МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ТА ЕЛЕКТРОННИХ ДОКАЗІВ У РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

ПАЗЮК Андрій Валерійович - доктор юридичних наук, професор кафедри міжнародного та європейського права факультету міжнародних відносин Національного авіаційного університету

ORCID ID: https://orcid.org/0000-0002-1622-1671

ГЛИНСЬКА Наталія Валеріївна - доктор юридичних наук, професор кафедри міжнародного та європейського права факультету міжнародних відносин Національного авіаційного університету

ORCID ID: https://orcid.org/0000-0001-5835-3798

DOI: https://doi.org/10.32782/ep.2024.3.49

У статті досліджуються питання міжнародно-правового регулювання використання відкритих джерел інформації (OSINT) та електронних доказів у розслідуванні воєнних злочинів, з особливим акцентом на український контекст. В умовах російської агресії проти України, розслідування воєнних злочинів стикається з новими викликами, включаючи складність збору доказів у зонах конфлікту та обмежену співпрацю з агресором. Відкриті джерела, такі як соціальні мережі, медіа та інші публічно доступні платформи, стали важливим інструментом для документування злочинів. Суттєвий розвиток використання електронних доказів відбувається в Європейському Союзі. Електронні докази, отримані через OSINT та сучасні цифрові технології, дедалі частіше визнаються у міжнародних судах, таких як Міжнародний кримінальний суд та Європейський суд з прав людини. Стаття аналізує основні виклики, пов'язані з автентифікацією та прийнятністю електронних доказів у судових процесах, та пропонує рекомендації для вдосконалення правових і технічних процедур їх збору і використання в розслідуванні воєнних злочинів. Особлива увага приділяється європейському досвіду щодо збору, збереження та обробки електронних доказів, а також шляхам удосконалення національного законодавства для досягнення відповідності міжнародним стандартам.

Ключові слова: OSINT, електронні докази, воєнні злочини, міжнародне право, кіберзлочин, Міжнародний кримінальний суд, Будапештська конвенція.

Постановка проблеми

З розвитком технологій та зростанням ролі кіберпростору у сучасних конфліктах питання ефективного використання електронних доказів та відкритих джерел інформації (OSINT) у розслідуванні воєнних злочинів набуває особливої актуальності. Традиційні методи збору доказів часто стають неефективними в умовах, коли агресор не співпрацює, а доступ до місць злочину є обмеженим. У випадку України, яка потерпає від збройної агресії з боку Росії, ці виклики є особливо гострими, зважаючи на масові воєнні злочини, порушення прав людини та систематичні кібератаки на критичну інфраструктуру.

Проблема полягає в тому, що, незважаючи на те, що OSINT та електронні докази можуть стати ключовими джерелами для документування та розслідування таких злочинів, існують значні правові та технічні перепони щодо їх прийнятності у судовому процесі. Зокрема, чинне законодавство

України, попри зміни, які впроваджуються в умовах війни, все ще не забезпечує чіткого регулювання процедур збору, обробки та подання електронних доказів. Відсутність системних стандартів, процедур і внутрішніх інструкцій, а також проблеми з автентифікацією та захистом таких доказів від втрати чи маніпуляцій є серйозною перешкодою для їх ефективного використання у розслідуванні воєнних злочинів.

Більш того, міжнародні інституції, такі як Міжнародний кримінальний суд, ще не мають усталених механізмів визнання кібератак як воєнних злочинів, що додатково ускладнює процес притягнення винних до відповідальності. Таким чином, існує потреба в розробці правових та технічних стандартів, що дозволять більш ефективно використовувати OSINT та електронні докази як на національному, так і на міжнародному рівні.

Аналіз останніх досліджень і публікацій

Останні дослідження, присвячені використанню відкритих джерел (OSINT) та електронних доказів у розслідуванні воєнних злочинів, демонструють зростаючу увагу до ролі цифрових технологій у забезпеченні справедливості під час збройних конфліктів. Міжнародні організації, зокрема Рада Європи, ООН та Міжнародний кримінальний суд (МКС), все більше акцентують на необхідності застосування електронних доказів у судових процесах щодо воєнних злочинів та злочинів проти людяності.

