УДК 343.98:004.056:355.02
DOI https://doi.org/10.24144/2307-3322.2025.89.2.61

COUNTER FORENSICS ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ: ПРОБЛЕМАТИКА СУДОВОЇ ЕКСПЕРТИЗИ ЦИФРОВИХ ДОКАЗІВ У РЕАЛІЯХ ВІЙНИ

Довгань О.Д.,
Заслужений діяч науки і техніки,
доктор юридичних наук, професор,
радник дирекції Державної наукової установи
«Інститут інформації, безпеки і права
Національної академії правових наук України».
ORCID: 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: 0000-0002-4620-3300

Тарасюк А.В.,
доктор юридичних наук, професор,
головний науковий співробітник
Державної наукової установи «Інститут інформації, безпеки і права
Національної академії правових наук України».
ORCID: 0000-0002-0479-0666

Довгань О.Д., Ткачук Т.Ю., Тарасюк А.В. Counter forensics як загроза інформаційній безпеці України: проблематика судової експертизи цифрових доказів у реаліях війни.

Вказується, нинішня військова агресія щодо України характеризується масштабними кібератаками та інформаційними операціями, які створюють серйозні ризики для державної інформаційної безпеки. Серед нових загроз особливе місце займає феномен *контрфорензіки* – комплекс технік, призначених для ускладнення або викривлення електронних доказів з метою уникнення покарання.

У статті досліджується феномен *counter forensics* як складова гібридної загрози інформаційній безпеці України в умовах повномасштабної війни. Автори статті здійснили комплексний аналіз понять, технологій і практик, спрямованих на ускладнення або спотворення цифрових доказів з метою перешкоджання кримінальному провадженню. Визначено основні види контрфорензічних впливів – від знищення слідів, фальсифікації метаданих, стеганографії до атак на інструменти судово-експертного аналізу. Особливу увагу приділено вразливості цифрових доказів під час війни та практиці їх використання у кримінальних провадженнях щодо воєнних і кіберзлочинів.

Проаналізовано окремі приклади із судової та слідчої практики, а також конкретні кіберінциденти російсько-української війни 2022–2024 рр., які свідчать про застосування методів *counter forensics* з боку агресора. Встановлено, що системне використання таких технік підриває довіру до електронних доказів, ускладнює встановлення істини та ставить під загрозу ефективність правосуддя. Водночас автор окреслює ключові проблеми судово-експертної діяльності в цифровій сфері – фрагментарність нормативного регулювання, нестачу кадрового та технічного потенціалу, відсутність єдиного центру компетенції з цифрової криміналістики.

На основі проведеного аналізу сформульовано рекомендації щодо вдосконалення нормативно-правового забезпечення, оновлення методик судової експертизи цифрових доказів, впрова-

дження міжнародних стандартів (ISO/IEC), підвищення кваліфікації експертів і створення національного центру цифрової криміналістики. Наголошується, що ефективна протидія *counter forensics* є необхідною умовою забезпечення інформаційної безпеки та справедливості в умовах сучасних воєнних конфліктів.

Ключові слова: інформаційна безпека, counter forensics, цифрові докази, судова експертиза, кіберзлочинність, воєнні злочини, фальсифікація доказів, кібероперації, криміналістика.

Dovhan O.D., Tkachuk T.Yu., Tarasiuk A.V. Counter forensics as a threat to the information security of Ukraine: the problem of forensic expertise of digital evidence in the realities of war.

It is indicated that the current military aggression against Ukraine is characterized by large-scale cyberattacks and information operations that create serious risks for state information security. Among the new threats, a special place is occupied by the phenomenon of counter-forensics - a set of techniques designed to complicate or distort electronic evidence in order to avoid punishment.

