УДК 34:342/35

ДОВГАНЬ О.Д., *заслужений діяч науки і техніки, доктор юридичних наук, професор,* радник при дирекції Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України».
ORCID: https://orcid.org/0000-0002-3453-4938

ТКАЧУК Т.Ю., *доктор юридичних наук, професор,* учений секретар наукової лабораторії (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз.
ORCID: https://orcid.org/0000-0002-4620-3300

ПРОТИДІЯ COUNTER-FORENSICS ЯК СКЛАДОВА ЦИФРОВОЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334135

Анотація. *У статті досліджується контрфорензіка як одна з найбільш небезпечних форм цифрового втручання, що становить пряму загрозу цифровій безпеці об'єктів критичної інфраструктури України в умовах повномасштабної війни. Обґрунтовано, що контрфорензічні технології – зокрема wiping, fileless-атаки, стеганографія, діпфейки та інші інструменти приховування цифрових слідів – активно використовуються у сучасних кібератаках, спрямованих на підрив стійкості ключових елементів інфраструктури держави.*

У роботі проведено міждисциплінарний аналіз технічних, правових і організаційних аспектів протидії контрфорензіці. Розглянуто реальні кейси втручань у роботу енергетичних, логістичних, телекомунікаційних та адміністративних систем, під час яких зловмисники здійснювали спроби приховати або знищити цифрові докази. Особливу увагу приділено національному та міжнародному досвіду захисту цифрових слідів, зокрема методам резервного збереження журналів, використанню засобів аналітики на основі штучного інтелекту, інституційним моделям співпраці між державними та приватними структурами.

Стаття містить пропозиції щодо удосконалення нормативно-правового регулювання електронних доказів для об'єктів критичної інфраструктури, а також рекомендації з технічного переоснащення судово-експертної та оперативної інфраструктури. Обґрунтовано доцільність створення Національного архіву цифрових доказів та запровадження обов'язкової сертифікації фахівців з цифрової криміналістики з урахуванням компоненту контрфорензіки.

Узагальнено, що ефективна протидія контрфорензіці є не лише питанням кримінального переслідування, а й ключовою умовою функціональної стійкості критичної інфраструктури та цифрової безпеки держави в умовах збройної агресії.

Ключові слова: *контрфорензіка, цифрова безпека, критична інфраструктура, цифрові докази, wiping, інформаційна війна, фальсифікація доказів, кіберзлочини, цифрова криміналістика, національна стійкість.*

Abstract. *The article examines counter-forensics as one of the most dangerous forms of digital interference, which poses a direct threat to the digital security of critical infrastructure of Ukraine in the conditions of a full-scale war. It is substantiated that counter-forensic technologies — including wiping, fileless attacks, steganography, deepfakes, and other tools designed to conceal digital traces — are actively employed in contemporary cyberattacks targeting the stability of critical elements of state infrastructure.*

The paper provides an interdisciplinary analysis of the technical, legal and organizational aspects of combating counter-forensics. Real cases of interference in the work of energy, logistics,

telecommunications and administrative systems are considered, during which attackers attempted to hide or destroy digital evidence. Special attention is paid to national and international experience in protecting digital traces, in particular, methods of backup storage of logs, the use of analytical tools based on artificial intelligence, institutional models of cooperation between state and private structures.

The article contains proposals for improving the regulatory and legal regulation of electronic evidence for critical infrastructure, as well as recommendations for the technical re-equipment of forensic and operational infrastructure. The feasibility of creating a National Archive of Digital Evidence and introducing mandatory certification of digital forensics specialists, taking into account the counter-forensics component, is substantiated.

It is summarized that effective counteraction to counter-forensics is not only a matter of criminal prosecution, but also a key condition for the functional resilience of critical infrastructure and digital security of the state in conditions of armed aggression.

Keywords: *counter-forensics, digital security, critical infrastructure, digital evidence, wiping, information warfare, evidence falsification, cybercrime, digital forensics, national resilience.*

Постановка проблеми. Повномасштабна військова агресія російської федерації проти України радикально змінила уявлення про сучасні загрози національній безпеці, висунувши на перший план питання захисту критичної інфраструктури держави в умовах тотальної війни. Паралельно з веденням активних бойових дій противник здійснює масштабні кібератаки, інформаційно-психологічні операції та технологічно складні деструктивні впливи на цифрові системи. Особливого значення набуває питання цифрової безпеки об'єктів критичної інфраструктури, адже їхнє функціонування забезпечує стійкість оборони, енергетичної системи, транспорту, зв'язку, медицини та інших ключових секторів життєзабезпечення.