Однією з ключових робіт у цій галузі є настанова Ради Європи щодо електронних доказів, яке надає практичні рекомендації для слідчих і суддів щодо збору, збереження та оцінки електронних доказів [1]. У цьому керівництві значна увага приділяється питанням автентичності й допустимості даних, отриманих з відкритих джерел, що є важливим для країн, які перебувають у стані конфлікту, таких як Україна. Дослідження також підкреслюють важливість прийняття міжнародних стандартів, таких як Будапештська конвенція про кіберзлочинність та Другий додатковий протокол щодо електронних доказів, які закладають основу для правового регулювання обміну електронними доказами на міжнародному рівні [2].

Серед останніх публікацій виділяються дослідження МКС та його практика прийняття електронних доказів у судових процесах [3]. У справі «Україна та Нідерланди проти росії» у Європейському суді з прав людини, було використано значну кількість електронних доказів, отриманих через OSINT та неурядові організації [4]. Цей випадок створив прецедент для прийняття таких доказів у майбутніх розслідуваннях.

Дослідження, проведені в рамках проєкту CyberEast під егідою Ради Європи, вказують на важливість впровадження технологій для моніторингу кіберзлочинів і кібератак, які можуть бути кваліфіковані як воєнні злочини [5]. У цих дослідженнях аналізуються правові механізми, які можуть бути застосовані до кіберзлочинів під час збройних конфліктів, зокрема у контексті російської агресії проти України.

Дослідження у сфері OSINT також фокусуються на питаннях етичних стандартів, автентифікації інформації та збереженні ланцюга доказів, що особливо важливо в умовах війни, коли доступ до територій і джерел інформації може бути обмежений. Наприклад, Берклійський протокол з цифрових розслідувань відкритих джерел визначає стандарти роботи з OSINT, акцентуючи увагу на важливості дотримання принципів прозорості та точності у процесі збору доказів [6].

Таким чином, сучасні дослідження та публікації показують, що питання використання відкритих джерел та електронних доказів у розслідуванні воєнних злочинів перебуває на передовій правових досліджень. Однак, в умовах постійних змін у цифровому середовищі, міжнародна спільнота й далі шукає шляхи вдосконалення правових механізмів для забезпечення справедливості у воєнних конфліктах, таких як агресія проти України.

Мета і завдання дослідження

Метою дослідження є аналіз правових, технічних та процедурних аспектів використання відкритих джерел (OSINT) і електронних доказів у розслідуванні воєнних злочинів, а також розробка рекомендацій

для вдосконалення їх застосування в Україні та на міжнародному рівні. Завдання включають вивчення міжнародних правових рамок, аналіз української законодавчої бази, дослідження судових прецедентів та викликів у зборі й поданні електронних доказів, а також оцінку ролі новітніх технологій у цьому процесі.

Виклад основного матеріалу

Використання відкритих джерел (OSINT) та електронних доказів є важливим інструментом у розслідуванні воєнних злочинів у сучасних конфліктах, де традиційні методи збору доказів стають неефективними або недоступними. Україна, яка зазнає масованих воєнних злочинів та кібернападів внаслідок збройної агресії російської федерації, стикається з необхідністю адаптації законодавства та розробки нових правових та технічних механізмів для забезпечення належного документування та використання таких доказів у національних і міжнародних судових процесах.

1. Правові виклики використання електронних доказів

Одним із ключових викликів, з якими стикається Україна, є відсутність чіткого законодавчого визначення електронних доказів як окремого джерела доказів у Кримінальному процесуальному кодексі (КПК) України. На даний момент електронні дані класифікуються як документи, що створює плутанину та ускладнює їх прийняття в суді. Попри зміни до КПК у 2022 році, які розширили поняття «документу», включивши до нього комп'ютерні дані, все ще відсутня системна процедура збору, документування та збереження таких доказів, що відповідає вимогам судового процесу. Наприклад, стаття 236 КПК дозволяє проведення «розширеного обшуку», але тільки в межах території України, що створює обмеження для доступу до даних, які зберігаються в хмарних сервісах за кордоном.

Міжнародні правові стандарти, такі як Будапештська конвенція про кіберзлочинність, є важливим інструментом для забезпечення процедурного збереження електронних доказів. Зокрема, статті 16 та 17 цієї конвенції передбачають прискорене збереження комп'ютерних даних та часткове розкриття даних про трафік, що є особливо важливим у розслідуваннях воєнних злочинів та кіберзлочинів. Однак національні законодавства повинні забезпечити імплементацію цих міжнародних положень для ефективної роботи з електронними доказами, і наразі в Україні необхідно внести відповідні зміни.