The article examines the phenomenon of counter forensics as a component of a hybrid threat to the information security of Ukraine in the conditions of a full-scale war. The authors of the article carried out a comprehensive analysis of concepts, technologies and practices aimed at complicating or distorting digital evidence in order to hinder criminal proceedings. The main types of counter forensic influences are identified - from the destruction of traces, falsification of metadata, steganography to attacks on forensic analysis tools. Particular attention is paid to the vulnerability of digital evidence during war and the practice of their use in criminal proceedings regarding war and cybercrimes.

Separate examples from judicial and investigative practice, as well as specific cyber incidents of the Russian-Ukrainian war of 2022–2024, are analyzed, which indicate the use of counter forensics methods by the aggressor. It is established that the systematic use of such techniques undermines trust in electronic evidence, complicates the establishment of the truth and jeopardizes the effectiveness of justice. At the same time, the author outlines the key problems of forensic activity in the digital sphere - fragmentation of regulatory regulation, lack of human and technical potential, lack of a single center of competence in digital forensics. Based on the analysis, recommendations are formulated to improve regulatory support, update methods for forensic examination of digital evidence, implement international standards (ISO/IEC), improve the skills of experts and create a national center for digital forensics. It is emphasized that effective counter-forensics is a necessary condition for ensuring information security and justice in the conditions of modern military conflicts.

Key words: information security, counter forensics, digital evidence, forensics, cybercrime, war crimes, evidence falsification, cyber operations, forensics.

Постановка проблеми. Сучасна воєнна агресія проти України супроводжується безпрецедентними кіберопераціями та інформаційними атаками, які ставлять під загрозу національну інформаційну безпеку. Одним із новітніх викликів є явище *counter forensics* (контрфорензіка) – сукупність методів, спрямованих на утруднення або спотворення цифрових доказів з метою уникнення відповідальності. Противник активно застосовує такі методи: зокрема, зафіксовано кібератаки російських хакерів на Офіс Генерального прокурора України та навіть на Міжнародний кримінальний суд з метою отримати або видалити доказові дані воєнних злочинів [1]. Подібні кібератаки, націлені на зміну або знищення інформації про злочини, підривають роботу трибуналів щодо воєнних злочинів. Отже, питання протидії *counter forensics* набуває особливої ваги для забезпечення справедливості й верховенства права під час війни.

Мета дослідження полягає у всебічному аналізі контрфорензічних загроз інформаційній безпеці України в умовах війни та обґрунтуванні шляхів удосконалення судово-експертної діяльності з цифровими доказами для їх нейтралізації. Для реалізації визначеної мети передбачається вирішення таких наукових завдань: визначити сутність і класифікацію counter forensics, проаналізувати його методи та інструменти; дослідити вразливість цифрових доказів до контрфорензічних впливів у контексті воєнного часу; оцінити вплив контрфорензіки на інформаційну безпеку України на прикладах кібероперацій російсько-української війни; обґрунтувати напрями вдосконалення судово-експертної практики щодо цифрових доказів з урахуванням новітніх загроз.

Методологічна основа дослідження. Робота спирається на міждисциплінарний підхід, що поєднує кілька методів. Порівняльно-правовий метод застосовано для аналізу зарубіжної та української нормативної бази і практики щодо цифрових доказів та кіберзлочинів. Системний підхід

дозволив розглядати counter forensics як елемент загальної системи інформаційної безпеки держави. Інформаційно-аналітичний метод використовувався при опрацюванні відкритих джерел, аналітичних звітів і наукових праць з цифрової криміналістики. Криміналістичний підхід забезпечив глибоке вивчення технічних аспектів збору, аналізу та фальсифікації цифрових слідів. Така методологічна комбінація дала змогу всебічно дослідити проблему – від теоретичних визначень до прикладних аспектів експертної діяльності.

