

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

Матеріали Міжнародної науково-практичної конференції

2



ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

*Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)*

За загальною редакцією **С. В. Ківалова**

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск **М. Р. Аракелян**

ISBN 978-617-8430-61-0

© НУ «Одеська юридична академія, 2025
© Автори статей, 2025

<i>Кухаренко Сергій Вікторович</i> СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ МЕДІА В УКРАЇНІ	546
<i>Чепурна Олена Євгенівна</i> АНАЛІЗ ТЕОРЕТИКО-ІГРОВИХ МЕТОДІВ СУЧАСНОЇ КІБЕРБЕЗПЕКИ	548
<i>Соколов Артем Вікторович, Баландіна Наталія Миколаївна, Зігінова Юлія Костянтинівна</i> КОНЦЕПТУАЛЬНА ІДЕЯ ЗБІЛЬШЕННЯ БЛОКУ ДЛЯ МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ	551
<i>Черевко Євген Володимирович</i> ЧИСЕЛЬНЕ РОЗВ'ЯЗУВАННЯ РІВНЯННЯ СТРУНИ ЗАСОБАМИ БІБЛІОТЕК PYTHON	555
<i>Овчинников Микола Юрійович</i> КОМПАРАТИВНИЙ АНАЛІЗ МЕТОДІВ ВПРОВАДЖЕННЯ ЦВЗ В АУДІОФАЙЛИ	558
<i>Слатвінська Валерія Миколаївна</i> ІНТЕГРАЦІЯ УМОВНОГО ГЕНЕРАТИВНО-ЗМАГАЛЬНОГО ПІДХОДУ ТА LSTM-МЕРЕЖ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ДІАГНОСТИКИ АНОМАЛІЙ У КІБЕРБЕЗПЕЦІ МЕРЕЖЕВОГО ОБЛАДНАННЯ	563
<i>Скідан Владислав Сергійович</i> ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ГЕЙМІФІКАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ	565
<i>Поворознюк Олексій Олегович</i> МЕТОДИ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ ПІД ЧАС ВІЙНИ	568

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

<i>Томчаковська Юлія Олегівна</i> ТИПОЛОГІЯ АНГЛОМОВНИХ МЕДІАТЕКСТІВ	571
<i>Строченко Леся Василівна</i> ДОСЛІДНИЦЬКІ ПРИНЦИПИ ПАРАДИГМАЛЬНОГО ПРОСТОРУ СУЧАСНОЇ ЛІНГВІСТИКИ	573
<i>Varieshkina Natalia</i> COMMUNICATIVE PRINCIPLE IN READING SKILLS FORMATION	575
<i>Дихта Наталія Миколаївна</i> ОСОБЛИВОСТІ ПСИХОЛОГІЧНОЇ ТЕРМІНОЛОГІЇ ТА АКТУАЛЬНІСТЬ ЇЇ ВЖИВАННЯ	578
<i>Єрьоменко Світлана Василівна</i> ОСОБЛИВОСТІ АНГЛОМОВНОГО ВІЙСЬКОВО-МОРСЬКОГО ДИСКУРСУ	580
<i>Іванова Наталія Георгіївна</i> ЦИФРОВІ СТРАТЕГІЇ ВИВЧЕННЯ ІСПАНСЬКОЇ МОВИ ЯК ТРЕТЬОЇ ІНОЗЕМНОЇ: РЕАЛІЗАЦІЯ ДЕСКРИПТОРІВ INTERACCIÓN EN LÍNEA НА ПОЧАТКОВОМУ РІВНІ В УМОВАХ ВИЩОЇ ФІЛОЛОГІЧНОЇ ОСВІТИ	583
<i>Козак Тетяна Борисівна</i> БІНАРНІСТЬ ПОНЯТТЯ 'ЧОРНИЙ'/'БІЛИЙ' У МОВАХ ПЕРВІСНОЇ ФОРМАЦІЇ	586
<i>Марчук Ірина Петрівна</i> DEVELOPING INDIVIDUAL PROFESSIONAL PROGRAMS OF A TUTOR	589
<i>Пеліван Оксана Костянтинівна</i> ВВІЧЛИВІСТЬ В ІСТОРИЧНОМУ АСПЕКТІ	592
<i>Потенко Людмила Олександрівна</i> ЕФЕКТИВНІСТЬ РЕАЛІЗАЦІЇ ІНКЛЮЗИВНОГО НАВЧАННЯ У ВИЩІЙ ШКОЛІ В УМОВАХ ВІЙНИ	595
<i>Телецька Тетяна Володимирівна</i> ПРОФЕСІЙНО-ОРІЄНТОВАНЕ НАВЧАННЯ ІНОЗЕМНОЇ МОВИ У ПІДГОТОВЦІ ФАХІВЦІВ ПРАВНИЧОЇ ГАЛУЗІ: КОМПЕТЕНТНІСНИЙ ПІДХІД	598

