УДК 004.056.5:343.326

ГУЦАЛЮК М.В., *кандидат юридичних наук, доцент, с.н.с.,*
провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

КІБЕРЗАГРОЗИ ПІД ЧАС ГІБРИДНОЇ ВІЙНИ ТА ПРОТИДІЯ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ

DOI: https://doi.org/10.37750/2616-6798.2025.1(52).324708

Анотація. *У статті розглядаються основні виклики кібербезпеки для України в умовах гібридної війни та зростаючої загрози організованої кіберзлочинності. Особливу увагу приділено аналізу масштабних кібератак на критичну інфраструктуру, загрозам дезінформації, кібершпигунству та використанню новітніх технологій у злочинних цілях. Окреслено ключові напрямки протидії кіберзагрозам, включаючи вдосконалення законодавства, міжнародну співпрацю, впровадження сучасних технологій та підготовку спеціалізованих кадрів. Акцентовано увагу на введенні поняття електронних доказів в Кримінальний процесуальний кодекс України. Підкреслюється важливість стратегічного підходу до кіберзахисту для забезпечення національної безпеки України.*

Ключові слова: *кібербезпека, кіберзлочинність, кібератака, організована злочинність, електронні докази, міжнародне співробітництво.*

Summary. *The article examines the main cybersecurity challenges Ukraine is facing in the context of hybrid warfare and the growing threat of organized cybercrime. Special attention is given to the analysis of large-scale cyberattacks on critical infrastructure, disinformation threats, cyber espionage, and the use of advanced technologies for criminal purposes. Key directions for countering cyber threats are outlined, including improving legislation, fostering international cooperation, implementing modern technologies, and training specialized personnel. Emphasis is placed on introducing the concept of electronic evidence into Ukraine's Criminal Procedure Code. The importance of a strategic approach to cybersecurity for ensuring Ukraine's national security is highlighted.*

Keywords: *cybersecurity, cybercrime, cyberattack, organized crime, electronic evidence, international cooperation.*

Постановка проблеми. Однією з ознак динамічного розвитку сучасної цивілізації є бурхливий розвиток методів обробки, аналізу, передачі даних та зберігання інформації. Такі технології як Хмарні обчислення, аналітика Великих Даних, штучний інтелект (далі – ШІ), блокчейн використовуються в різноманітних сферах суспільства, починаючи від фінансової сфери, освіти, енергетики, закінчуючи військовою та сферою правоохоронної діяльності.

Україна досягла значних успіхів у цьому напрямі. Зокрема відповідно до Міжнародного рейтингу ООН, у 2024 році наша країна за рівнем розвитку цифрових держпослуг посіла п'яте місце у світі [1]. Особливо примітною вітчизняною розробкою є платформа "Дія", якою користується понад 21 млн. українців.

Поряд з цим стрімко розвивається і сучасний ландшафт кіберзагроз, оскільки зловмисники постійно адаптують свої методи та тактики до нових умов. Серйозною загрозою для міжнародної безпеки та стабільності залишається кіберзлочинність, включаючи організовані її форми, у тому числі за підтримки державними органами деяких країн.

З кожним роком кількість кіберінцидентів зростає, і це стосується як приватного сектору, так і державних установ. В умовах цифровізації економіки та повсюдного використання технологій, кіберзлочинці дедалі частіше застосовують нові техніки для досягнення своїх цілей.

За оцінками багатьох експертів з управління ризиками, кіберінциденти є найзагрозливішою причиною переривання бізнесу, навіть більше, ніж стихійні лиха чи енергетичні проблеми, а глобальні втрати від кіберзлочинів у 2024 році можуть перевищити $9,5 трильйона [2].