Стан опрацювання проблематики. Сучасний стан досліджень демонструє активне опрацювання тематики *counter forensics* у зарубіжній літературі. Зокрема, Rhiannon Neilsen (2024) звертає увагу на цілеспрямовані кібератаки Росії з метою знищення чи фальсифікації цифрових доказів воєнних злочинів в Україні, що становить прецедент у міжнародному кримінальному праві. Класичну типологію антифорензічних впливів (приховування, знищення, спотворення слідів та атаки на засоби аналізу) ще у 2005 році запропонував Marcus Rogers. Комплексний технічний аналіз інструментів і методів антифорензіки подають Hussein Majed, Noura Hassan та Ali Chehab (2020), які також підкреслюють виклики для криміналістів у контексті швидкої еволюції загроз. Міжнародну увагу до кіберзлочинів як потенційних воєнних злочинів підтверджує розслідування МКС, описане в матеріалі Anthony Deutsch, Stephanie van den Berg та James Pearson (2024).

В Україні дослідження О.П. Метелева (2023) дає класифікацію цифрових доказів у кримінальному процесі, проте не охоплює аспектів контрфорензіки. С. Ханін (2024) акцентує на проблемах процесуального оформлення електронних доказів відповідно до ст. 290 КПК України. Разом із цим, Консультативна місія ЄС (2023) наголошує на зміцненні слідчих і експертних спроможностей України шляхом міжнародного співробітництва в галузі цифрової криміналістики. Незважаючи на окремі прогресивні публікації, українська наукова традиція поки що не сформувала цілісної доктрини протидії *counter forensics*, що підкреслює актуальність і новизну пропонованого дослідження.

Виклад основного матеріалу. Термін *counter forensics* (або «анти-криміналістика», «анти-форензика») виник на початку 2000-х років у середовищі фахівців з безпеки та хакерів. Його поява була зумовлена розвитком комп'ютерної криміналістики: з одного боку, правоохоронці все активніше залучали цифрові докази для розкриття злочинів, з іншого – злочинці шукали способи уникнути викриття, знищуючи або приховуючи електронні сліди. Перші детальні описи методів анти-форензики з'явилися в неформальних публікаціях (наприклад, у згаданому журналі *Phrack* у 2002 р.), а згодом поняття увійшло й у науковий обіг. Американський дослідник Маркус Роджерс запропонував одну з перших таксономій *counter forensics*, визначивши чотири ключові категорії методів: приховування даних, знищення артефактів, заплутування слідів і атаки на процеси та інструменти комп'ютерної криміналістики [2]. Таким чином, уже на етапі становлення явища була усвідомлена його багатогранність – від простих дій із файлів до складних атак на самі судово-експертні засоби.

Генеза контрфорензіки пов'язана передусім з кіберзлочинністю та діяльністю хакерських груп. У 2000–2010-х роках з розвитком інструментів цифрової криміналістики (утиліт для відновлення видалених файлів, аналізу пам'яті тощо) зловмисники стали цілеспрямовано впроваджувати контрзаходи. Спочатку ці заходи були переважно оборонними – щоб уникнути викриття після злому системи чи проведення кіберзлочину, зловмисник видаляв логи, шифрував компрометуючі файли. З часом контрфорензіка набуває все більш наступального характеру: її методи інтегруються у шкідливе програмне забезпечення, стають складовою державних кібероперацій (наприклад, для приховування слідів шпигунства або диверсій). Сьогодні *counter forensics* – це окрема сфера протиборства в кіберпросторі, де постійно змагаються «міра та протиміра»: розробники судово-експертних інструментів вдосконалюють засоби виявлення прихованих слідів, а противна сторона шукає нові шпарини та вразливості, щоб ці сліди приховати або спотворити [3]. Як зауважують дослідники, методи анти-форензики стають все складнішими, і водночас кількість наукових робіт про них залишається обмеженою, що ускладнює підготовку фахівців. Це підтверджує актуальність дослідження *counter forensics* як окремого феномена.