2. Матківський М. П., Тарас Т. М., Лучкевич Є. Р. Роль гейміфікації у покращенні мотивації та навчальних результатів учнів середньої школи в умовах цифрової трансформації освіти в Україні. *Педагогічна Академія: наукові записки*. 2025. № 14. URL: <https://pedagogical-academy.com/index.php/journal/article/view/571/455> (дата звернення: 01.04.2025).

3. Годлевська К. Особливості технологічного аспекту ефективної реалізації змішаного навчання в сучасних умовах сьогодення. *UNESCO Chair Journal Lifelong Professional Education in the XXI Century*. 2024. № 2(10). С. 46-56.

4. Ткаченко К. О., Ісаченко Б. О. Використання гейміфікації в інтелектуальних навчальних системах та їх вебдизайні. водний транспорт. *Водний транспорт*. 2023. № 2(38). С. 299-311.

5. Козуб Г. О., Шинкаренко Я. М., Козуб В. Ю. Гейміфікація в освіті: інтеграція Classcraft в навчальний процес. *Педагогічна Академія: наукові записки*. 2024. № 7. <https://doi.org/10.57125/pedacademy.2024.06.29.02>

Ключові слова: гейміфікації, захист інформації, безпека, освітня програма, інструменти.

Keywords: gamification, information protection, security, educational program, tools.

Поворознюк Олексій Олегович

*Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки*

МЕТОДИ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ ПІД ЧАС ВІЙНИ

У сучасних збройних конфліктах між Україною та росією інформація розповсюджується миттєво, а візуальні та аудіовізуальні матеріали формують сприйняття війни як всередині нашої країни, так і за її межами. Фотографії, відеозаписи, аудіофайли та текстові повідомлення можуть містити критично важливу інформацію, яка, у разі потрапляння до рук противника, здатна призвести до катастрофічних наслідків. Саме тому питання захисту мультимедійних даних набуває особливої актуальності, адже війна ведеться не лише на полі бою, а й у кіберпросторі [1].

Сучасні технології дозволяють противнику перехоплювати та аналізувати цифрові матеріали, а тому важливо використовувати методи шифрування та анонімізації, які ускладнюють витік інформації. Зокрема, військові, волонтери, журналісти та цивільні особи повинні враховувати ризики, пов'язані з використанням відкритих каналів передачі даних, таких як месенджери чи соціальні мережі. Недостатній рівень захисту може спричинити викриття позицій військових, розкриття особистих даних людей, які перебувають у зоні бойових дій, або навіть створення дезінформаційних кампаній на основі викрадених матеріалів.

Фальсифікація зображень і відео, поширення дезінформації та фабрикація доказів є частиною стратегії ворога, спрямованої на дестабілізацію суспільства.

Захист даних у цьому контексті включає як технологічні аспекти, так і підвищення рівня медіаграмотності серед населення [2]. Але це базові методи, що можуть мінімізувати можливості появи таких ризиків. Тому є необхідність впровадження нових професійних методик. Розроблені методи захисту мультимедійних даних можливо поділити на категорії, які зображено на рисунку 1.