У контексті війни критична інфраструктура України стає ціллю не лише фізичних ударів, а й високотехнологічних диверсій, спрямованих на фальсифікацію, знищення або приховування цифрових доказів. Одним із таких викликів є явище контрфорензіки — свідоме застосування технік і засобів для уникнення виявлення цифрових слідів та унеможливлення розслідування кіберзлочинів. Такі дії загрожують не лише ефективному кримінальному переслідуванню, а й оперативному реагуванню на загрози, що виникають в цифровому просторі. Як відмічає *Емре Хосгор*, контрфорензіка спрямована на те, щоб "*ускладнити пошук зловмисника і зробити неможливим доведення його вини"* шляхом приховування, спотворення або знищення інформації, яка може бути доказом злочину. Такі методи стали предметом активного вивчення лише нещодавно, хоча на практиці застосовуються кіберзлочинцями вже понад два десятиліття [1].

На тлі системного використання контрфорензічних засобів з боку держави-агресора постає нагальна потреба в розробці та впровадженні ефективних механізмів протидії цій загрозі. В умовах війни протидія контрфорензіці перетворюється на один із ключових елементів цифрової безпеки критичної інфраструктури, а її належне правове й технологічне забезпечення — на обов'язкову умову національної стійкості.

Мета статті – комплексне дослідження контрфорензіки як деструктивного інструменту, що застосовується у воєнній агресії проти України, з урахуванням міжнародного досвіду та національних викликів у сфері захисту цифрової безпеки критичної інфраструктури. Увага буде приділена як технологічним аспектам виявлення та нейтралізації контрфорензіки, так і необхідності нормативного закріплення відповідних протидій у національній правовій системі. Для реалізації визначеної мети передбачається вирішення таких *наукових завдань*: розкрити сутність явища

контрфорензіки як цілеспрямованої діяльності, що унеможливлює або ускладнює виявлення цифрових доказів, та охарактеризувати її ключові технологічні й правові ознаки; проаналізувати актуальні ризики та загрози, які контрфорензіка становить для функціонування цифрової інфраструктури критичних секторів України в умовах воєнного стану; запропонувати стратегічні підходи та практичні рекомендації щодо інтеграції інструментів протидії контрфорензіці в систему цифрової безпеки критичної інфраструктури України.

Аналіз сучасного стану досліджень у сфері протидії контрфорензіці свідчить про зростання наукового та практичного інтересу до цієї проблематики, особливо у контексті стрімкого розвитку кіберзлочинності, фальсифікації цифрових доказів та інформаційних загроз, що ставлять під загрозу функціонування критичної інфраструктури держав. Перші системні підходи до класифікації контрфорензічних методів запропоновані у роботах технічного спрямування, зокрема в публікації Е. Хосгора, де розглянуто категорії деструктивних інструментів — від прихованого шифрування до знищення журналів подій — та окреслено основні напрями виявлення та реагування на подібні загрози. У доповнення до цього, класичні дослідження The Grugq та Берінато заклали підґрунтя для розуміння логіки поведінки зловмисників, які використовують anti-forensics з метою приховування слідів у комп'ютерних системах.

Проблема набула особливої актуальності у світлі масштабних кібератак на українську критичну інфраструктуру, що почастішали з початку повномасштабної війни. У звітах CERT-UA, аналітичних публікаціях Industrial Cyber та Google Threat Intelligence виявлено численні приклади спроб дестабілізації систем енергетики, логістики й комунікацій із застосуванням засобів знищення цифрових слідів, як-от Industroyer2, CaddyWiper, ShadowMist тощо. Однак, попри високий рівень технічної деталізації, ці джерела не містять глибокого аналізу правових, процесуальних або інституційних механізмів реагування на такі загрози.

У межах міжнародного досвіду значна увага приділяється розробці механізмів відновлення цифрової довіри. Зокрема, GAO у звіті за 2024 рік наголошує на необхідності поєднання автоматичних інструментів виявлення та аутентифікації контенту для боротьби з діпфейками, що створює паралелі з концепцією багаторівневої протидії контрфорензіці. Ініціативи, як-от Content Authenticity Initiative, надають практичні підходи до маркування та верифікації цифрових доказів, однак залишаються переважно орієнтованими на сферу інформаційної безпеки та ЗМІ, без належної адаптації до потреб об'єктів критичної інфраструктури.

В українському науковому просторі перші спроби осмислення правових і організаційних аспектів протидії кіберзагрозам здійснені у працях М. Гуцалюка, зокрема щодо специфіки кіберзлочинності у воєнний період та особливостей обігу цифрових доказів. Проте ці дослідження здебільшого не торкаються вузько спеціалізованих технологій антифорензіки, а також не акцентують увагу на комплексній загрозі, яку становить їхнє застосування проти цифрових систем критичних об'єктів.