Окрім суто злочинного застосування, в літературі звертають увагу й на *«подвійне призначення»* деяких анти-форензічних інструментів. Деякі з них можуть використовуватися легально, наприклад, для захисту приватності (шифрування даних задля убезпечення від несанкціонованого доступу) або для тестування надійності систем (демонстрація вразливостей цифрової криміналістики через створення умов, коли доказ неможливо знайти чи підтвердити). Проте у

контексті інформаційної безпеки держави контрфорензіка розглядається передусім як **загроза** – адже її функціонал (нищити, приховувати, фальсифікувати) безпосередньо підриває можливості правоохоронних органів встановити істину та притягнути винних до відповідальності. Особливо небезпечним є використання контрфорензіки у війні, де вона стає інструментом інформаційно-психологічних операцій: наприклад, видалення доказів воєнних злочинів ворогом або підміна їх фальшивками прямо впливає на післявоєнне правосуддя і сприйняття правди про війну. Таким чином, функціональне призначення *counter forensics* можна сформулювати як зворотній бік цифрової криміналістики: якщо остання служить встановленню об'єктивної істини на основі цифрових слідів, то контрфорензіка – це діяльність, що намагається цю істину сховати або спотворити.

Цифрові (електронні) докази наразі відіграють ключову роль у фіксації воєнних злочинів, терористичних актів, кіберзлочинів та інших правопорушень, пов'язаних з військовою агресією. Вони мають низку специфічних рис, які одночасно є їхньою силою і слабкістю. З одного боку, цифрові докази можуть у великому обсязі збиратися навіть у розпал бойових дій – за рахунок камер спостереження, безпілотників, смартфонів очевидців, даних з мережевих систем тощо. Приміром, фото- і відеоматеріали з місць обстрілів чи перехоплені електронні комунікації окупантів стали важливими доказами злочинів проти цивільних. З іншого боку, **нематеріальна природа** цифрових даних робить їх надзвичайно крихкими в юридичному сенсі. На відміну від речових доказів, які існують фізично, електронна інформація легко копіюється, змінюється або знищується без видимих слідів втручання. Законодавче регулювання цієї сфери в Україні поки відстає від практики: як відзначають дослідники, питання використання цифрової інформації як доказу залишається недостатньо дослідженим і врегульованим, а місце цифрових доказів у системі процесуальних джерел доказів чітко не визначено [4]. КПК України [5] фактично не оперує поняттям «цифровий доказ» – електронні матеріали процесуально оформлюються переважно як додатки до протоколів або як документи (ст. 99 КПК), що не повною мірою враховує їх специфіку. Під час дії воєнного стану та активних бойових дій виникають додаткові складнощі: обмежений доступ експертів до місць подій, нерегулярність роботи інфраструктури, ризик знищення носіїв інформації. Тому **вразливість цифрових доказів** у воєнний час ще зростає – агресор може цілеспрямовано знищувати сервери з доказовою інформацією, глушити канали зв'язку, проводити хакерські атаки на реєстри і бази даних правоохоронних органів.

Коли до рук експерта потрапляє змінений чи пошкоджений цифровий носій, перед ним постає двоєдине завдання: по-перше, максимально відновити вихідні дані, по-друге – з'ясувати, що саме було змінено і яким чином. Обидва аспекти обмежені рядом чинників. Технічні обмеження пов'язані з незворотністю деяких операцій: якщо дані було перезаписано (наприклад, стерто утилітою безповоротного видалення), то відновити їх неможливо жодними інструментами – експерт може лише констатувати сам факт стирання. Якщо доказ був зашифрований сучасним алгоритмом (AES-256 тощо) і ключ відсутній, то фактично неможливо розкрити шифр в прийнятний часовий проміжок. Навіть у випадку підробки метаданих є проблема: іноді неможливо достеменно визначити початкове значення – можна тільки підтвердити, що **метадані виглядають підозріло і могли бути змінені штучно**. Відтак, експертний висновок у такій ситуації носить імовірнісний характер («не можна виключити втручання», «виявлено ознаки модифікації»), що юридично слабше, ніж чітка констатація факту.

