КІБЕРБЕЗПЕКА: освіта, наука, техніка № 2 (30), 2025
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.904
УДК 004.056:355.01

Лунгол Ольга Миколаївна
кандидат педагогічних наук, доцент,
т.в.о. завідувача кафедри оперативно-розшукової діяльності та інформаційної безпеки
Донецький державний університет внутрішніх справ, м. Кропивницький, Україна
ORCID: 0000-0001-8128-0072
olyalungol@gmail.com

МЕТОДОЛОГІЧНІ ЗАСАДИ АТРИБУЦІЇ СУБ'ЄКТІВ ГІБРИДНОЇ АГРЕСІЇ В НАЦІОНАЛЬНОМУ КІБЕРПРОСТОРІ

Анотація. В умовах триваючої гібридної агресії проти України, здатність точно ідентифікувати джерела ворожих дій у кіберпросторі є не просто технічним завданням, а критично важливим елементом національної безпеки. В даній статті запропоноване одне з вирішень наукової проблеми розробки комплексних методологічних засад для атрибуції суб'єктів гібридних загроз. У вступі акцентовано увагу на актуальність проблеми, що зумовлена необхідністю ефективної протидії скоординованим кібер- та інформаційно-психологічним операціям. Аналіз сучасних досліджень вітчизняних та закордонних науковців показує, що існуючі підходи до атрибуції часто є фрагментарними, зосереджуючись на технічних аспектах, контент-аналізі тощо, що створює нагальну потребу в єдиній, системній методології. Метою даної роботи є розробка цілісної методології атрибуції суб'єктів гібридної агресії, що дозволяє інтегрувати та синтезувати різнорідні дані для формування обґрунтованих висновків. Теоретичною базою дослідження стали концепції гібридної війни та сучасні підходи до аналізу великих даних. Методологія включає системний аналіз, діалектичний метод та моделювання, що дозволило структурувати складний, багатоетапний процес атрибуції. Ключовим науковим результатом є запропонована багаторівнева модель атрибуції, яка об'єднує аналіз на трьох рівнях: технічному (аналіз інфраструктури, шкідливого коду та інших цифрових артефактів), тактичному (ідентифікація стійких поведінкових дій, тактик, технік і процедур) та стратегічному (аналіз наративів, цілей та їх кореляції з геополітичними інтересами держави-агресора). Також у статті сформульовано систему критеріїв для верифікації та оцінки достовірності атрибутивних висновків. У висновках аргументовано, що запропонована модель дозволяє значно підвищити доказову цінність та обґрунтованість атрибуції, забезпечуючи глибоке розуміння стратегії супротивника. Перспективи подальших досліджень включають розробку прикладних аналітичних інструментів на базі штучного інтелекту та дослідження правових механізмів імплементації результатів дослідження.

Ключові слова: атрибуція кібератак; гібридна війна; національна кібербезпека; інформаційно-психологічні операції.

ВСТУП

Гібридна агресія російської федерації проти України давно вийшла за межі традиційного протистояння на фізичному фронті. Сьогодні кіберпростір є повноцінним засобом воєнних дій, де технічні атаки на критичну інфраструктуру, кібершпигунство та масштабні дезінформаційні кампанії стали буденністю. У цій новій реальності питання «Хто за цим стоїть?» перестає бути суто технічним. Точна та своєчасна атрибуція – тобто чітка та якісна ідентифікація суб'єкта, відповідального за атаку, є ключовим фактором, що дозволяє державним органам отримати чітку відповідь й перейти до запровадження санкцій та здійснення власних кібероперацій. У сукупності все це перетворює атрибуцію

на одне з найважливіших та актуальніших наукових й практичних завдань у сфері національної кібербезпеки.

Постановка проблеми. В умовах гібридної агресії атрибуція ворожих дій у кіберпросторі перетворюється з суто технічної задачі на складну аналітичну проблему, що лежить на перетині кількох дисциплін. Традиційні підходи до атрибуції, що здебільшого спираються на аналіз технічних артефактів (таких, як IP-адреси, хеші шкідливого програмного забезпечення, доменні імена тощо), демонструють свою недостатність. Суб'єкти гібридної агресії, маючи значні державні ресурси, активно використовують методи маскування, фальсифікації цифрових слідів та операції під «чужим прапором», що робить технічні докази ненадійними, якщо розглядати їх окремо [1; 2].