2. Використання OSINT у розслідуванні воєнних злочинів

З початком агресії Росії проти України OSINT став одним із ключових інструментів для документування воєнних злочинів. Відкриті джерела, такі як соціальні медіа, блоги, супутникові зображення та журналістські розслідування, активно використовуються для збору доказів щодо воєнних злочинів та порушень прав людини. Наприклад, громадянське суспільство України активно бере участь у зборі даних про воєнні злочини, співпрацюючи з правоохоронними органами та міжнародними організаціями. Це дозволяє документувати злочини навіть у тих випадках, коли доступ до місця злочину є обмеженим через окупацію чи бойові дії.

Рішення Європейського суду з прав людини (ЄСПЛ) у справі «Україна та Нідерланди проти Росії» стало знаковим щодо прийняття OSINT як допустимого джерела доказів. ЄСПЛ визнав звіти неурядових організацій, журналістські розслідування та інші джерела відкритих даних важливими елементами доказової бази, за умови, що вони пройшли відповідну перевірку на автентичність та достовірність. Це створює прецедент для використання OSINT у подальших судових процесах, зокрема у Міжнародному кримінальному суді.

3. Кібератаки як воєнні злочини

Однією з особливостей сучасної війни є зростаюча роль кібератак як елемента гібридної агресії. Російська Федерація здійснює масовані кібернапади на критичну інфраструктуру України, зокрема енергетичні об'єкти, транспорт, комунікації та банківську систему. Наприклад, кібератаки на енергетичну систему України в поєднанні з ракетними ударами мали на меті позбавити населення тепла, електрики та води під час зимових місяців, що кваліфікується як во-

єнний злочин відповідно до міжнародного права.

Однак на сьогоднішній день відсутні чіткі міжнародні правові механізми, що однозначно класифікують кібератаки як воєнні злочини. У березні 2023 року Прокурор МКС Карім Хан оголосив, що його офіс розслідуватиме можливі кібератаки як воєнні злочини або злочини агресії, що може стати важливим кроком для розширення правової бази у цій сфері [7]. Кібератаки можуть бути розглянуті МКС у випадках, коли їх наслідки відповідають критеріям серйозності, встановленим Статутом Риму, що вимагає значного рівня шкоди, завданої цивільному населенню або критичній інфраструктурі.

4. Технічні інструменти та технологічні виклики

Технології відіграють ключову роль у зборі та аналізі електронних доказів та OSINT. Сучасні інструменти для аналізу великих даних та штучний інтелект можуть бути використані для ідентифікації злочинців та обробки великих обсягів цифрової інформації, таких як відео- та аудіозаписи, соціальні медіа та інші джерела даних. Наприклад, технології розпізнавання голосу використовуються для ідентифікації осіб, які здійснювали заклики до геноциду або агресії.

Такі технології, як *Palantir* та інструменти *Microsoft*, вже застосовуються в Україні для аналізу великих масивів даних та забезпечення збереження доказів. Використання цих технологій є критичним для забезпечення ланцюга збереження доказів та їх подальшої обробки у судових процесах. Водночас існує потреба у розробці національних стандартів та інструкцій, що регулюють використання таких технологій і гарантують їхнє відповідність міжнародним правовим вимогам.

5. Участь України в Другому додатковому протоколі до Будапештської конвенції.

З моменту ухвалення Другого додаткового протоколу до Будапештської конвенції у травні 2022 року міжнародна спільнота зробила важливий крок до вдосконалення механізмів боротьби з кіберзлочинністю та забезпечення швидкого доступу до електронних доказів [8]. Цей документ, як розширення основних положень Конвенції про кіберзлочинність, значно посилює правові інструменти для обміну інформацією між країнами, спрощує процедури отримання цифрових даних та захищає права осіб під час передачі й обробки таких даних. Для України цей протокол відкриває нові можливості у сфері боротьби з кіберзлочинністю та розслідуванні воєнних злочинів, зокрема тих, що пов'язані з агресією російської федерації.