Правові обмеження виникають при оцінці модифікованих даних у суді. За принципом презумпції невинуватості будь-який сумнів щодо цілісності доказу трактуватиметься на користь підозрюваного. Якщо захист доведе, що слідство не забезпечило належного збереження електронного доказу або не може підтвердити його автентичність, суд найімовірніше визнає такий доказ недопустимим. Наприклад, відповідно до вимог ст. 290 КПК України, сторона обвинувачення зобов'язана відкрити стороні захисту матеріали, у тому числі електронні носії інформації, для ознайомлення; якщо цього не зроблено належним чином, суд не має права брати відповідні відомості до уваги [6]. Отже, якщо під час відкриття стороною обвинувачення електронні докази були надані не в оригіналі або з технічними проблемами (пошкоджені файли, змінені хеш-значення), захист обов'язково поставить питання про їх допустимість. Крім того, закон не зобов'язує обвинуваченого сприяти розшифруванню своїх даних (відмова надати пароль не вважається окремим злочином в Україні, на відміну від деяких країн). Таким чином, правове поле поки що більше захищає потенційного маніпулятора, ніж дає інструменти слідству – і це потребує змін, про що скажемо далі.

Загалом, цифрові докази, модифіковані через дії контрфорензіки, становлять *складний об'єкт експертизи*: часто експерт змушений не тільки аналізувати зміст даних, а й виконувати роль «дослідника другої черги» – спершу відновлюючи, перевіряючи сам доказ, а вже потім роблячи висновки щодо його значення для справи. Це вимагає від нього високої кваліфікації, доступу до сучасних інструментів та, часом, творчого підходу.

Ціллю контрфорензіки на стратегічному рівні часто є навіть не знищення конкретної інформації, а саме підрив довіри до **всієї системи електронних доказів**. Російська інформаційна війна активно експлуатує будь-які приводи поставити під сумнів докази злочинів РФ. Якщо хакерам вдається бодай проникнути в систему, що зберігає докази, це вже створює інформаційний привід заявити: «усі матеріали скомпрометовано, нічому вірити не можна». Як слушно зауважують експерти, навіть *сама лише новина про те, що базу даних з доказами зломували, хай навіть без доказів знищення даних, підриває довіру до цієї бази* [1]. Суспільству і міжнародним партнерам починає здаватися, що матеріали могли бути змінені, отже будь-який вирок на їх основі можуть поставити під сумнів. Це – класична тактика російської дезінформації: сіяти сумніви і розбрат **навіть без прямого наведення доказів фальсифікації**, достатньо заявити про «можливість підробки». Таким чином, контрфорензіка працює у симбіозі з інформаційно-психологічними операціями: там, де технічне втручання не може знищити правду, її намагаються задушити сумнівами. Втрата довіри до електронних доказів надзвичайно небезпечна для правової системи: адже сучасні війни значною мірою документуються саме цифровими засобами, і якщо їхня легітимність нівелюється, злочинці отримують шанс уникнути кари або принаймні затягнути правосуддя. Вже зараз експерти відзначають, що кібератаки на докази можуть **значно затягнути судові процеси** (адже доведеться додатково все перевіряти, проводити експертизи достовірності) і тим самим відтермінувати справедливість для жертв [1].

Протистояння контрфорензіці вимагає не лише реагування на окремі випадки, але й **системного удосконалення всієї інфраструктури судово-експертної діяльності** у сфері цифрових доказів. Поточна війна оголила цілий спектр проблем – інституційних, правових, технічних – які заважають ефективно долати контрфорензічні загрози. Водночас виникла й безпрецедентна мотивація для розвитку: потреба розслідувати тисячі воєнних і кіберзлочинів змушує шукати нові рішення, впроваджувати кращі світові практики, розбудовувати кадровий потенціал.