Сучасні виклики формують низку невирішених науково-практичних завдань, серед яких особливого значення набувають фрагментарність існуючих методологій, проблема валідації даних з відкритих джерел та відсутність зв'язку між тактичними діями й стратегічними цілями. У результаті, наявні підходи до атрибуції часто є вузькоспеціалізованими: одні зосереджені на технічному аналізі (Malware Analysis, Network Forensics), інші – на контент-аналізі (наприклад, аналіз дезінформаційних наративів). Відсутня єдина, системна методологія, яка б дозволяла комплексно аналізувати технічні, тактичні та стратегічні аспекти гібридних операцій, поєднуючи розрізнені дані в єдину доказову базу [3; 4]. У той час, як розвідка на основі відкритих джерел (OSINT) надає величезні масиви потенційно корисної інформації, проте дані є неструктурованими, часто суперечливими та можуть бути навмисно сфабрикованими агресором для введення в оману. Це також створює нагальну потребу в розробці науково обґрунтованих критеріїв та інструментів верифікації, оцінки достовірності та кореляції даних з OSINT.

Відсутність зв'язку між тактичними діями й стратегічними цілями призводить до того, що атрибуція може завершуватися на ідентифікації конкретної групи хакерів або використаного інструментарію. Проте для ефективної протидії, особливо на державному рівні, необхідно не просто знати хто і як виконав атаку, а й розуміти, навіщо це було зроблено. Виникає проблема встановлення стійких зв'язків між окремими кіберінцидентами, інформаційними кампаніями та довгостроковими геополітичними цілями агресора.

Таким чином, виникає ключова наукова проблема: відсутність комплексних методологічних засад для атрибуції суб'єктів гібридної агресії, які б дозволяли системно інтегрувати та аналізувати різнорідні дані (технічні, поведінкові, контентні тощо) для формування доказових, достовірних та значущих висновків. Вирішення цієї проблеми є критично важливим для розробки ефективних стратегій протидії, притягнення агресора до відповідальності та зміцнення національної кіберстійкості.

Аналіз останніх досліджень і публікацій. Значний внесок у розуміння природи сучасного інформаційного протистояння робить І. Верховцева [5]. Авторка комплексно розглядає кіберпростір не лише як технологічне середовище, а й як новий вимір геополітичного суперництва та простір людського буття. Особливо цінними для даного дослідження є введені та проаналізовані нею поняття «інформаційна агресія» та «інформаційне насильство», які визначаються як цілеспрямований несиловий вплив на ментальну сферу через маніпулювання, поширення дезінформації та ворожих пропагандистських наративів. В її роботі також наведене обґрунтування, що ворожі операції у кіберпросторі є не хаотичними атаками, а частиною довгострокової державної стратегії агресора. Це, у свою чергу, підкреслює необхідність розробки саме

комплексних методологій атрибуції, які б дозволяли виявляти не лише безпосередніх виконавців (тактичний рівень), а й встановлювати їхній зв'язок зі стратегічними цілями держави-агресора.

Зарубіжний дослідник Т. Рід [6], детально аналізує складність атрибуції суб'єктів гібридної агресії, вказуючи на проблему «туману війни» в цифровій сфері. Експерти з NATO Cooperative Cyber Defence Centre of Excellence регулярно публікують звіти, присвячені технічним та правовим викликам ідентифікації зловмисників [7]. Українські науковці переважно зосереджуються на аналізі гібридних загроз, спрямованих саме проти України [7 – 10].

