ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

ББК 32.81+78.362

Інформаційна безпека та інформаційні технології: збірник тез доповідей VII Всеукраїнської науково-практичної конференції, м. Львів, 27 листопада 2025 року. Львів, ЛДУ БЖД, 2025, 493 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

УДК 004.056.5

ПРОТИДІЯ ГІБРИДНИМ ІНФОРМАЦІЙНИМ ВІЙНАМ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Даниіл ЗАХАРЕВИЧ, Валентина ЯЩУК, Ростислав ТКАЧУК
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено сутність, структуру та особливості гібридних інформаційних війн у сучасному цифровому середовищі, проаналізовано ефективні стратегії протидії цим явищам. Визначено основні технологічні, психологічні та комунікаційні інструменти, що використовуються для дестабілізації суспільної свідомості, впливу на політичні процеси та руйнування інформаційної безпеки держави. Розкрито роль цифрових медіа, соціальних мереж, штучного інтелекту та автоматизованих бот-мереж у створенні та поширенні дезінформації. Запропоновано системний підхід до протидії гібридним інформаційним впливам, що базується на поєднанні технологічних, освітніх та регуляторних інструментів.*

Ключові слова: *гібридна війна, інформаційна безпека, дезінформація, цифрове середовище, кіберзахист.*

Abstract. *The essence, structure and features of hybrid information wars in the modern digital environment are studied, effective strategies for countering these phenomena are analyzed. The main technological, psychological and communication tools used to destabilize public consciousness, influence political processes and destroy the information security of the state are identified. The role of digital media, social networks, artificial intelligence and automated botnets in the creation and spread of disinformation is revealed. A systematic approach to countering hybrid information influences is proposed, based on a combination of technological, educational and regulatory tools.*

Keywords: *hybrid war, information security, disinformation, digital environment, cyber defense.*

У XXI столітті інформаційний простір став ключовим театром ведення гібридних конфліктів, у яких цифрові технології використовуються як зброя стратегічного впливу. Гібридна інформаційна війна поєднує традиційні засоби пропаганди з інноваційними технологіями кібернетичного, психологічного та когнітивного тиску на масову свідомість. Особливістю сучасного етапу є синергія між класичними інформаційними операціями та інструментами штучного інтелекту — генерацією контенту (deepfake), таргетованими кампаніями у соціальних мережах, маніпуляціями з метаданими та автоматизованим поширенням фейкової інформації через бот-мережі.

Гібридна агресія спрямована не лише на підрив політичної стабільності, а й на формування викривлених уявлень про реальність. Її головна мета — не знищення інформаційної інфраструктури, а дестабілізація сус-

пільної довіри до державних інституцій, ЗМІ та наукової спільноти. У цьому контексті інформаційна війна набуває характеру довготривалого процесу, де межа між миром і конфліктом стає розмитою.

Для ефективної протидії гібридним інформаційним впливам необхідна комплексна стратегія, що поєднує технічні, організаційні та освітні підходи. На технологічному рівні першочерговим є створення систем раннього виявлення дезінформаційних кампаній, здатних здійснювати автоматичний моніторинг інформаційних потоків у реальному часі із застосуванням методів машинного навчання, аналізу соціальних графів та семантичного кластерування контенту. Такі системи дозволяють ідентифікувати координацію між бот-акаунтами, виявляти ознаки штучної вірусності контенту та визначати першоджерела інформаційних атак.

На когнітивно-комунікативному рівні актуальним є розвиток медіаграмотності та критичного мислення як базових компетенцій громадян цифрової доби. Формування здатності розпізнавати маніпуляції, фейки та інформаційні пастки знижує вразливість суспільства до деструктивного впливу. У цьому контексті важливим завданням держави та освітніх інституцій є інтеграція навчальних програм з інформаційної гігієни, фактчекінгу та етичного споживання медіаконтенту на всіх рівнях освіти.

Водночас, стратегічна протидія потребує інституційного зміцнення системи національної інформаційної безпеки, удосконалення законодавства щодо відповідальності за поширення дезінформації, регулювання діяльності цифрових платформ і створення незалежних аналітичних центрів для оцінювання інформаційних ризиків. Особливе значення має співпраця державних структур із науковими установами, медіа та громадським сектором, що забезпечує багаторівневу координацію та ефективність протидії гібридним загрозам.