Особливу загрозу становить активність організованих кіберзлочинних угруповань, що здійснюють цільові атаки на критичну інфраструктуру, фінансові установи та державні системи. Зокрема, авторитарні держави та транснаціональні угруповання використовують кіберпростір для шпигунства, крадіжки даних і навіть для дестабілізації політичних ситуацій у різних країнах. Такі кіберзагрози, як *ransomware-атаки* (“вимагання за шифрування даних”), фішинг і *malware* (“шкідливе програмне забезпечення”), стають дедалі складнішими, що утруднює кіберзахист навіть для висококваліфікованих фахівців.

Для України кібербезпека має особливу актуальність через гібридну війну, яку веде рф. З 2022 році, Україна зіткнулася зі значним зростанням кількості кібератак на критичну інфраструктуру, зокрема на енергетичні та фінансові системи. Наприклад, атака Black Energy у 2015 році спричинила значні збої в електропостачанні в західних регіонах України, а атака Not Petya у 2017 році завдала збитків на мільярди доларів, не лише Україні, а й усьому світу. Одна з наймасштабніших кібератак на телекомунікаційну систему України була здійснена у грудні 2023 року, коли на декілька днів без зв’язку та Інтернет послуг залишилося більше 20 мільйонів людей [3].

Загострення кіберзагроз також відзначається у сфері дезінформації та кібершпигунства, що підриває національну безпеку та соціально-політичну стабільність країни. Український уряд активно працює над зміцненням кібербезпеки, запроваджуючи нові законодавчі ініціативи, співпрацюючи з міжнародними партнерами, такими як ЄС та НАТО, впроваджуючи сучасні технології для захисту від кіберзагроз, використовуючи підтримку іноземних партнерів, у тому числі у рамках Талліннського механізму – міжнародного інструменту для підтримки та зміцнення кібербезпеки та кіберстійкості, захисту критичної інфраструктури України.

Отже, актуальність боротьби з кіберзлочинністю, у тому числі й організованою є надзвичайно високою як на глобальному рівні, так і в Україні. Це обумовлено збільшенням числа складних та організованих кіберзлочинів, які загрожують як економічній стабільності, так і національній безпеці. Ефективна протидія кіберзагрозам потребує вдосконалення чинного законодавства, впровадження сучасних технологій, посилення міжнародної співпраці та розвитку спеціалізованих кадрів у цій сфері.

Результати аналізу наукових публікацій. Останніми роками у зв’язку з високою актуальністю проблеми забезпечення кібербезпеки та протидії кіберзлочинності з’явилося багато публікацій та дисертаційних досліджень як зарубіжних так і вітчизняних науковців. Зокрема це B. Schneier, G. Spafford, D. Song, Н. Ахтирська, В. Гавловський, А. Марущак, Н. Ткачук, В. Шеломенцев та інші. Досліджувалися також проблеми використання електронних доказів такими науковцями як Д. Алєксєєва-Процюк, П. Антонюк, О. Брисковська, В. Хахановський, В. Школьніков та ін.

Водночас окремі положення їх використання, особливо з врахуванням сучасної європейської нормативної бази, залишаються дослідженими не повною мірою.

Метою статті є визначення кіберзагроз під час гібридної війни та надання пропозицій щодо посилення кібербезпеки, включно з протидією кіберзлочинності, у тому числі з організованими її формами.

Виклад основного матеріалу. Основні виклики та кіберзагрози, а також способи їм протидіяти визначені в Стратегії кібербезпеки України [4]. Зокрема до викликів для України в сфері кібербезпеки віднесено:

активне використання кіберзасобів у міжнародній конкуренції;

змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема Хмарних та квантових обчислень, 5G-мереж, Великих Даних, Інтернету речей, ШІ тощо;

мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

До загроз у сфері кібербезпеки відносяться:

гібридна агресія російської федерації проти України у кіберпросторі. РНБО зазначило, що держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки рф спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об’єкти критичної інформаційної інфраструктури. А кібератаки активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності;

кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Також в документі зазначено, що набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов’язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів тощо;

організовані та спонсоровані урядами інших держав кібератаки, що пов’язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності [4].