Однак, попри велику кількість публікацій та досліджень, виділяємо системну проблему – фрагментарність підходів. Більшість досліджень фокусуються на чомусь одному, наприклад, технічному аналізі шкідливого програмного забезпечення, або на лінгвістичному аналізі дезінформаційних наративів. Як результат, на сьогодні існує нагальна потреба в розробці комплексної, системної методології атрибуції, яка б дозволила аналізувати подію або події цілісно, пов'язуючи технічні сліди з тактикою та стратегічними цілями агресора. Таким чином, ключова наукова проблема полягає у відсутності комплексних методологічних засад атрибуції, які б дозволяли системно інтегрувати та аналізувати різнорідні дані (технічні, поведінкові, контентні тощо) для формування доказових та достовірних висновків. *Метою статті* є розробка та обґрунтування такої методології.

МЕТОДИКА ДОСЛІДЖЕННЯ

Для розробки моделі використано кілька наукових методів: *системний аналіз* (дозволив розглянути процес атрибуції як складну, багатокомпонентну систему, що складається із взаємопов'язаних елементів – даних, інструментів, аналітики, процедур тощо); *структурно-функціональний метод* (допоміг декомпозивати процес на окремі рівні – технічний, тактичний та стратегічний – та визначити функціональне призначення кожного з них); *діалектичний метод* (застосовано для обґрунтування необхідності синтезу суперечливих даних з різних джерел для отримання об'єктивної картини); методи *синтезу та моделювання* (використано для об'єднання елементів у єдину, логічно послідовну та практично застосовну модель).

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Ключовим результатом наукової роботи є розробка багаторівневої моделі атрибуції, що долає фрагментарність існуючих підходів. Модель структурує аналітичний процес у вигляді трьох взаємопов'язаних рівнів: технічного, тактичного та стратегічного. Розглянемо кожен із даних рівнів більш детально.

Технічний рівень атрибуції – це початковий етап аналітичного процесу. Його основна мета полягає не просто в зборі даних, а у відтворенні інструментарію та інфраструктури, задіяних в операції й формуванні первинної бази об'єктивних, верифікованих індикаторів компрометації. Аналітик на цьому етапі відповідає на ключове питання: «Які технічні засоби та інфраструктура були використані?». Успіх цього рівня є критично важливим, оскільки будь-які подальші тактичні та стратегічні висновки, не підкріплені міцною технічною базою, будуть розцінюватися як припущення.

Джерелами інформації на даному етапі є поєднання даних з різних каналів, наприклад, таких як:

- дані цифрової криміналістики, що можуть включати інформацію, отриману безпосередньо зі скомпрометованих систем – образи дисків, дампи оперативної пам'яті, системні логи, мережевий трафік тощо;
- відомості, отримані в ході оперативно-розшукової діяльності, що є унікальною перевагою державних структур;
- результати моніторингу відкритих джерел (Open Source Intelligence, розвідка на основі відкритих джерел), які можуть включати аналіз публічних репозиторіїв коду, звітів антивірусних компаній, форумів у даркнеті, даних з OSINT сервісів, соціальних мереж та інших загальнодоступних ресурсів;
- дані міжнародного обміну інформацією, які можуть включати відомості, отримані від партнерських спецслужб та центрів реагування на кіберінциденти (CERTs), що дозволяють відстежувати глобальні кампанії. Частиною таких атак може бути й атака на українські об'єкти.

Об'єкти аналізу на технічному рівні доцільно згрупувати за напрямками дослідження (див. табл. 1).

Таблиця 1.

Об'єкти аналізу на технічному рівні

Напрямок аналізу	***Мета та сутність***	***Об'єкти аналізу та їх значення***
Аналіз мережевої інфраструктури	Картування операційного плацдарму противника; виявлення та зв'язування серверів управління, проксі-серверів, фішингових доменів та інших вузлів	IP-адреси, дані WHOIS, історія DNS та ін., які дозволяють встановити зв'язки між доменами за реєстраційними даними, спільним хостингом. Історія DNS може виявити початкову тестову інфраструктуру. Потужним індикатором зв'язку між різними доменами є повторне використання одного SSL/TLS-сертифіката або наявність у ньому унікальних полів.
Аналіз програмних артефактів та шкідливого коду	Дослідження «зброї», яку використав противник. Виявлення унікального цифрового стилю конкретної APT-групи (Advanced Persistent Threat)	Повторне використання унікальних фрагментів коду, власних напрацювань або рідкісних бібліотек є доказом походження з одного джерела. Аналіз метаданих та конфігураційних файлів дозволяє встановити, що часові мітки компіляції вказують на часовий пояс і робочі години, а внутрішні шляхи до файлів слугують унікальними маркерами. Ідентичні криптографічні помилки, виявлені при реалізації алгоритмів у різних зразках ПЗ, є індикатором спільного авторства.