Невирішеними залишаються питання адаптації інституційної спроможності держави до роботи з новими формами цифрової фальсифікації, створення захищених архітектур обміну слідами цифрових інцидентів, правового врегулювання протидії саме контрфорензічним діям як окремому напрямові, а також інтеграції міжнародних рішень (як-от CAI або ініціатив CCDCOE) у національний контекст. Саме цим аспектам — недослідженим, але критично важливим для забезпечення цифрової безпеки критичної інфраструктури України в умовах війни — і присвячена дана стаття.

Виклад основного матеріалу. Поняття контрфорензіки (anti-forensics) увійшло до наукового та практичного обігу на початку 2000-х років для опису цілеспрямованих дій, що перешкоджають цифровій криміналістиці. У літературі контрфорензіку визначають як сукупність технік і заходів, які покликані "**скомпрометувати доступність або корисність доказів для процесу розслідування"** [2]. На відміну від власне цифрової криміналістики (Digital Forensics), що займається виявленням та аналізом доказів, контрфорензіка має протилежну мету – унеможливити або максимально ускладнити такі дії. Характерно, що деякі інструменти контрфорензіки можуть мати і легітимне застосування (наприклад, шифрування для захисту приватних даних), однак у контексті цього дослідження розглядаються саме зловмисні практики їх використання. Одне з найбільш відомих і широко прийнятих визначень поняття контрфорензіки запропонував Марк Роджерс. У своїй публікації в журналі *Phrack* у 2002 році, яка стала однією з перших обґрунтованих презентацій антикриміналістики, він визначає її як "видалення або приховування доказів із зниженням ефективності судово-медичного розслідування" [3].

На сьогодні відомо цілу низку антифорензічних методів, які зловмисники застосовують для приховування слідів своїх дій або спотворення картини злочину. Серед найпоширеніших – навмисне знищення даних (видалення файлів, стирання диска), шифрування інформації, приховування даних (стеганографія), підробка часових міток і метаданих (timestomping), "зачищення" записів журналів подій, а також більш витончені прийоми на кшталт маніпулювання вмістом файлів чи створення фальшивих зображень і відео. Наслідком усіх цих прийомів є або повністю ліквідовані сліди злочину, або змінені таким чином, щоб слідчі зробили неправильні висновки. Наприклад, за даними спеціалізованого огляду CISO MAG, зловмисник може змінювати заголовки файлів чи розширення (перемінювати .jpg на .mp3), щоб приховати справжній формат даних; інший приклад – використання утиліти для очищення системного журналу аудиту з метою видалити записи про шкідливі дії. У сфері кіберзлочинності також широко застосовуються інструменти шифрування та "затирання" даних, які роблять неможливим відновлення інформації традиційними методами. Окремо слід відзначити стрімкий розвиток технологій підробки мультимедійних даних: сьогодні доступні засоби високоякісного редагування зображень (видалення або вставки об'єктів без видимих слідів) і генерації фальшивого відео за допомогою штучного інтелекту (далі також – ШІ/AI) (так звані deepfake, коли обличчя або голос однієї особи накладаються на відео з іншою). Усе це створює суттєві виклики для експертів-криміналістів. Таким чином, фальсифікація цифрових доказів є серйозним викликом для криміналістики, особливо в умовах сучасних загроз.

Контрфорензіка становить пряму загрозу для цифрової безпеки критично важливих об'єктів, оскільки у разі кібератаки на такі об'єкти зловмисники прагнуть не лише завдати первинної шкоди, але й ускладнити подальше розслідування інциденту. Зокрема, російські хакерські групи, що діють проти України, відомі застосуванням методів стирання слідів у атаках на енергетику, транспорт, урядові інформаційні системи. Показовим є випадок кібератаки групи Sandworm на енергетичну інфраструктуру України наприкінці 2022 року: Група Sandworm, пов'язана з ГРУ РФ, спробувала повторити успіх кібератак 2015-2016 років, націлившись на одну з підстанцій "Укренерго". Схема атаки включала два етапи: спочатку – вимкнення обладнання через шкідливе ПЗ Industroyer2 (це викликало аварійне знеструмлення), а через два дні – **розгортання вайпера CaddyWiper у мережі ІТ для знищення журналів та інших слідів атаки** [4]. Однак цього разу ефект виявився мінімізованим.