Водночас сучасний ландшафт кіберзагроз стрімко розвивається, оскільки зловмисники постійно адаптують свої методи та тактики до нових умов.

У 2024 році спостерігаються такі ключові тенденції трансформації кіберзагроз:

Зловмисне використання ШІ: хакери все частіше використовують ШІ для автоматизації атак, включаючи фішинг, соціальну інженерію, генерацію шкідливого коду та навіть створення Deepfake-контенту для обману користувачів.

Зростання кібератак на критичну інфраструктуру: інфраструктурні об’єкти (енергетика, транспорт, медицина) систематично стають мішенями для кібератак, які можуть мати серйозні наслідки для суспільства.

Ransomware-as-a-Service (RaaS): зловмисники тепер продають або здають в оренду інструменти для запуску ransomware-атак, що значно знижує поріг для новачків у кіберзлочинному світі.

Зловмисники не тільки шифрують дані жертви, але й крадуть їх, погрожуючи опублікувати, якщо викуп не буде сплачено. Деякі йдуть далі, вимагаючи гроші від клієнтів компаній, чиї дані були викрадені.

Атаки на Хмарні сервіси: з ростом використання Хмарних технологій компаніями зловмисники переходять до експлуатації вразливостей у Хмарних середовищах.

Розвиток соціальної інженерії та фішингових атак: зловмисники дедалі частіше використовують персоналізовані підходи, використовуючи дані з соціальних мереж та зламаних баз даних для створення переконливих фішингових повідомлень.

Використання Deepfake: відео та голосові Deepfake використовуються для введення в оману керівників компаній і співробітників, що може призводити до фінансових втрат або витоку конфіденційної інформації.

Зростання атак на мобільні пристрої та додатки: збільшується кількість шкідливих додатків для Android та iOS, які використовуються для крадіжки фінансової інформації, паролів або для шпигунства за користувачами.

Кіберзагрози, пов’язані з криптовалютами: хакери зосереджуються на вразливостях смарт-контрактів, криптогаманців та децентралізованих фінансових (DeFi) платформ.

Кібербезпека в умовах геополітичної напруги: кіберзагрози дедалі частіше використовуються як інструмент гібридних війн, де державні та приватні актори атакують критичну інфраструктуру ворогів, шпигують або дестабілізують ситуацію в країнах-цілях.

Тобто сучасні кіберзагрози стають більш складними, інтелектуальними та цілеспрямованими, що потребує нових підходів до кіберзахисту.

Дедалі більш серйозну загрозу становить організована кіберзлочинність, оскільки її діяльність характеризується систематичним підходом, масштабністю та значним впливом на різні сфери суспільства. Перехід діяльності організованих злочинних угруповань у кіберпростір дозволяє їм значно збільшити свій вплив, охоплюючи ширші географічні області та використовуючи нові інструменти для здійснення злочинної діяльності.

Серед причин трансформації традиційних злочинних груп у цифрове середовище слід зазначити такі, як:

анонімність і безпека: Інтернет забезпечує значно вищий рівень анонімності, ніж традиційні методи ведення злочинного бізнесу. Використання мереж типу Tor і VPN, а також криптовалют (наприклад, Bitcoin) ускладнює відстеження злочинців;

зниження витрат і підвищення ефективності: кіберзлочини часто не потребують значних фінансових інвестицій або фізичної присутності, що робить їх менш ризикованими порівняно зі звичайною злочинною діяльністю (наприклад, торгівлею наркотиками чи зброєю).

масштабованість: кіберзлочинці можуть впливати на тисячі жертв одночасно через використання автоматизованих інструментів, таких як Ботнети та шкідливе програмне забезпечення.