Аналіз веб-ресурсів та цифрової присутності	Дослідження інфраструктури, з якою безпосередньо взаємодіють «жертви» (фішингові сайти, сайти-клони, підроблені сторінки входу тощо)	Однакові ідентифікатори аналітики (наприклад, Google Analytics), коментарі в коді або унікальні скрипти, виявлені у вихідному коді сайтів та аналітичних трекерах, дозволяють об'єднати десятки ресурсів в одну мережу. Використання однакових веб-шрифтів, іконок, версій CMS чи плагінів дозволяє встановити зв'язки між доменами, оскільки це вказує на створення сайтів за єдиним шаблоном.

Результатом технічного рівня є не просто набір розрізнених фактів, а структурована база даних доказових індикаторів, яка дозволяє сформулювати первинні гіпотези та слугує емпіричною основою для переходу на наступний, тактичний рівень аналізу.

Метою наступного рівня атрибуції – *тактичного* – є перехід від розрізнених технічних індикаторів до ідентифікації стійких поведінкових дій. На даному рівні аналітик відповідає на питання: «Як діє суб'єкт агресії?».

При цьому процес аналізу може включати:

- кластеризацію індикаторів через об'єднання технічних артефактів у групи за спільними характеристиками;
- ідентифікацію тактик, технік та процедур, що можуть містити аналіз послідовності дій, використаного інструментарію, методів соціальної інженерії тощо;
- аналіз каналів поширення контенту через вивчення координації між бот-мережами, просування фейкових акаунтів тощо.

Кінцевим результатом аналітичної роботи на тактичному рівні є доказове віднесення (атрибуція) серії розрізнених кіберінцидентів до єдиної, скоординованої кампанії, що проводиться конкретним хакерським угрупованням, наприклад, відомою APT-групою. На відміну від технічного рівня, де результатом був набір об'єктивних індикаторів, тут аналітик формує цілісний профіль зловмисника. Цей профіль ґрунтується не на окремих слідах, а на стійкій та унікальній моделі поведінки – цифровому «почерку» [11; 12]. Таким чином, хаотичні на перший погляд події об'єднуються в логічну послідовність, що дозволяє не лише ідентифікувати виконавця, а й прогнозувати його наступні кроки. Саме цей структурований висновок стає відправною точкою для переходу на найвищий, стратегічний рівень атрибуції.

На *стратегічному рівні* атрибуції відбувається встановлення зв'язку між тактичними діями та довгостроковими геополітичними, економічними чи військовими цілями держави-агресора. Аналітик шукає відповідь на ключове питання: «Навіщо ця операція проводилася і хто є кінцевим бенефіціаром?». В процесі аналізу може відбуватися визначення секторів (енергетика, фінанси, оборона), проти яких були спрямовані атаки; співставлення часу проведення кібероперацій з важливими політичними подіями (вибори, саміти, військові дії тощо); ідентифікація ключових дезінформаційних повідомлень та їх відповідності офіційній політичній лінії держави-агресора тощо.

Результатом стратегічномого рівня може бути формування обґрунтованого висновку про приналежність операції до конкретного державного суб'єкта. На цьому рівні відбувається синтез даних з усіх попередніх етапів з геополітичним аналізом.