З огляду на сучасні глобальні виклики, що постали перед Україною в умовах війни, країна потребує інструментів, які можуть швидко та ефективно забезпечити доступ до електронних доказів, необхідних для розслідувань воєнних злочинів і кібернападів. Другий додатковий протокол вирішує цю проблему, надаючи нові механізми для міжнародної взаємодії та прямого доступу до інформації, що зберігається на серверах іноземних провайдерів послуг.

Одним із ключових положень протоколу є можливість для правоохоронних органів однієї країни безпосередньо запитувати електронні докази у постачальників послуг іншої держави, оминаючи тривалі бюрократичні процеси, пов'язані з традиційними запитами через взаємну правову допомогу. Це суттєво прискорює процес отримання даних, що є критично важливим у контексті воєнних злочинів, де швидкість доступу до інформації може вирішально впливати на результати розслідування. Зокрема, Україна, де велика частина інформації зберігається у закордонних хмарних сервісах, отримує змогу без зволікань звертатися до міжнародних постачальників електронних послуг для збору доказів.

Протокол також полегшує доступ до інформації про абонентів, що є важливим для ідентифікації осіб, пов'язаних з воєнними та кіберзлочинами. У такій ситуації, коли багато злочинців діють через анонімні облікові записи, ідентифікаційні дані можуть стати ключовими доказами для переслідування винних.

Крім того, протокол забезпечує належний захист персональних даних та права людини. Це особливо важливо в умовах зростання кіберзлочинності, коли збирання

та передача даних може становити загрозу для приватності. Положення протоколу передбачають необхідність дотримання принципів конфіденційності та пропорційності, що дозволяє збалансувати ефективність розслідувань і захист прав осіб.

Участь України в цьому протоколі також сприяє зміцненню міжнародної співпраці у сфері боротьби з кіберзлочинністю. Протокол передбачає спрощені механізми взаємної правової допомоги, включно зі створенням спільних слідчих груп для розслідування складних міжнародних справ. Це дозволяє українським слідчим активно співпрацювати з іноземними колегами, використовуючи сучасні технологічні інструменти для аналізу великих обсягів даних та проведення слідчих дій, зокрема через відеоконференції.

Однак для повного використання можливостей протоколу Україна має адаптувати своє національне законодавство. Це передбачає внесення змін до Кримінального процесуального кодексу щодо чіткого регулювання запитів на електронні докази, а також призначення відповідальних органів для забезпечення виконання міжнародних зобов'язань. Крім того, потрібно розробити національні стандарти для захисту прав осіб під час передачі й обробки електронних доказів, щоб відповідати міжнародним стандартам.

Таким чином, Другий додатковий протокол до Будапештської конвенції є важливим кроком вперед у забезпеченні швидкого та ефективного доступу до електронних доказів, необхідних для боротьби з кіберзлочинністю та воєнними злочинами. Його імплементація в Україні дозволить значно підвищити ефективність розслідувань і сприятиме зміцненню міжнародного правопорядку, що особливо важливо для країни, яка веде боротьбу з агресором на кіберфронті та в фізичному просторі.

6. Правове регулювання електронних доказів у Європейському Союзі.

Останні зміни у правовому регулюванні електронних доказів на рівні Європейського Союзу суттєво впливають на збирання, збереження та використання цифрових даних у кримінальних розслідуваннях. У червні 2023 року Європейський парламент і Рада ЄС ухвалили два ключових нормативних акти: Регламент (ЄС) 2023/1543 [9] та Директиву (ЄС) 2023/1544 [10], що спрямовані на вдосконалення правових інструментів для доступу до електронних доказів у кримінальних справах. Ці акти дозволяють правоохоронним та судовим органам ЄС безпосередньо звертатися до провайдерів електронних послуг із запитами на надання або тимчасове збереження електронних даних, незалежно від того, де ці дані зберігаються.

Регламент про європейські постанови щодо збирання та збереження електронних доказів дозволяє компетентним органам однієї держави-члена ЄС запитувати електронні дані у провайдерів послуг, розташованих в інших державах-членах. Він запроваджує дві нові заходи: Європейську постанову про збирання, яка зобов'язує надавати дані протягом 10 днів (або 6 годин у надзвичайних ситуаціях), та Європейську постанову про збереження, що передбачає тимчасове збереження даних на 60 днів, щоб уникнути їх видалення до надання за запитом.

Директива про призначення юридичних представників вимагає від усіх провайдерів електронних послуг, які працюють на ринку ЄС, призначити юридичного представника в ЄС. Цей представник виконує функції контактної особи для отримання запитів від національних компетентних органів та забезпечення їх виконання [11].