У звіті Європолу “Internet Organised Crime Threat Assessment” (IOCTA) 2024 [5] зазначається, що мільйони жертв у всьому ЄС щодня зазнають кібератак. Групи програм-вимагачів дедалі частіше націлюються на малий та середній бізнес, оскільки вони мають нижчий рівень кіберзахисту. Користувачі Інтернет продовжують ставати жертвами інвестиційного та романтичного шахрайства. Зростає кількість випадків сексуального домагання через Інтернет, особливо спрямованого на неповнолітніх. Інструменти та сервіси, засновані на ШІ, стають звичайним товаром для кіберзлочинців на ринку “злочин як послуга”. “Даркнет” продовжує залишатися ключовим джерелом кіберзлочинності, дозволяючи правопорушникам ділитися знаннями, інструментами та послугами у прихований спосіб [6].

У жовтні 2023 року оперативники Департаменту кіберполіції спільно із колегами з Європолу, Євроюсту, із залученням правоохоронців Франції, Чехії, Німеччини, Італії, Латвії, Нідерландів, Іспанії, Швеції, Японії та Канади провели масштабну міжнародну операцію зі знешкодження небезпечного хакерського угруповання.

Починаючи з 2020 року зловмисники атакували вірусом-вимагачем 168 міжнародних компаній у країнах Європи та Америки. Зловмисники заражали сервери шкідливим програмним забезпеченням та викрадали з них інформацію. У подальшому дані на комп'ютерах жертв зашифровувалися і робилися непридатними для використання. За відновлення доступу члени угруповання вимагали від $5 до 70 мільйонів у криптовалюті. У разі несплати викупу або звернення до правоохоронців погрожували розповсюдити викрадені дані у "Даркнеті".

Організатори чітко розподіляли обов'язки між учасниками групи. Окремі члени відповідали за збір інформації та пошук вразливих місць в архітектурі кібербезпеки жертв.

Зібрану інформацію вони передавали спільникам з навичками комп'ютерного програмування. Останні відповідали за створення та модифікування шкідливого програмного забезпечення з метою подальшого ураження конкретної компанії.

У рамках проведення спільного міжнародного розслідування українські правоохоронці провели масові обшуки на території Києва у приміщеннях одного з учасників угруповання. Вилучені ноутбуки, мобільні телефони та електронні носії інформації.

Наразі французькі компетентні органи розслідують дане кримінальне провадження за фактами несанкціонованого доступу, перешкоджання роботі системи автоматичної обробки даних, вимагання (здирство) в складі організованого кримінального угрупування, відмивання коштів (легалізація) в складі організованого кримінального угрупування, які передбачені рядом статей Кримінального кодексу Франції [7].

Отже на сьогодні організована кіберзлочинність – це глобальна проблема, що потребує комплексного підходу та постійного вдосконалення заходів кібербезпеки.

Враховуючи міжнародний характер кіберзлочинності, ще на початку нашого століття були прийняті відповідні законодавчі акти, у тому числі Конвенція про кіберзлочинність (також відома як Будапештська Конвенція або Європейська), ухвалена Радою Європи у 2001 році. Даний документ підписали не тільки європейські країни, але й всього 76 країн світу. Примітно, що рф не підписала цей міжнародний договір.

Мета цієї Конвенції полягає у забезпеченні спільної правової основи для запобігання, розслідування та переслідування кіберзлочинів, а також сприяння міжнародній співпраці між державами-членами для ефективної протидії кіберзлочинності.

Конвенція визначає категорії злочинів, які країни-учасниці повинні включити у свої національні законодавства:

До першої категорії відносяться злочини проти конфіденційності, цілісності та доступності інформації і систем:

- незаконний доступ до комп'ютерних систем.
- незаконне перехоплення даних.
- втручання в дані (знищення, пошкодження, змінення даних).
- втручання в роботу комп'ютерних систем.

До другої категорії відносяться комп'ютерні злочини, пов'язані з контентом:

- розповсюдження дитячої порнографії.
- злочини, пов'язані з порушенням авторських прав та інших прав інтелектуальної власності.