Важливим етапом кожного рівня є оцінка достовірності атрибуції. Для забезпечення об'єктивності висновків, у рамках розробленої методології, пропонуємо наступну системи критеріїв верифікації:

- якість та кількість доказів, що включає наявність множинних, незалежних індикаторів на кожному з рівнів. Перевага при цьому надається унікальним та важким для фальсифікації індикаторам;

- порівняння моделі поведінки зловмисника з відомими профілями, наприклад, оцінка того, чи відповідають тактики, техніки та процедури (TTPs), застосовані в атаці, раніше задокументованій та характерній діяльності конкретних APT-угруповань;

- когерентність (міжрівнева кореляція), що передбачає наявність логічного та послідовного зв'язку між технічними артефактами, тактичними діями та стратегічними наративами;

- фальсифікація альтернативних гіпотез через аналіз та спростування альтернативних версій (напр., операція під «чужим прапором», дії незалежних хактивістів тощо).

Застосування даної моделі та критеріїв дозволяє перетворити процес атрибуції на структуровану науково-аналітичну діяльність, що значно підвищує доказову цінність висновків.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході проведеного дослідження було вирішено актуальну наукову проблему, яка полягала у відсутності комплексних методологічних засад для атрибуції суб'єктів гібридної агресії в кіберпросторі. Фрагментарність існуючих підходів, які зосереджуються на окремих аспектах ворожих операцій, не дозволяє сформувати цілісну, об'єктивну картину та доказово встановити зв'язок між технічними виконавцями та державними замовниками.

Основним науковим результатом даної роботи є розробка та обґрунтування багаторівневої моделі атрибуції, що інтегрує аналіз на технічному, тактичному та стратегічному рівнях. Запропонована модель має низку ключових переваг, таких, як системність, комплексність та підвищенна доказова цінність. Запропонована модель перетворює процес атрибуції з хаотичного аналізу розрізнених фактів на структуровану, логічно послідовну аналітичну діяльність. Модель забезпечує синтез різнорідних даних – від цифрових артефактів та поведінкових закономірностей до геополітичного контексту й пропагандистських наративів. Послідовний перехід між рівнями та застосування запропонованих критеріїв верифікації значно підвищують обґрунтованість та достовірність кінцевих висновків, що є критично важливим для прийняття відповідальних державних рішень.

Таким чином, представлена методологія дозволяє не лише реагувати на окремі кіберінциденти, а й розуміти стратегічний задум агресора, що є фундаментальною передумовою для розробки ефективних превентивних та асиметричних заходів протидії.

Подальший розвиток представлених у статті результатів вбачається у кількох перспективних напрямках. Оскільки модель описує аналітичний процес, значну частину якого можна автоматизувати, то перспективним є створення спеціалізованих програмних платформ на основі штучного інтелекту та машинного навчання (AI/ML). Такі системи могли б в автоматичному режимі здійснювати збір та первинну кореляцію технічних індикаторів, виявляти стійкі TTPs у великих масивах даних та ідентифікувати аномалії, дозволяючи аналітику зосередитись на найскладнішому – стратегічному аналізі.

Також, однією з найгостріших проблем залишається легалізація результатів атрибуції. Тому, у перспективах подальших досліджень є проведення детального дослідження щодо розробки механізмів імплементації аналітичних висновків,