По-перше, система була краще захищена: Industroyer2 не призвів до катастрофічних пошкоджень, енергетики швидко перемкнули живлення і відновили постачання. По-друге, **форензічна готовність**: після подій 2015 року "Укренерго" впровадило централізований збір логів з підстанцій, тому навіть знищивши локальні журнали, зловмисники не змогли стерти їх копії на центральному сервері. Експерти CERT-UA спільно з ESET і Microsoft проаналізували ці збережені дані та відстежили дії Sandworm, навіть попри спроби приховування (саме завдяки журналам виявлено, що зараження почалося з компрометації облікового запису, з якого було розгорнуто шкідливі GPO в домені) [4]. Таким чином, атака була атрибутована і про неї повідомлено публічно, що зруйнувало плани рф в інформаційному полі (очевидно, вони хотіли здійснити "тиху" диверсію без явних слідів). Цей кейс демонструє, що **інвестиції в кібербезпеку і моніторинг** (створення SOC, резервування логів) себе виправдовують: навіть якщо атакувальник сильний, добре налагоджена система дає змогу протидіяти його анти-форензічним прийомам і залишити достатньо даних для розслідування.

Така тактика – паралельне використання руйнівного ПЗ для знищення логів та даних – стала своєрідною "візитною карткою" російських кібероперацій, починаючи з вірусу NotPetya (2017) і до сучасних воєнних інцидентів. Відтак, для критичної інфраструктури анти-форензіка небезпечна тим, що не дозволяє оперативно з'ясувати обставини та методи атаки, що ускладнює реагування і запобігання повторним ударам.

Наведемо ще декілька подібних кейсів. У листопаді 2023 року хакерське угруповання, імовірно пов'язане з APT28 (також контрольоване гру рф), провело кібератаку на муніципальний дата-центр в одному з обласних центрів. Після короткотривалого відключення сервісів у системі було виявлено спробу повного знищення слідів вторгнення. Зловмисники використали спеціалізоване програмне забезпечення для перезапису даних (wiper-засіб із функціями "data remanence removal"), а також програму, що унеможливлює відновлення логів (log-killer з компонентами low-level disk access) [5].

Однак адміністрація дата-центру, яка з початку 2023 року впровадила політику "immutable logs" із реплікацією на хмарну платформу та використанням timestamp-захисту, змогла зберегти більшість даних для аналізу.

Інформацію про атаку було передано СБУ та Національному координаційному центру кібербезпеки, які на основі збережених цифрових слідів змогли ідентифікувати використаний маршрут проникнення — через уразливість у VPN-шлюзі та несанкціоноване підключення до бекап-серверів.

Цей інцидент доводить важливість архітектурної розподіленості цифрового середовища та використання хмарних рішень для збереження слідів у разі застосування антифорензічних методів.

У березні 2024 року CERT-UA за підтримки міжнародних партнерів виявила спробу проникнення у логістичну платформу, яка обслуговує переміщення вантажів для ЗСУ. Особливістю цієї атаки було використання інструменту під назвою *ShadowMist*, здатного динамічно підлаштовуватися під систему та уникати слідкування: він виявляв запущені моніторингові процеси, знищував сесії трасування, модифікував дані в оперативній пам'яті без запису на диск [6].

Ця атака була майже успішною: лише завдяки випадковому спрацюванню автоматичного алерту на зміну ключових конфігурацій в одному із сегментів системи вдалось виявити проникнення. У ході аналізу було встановлено, що основною метою зловмисників було не виведення системи з ладу, а періодична зміна даних про маршрути та вантажі з метою створення хаосу.

Факт знищення цифрових слідів унеможливив класичну форензічну реконструкцію, однак збереження оперативних резервних копій дозволило частково відновити перебіг подій та встановити вікно часу атаки.

Цей кейс ілюструє підвищений рівень складності атак на військову логістику та використання контрфорензіки як інструменту впливу на ефективність військових дій.

Наведеними прикладами перелік не вичерпується – насправді кожне розслідування воєнних злочинів чи кібератаки супроводжується тією чи іншою формою протидії анти-форензіці, і кожного разу наші фахівці здобувають новий досвід. Головне, що можна зробити висновок: **контрфорензіка хоч і ускладнює роботу, але не є непереборною перешкодою**. Комбінація сучасних засобів, добре продумана організація роботи та підтримка міжнародної спільноти дозволяють успішно викривати навіть наймайстерніше приховані злочини.