Важливим аспектом нової регламентації є чітка класифікація електронних даних за рівнем втручання в приватність:

- дані абонента (особиста інформація, така як ім'я, адреса, платіжні дані);
- дані доступу (дані про початок і завершення сеансу доступу користувача);
- транзакційні дані (метадані, такі як інформація про місцезнаходження або використання послуги);
- контент-дані (цифрові матеріали, такі як текстові повідомлення, відео та аудіо). Ця категоризація дозволяє чітко визначити рівень інтервенції та регламентувати порядок доступу до таких даних у межах кримінальних розслідувань.

Нові правила також враховують важливість міжнародної співпраці, використовуючи елементи, взяті з Будапештської конвенції та Закону США про CLOUD. Проте однією з основних проблем, яку намагаються вирішити нові акти, є конфлікти юрисдикцій та тривалі строки отримання відповіді на запити про електронні докази. Зокрема, попередня практика взаємної правової допомоги (MLA) і Європейського розпорядження про розслідування (EIO) потребували значних ресурсів і часу для виконання запитів, тоді як нові механізми значно прискорюють цей процес.

Законодавство передбачає певні гарантії для захисту прав осіб, чиї дані запитуються, такі як можливість оскаржити законність, необхідність і пропорційність постанови. Однак залишаються питання щодо потенційних конфліктів із законами третіх країн, що може призвести до правової невизначеності для всіх сторін.

Незважаючи на значну критику з боку представників приватного сектору, зокрема провайдерів послуг, та організацій громадянського суспільства, які висловлювали занепокоєння щодо можливих порушень приватності, нові правила націлені на забезпечення ефективного доступу до електронних доказів у межах ЄС. Важливими є також встановлені чіткі терміни для виконання запитів, що повинні сприяти прискоренню процесу розслідувань і забезпеченню справедливості у кримінальних справах, пов'язаних із цифровими доказами.

Ці зміни відображають зростаючу роль цифрових доказів у сучасних кримінальних розслідуваннях і необхідність оновлення правових рамок для забезпечення швидкого та ефективного доступу до таких даних у межах Європейського Союзу.

7. Рекомендації щодо вдосконалення законодавства України

З огляду на важливість OSINT та електронних доказів у розслідуванні воєнних злочинів, необхідно вдосконалити національне законодавство України для забезпечення їх ефективного використання.

По-перше, необхідно внести зміни до КПК України, щоб чітко визначити електронні докази як окреме джерело доказів та регламентувати процедури їх збору, обробки та подання в суд. Це включає питання збереження даних у хмарних сервісах та використання міжнародної правової допомоги для отримання доступу до даних, які зберігаються за кордоном.

По-друге, слід розробити внутрішні стандарти та інструкції для українських правоохоронних органів, які враховували б міжнародні найкращі практики, такі як Берклійський протокол з цифрових розслідувань. Це допоможе забезпечити належне документування електронних доказів та дотримання стандартів ланцюга збереження доказів, що є критичним для їх допустимості в судових процесахє

По-третє, законодавство України повинно передбачати можливість оперативного запиту електронних доказів у провайдерів послуг, подібно до механізму європейських постанов про збирання та збереження даних. Такий механізм дозволить правоохоронним органам України швидше отримувати доступ до даних, необхідних для розслідування злочинів, із забезпеченням обов'язку провайдерів надавати або зберігати дані протягом визначених термінів (наприклад, 10 днів або 6 годин у надзвичайних ситуаціях).

По-четверте, запровадження вимоги щодо призначення юридичних представників. Відповідно до Директиви ЄС 2023/1544, Україна може вимагати від провайдерів електронних послуг, які працюють на українському ринку, призначати юридичного представника в Україні. Цей представник повинен бути відповідальним за отримання запитів на надання електронних доказів від правоохоронних органів і забезпечення виконання цих запитів. Це сприятиме підвищенню ефективності збору доказів та правовій визначеності для провайдерів.

По-п'яте, удосконалення класифікації та захисту різних типів даних. Як і в ЄС, законодавство України повинно чітко розрізняти категорії електронних даних за рівнем втручання в приватність: дані абонента, дані доступу, транзакційні дані та контент-дані. Це дозволить регламентувати, які типи даних можуть бути запитувані для різних ка-

тегорій злочинів, і забезпечити баланс між ефективністю розслідування та захистом прав людини.