отриманих з різних джерел у вітчизняне законодавство. Важливо розробити чіткі науково-методичні рекомендації та нормативні процедури, які б дозволили перетворити розвідувальну інформацію на повноцінні процесуальні докази, придатні для використання у вітчизняних та міжнародних судах для притягнення до відповідальності як безпосередніх виконавців, так і організаторів гібридної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Офіційний сайт Кіберполіції України. Національна поліція України*. (n.d.). https://cyberpolice.gov.ua/
2. *Державна служба спеціального зв'язку та захисту інформації України. Офіційний сайт.* (n.d.). https://cip.gov.ua/ua/news
3. Буряченко, О. (2024). Гібридна війна як нова форма глобального протистояння. *Наукові праці Міжрегіональної академії управління персоналом*, (2), 74. 24 – 31.
4. Зінченко, О.І. (2025). Протидія кібертероризму як загрозі сучасній національній безпеці держав Європейського регіону : дисертація ... доктора філософії за спеціальністю 052 Політологія. Харків : Харківський національний університет імені В. Н. Каразіна, 272.
5. Верховцева, І.Г. (2024). Глобальний кіберпростір та опір інформаційній агресії: кібердипломатія України у протидії російській інформаційній інвазії. *Глобальний кіберпростір: сучасні виклики та рішення. Розділ 9.* 213-243. http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/510/13505/28342-1
6. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. *Center for the Study of Intelligence.* Vol 64, No. 1. https://www.cia.gov/resources/csi/static/active-measures-and-information-wars.pdf
7. *The NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/
8. Лунгол, О.М. (2025). Синергія цифрової розвідки та алгоритмів штучного інтелекту для ефективного виявлення кіберзагроз. *Наука і техніка сьогодні: журнал*, 2(43), 1320 – 1332.
9. Лунгол, О. (2024). Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 1(25), 379 – 389.
10. Popov, G., & Orobets, K. (2025). Assessing War Crimes During Armed Conflicts: Insights from Ukraine and Global Standards. *Journal of Lifestyle and SDGs Review*, 5(1), e03391. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe03391
11. Бойко, Р. (2024). Цифрові інновації в запобіганні злочинності та профілактиці кримінальних правопорушень. *Взаємодія державних органів та громадськості у сфері протидії кримінальним правопорушенням у центральних регіонах України*: збірник матеріалів круглого столу (м. Кропивницький, 17 квітня 2024 р.), Кропивницький: ДонДУВС, 144 – 146.
12. Шаєц, Є., & Лунгол, О. (2022). Використання ханіпотів для виявлення мережевих атак. *Інформаційна безпека та інформаційні технології*: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. Львів: Растр-7, 93 – 95.

КІБЕРБЕЗПЕКА: освіта, наука, техніка № 2 (30), 2025
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
Спеціальний випуск ISSN 2663 – 4023
Special issue

Olha M. Lunhol
Ph.D. in Pedagogical Sciences, Docent,
Acting Head of the Department of Operational-Search Activities and Information Security
Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
ORCID: 0000-0001-8128-0072
olyalungol@gmail.com

METHODOLOGICAL FRAMEWORK FOR THE ATTRIBUTION OF HYBRID AGGRESSION ACTORS IN THE NATIONAL CYBERSPACE

Abstract. In the context of the ongoing hybrid aggression against Ukraine, the ability to accurately attribute the sources of hostile actions in cyberspace is not merely a technical task but a critical element of national security. This article proposes a solution to the scientific problem of developing a comprehensive methodological framework for the attribution of hybrid threat actors. In the introduction, the author reveals the urgency of the problem, driven by the need for effective counteraction to coordinated cyber and information-psychological operations. An analysis of contemporary research by domestic and foreign scholars shows that existing approaches to attribution are often fragmented, focusing on either technical aspects or content analysis, which necessitates a unified, systemic methodology. The purpose of this work is to develop a holistic methodology for the attribution of hybrid aggression actors, which allows for the integration and synthesis of diverse data to form substantiated conclusions. The theoretical basis of the research includes concepts of hybrid warfare and modern approaches to big data analysis. The methodology involves systemic analysis, the dialectical method, and modeling, which enabled the structuring of the complex, multi-stage attribution process. The key scientific result is the proposed multi-level attribution model, which combines analysis on three levels: technical (analysis of infrastructure, malicious code, and other digital artifacts), tactical (identification of persistent behavioral patterns, tactics, techniques, and procedures), and strategic (analysis of narratives, objectives, and their correlation with the aggressor state's geopolitical interests). The article also formulates a system of criteria for the verification and assessment of the reliability of attribution findings. In the conclusions, the author argues that the proposed model can significantly enhance the evidential value and validity of attribution, providing a deeper understanding of the adversary's strategy. Prospects for further research include the development of applied analytical tools based on artificial intelligence and the study of legal mechanisms for implementing the research results.