Сучасні загрози контрфорензіки безпосередньо позначаються на здатності притягнути винних до відповідальності. Якщо цифрові докази викрадено, знищено або спотворено – слідство може зайти в глухий кут, або ж сторона захисту отримає можливість ставити під сумнів їхню допустимість. В умовах війни це особливо критично: величезний масив цифрових свідчень воєнних злочинів (фото, відео, аудіозаписи, дані з телефонів, записи камер тощо) має бути збережено і перевірено, інакше міжнародні судові інстанції не матимуть належної доказової бази. Аналогічно, для кібератак на критичну інфраструктуру – якщо через анти-форензіку неможливо встановити, хто і як атакував, зловмисник уникне покарання і може повторити напад. Таким чином, контрфорензіка загрожує не лише конкретним системам, а й принципу невідворотності правосуддя. Це висуває підвищені вимоги до правоохоронних органів щодо так званої **форензічної готовності**: мають бути створені умови, за яких навіть у разі спроб приховати сліди все одно залишатимуться резервні дані або альтернативні докази, достатні для розслідування. У світі набуває популярності концепція *digital resilience* (цифрова стійкість), яка включає здатність систем не лише протидіяти вторгненням, а й зберігати необхідну інформацію про інциденти для подальшого аналізу. Для України ця концепція надзвичайно актуальна як складова загальної стратегії кібербезпеки та безпеки критичної інфраструктури.

Підсумовуючи, контрфорензіка сьогодні є реальним фактором ризику у цифровій сфері, який використовується як організованою злочинністю, так і державами-агресорами. Вона ускладнює розкриття злочинів та створює інформаційний хаос, підриваючи довіру до цифрових даних. Відповідно, протидія їй повинна стати пріоритетом для сектору безпеки.

Протидія анти-форензіці потребує комплексного підходу, що включає правові норми, стандарти якості, міжнародну кооперацію та впровадження передових технологій. Розвинені країни та міжнародні організації усвідомили цю проблему в останні роки, результатом чого стали як нові нормативні акти, так і створення спеціалізованих робочих груп. Розглянемо ключові напрямки міжнародного досвіду, що є релевантними для України.

У Європі важливу роль відіграє **Європейська мережа судово-експертних установ (ENFSI)**, що об’єднує понад 70 лабораторій із 39 країн. ENFSI має робочу групу з цифрової криміналістики, яка регулярно проводить тренінги, порівняльні тестування (proficiency tests) та видає рекомендації щодо нових методик. Україна (ІСТЕ СБУ) з 2016 р. є членом ENFSI і активно бере участь у заходах мережі. Це дозволяє українським експертам тримати руку на пульсі світових тенденцій: наприклад, дізнаватися про нові анти-форензічні інструменти, що з’явилися десь у Європі, і одразу шукати способи їх

виявлення. ENFSI також сприяє налагодженню контактів з європейськими колегами – можна в будь-який момент запитати поради або попросити допомоги у спеціалістів з інших країн (скажімо, якщо захоплено новий зразок шкідливого ПЗ, який наші антивіруси ще не бачили, можна переслати його у лабораторію партнера для спільного аналізу) [7]. Отже, участь у таких мережах значно підсилює наші можливості протидії контрфорензіці.

В межах НАТО діє **Кооперативний центр з кібероборони (CCDCOE)** в Таллінні, який, окрім іншого, досліджує методи анти-форензіки та способи протидії їм. Експерти CCDCOE у 2018 році опублікували ґрунтовне дослідження з класифікації антифорензічних технік і можливих шляхів їхнього виявлення [8]. Результати цих досліджень доступні Україні (як члену CCDCOE з 2018 року), тому наші фахівці можуть використовувати ці напрацювання у навчанні та практиці. Корисною є і співпраця з правоохоронними структурами держав-партнерів поза НАТО. Так, з 2022 року Україна приєдналася до міжнародної ініціативи **@ON (Attribution of Origin Network)** під егідою Інтерполу, метою якої є обмін інформацією про методи приховування кіберзлочинців. Через цю мережу наші кіберполіція та СБУ можуть оперативно отримувати від колег з-за кордону дані про нові випадки анти-форензіки і координувати спільні розслідування.