По-шосте, міжнародна співпраця та гармонізація із Будапештською конвенцією та Другим додатковим протоколом щодо електронних доказів. Україна має посилити співпрацю з міжнародними організаціями в рамках Будапештської конвенції про кіберзлочинність, яка вже є важливим інструментом для міжнародної взаємодії у сфері електронних доказів. Необхідно також розглянути можливість впровадження додаткових інструментів для прискорення обміну електронними доказами на міжнародному рівні, подібно до положень про прискорене збереження даних, передбачених у законодавстві ЄС.

По-сьоме, розробка процедурних гарантій захисту приватності та прав осіб. Україна повинна інтегрувати механізми для забезпечення захисту приватності осіб, чиї дані запитуються у межах кримінальних розслідувань. Як і в ЄС, необхідно забезпечити можливість оскарження запитів на надання електронних доказів за критеріями законності, необхідності та пропорційності. Це включає запровадження чітких процедур щодо повідомлення осіб, чиї дані збираються, та забезпечення їхнього права на оскарження.

По-восьме, удосконалення механізмів протидії правовим конфліктам. З урахуванням можливих конфліктів законодавства різних країн (наприклад, коли дані зберігаються за межами України або у провайдерів, зареєстрованих в іншій юрисдикції), українське законодавство має передбачати механізми вирішення таких правових конфліктів. Це може бути зроблено шляхом розробки міжнародних угод про обмін електронними доказами, подібних до тих, які обговорюються між ЄС та США у рамках CLOUD Act.

Запровадження цих заходів дозволить Україні посилити свою спроможність у боротьбі з кіберзлочинністю та забезпеченні справедливості у цифровому середовищі, узгоджуючи правову базу з кращими європейськими практиками та міжнародними стандартами. У підсумку, ефективне використання OSINT та електронних доказів у розслідуванні воєнних злочинів в Україні вимагає комплексного підходу, який включає вдосконалення національного законодавства.

Висновки

Зі стрімким розвитком технологій та зростанням ролі кіберпростору у сучасних конфліктах використання відкритих джерел інформації (OSINT) і електронних доказів у розслідуванні воєнних злочинів набуває ключового значення. Для України, яка стикається з масовими воєнними злочинами та систематичними кібератаками в умовах збройної агресії Росії, це питання набуває особливої актуальності. Традиційні методи збору доказів часто є неефективними через обмежений доступ до місць злочинів та відсутність співпраці з агресором. Водночас електронні докази та інформація з відкритих джерел можуть бути вирішальними для документування злочинів і доведення вини. Однак, існує низка викликів, пов'язаних з їхньою прийнятністю в суді, зокрема правові, технічні та процедурні проблеми.

Чинне законодавство України, попри внесені зміни у зв'язку з війною, все ще не надає чіткого правового механізму для збору, обробки та подання електронних доказів. Відсутність системних стандартів, чітких процедур автентифікації даних і їхнього захисту від маніпуляцій є серйозною перешкодою для використання таких доказів у судових процесах. Це ускладнює розслідування воєнних злочинів та кібератак, а також їхнє документування на національному та міжнародному рівнях.

Міжнародні дослідження підкреслюють зростаючу роль цифрових технологій у забезпеченні справедливості під час збройних конфліктів. Такі організації, як Рада Європи, ООН та Міжнародний кримінальний суд (МКС), все більше акцентують на необхідності використання електронних доказів у розслідуванні воєнних злочинів та злочинів проти людяності. Одним із ключових джерел у цій сфері є керівництво Ради Європи щодо електронних доказів, яке надає практичні рекомендації щодо їхнього збору, збереження та оцінки. Крім того, судова

практика ЄСПЛ, зокрема у справі «Україна та Нідерланди проти росії», де використовувались дані, зібрані через OSINT та неурядові організації, створила прецедент для їхнього визнання у судових процесах. Однак, існує гостра потреба в міжнародних правових стандартах, що дозволять визнати кібератаки воєнними злочинами, що наразі є одним із головних викликів у міжнародній правовій системі.