Keywords: cyberattack attribution; hybrid warfare; national cybersecurity; information-psychological operations.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Natsionalna politsiia Ukrainy [National Police of Ukraine]. (n.d.). *Ofitsiinyi sait Kiberpolitsii Ukrainy [Official site of the Cyberpolice of Ukraine*]. Retrieved August 3, 2025, from https://cyberpolice.gov.ua/
2. *Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy [State Service of Special Communications and Information Protection of Ukraine]*. (n.d.). Ofitsiinyi sait [Official site]. Retrieved August 3, 2025, from https://cip.gov.ua/ua/news
3. Buriachenko, O. (2024). Hibrydna viina yak nova forma hlobalnoho protystoiannia [Hybrid warfare as a new form of global confrontation]. *Naukovi pratsi Mizhrehionalnoi akademii upravlinnia personalom [Scientific works of the Interregional Academy of Personnel Management*], (2), 24–31.
4. Zinchenko, O.I. (2025). Protydiia kiberteroryzmu yak zahrozi suchasnii natsionalnii bezpetsi derzhav Yevropeiskoho rehionu [Countering cyberterrorism as a threat to the modern national security of the states of the European region] [Doctoral dissertation, V. N. Karazin Kharkiv National University].
5. Verkhovtseva, I.H. (2024). Hlobalnyi kiberprostir ta opir informatsiinii ahresii: kiberdyplomatiia Ukrainy u protydii rosiiskii informatsiinii invazii [Global cyberspace and resistance to information aggression: Cyberdiplomacy of Ukraine in countering the Russian information invasion]. In *Hlobalnyi kiberprostir: suchasni vyklyky ta rishennia [Global cyberspace: Modern challenges and solutions]* (pp. 213–243). Baltija Publishing. http://www.baltijapublishing.lv/omp/index.php/bp/catalog/view/510/13505/28342-1

6. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. *Center for the Study of Intelligence*. https://www.cia.gov/resources/csi/static/active-measures-and-information-wars.pdf
7. *The NATO Cooperative Cyber Defence Centre of Excellence.* (n.d.). *The NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved August 23, 2025, from https://ccdcoe.org/
8. Lunhol, O.M. (2025). Synerhiia tsyfrovoi rozvidky ta alhorytmiv shtuchnoho intelektu dlia efektyvnoho vyiavlennia kiberzahroz [Synergy of digital intelligence and artificial intelligence algorithms for effective detection of cyber threats]. *Nauka i tekhnika sohodni [Science and Technology Today*], (2), 1320–1332.
9. Lunhol, O. (2024). Ohliad metodiv ta stratehii kiberbezpeky zasobamy shtuchnoho intelektu [Review of cybersecurity methods and strategies by means of artificial intelligence]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» [Electronic professional scientific publication "Cybersecurity: education, science, technology"]*, (1), 379–389.
10. Popov, G., & Orobets, K. (2025). Assessing War Crimes During Armed Conflicts: Insights from Ukraine and Global Standards. *Journal of Lifestyle and SDGs Review*, 5(1), e03391. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe03391
11. Boiko, R. (2024). Tsyfrovi innovatsii v zapobihanni zlochynnosti ta profilaktytsi kryminalnykh pravoporushen [Digital innovations in crime prevention and prophylaxis of criminal offenses]. In Vzaiemodiia derzhavnykh orhaniv ta hromadskosti u sferi protydii kryminalnym pravoporushenniam u tsentralnykh rehionakh Ukrainy: zbirnyk materialiv kruhloho stolu [*Interaction of state bodies and the public in the field of countering criminal offenses in the central regions of Ukraine: Collection of materials of the round table*] (pp. 144–146). DonDUVS.
12. Shaiets, Ye., & Lunhol, O. (2022). Vykorystannia khanipotiv dlia vyiavlennia merezhevykh atak [The use of honeypots for detecting network attacks]. In Informatsiina bezpeka ta informatsiini tekhnolohii: zbirnyk tez dopovidei IV Mizhnarodnoi naukovo-praktychnoi konferentsii, IBIT 2022 [*Information security and information technologies: Collection of abstracts of the IV International scientific and practical conference, ISIT 2022*] (pp. 93–95). Rastr-7.