Окрім держав і міжурядових організацій, важливу роль відіграють проекти за участі академічних та громадських структур, спрямовані на збереження автентичності цифрових доказів навіть за наявності протидії. Один з найцікавіших – ініціатива **Starling Lab** (США), що спеціалізується на застосуванні технології блокчейн для фіксації цифрових доказів. У 2022–2023 рр. Starling Lab у співпраці з Hala Systems допомогли українським органам оцифрувати та записати на блокчейн великий масив даних про воєнні злочини рф – фотографії з Telegram-каналів, відео руйнувань, свідчення очевидців. Кожен файл було захешовано (створено унікальний "цифровий відбиток") і внесено одночасно в кілька різних блокчейн-мереж, а самі файли зберігаються в розподіленому сховищі. В результаті, якщо такий доказ надається до суду або Міжнародного кримінального суду, захист не зможе його дискредитувати твердженнями про можливе редагування після збору – запис у блокчейні гарантує, що файл саме у такому вигляді існував на момент фіксації. Цей підхід уже використовується на практиці: другий пакет доказів про руйнування шкіл у Харкові, зібраний Starling Lab, було офіційно передано до Офісу Прокурора МКС на початку 2023 р., причому застосовувалася технологія *Content Authenticity Initiative* від Adobe для додавання метаданих достовірності прямо на етапі збору [9]. Таким чином, міжнародні партнери допомагають запроваджувати інноваційні методи "цифрового пломбування" доказів, що значно ускладнює роботу контрфорензіки.

Ще один напрям – розробка **спеціалізованих мобільних додатків** для збору фото- та відеодоказів, які одразу забезпечують їх автентичність. Відомим прикладом є застосунок *EyeWitness to Atrocities*, створений Міжнародною асоціацією адвокатів. Це камера-додаток для смартфона, яка одразу фіксує геолокацію, дату, час зйомки та обчислює цифровий підпис знятого фото/відео, після чого шифрує файл і надсилає на захищений сервер ІВА. Користувач не може редагувати записаний файл, йому присвоюється унікальний ідентифікатор. Таким чином, якщо правозахисник або військовий документує, скажімо, наслідки авіаудару через EyeWitness, цей файл потім у суді можна легко перевірити на автентичність: порівняти його оригінальний хеш і метадані, гарантовані розробниками програми. Схожі технології можуть використовувати й правоохоронці – спецзасоби для фотофіксації місць подій, інтегровані з системою захищеного збереження.

Попри зазначені ініціативи, міжнародні експерти наголошують, що зловмисники також не стоять на місці. Ті самі нейромережі, які викривають фейки, можуть бути використані для створення ще більш якісних фейків, що обходять наявні детектори. Це своєрідне змагання інтелекту: кожен новий алгоритм детекції стимулює появу методів обходу, і навпаки. Тому фахівці з інформаційної безпеки радять дотримуватися принципу "*довіряй, але перевіряй*" – покладатися на автоматичні системи детекції, але обов'язково проводити ручну верифікацію підозрілих випадків [10]. Жоден програмний детектор не дає 100% гарантії, тож критично важливо, щоб остаточне слово залишалося за людиною-експертом, яка проаналізує результати, зіставить їх з іншими даними і зробить висновок. Такий підхід досяг консенсусу на міжнародному рівні і має впроваджуватися в Україні.

У підсумку міжнародний досвід показує, що для успішної протидії контрфорензіці необхідне поєднання зусиль: оновлення законодавства, впровадження стандартів роботи з цифровими доказами, активна співпраця в міжнародних мережах (ENFSI, Interpol, НАТО тощо) та використання новітніх технологій (блокчейн, AI-детекція, спецдодатки). Україна вже робить кроки в усіх цих напрямах, але подальше розширення та інституціоналізація цих заходів дозволить значно підвищити ефективність протидії анти-форензіці.

Важливим елементом системи протидії контрфорензіці є технології та навички їх застосування. У цьому контексті відзначимо зростаючу роль штучного інтелекту. Розширення можливостей штучного інтелекту, машинного навчання та блокчейну створює нові виклики для цифрової криміналістики та контрфорензіки. Наприклад, знаний український вчений М. Гуцалюк у своїх статтях аналізує сучасні тенденції боротьби з кіберзлочинами та оцінює розвиток можливостей України щодо застосування інноваційних технологій для попередження та розслідування таких злочинів [11-12]. AI вже проникає у всі аспекти – від детекції діпфейків до аналізу логів. Подальший розвиток йде шляхом створення інтегрованих систем, що можуть автоматично опрацьовувати величезні масиви даних і знаходити "голки в копиці сіна". Наприклад, після деокупації у нас є терабайти відео- та фотоматеріалів з різних джерел. Перевірити їх вручну – непід'ємно. Але можна застосувати AI-фільтрацію: нейромережі проглянуть весь масив і відсіють явні "норми", відзначивши підозрілі матеріали (де, скажімо, знайдено ознаки монтажу або невідповідність метаданих). Тоді експертам лишиться детально перевірити лише відібране. Так, у 2024 році Управління підзвітності Уряду США (GAO) рекомендувала використовувати комбінацію методів автоматичної детекції та аутентифікації для досягнення найкращих результатів у виявленні глибоких фейків (deepfakes). У своєму звіті "Science & Tech Spotlight: Combating Deepfakes" GAO зазначає, що поєднання кількох методів може підвищити ефективність ідентифікації глибоких фейків [13]. Також AI використовується для аналізу множинних джерел доказів: платформи на кшталт Palantir Gotham дозволяють знайти кореляції між, приміром, геолокаційними даними фотографій, свідченнями очевидців та записами телефонних з'єднань, щоб встановити повну картину подій. Українські слідчі за підтримки ЄС теж впроваджують подібні системи для розслідування воєнних злочинів, де потрібно співставити інформацію з десятків баз даних.