Конвенція визначає також процесуальні заходи та встановлює мінімальні стандарти для країн-учасниць щодо:

- зберігання даних, пов’язаних із кіберзлочинами;
- доступу до комп’ютерних даних;
- перехоплення даних у реальному часі;
- конфіскації або збереження доказів у цифровій формі.

Конвенція підкреслює важливість глобальної співпраці, та зокрема швидкий обмін інформацією для розслідування злочинів.

Зважаючи на зростаюче використання ІКТ організованою злочинністю у всіх “секторах” (сексуальна експлуатація, обіг наркотиків, контрабанда, тероризм) в травні 2023 року у Римі був прийнятий Другий додатковий протокол до Конвенції про кіберзлочинність.

Протокол надає інструменти для посиленого співробітництва та розкриття електронних доказів, таких як пряма співпраця з постачальниками послуг і реєстраторами, ефективні засоби отримання інформації про абонентів і даних про трафік, негайне співробітництво в надзвичайних ситуаціях або спільні розслідування, які підпадають під дію прав людини та верховенства права, включаючи гарантії захисту даних [8].

Україна серед інших держав підписала даний протокол. Наразі необхідно його ратифікувати та імплементувати у чинне законодавство.

На Саміті майбутнього, який відбувся в рамках ООН у Нью-Йорку 20 – 23 вересня 2024 року, був прийнятий Пакт в ім’я майбутнього, який включає Глобальний цифровий договір і Декларацію про майбутні покоління. Пакт охоплює широкий спектр тем, включаючи мир і безпеку, сталий розвиток, зміну клімату, цифрове співробітництво, права людини, гендер, молодь і майбутні покоління, а також трансформацію глобального управління [9].

В документі, зокрема зазначається, що транснаціональна організована злочинність і пов’язані з нею незаконні фінансові потоки можуть становити серйозну загрозу міжнародному миру та безпеці, правам людини та сталому розвитку, зокрема через можливі зв’язки, які можуть існувати в деяких випадках між транснаціональною організованою злочинністю та терористичними групами. Ми вирішуємо: (a) активізувати зусилля щодо боротьби з транснаціональною організованою злочинністю та пов’язаними з нею незаконними фінансовими потоками за допомогою комплексних стратегій, включаючи запобігання, раннє виявлення, розслідування, захист і правоохоронну діяльність, боротьбу з рушійними факторами та взаємодію з відповідними зацікавленими сторонами; (b) Зміцнити міжнародне співробітництво з метою запобігання та боротьби з транснаціональною організованою злочинністю в усіх її формах, у тому числі коли вона вчиняється за допомогою систем інформаційно-комунікаційних технологій, і ми вітаємо розробку проекту Конвенції ООН проти кіберзлочинності.

Проект конвенції ООН у серпні 2024 року був узгоджений спеціальним комітетом, створеним Генеральною Асамблеєю ООН. Остаточне прийняття документа передбачається Генеральною Асамблеєю ООН у грудні 2024 року або січні 2025-го.

Як зазначено в проекті конвенції, технологія створила можливості для більшого масштабу, швидкості та розмаху злочинів, від тероризму до торгівлі наркотиками, торгівлі людьми, контрабанди мігрантів, торгівлі вогнепальною зброєю тощо.

Проект конвенції містить інструменти, які посилять міжнародну співпрацю, зусилля правоохоронних органів, технічну допомогу та розбудову спроможності щодо кіберзлочинності [10].

Отже сучасні міжнародні правові документи у сфері боротьби з кіберзлочинністю підкреслюють важливість міжнародної співпраці та обміну інформацією, яка в основному зберігається в електронній формі. Крім того, сьогодні розслідування традиційних злочинів, а також військових злочинів, скоєних під час агресії рф, в переважній більшості також вимагає отримання, аналіз та зберігання електронних доказів.

