЬ 221

Горячий О., Журавель І. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОСТИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ 225

Малець О.-С., Смотр О. СТАН ДОСЛІДЖЕНЬ У СФЕРІ ЦИФРОВОГО МАРКУВАННЯ ДЛЯ АУДІОФАЙЛІВ 230

Олег Г., Захар Я. АНАЛІЗ ЕФЕКТИВНОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КВАДРАТНОГО КОРЕНЯ ПРОСТОГО ЧИСЛА 234

НАПРЯМ 7.
КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ

Танчин І. СТРАТЕГІЇ РЕАЛІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ В АРХІТЕКТУРІ IIoT ПОЛІГРАФІЧНОГО ПІДПРИЄМСТВА 238

Чепурной К., Тимошенко Л. ЗАХИСТ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ 243

Weigang G., Myronchuk K. DATA ENCRYPTION ALGORITHMS IN MASS SERVICE SYSTEMS 246

Балацька В., Опірський І. ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОВІРИ ТА ПРОЗОРОСТІ У ДЕРЖАВНИХ РЕЄСТРАХ 251

Demydova A., Маслова Н., Кіс Т. ЗАСТОСУВАННЯ МЕТОДІВ ШИФРУВАННЯ В СИСТЕМАХ ЗАХИСТУ МЕДИЧНИХ ДАНИХ 254

Піх І., Браташ С. ВІДМОВОСТІЙКІСТЬ ЯК КРИТЕРІЙ ЯКОСТІ

Наукове видання

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Збірник доповідей
V Міжнародної науково-практичної конференції
ІБІТ 2024

Відповідальні за випуск **Ростислав ТКАЧУК**
Назарій БУРАК

Оригінал-макет **Ростислав ТКАЧУК**

Друк на різографі **Маріанна КЛИМУС**

Підписано до друку 13.12.2024 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 17,8.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, ndr@ ubgd.lviv.ua

V International Scientific and Practical Conference CYBERSUCURITY AND INFORMATION TECHNOLOGY

CIT 2024

November 27 - 2024 Lviv-Ukraine