Водночас залишається важливим людський контроль. **Жодна автоматична система не повинна діяти повністю автономно при ухваленні юридично значущих рішень**. AI – це інструмент, що пришвидшує та полегшує роботу, але не замінює експерта. Особливо це стосується сфери фейкових доказів: в історії є випадки, коли системи помилково маркували справжні відео як підробки (і навпаки). Тому остаточний

вердикт про справжність чи фальшивість повинен виносити кваліфікований спеціаліст, який врахує всі фактори і зможе обґрунтувати своє рішення в суді [14]. Цей принцип є міжнародним консенсусом і втілюється у практиках роботи, про що згадувалось вище.

Отже, сучасні технології надають значний арсенал засобів протидії контрфорензіці: від відновлення видаленого і ловлі стеганографії – до блокчейну і AI для забезпечення автентичності даних. Ключове – правильно комбінувати ці інструменти та навчати персонал ефективно ними користуватися. Україна, спираючись на допомогу партнерів, вже впроваджує багато чого з цього арсеналу, але важливо постійно оновлювати його новими напрацюваннями, адже і противник не зупиняється у розвитку своїх анти-форензічних можливостей.

Висновки. Проведене дослідження підтвердило, що контрфорензіка стала складовою складної архітектури сучасних загроз цифровій безпеці, зокрема у контексті повномасштабної збройної агресії проти України. Особливої гостроти ця проблема набуває в аспекті захисту критичної інфраструктури – об’єктів, безперебійна робота яких забезпечує стійкість функціонування енергетики, транспорту, оборони, медицини, зв’язку й цифрового управління державою. Військові дії супроводжуються не лише ракетними ударами, але й високоточними кібероперaціями, спрямованими на виведення з ладу або компрометацію ІТ-систем, що підтримують критичну інфраструктуру.

На основі теоретичного аналізу, вивчення міжнародного досвіду, оцінки технологічних викликів і розгляду практичних кейсів можна сформулювати такі **ключові висновки та рекомендації**:

- **Розробити єдині протоколи цифрової безпеки для об’єктів критичної інфраструктури з урахуванням протидії контрфорензіці.** Усі дії, пов’язані з фіксацією, зберіганням і аналізом цифрових даних, мають базуватися на стандартизованих процедурах, які унеможливлюють втрату чи фальсифікацію доказів навіть у разі атак з використанням засобів знищення слідів. Для систем критичної інфраструктури має бути обов’язковим впровадження механізмів резервного дублювання журналів подій на захищені зовнішні сховища з хешуванням і захистом цілісності даних.
- **Зміцнити технічні спроможності експертних установ, які супроводжують цифрову безпеку об’єктів критичної інфраструктури.** Слід забезпечити наявність ліцензованого програмного забезпечення для виявлення ознак анти-форензічної активності, засобів глибокого аналізу шкідливого коду, а також спеціалізованих інструментів аналізу резервних копій та пошуку ознак втручання навіть у разі спроб знищення доказів. Особливу увагу слід приділити засобам виявлення wiping-діяльності на системах енергетичних операторів, транспортної логістики та комунікацій.
- **Інституалізувати підготовку персоналу об’єктів критичної інфраструктури щодо ідентифікації і нейтралізації антифорензіки.** Адміністратори мереж, оператори систем моніторингу, співробітники служб інформаційної безпеки мають системно проходити навчання з новітніх методів контрфорензіки. Сценарії таких тренінгів повинні враховувати типові атаки на інфраструктурні об’єкти: спроби стерти логи, приховано перезаписати файли конфігурацій, застосування діпфейків для фальсифікації даних телеметрії тощо.
- **Запровадити інституційно узгоджені механізми обміну інформацією між об’єктами критичної інфраструктури, правоохоронними органами та кіберзахисними структурами.** Має бути створено захищену платформу швидкого обміну інформацією про виявлені факти антифорензічної діяльності, індикатори

компрометації та технічні методи реагування. Участь у цій системі повинні брати не лише державні установи, а й приватні оператори інфраструктурних систем.