Рис. 1. Категорії методів захисту мультимедійних даних
Джерело: складено автором

Основні методи зосереджуються на забезпеченні конфіденційності, автентичності та цілісності інформації. Криптографія є одним з найефективніших способів захисту, зокрема методи шифрування, такі як AES-256 [3], забезпечують надійне шифрування даних для збереження їх конфіденційності навіть у випадку перехоплення. Постквантова криптографія, яка також активно розвивається, дозволяє захистити інформацію від можливих атак майбутніх квантових комп'ютерів, що є важливим аспектом у світі технологічних прогресів.

Цифрові підписи служать для перевірки автентичності даних, що є критичним у ситуаціях, коли потрібно підтвердити, що інформація не була змінена чи підроблена. Стеганографія забезпечує приховання даних в мультимедійних файлах, що може використовуватись для секретного передавання важливої інформації, прихованої від несанкціонованих осіб. Водяні знаки, зокрема методи, такі як QIM та Spread Spectrum, дозволяють вбудовувати ідентифікаційні маркери в мультимедійний контент, що допомагає виявляти підробки та відновлювати авторські права [4].

Сучасні методи III-аналізу, зокрема нейронні мережі ResNet-50 [5] і CNNs, можуть бути використані для виявлення маніпуляцій із мультимедійними даними, таких як створення deepfakes або інших фальшивих контентів. Це дозволяє виявляти потенційні загрози для безпеки і автентичності інформації. Використання блокчейну дозволяє реєструвати хеші мультимедійних даних у розподіленому реєстрі, що створює прозорість і допомагає забезпечити захист від несанкціонованих змін.

Гомоморфне шифрування, як метод обробки зашифрованих даних без необхідності їх розшифровки, дає змогу працювати з конфіденційними даними

без ризику їх витоку, що є особливо важливим в умовах обмеженого доступу до інформації в умовах війни. Квантова криптографія, зокрема використання алгоритму CRYSTALS-Kyber, дає змогу захистити дані від майбутніх загроз, пов'язаних з розвитком квантових комп'ютерів, що можуть становити загрозу для традиційних методів захисту [6].

Успішна оборона держави відбувається не лише на полі бою, а й у кіберпросторі, де дані можуть стати як потужною зброєю, так і серйозною вразливістю. Лише завдяки свідомому використанню цифрових технологій та впровадженню надійних методів захисту можна запобігти витоку критично важливих даних та зберегти інформаційну стійкість суспільства.

Список використаних джерел:

1. Романова О. М. Кібербезпека під час повномасштабного вторгнення рф. *Часопис Київського університету права*. 2024. Вип. 2. С. 56-59.
2. Горбань Ю., Олійник О. Медіаграмотність як чинник захисту інформаційного простору від ворожої дезінформації в час війни. *Український інформаційний простір*. 2024. С. 194-205.
3. Boussif M. On the Security of Advanced Encryption Standard (AES). *8th International Conference on Engineering, Applied Sciences, and Technology (ICEAST)*. Chiang Mai, 2022. P. 83-88.
4. Зубко І. С., Мартовицький В. О., Пунченко А. В., Карачевцев Д. Д. Огляд методів нанесення цифрових водяних знаків для захисту зображень. *Системи управління, навігації та зв'язку*. 2024. № 3. С. 121–125.
5. Koonce B. ResNet 50. *Convolutional Neural Networks with Swift for Tensorflow, Image Recognition and Dataset Categorization*, 2021. P. 63-72.
6. Panthi S., Bhuyan B. Safeguarding multimedia in the quantum age. In: *Securing the Digital World*. CRC Press, 2025. P. 63-81.

Ключові слова: мультимедійні дані, захист, конфіденційність даних, автентичність даних, цілісність даних.

Keywords: multimedia data, protection, data confidentiality, data authenticity, data integrity.