В Україні судово-експертну діяльність у цифровій сфері здійснюють різні суб'єкти – від відомчих експертних установ (Експертна служба МВС, науково-дослідні установи судових експертиз Мін'юсту, експертні підрозділи СБУ тощо) до приватних структур, що можуть залучатися у ролі спеціалістів. Така фрагментація призводить до розпорошення ресурсів і нерівномірності професійного рівня. На сьогодні немає єдиного центру координації або методичного забезпечення цифрової криміналістики. Кожне відомство фактично саме розробляє методики і навчає кадри у межах своєї компетенції. В умовах інформаційної війни це недолік: атаки контрфорензіки можуть цілити одразу по кількох фронтах (наприклад, з одного боку ускладнювати розслідування кіберполіції, з іншого – знищувати докази, які збирає військова розвідка). Потрібен **єдиний підхід і обмін інформацією** між всіма структурами, що працюють з цифровими доказами. Наразі кроком у цьому напрямі є міжвідомчі навчання та спільні проекти: так, у червні 2023 р. за підтримки ЄС відбувся інтенсивний тренінг з цифрової криміналістики у Відні, де брали участь представники Національної поліції, СБУ та ДБР [7] – тобто різних відомств, що отримали змогу спільно підвищити кваліфікацію. Це позитивний приклад міжвідомчої взаємодії. Однак інституційно потрібно рухатися далі: *необхідне створення центрального координаційного органу або центру компетенції з цифрової криміналістики*. Його функції могли б включати розробку єдиних стандартів, атестацію методик, формування спільних баз даних (наприклад, відомостей про відомі інструменти контрфорензіки, щоб експерти швидше їх впізнавали), організацію регулярних навчань. Своєрідним прототипом є Національний координаційний центр кібербезпеки при РНБО – однак його мандат ширший (координація кіберзахисту), а ось спеціалізованого саме на *digital forensics* центру поки немає.

На законодавчому рівні вже назріла потреба чіткішого регулювання роботи з цифровими доказами. Передусім, доцільно внести зміни до КПК України, закріпивши *цифрові (електронні) докази* як окрему категорію доказів із визначенням їх процесуального режиму. Як показують наукові дослідження, існуюча концепція класифікації видів доказів потребує доповнення з урахуванням особливої природи цифрових доказів. Пропонується законодавчо визнати, що електронна інфор-

мація в цифровій формі (файли, електронні носії) – це самостійний вид доказів, не тотожний ані речовим доказам, ані документам. Це дало б змогу сформувати спеціальні правила поводження: наприклад, вимоги щодо фіксації й копіювання цифрових даних (обов'язковість створення копії-дубліката при вилученні носія, зняття хеш-суми тощо), правила щодо допустимості роздруківок і скриншотів (щоб уникнути маніпуляцій), процедурі засвідчення автентичності (через залучення експерта чи спеціального сертифікованого ПЗ). Також варто розглянути зміни до законодавства про експертну діяльність: наразі не існує окремої експертної спеціальності саме з дослідження контрфорензіки, проте, можливо, варто запровадити підвиди експертиз чи методик, спрямованих конкретно на виявлення фактів приховування/фальсифікації цифрових слідів.

Окремий блок – **міжнародно-правові аспекти**. Україна є учасником Будапештської конвенції про кіберзлочинність (2001 р.), яка серед іншого встановлює обов'язки зі збереження комп'ютерних даних та міжнародної правової допомоги у їх отриманні. Проте міжнародні механізми варто розвивати далі: зокрема, ініціювати визнання *знищення цифрових доказів воєнних злочинів* – окремим злочином (перешкоджання правосуддю на міжнародному рівні). Наразі МКС уперше розглядає кібератаки як можливі воєнні злочини, і це знаковий прецедент [8]. Україна має сприяти формуванню практики, де умисне перешкоджання розслідуванню (в тому числі через хакерські засоби) тягне серйозні наслідки. На національному рівні теж доцільно розглянути криміналізацію певних контрфорензічних дій – наприклад, внести до Кримінального кодексу норму про відповідальність за знищення речових доказів у цифровій формі або за відмову надати ключ до зашифрованих даних за рішенням суду (питання дискусійне з точки зору прав людини, але у воєнний час може бути актуальним для випадків, коли за шифруванням приховано інформацію про теракти тощо).