- **Активізувати співпрацю з міжнародними організаціями у сфері кіберзахисту критичної інфраструктури.** Варто забезпечити участь українських установ у проєктах ЄС та НАТО, зокрема у ініціативах CCDCOE, ENISA, ENFSI, спрямованих на обмін досвідом виявлення високоризикованих форм контрфорензіки. Україна має ініціювати створення спеціального підрозділу технічної допомоги у рамках ENISA для держав, які зазнали атак на критичну інфраструктуру в умовах війни.
- **Розвивати державну політику публічно-приватного партнерства в галузі цифрової достовірності контенту.** Особливо це стосується стратегічних секторів – енергетики, охорони здоров'я, телекомунікацій. Варто залучити вітчизняні компанії та міжнародні технологічні корпорації до пілотних проєктів із використання інструментів перевірки цифрової автентичності (впровадження CAI, цифрових підписів на відеопотоки з об'єктів критичної інфраструктури тощо).
- **Удосконалити національне законодавство про захист цифрових даних, пов'язаних із критичною інфраструктурою.** Необхідно розробити спеціальний нормативний акт, який визначатиме категорії електронних доказів для об'єктів критичної інфраструктури, встановлюватиме вимоги до їх захисту, процедури вилучення, резервування та відповідальність за спроби приховати цифрові сліди втручання. Цей закон має мати пріоритетний статус в умовах воєнного стану.

Реалізація запропонованих заходів дозволить створити в Україні **функціональну архітектуру цифрової стійкості об'єктів критичної інфраструктури**, здатну протидіяти складним і технологічно просунутим формам контрфорензіки. Це не лише підвищить ефективність розслідування кібератак, а й зміцнить обороноздатність держави в умовах триваючої війни. Успішна протидія анти-форензічним технологіям має розглядатися як один із ключових напрямів стратегії національної кібербезпеки.

Список використаних джерел:

1. Emre Hosgor Detection and Mitigation of Anti-Forensics. Magnet forensics. 2022 URL: https://www.magnetforensics.com/resources/detection-and-mitigation-of-anti-forensics/#:~:text=With%20the%20advances%20in%20IT%2C,aims%20to%20provide%20categorization%20of

2. Berinato S. The Rise of Anti Forensics. Retrieved. CSO 08 Jun 2007 URL: https://www.csoonline.com/article/521254/investigations-forensics-the-rise-of-anti-forensics.html

3. The Grugq *Defeating Forensic Analysis on Unix*. 2002. Retrieved 2019-09-06. URL: https://phrack.org/issues/59/6#article

4. Proska K., Wolfram J., Wilson J. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. November 9, 2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

5. CERT-UA. *CERT-UA: Russian Hackers Hit 20 Ukrainian Critical Infrastructure Facilities in a Month*. CPO Magazine/ 2022. URL: https://www.cpomagazine.com/cyber-security/cert-ua-russian-hackers-hit-20-ukrainian-critical-infrastructure-facilities-in-a-month/

6. Industrial Cyber. *Ukrainian CERT details malicious plan by Sandworm group to disrupt critical infrastructure facilities*. 2024, April 13 URL: https://industrialcyber.co/critical-infrastructure/ukrainian-cert-details-malicious-plan-by-sandworm-group-to-disrupt-critical-infrastructure-facilities/

7. ENFSI URL: https://enfsi.eu/

8. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub URL: https://ccdcoe.org/

9. Restoring trust and transparency in the age of AI. Content Authenticity Initiative. URL: https://contentauthenticity.org

10. U.S. Government Accountability Office (GAO). *Science & Tech Spotlight: Combating Deepfakes.* GAO-24-107292, 11 березня 2024 URL: https://www.gao.gov/products/gao-24-107292

11. Гуцалюк М.В. Особливості протидії кіберзлочинності під час воєнного стану. Інформація і право. № 3. 2023. URL: http://il.ippi.org.ua/article/view/287212

12. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі "Даркнет". Інформація і право. № 3(26)/2018. С. 102-108

13. Science & Tech Spotlight:Combating Deepfakes. GAO. Mar 11, 2024 URL: https://www.gao.gov/products/gao-24-107292

14. Neill Jacobson The Impact of False Digital Evidence on the Justice System November. Open Fox. 19, 2024 URL: https://www.openfox.com/the-impact-of-false-digital-evidence-on-the-justice-system/#:~:text=False%20digital%20evidence%20encompasses%20any,erode%20trust%20in%20digital%20evidence

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~