Для обміну електронними доказами країни Великої сімки у 1998 році створили мережу контактних пунктів "The G7 24/7 Cybercrime Network", які функціонують цілодобово та щорічно обмінюються тисячами інформаційних запитів та відповідей.

Пізніше подібну мережу контактних пунктів 24/7 створили і держави-підписанти Конвенції про кіберзлочинність, у тому числі і Україна. Для ефективного обміну електронними доказами в Європейському Союзі пропонується використовувати Європейський наказ про пред'явлення (European Production Order), який дозволить судовому органу в одній державі-члені отримати електронні докази (такі як електронні листи, текстові повідомлення або повідомлення в програмах, а також інформацію для ідентифікації злочинця) безпосередньо від постачальника послуг в іншій державі-члені, який буде зобов'язаний відповісти протягом 10 днів, а в екстрених випадках – протягом 8 годин та Європейський наказ про збереження даних (European Preservation Order), який дозволить судовому органу в одній державі-члені вимагати, щоб постачальник в іншій державі-члені зберіг певні електронні дані [11].

На жаль в чинному Кримінальному процесуальному кодексі України термін "електронний доказ" відсутній, на відміну, наприклад, Цивільного процесуального кодексу України (стаття 100).

Натомість законодавець пропонує вважати комп'ютерні дані документом (п. 2 статті 99 КПК України). Проте, документ – це сталий, фіксований матеріальний об'єкт, а комп'ютерні дані мають властивість швидко змінюватися та видалятися, причому дистанційно, також візуалізація електронної інформації суттєво залежить від програмних та апаратних засобів, за допомогою яких здійснюється їх перегляд. Крім того, на практиці, навіть серед науковців, існує плутанина щодо понять електронні докази та електронний документ, який визначений Законом України "Про електронні документи та електронний документообіг" [12].

Робочою групою, створеною Д.А. Монастирським при Комітеті Верховної Ради України з питань правоохоронної діяльності, у 2019 році були підготовлені, а пізніше підтримані низкою народних депутатів проекти Закону України "Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів" та "Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам" (законопроекти №№ 4004, 4003).

В даних законопроектах надано визначення поняття та видів електронних доказів, розмежувавши поняття електронного документу як різновиду електронного доказу та інших документів, які подаються в електронній формі регламентації порядку спеціальної конфіскації віртуальних активів.

Також пропонується відповідно до Конвенції про кіберзлочинність застосовувати такий захід забезпечення кримінального провадження як термінове збереження інформації під час досудового розслідування кіберзлочинів, надати можливості прокурору, слідчому, оперативним підрозділам під час проведення обшуку законним

чином отримувати доступ до комп'ютерних систем, які фізично розташовані за межами місця проведення обшуку та інші процесуальні дії.

Ці питання сьогодні разом з ратифікацією Другого протоколу до Конвенції про кіберзлочинність є вкрай актуальними і потребують відповідного рішення Верховної Ради України.

Додатково зазначимо, що забезпечення унормування в установленому порядку питання щодо електронних доказів з використанням кращих практик з цих питань та урахуванням сучасних викликів і тенденцій у сфері кібербезпеки передбачено пунктом 15 Плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України [13].

Також необхідною умовою ефективного використання електронних доказів є відповідна підготовка правоохоронців. У Міжвідомчому центрі з проблем боротьби з організованою злочинністю при РНБО України спільно з групою науковців були підготовлені відповідні Методичні рекомендації [14]. Проте сфера інформаційних технологій постійно розвивається і сьогодні серед іншого доцільно використовувати можливості "Проекту SIRIUS", який спільно реалізований Європолом і Євроюстом та допомагає правоохоронним і судовим органам отримати доступ до транскордонних електронних доказів у контексті кримінальних розслідувань і проваджень. Проект підтримує слідчих за допомогою різноманітних послуг, таких як рекомендації, тренінги та є центральною опорною точкою в ЄС для обміну знаннями щодо транскордонного доступу до електронних доказів [15].

Висновки.