Висновки. Проведене дослідження підтвердило, що *counter forensics* становить реальну та багатовимірну загрозу інформаційній безпеці України, особливо в умовах розв'язаної проти неї війни. **По-перше**, контрфорензіка як явище еволюціонувала від поодиноких хакерських прийомів до інструменту державних кібероперацій: ворог системно застосовує техніки знищення та приховування цифрових слідів, прагнучи уникнути викриття своїх злочинів і підірвати можливість притягнення до відповідальності винних. **По-друге**, цифрові докази, які стали невід'ємною частиною сучасного кримінального провадження, виявилися вразливими до таких впливів – їхня нематеріальність і залежність від технічних умов відкривають широкий простір для маніпуляцій. Війна лише загострила ці проблеми: масовість воєнних злочинів і кібернападів породила величезний масив електронних доказів, захист цілісності та достовірності яких перетворився на першочергове завдання держави.

Для вдосконалення судово-експертного забезпечення у сфері цифрових доказів в умовах інформаційної війни доцільно здійснити такі кроки:

Законодавчі зміни: внести до КПК України окреме визначення електронних (цифрових) доказів та процедурні гарантії їх цілісності (обов'язкова фіксація хеш-значень, порядок вилучення копій, аутентифікація електронних документів тощо). Розглянути криміналізацію умисного знищення або підробки електронних доказів як перешкоджання правосуддю. Ратифікувати (після розробки) міжнародні угоди, що посилюють співпрацю в сфері отримання та захисту електронних доказів (напр. Другий протокол до Будапештської конвенції про посилення співробітництва, 2022 р.).

Інституційний розвиток: створити національний центр або координаційний орган цифрової криміналістики, який об'єднає зусилля різних відомств, буде відповідальний за напрацювання стандартів та взаємодію з міжнародними партнерами. Забезпечити регулярну міжвідомчу комунікацію – наприклад, через спільні робочі групи СБУ, МВС, прокуратури, ЗСУ – для обговорення нових викликів контрфорензіки та узгодження протидії. Активніше залучати приватний сектор і волонтерів з кіберспільноти: досвід кібервійськ (IT-армії) може бути корисним і в експертизі.

Методичне оновлення і стандартизація: імплементувати міжнародні стандарти (ISO/IEC 27037, 27041, 27042, 27043 тощо) у практику українських експертів; переглянути існуючі методики судових експертиз з урахуванням сучасних загроз (передбачити окремі розділи про ознаки втручання, про роботу з зашифрованими даними, алгоритми дій при виявленні слідів анти-форензики). Розробити методичні рекомендації щодо аналізу специфічних випадків: виявлення deepfake, аналіз даних з хмарних сервісів, оцінка цілісності логів і метаданих. Регламентувати процедури міжнародного обміну зразками та контролю якості: наприклад, запровадити практику

peer-review (рецензування) важливих експертиз іншими експертами чи установами, можливо – за кордоном, щоб упевнитись, що жоден аспект не пропущено.

Технічне забезпечення: здійснити аудит матеріально-технічних потреб експертних установ та закласти фінансування (в тому числі за рахунок допомоги партнерів) на придбання сучасних програмних комплексів для цифрової криміналістики і аналізу шкідливого ПЗ. Створити резервні сховища для ключових доказових даних, можливо – територіально віддалені (на випадок загроз фізичного знищення серверів). Впровадити системи моніторингу спроб несанкціонованого доступу або зміни даних у критичних базах (такий собі IDS/IPS для доказових сховищ). Паралельно – розробляти власні утиліти, скрипти для специфічних задач (скажімо, сканування файлової системи на предмет аномалій, порівняння зображень на наявність ознак монтажу тощо).