З огляду на стрімкий розвиток технологій штучного інтелекту, особливо в галузі оброблення природної мови (Natural Language Processing, NLP), одним із найбільш перспективних напрямів сучасних досліджень є створення інтелектуальних систем автоматичного виявлення дезінформації на основі глибинних нейронних мереж. Такі системи мають на меті аналізувати текстові повідомлення з урахуванням їхніх синтаксичних, семантичних і прагматично-емоційних характеристик, що дає змогу виявляти не лише відверті неправдиві твердження, а й приховані маніпулятивні патерни, риторичні викривлення та когнітивні упередження.

У межах цього підходу застосовуються архітектури нейронних мереж типу Transformer (зокрема, BERT, RoBERTa, GPT, T5), які здатні враховувати контекст між словами та реченнями, моделюючи смислові зв’язки в тексті. Аналіз дезінформації відбувається у кілька етапів: семантична нормалізація (очищення тексту від шумових елементів), векторизація (перетворення лінгвістичних ознак у числові представлення), класифі-

кація (розмежування достовірної й маніпулятивної інформації) та оцінка впевненості моделі.

Водночас проблема достовірності джерел інформації залишається ключовою. У цьому контексті перспективним є поєднання технологій штучного інтелекту з блокчейн-архітектурою, яка може забезпечити верифікацію походження інформаційних повідомлень і незмінність цифрових записів. Застосування блокчейну дозволяє створити децентралізовану систему маркування контенту, де кожне повідомлення має унікальний цифровий підпис, що підтверджує його джерело, час створення та історію змін. Такий підхід сприяє підвищенню рівня довіри до інформаційних ресурсів і формуванню механізмів відповідальності за поширення фейків. Таким чином, розвиток нейромережевих систем детекції дезінформації у поєднанні з блокчейн-технологіями є ключовим елементом формування стійкої цифрової інфраструктури безпеки, яка базується на принципах прозорості, достовірності та відповідальності за інформаційний вплив.

Протидія гібридним інформаційним війнам потребує системного підходу, який поєднує технологічні інновації, освітню політику та державне регулювання. Ефективність інформаційного захисту визначається не лише наявністю технічних засобів моніторингу, а й рівнем критичного мислення населення, здатністю суспільства протистояти маніпуляціям і формувати власний аналітичний погляд на інформаційні процеси. Запропонована концепція багаторівневої протидії, що включає кіберзахист, аналітичні системи, освіту та міжнародну співпрацю, є основою побудови сталого інформаційного простору. У перспективі подальші дослідження мають бути спрямовані на розроблення моделей когнітивної безпеки, систем штучного інтелекту для виявлення фейків і створення етичних стандартів комунікації в цифровому середовищі.

Література

1. Yashchuk V. The Role And Place Of Cyber Weapons In Ensuring The Information Security Of The State / Yashchuk V. // Інноваційні технології в лінгвістиці та перекладі: Зб. наук. праць Міжнародної наукової конференції. – Львів: ЛДУ БЖД, 2024. – С.41-44.

2. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави / В.І.Ящук // Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 364 (С. 259-286) 1,5 д.а. https://doi.org/10.52058/42-2024

3. Yashchuk, V., Demyanchuk, Y., & Savitska, V. (2025). Integrative approach to the analysis, modeling, and ensuring cyber security of critical information infrastructure under modern threats. Baltic Journal of Economic Studies, 11(2), 273-286. https://doi.org/10.30525/2256-0742/2025-11-2-273-286

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

Відповідальні за випуск **Назарій БУРАК**
Олександр ХЛЕВНОЙ

Оригінал-макет **Юлія НАЗАР, Ольга СМОТР, Роман ГОЛОВАТИЙ, Діана РАЙТА, Віра ДОВБНЯК, Іван РОВЕЦЬКИЙ, Наталія ЖЕЗЛО-ХЛЕВНА**

Підписано до друку 12.11.2025 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.