Важливим кроком для України є імплементація Другого додаткового протоколу до Будапештської конвенції, який було ухвалено в травні 2022 року. Протокол надає країнам нові можливості для обміну електронними доказами через прямі запити до іноземних провайдерів послуг, оминаючи складні бюрократичні процедури традиційної взаємної правової допомоги. Це дозволяє правоохоронним органам України швидко отримувати доступ до даних, які можуть зберігатися за межами країни, зокрема на серверах міжнародних провайдерів хмарних послуг. Імплементація протоколу значно прискорить і спростить процес отримання критично важливих доказів для розслідувань воєнних та кіберзлочинів.

Окрім цього, Протокол надає важливі інструменти для збирання інформації про абонентів та швидкої передачі даних під час надзвичайних ситуацій. Для України це є вкрай важливим, оскільки значна частина кібератак супроводжується анонімним використанням інтернет-ресурсів, а ідентифікація злочинців через дані абонентів є ключовою у багатьох випадках.

Також важливим аспектом є імплементація директив ЄС 2023/1543 і 2023/1544, які стосуються збору та збереження електронних доказів у межах ЄС. Вони забезпечують можливість для правоохоронних органів України отримувати дані від провайдерів, які працюють на території ЄС, через європейські механізми збору та збереження електронних доказів. Такі інструменти, як Європейська постанова про збирання та Європейська постанова про збереження даних, можуть бути взяті за основу для вдосконалення українського законодавства у сфері електронних доказів.

Ці механізми також включають новітні підходи до захисту прав людини та приватності в процесі збору доказів, що є важливим для забезпечення дотримання міжнародних стандартів у кримінальних розслідуваннях. Україна, у процесі імплементації цих інструментів, повинна забезпечити чітке регулювання процедури збору, передачі та збереження електронних доказів, а також створити правові механізми для захисту прав осіб, чиї дані запитуються.

Для підвищення ефективності використання OSINT та електронних доказів у розслідуванні воєнних злочинів необхідно внести зміни до Кримінального процесуального кодексу України. Ці зміни повинні чітко визначити електронні докази як окреме джерело доказів і встановити процедури для їхнього збору, збереження та подання в суд. Важливо впровадити інструменти для захисту цих даних від втрати чи маніпуляцій, а також забезпечити їхню автентифікацію.

Запровадження вимоги щодо призначення юридичних представників міжнародних провайдерів послуг, що працюють на українському ринку, також є важливим для підвищення ефективності співпраці між правоохоронними органами та провайдерами.

Україна повинна також гармонізувати своє законодавство з положеннями Будапештської конвенції та директив ЄС, щоб забезпечити швидкий доступ до електронних доказів, що зберігаються в інших юрисдикціях. Необхідно розробити внутрішні стандарти, які будуть відповідати міжнародним нормам, що регулюють процес збору, збереження та передачі електронних доказів, включно з питаннями конфіденційності та захисту прав людини.

У підсумку, імплементація Другого додаткового протоколу до Будапештської конвенції та директив ЄС є ключовим завданням для України на шляху вдосконалення механізмів розслідування воєнних злочинів та кібератак. Це дозволить забезпечити швидкий та ефективний доступ до електронних доказів, необхідних для судових процесів, і сприятиме зміцненню міжнародного правопорядку у сфері кібербезпеки та захисту прав людини.

Література

1. Electronic Evidence Guide v.3.0. Council of Europe. 2022. URL: https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0.

2. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/ show/994_575#Text; Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: https://rm.coe.int/1680a49dab

3. Rules of Procedure and Evidence. ICC. 2022. URL: https://www.icc-cpi.int/sites/default/files/2023-10/RulesProcedureEvidenceEng-Dec-2022.pdf

4. *Ukraine and the Netherlands v. Russia* (dec.) [GC], nos. 43800/14, 8019/16, and 28525/20, ECHR Grand Chamber Decision, 30 November 2022. URL: https://hudoc.echr.coe.int/eng?i=002-13989.

5. Kunnapu M., Paziuk A. *Study on electronic evidence of war crimes and related offences in the context of war of aggression against Ukraine*. Council of Europe. CyberEast, 2023. 30 p.

6. *The Berkeley Protocol on Digital Open Source Investigations*. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

7. Khan, K.A.A. (2024, January 22). *Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system*. International Criminal Court. URL: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

8. Ахтирська Н. *Одержання доказів в електронній формі в світлі другого додаткового протоколу до конвенції про кіберзлочиність* // Криміналістика і судова експертиза. Випуск 67, 2022. С. 188-200.

9. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. OJ L 191, 28.7.2023, p. 118–180. URL: http://data.europa.eu/eli/reg/2023/1543/oj

10. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. OJ L 191, 28.7.2023, p. 181–190. URL: http://data.europa.eu/eli/dir/2023/1544/oj

11. Bąkowski, Piotr. *Electronic Evidence in Criminal Matters*. European Parliamentary Research Service, PE 690.522, September 2023. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690522_EN

***Andrii Paziuk** – PhD, Doctor of Legal Science, Department of International and European Law, National Aviation University*
andrii.paziuk@npp.nau.edu.ua
***Nataliia Glynska** PhD, Doctor of Legal Science, Department of International and European Law National Aviation University*
nataglynska@gmail.com

INTERNATIONAL LEGAL REGULATION OF THE USE OF OPEN SOURCES AND ELECTRONIC EVIDENCE IN THE INVESTIGATION OF WAR CRIMES IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

The increasing role of technology and cyberspace in modern conflicts has highlighted the critical importance of effectively utilizing open sources of information (OSINT) and electronic evidence in the investigation of war crimes. The Russian-Ukrainian war has brought these challenges to the forefront, as traditional methods of evidence collection have often proven inadequate in circumstances where access to crime scenes is limited, and the perpetrator refuses to cooperate. In the case of Ukraine, which has suffered massive war crimes, human rights violations, and systemic cyberattacks on critical infrastructure, these challenges are especially acute.

This article explores the legal and procedural aspects of using OSINT and electronic evidence in war crimes investigations within the framework of international law, with a particular focus on Ukraine's context. Despite

OSINT and electronic evidence emerging as key tools for documenting and investigating war crimes, significant legal and technical barriers still exist regarding their admissibility in judicial proceedings. Ukrainian legislation, even with recent updates prompted by the war, continues to lack clear regulations on the procedures for collecting, processing, and presenting electronic evidence. Furthermore, there are gaps in ensuring the authenticity and security of such evidence, which impairs its effectiveness in war crimes investigations.

The article examines recent international developments, including the practices of international institutions such as the International Criminal Court (ICC) and the European Court of Human Rights (ECHR), which are gradually incorporating OSINT and electronic evidence into war crimes investigations. Key case studies, such as the «Ukraine and Netherlands v. Russia» case in the ECHR, demonstrate how OSINT gathered by non-governmental organizations has been utilized as admissible evidence, establishing important precedents for future cases.

Moreover, the article analyzes the role of new technologies in enhancing the efficiency of gathering and processing electronic evidence, with a focus on big data analysis, artificial intelligence, and voice recognition technologies. These tools are increasingly critical in managing vast amounts of digital information generated during conflicts and are vital for the verification and preservation of evidence. The challenges of using such technologies, including compliance with international data protection standards, are also considered.

The discussion further extends to the international legal framework governing the exchange of electronic evidence, emphasizing the relevance of the Budapest Convention on Cybercrime and the Second Additional Protocol to the Budapest Convention, which aims to simplify cross-border cooperation for the collection of electronic evidence. Ukraine's participation in these international instruments plays a crucial role in overcoming legal obstacles related to jurisdiction and expediting access to data stored abroad. Furthermore, the adoption of EU regulations and directives on electronic evidence offers valuable lessons for Ukraine in terms of harmonizing its legal framework with European standards.

In conclusion, the article proposes concrete recommendations for Ukraine to enhance its legal framework for the collection and use of electronic evidence in the investigation of war crimes. These recommendations include legislative amendments to the Criminal Procedure Code of Ukraine to clearly define electronic evidence as a distinct category, establish procedures for its collection and verification, and ensure the rapid access to data from international service providers. Additionally, the article highlights the need for Ukraine to fully implement the Second Additional Protocol to the Budapest Convention and align its legal framework with the latest EU directives on electronic evidence.

By addressing these challenges, Ukraine can significantly improve its capacity to investigate war crimes and cyberattacks, ensuring that justice is served while adhering to international legal standards. This will also contribute to the broader international effort to develop more robust legal mechanisms for the use of OSINT and electronic evidence in war crimes investigations in the digital age.

Keywords: OSINT, electronic evidence, war crimes, international law, cybercrime, International Criminal Court, Budapest Convention.