Кадри і тренінги: запровадити спеціалізовані навчальні модулі з контрфорензіки для діючих експертів та слідчих (наприклад, короткострокові курси чи семінари про сучасні методи приховування слідів). Заохочувати міжнародні стажування – відправляти українських експертів на навчання в Європол, FBI Academy, NATO Cooperative Cyber Defence Centre of Excellence тощо, де є нагода перейняти передові навички. Розширити підготовку в університетах: підтримати освітні програми з кібербезпеки і цифрової криміналістики, залучати практиків до викладання, пропонувати студентам реальні кейси для аналізу як курсові/дипломні роботи (наприклад, аналіз дампу пам'яті з підозрою на анти-VM техніки – це і навчання, і потенційна користь практиці). Внутрішньо в установах – практикувати настольні навчання і розбір польотів: після кожного інциденту проводити зустріч, де експерти та слідчі розбирають, що було зроблено добре, а що можна покращити у протидії анти-форензиці.

Міжнародна співпраця: продовжити активну співпрацю з Міжнародним кримінальним судом і іншими інституціями щодо обміну даними про кібернапади на докази. Запросити іноземних експертів долучатися до розслідування складних випадків (в рамках спільних слідчих груп чи як консультантів) – це додасть довіри результатам і дозволить перейняти досвід. Ініціювати створення міжнародної платформи з обміну інформацією про контрфорензіку (можливо, під егідою ООН чи Ради Європи), де країни, що стикаються з агресією та кіберзлочинністю, могли б ділитися методами виявлення й протидії.

Запропоновані кроки спрямовані на те, щоб українська система правосуддя була стійкою перед викликами інформаційної війни. Адже кінцева мета агресора – не просто зламати комп'ютери, а *зламати віру у здатність права перемогти зло*. Наше ж завдання – не допустити цього, озброївши правосуддя найсучаснішими знаннями і технологіями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Rhiannon Neilsen File Not Found: Russia Is Hacking Evidence of Its War Crimes. War on the Rocks Media. May 14, 2024. URL: https://warontherocks.com/2024/05/file-not-found-russia-is-hacking-evidence-of-its-war-crimes.
2. Rogers, D.M. Anti-Forensic Presentation given to Lockheed Martin. 2005San Diego. URL: https://www.researchgate.net/profile/Marcus-Rogers-2/publication/268290676_Anti-Forensics_Anti-Forensics/links/575969a908aec91374a3656c/Anti-Forensics-Anti-Forensics.pdf.
3. Hussein Majed, Hassan N. Noura, Ali Chehab Overview of Digital Forensics and Anti-Forensics Techniques. The 8th International Symposium on Digital Forensics and Security. May 2020. URL: https://www.researchgate.net/publication/341552920_Overview_of_Digital_Forensics_and_Anti-Forensics_Techniques#:~:text=,8%2C195%2C201%2C202%5D.
4. Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. № 1-2. 2023. URL: https://vkslaw.com.ua/index.php/journal/article/view/34.
5. Кримінально-процесуальний кодекс України № 4651. У редакції від від 09.05.2025. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
6. Ханін С. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета.* 26 червня 2024. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi-dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html.
7. Навчання цифровій криміналістиці зміцнює українські слідчі спроможності. Червень 02, 2023. Консультативна місія Європейського Союзу (КМЄС) в Україні. URL: https://

www.euam-ukraine.eu/ua/news/digital-forensics-training-strengthens-ukrainian-investigative-capabilities.

8. Anthony Deutsch, Stephanie van den Berg, James Pearson ICC probes cyberattacks in Ukraine as possible war crimes, sources say. Reuters. June 14, 2024 URL: https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14.