Сучасна боротьба з кіберзлочинністю вимагає тісної міжнародної співпраці, що підтверджується прийняттям та імплементацією таких документів, як Конвенція про кіберзлочинність та її Другого додаткового протоколу. Ці акти створюють єдину правову базу для попередження, розслідування та переслідування кіберзлочинів, а також забезпечують інструменти для оперативного обміну електронними доказами між державами.

Разом з тим законодавство України наразі не повною мірою відповідає сучасним викликам у сфері кіберзлочинності. Особливо актуальними є питання визначення статусу електронних доказів у Кримінальному процесуальному кодексі. Запропоновані законопроекти №№ 4003 та 4004 спрямовані на вдосконалення правової бази для ефективної протидії кіберзлочинам, а також гармонізацію з міжнародними стандартами.

Враховуючи зростання кількості злочинів, пов'язаних із використанням інформаційно-комунікаційних технологій, та вплив війни рф проти України, необхідність ратифікації Другого додаткового протоколу та удосконалення національного законодавства є критичною. Це включає чітке врегулювання використання електронних доказів, спеціальну конфіскацію віртуальних активів і можливість збереження даних на стадії досудового розслідування.

Таким чином, реалізація зазначених заходів дозволить не лише підвищити ефективність боротьби з кіберзлочинністю, але й забезпечити надійну основу для збереження та використання електронних доказів у розслідуванні як кіберзлочинів, так і традиційних злочинів із цифровим слідом. Разом з впровадженням заходів кіберзахисту це дозволить суттєво зменшити рівень кіберзагроз та підвищити рівень кібербезпеки, що в свою чергу є необхідною умовою розвитку цифрового суспільства.

Використана література

1. UN E-Government Survey 2024. URL: https://publicadministration.un.org/egovkb/en-us/ReportsUN-E-Government-Survey-2024

2. Cybercrime to Cost the World $9.5 Trillion USD Annually In 2024. URL: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

3. Гуцалюк М.В. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право.* № 2(49)/2024. С.164-177. DOI: https://doi. org/10.37750/2616-6798.2024.2(49).306199.

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України 26.08.21 р. № 447/2021. URL: https:// www.president.gov.ua/documents/4472021-40013

5. Internet Organised Crime Threat Assessment (IOCTA) 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

6. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі "Даркнет". *Інформація і право.* № 3(26)/2018. С. 102-108. DOI: https://doi.org/10.37750/2616-6798.2018.3(26).273306.

7. Кіберполіція спільно з іноземними колегами знешкодила транснаціональне хакерське угруповання. URL: https://www.npu.gov.ua/news/kiberpolitsiia-spilno-z-inozemnymy-kolehamy-zneshkodyla-transnatsionalne-khakerske-uhrupovannia

8. Посилена співпраця та розкриття електронних доказів: 22 країни підписали новий Протокол до Конвенції про кіберзлочинність. URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention

9. Pact for the Future. URL: https://www.un.org/en/summit-of-the-future

10. United Nations: Member States finalize a new cybercrime convention. URL: https://www.unodc.org/unodc/en/frontpage/2024/August/united-nations-member-states-finalize-a-new-cybercrime-convention.html

11. E-evidence – cross-border access to electronic evidence. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

12. Гуцалюк М.В., Антонюк П.Є. Проблемні аспекти процесуальної спроможності використання електронної (цифрової) інформації як доказів в кримінальному провадженні. *Інформація і право.* № 2(41)/2022. С. 116-122. URL: https://doi.org/10.37750/2616-6798.2022.2(41).270373

13. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.23 р. № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Texthttps://elar.naiau.kiev.ua/server/api/core/bitstrea ms/8e9e5637-7b62-475c-8c41-9850e317bfc4/content

14. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. / за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content

15. SIRIUS Cross-Border Access To Electronic Evidence. URL: https://www.europol.europa.eu/operations-services-innovation/sirius-project

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