Олександр ОНОПРІЄНКО,
заступник начальника кафедри забезпечення державної безпеки командно-штабного факультету Національної академії Національної гвардії України, полковник, доктор філософії (PhD), доцент,
ORCID: https://orcid.org/0000-0001-7935-4570
e-mail: alex.vog@ukr.net

Сергій ОНОПРІЄНКО,
науковий співробітник лабораторії інформаційно-аналітичного забезпечення судово-експертної діяльності, сертифікації та контролю якості досліджень Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України
ORCID: https://orcid.org/0000-0001-7574-7457
e-mail: osa-sa@ukr.net

DOI: https://doi.org/10.32620/pls.2025.8.66

КОНВЕНЦІЯ РАДИ ЄВРОПИ ПРО КІБЕРЗЛОЧИННІСТЬ: ВИСНОВКИ ДЛЯ УКРАЇНИ

Анотація. *У тезах доповіді розглядається значення Конвенції Ради Європи про кіберзлочинність (CETS № 185) та особливостей її адаптації до українського правового поля. Розглянуто ключові положення документа, а також механізми міжнародної взаємодії, що випливають із його імплементації. Оцінено актуальність Конвенції для України в контексті зростання кіберзагроз та викликів цифрової безпеки. Акцентовано увагу на необхідності гармонізації національного законодавства, налагодження міжвідомчої координації та інтеграції у європейський кіберпростір.*

Ключові слова: *кіберзлочинність, кібербезпека, Будапештська конвенція, міжнародне співробітництво, правове регулювання, кіберпростір, національна безпека, стандарти.*

Вступ. Упродовж останніх років Україна перебуває під постійним тиском масштабних, координованих та технічно складних кібератак, які стали невід'ємною складовою гібридної агресії, що системно ведеться проти нашої держави. Ці атаки не є випадковими чи ізольованими інцидентами — вони мають чітко виражений стратегічний характер, спрямований на дестабілізацію ключових елементів державного управління, порушення функціонування критичної інфраструктури, підрив суспільної довіри та ослаблення національної безпеки [1, с. 487-496]. Цифровий фронт, на якому ведеться ця боротьба, охоплює не лише технічні аспекти, а й інформаційно-психологічні операції, втручання у виборчі процеси, маніпуляції з даними та спроби паралізувати державні сервіси. В умовах такої багатовимірної загрози кібербезпека перетворюється на один із ключових елементів національної обороноздатності, а правове регулювання кіберпростору — на інструмент стратегічного захисту.

У цьому контексті імплементація міжнародних стандартів набуває особливої актуальності. Вони дозволяють не лише гармонізувати національне законодавство з міжнародними нормами, а й забезпечити ефективну міждержавну координацію, оперативне реагування на кіберінциденти та зміцнення цифрової стійкості України як демократичної держави, що протистоїть багатовекторній агресії. Саме тому побудова сучасної, адаптивної та інтегрованої системи кібербезпеки має базуватися на міжнародно визнаних правових і нормативних засадах. Одним із ключових документів у цій сфері є Конвенція Ради Європи про кіберзлочинність (CETS № 185), більш відома як Будапештська конвенція (далі – Конвенція), прийнята 23 листопада 2001 року [2]. Інтеграція положень цієї конвенції у національну систему кіберзахисту дозволяє Україні не лише посилити власну кіберстійкість, а й утвердитися як надійний партнер у глобальній цифровій безпеці.

Аналіз основних досліджень і публікацій. Окремі аспекти правового регулювання кіберпростору вже були предметом аналізу вітчизняних науковців. Вагомий внесок у розробку теоретичних і прикладних підходів до протидії кіберзлочинності зробили такі дослідники, як В. С. Венедіктов, В. А. Журавель, М. В. Карчевський, М. М. Коваленко, О. В. Кохановська, О. М. Литвинов, С.Ю. Лукашевич, М. І. Панов, Ф.П. Тарасенко, Л. К. Терещенко, Т. І. Тарахонич, Н. Є. Філіпенко, В. С. Харченко, В. М.

Шевчук, В. Ю. Шепітько та інші. Ці дослідники формують наукову основу для вдосконалення законодавства, розробки стратегій кіберзахисту та підвищення цифрової стійкості держави. Їхні праці є важливим джерелом для формування національної політики у сфері кібербезпеки, особливо в умовах гібридної агресії та трансформації інформаційного простору.

Викладення основного матеріалу. У XXI столітті кіберпростір перетворився не лише на універсальне середовище для комунікації, зберігання та обміну інформацією, а й на арену новітніх загроз, що мають транснаціональний, системний і дедалі агресивніший характер. Кіберзлочинність охоплює широкий спектр правопорушень — від несанкціонованого доступу до інформаційних систем і втручання в їхню роботу до поширення шкідливого програмного забезпечення, фінансових шахрайств, цифрового шантажу та атак на критичну інфраструктуру. Особливу небезпеку становлять цілеспрямовані атаки на державні реєстри, енергетичні системи, об'єкти управління та інформаційні ресурси, які можуть паралізувати функціонування держави, порушити суспільну стабільність і створити умови для масштабних інформаційно-психологічних операцій. Для України, яка перебуває в умовах гібридної війни, ці загрози мають не лише технічний, а й стратегічний вимір, оскільки кіберпростір став одним із ключових фронтів сучасної боротьби за суверенітет, безпеку та демократичний розвиток. У цьому контексті Будапештська конвенція про кіберзлочинність (CETS № 185), ухвалена Радою Європи у 2001 році, набуває особливої актуальності. Вона є першим і наразі єдиним міжнародним договором, що має юридично обов'язковий характер у сфері протидії злочинам, пов'язаним із використанням комп'ютерних систем та мереж. Її мета полягає у гармонізації кримінального законодавства держав-учасниць, удосконаленні процесуальних механізмів та зміцненні міжнародного співробітництва для ефективної протидії кіберзлочинності. Конвенція визнає, що кіберзлочини мають глобальний характер, а тому потребують узгоджених правових підходів, які дозволяють державам діяти скоординовано, незалежно від географічних меж. У цьому контексті вона виступає як нормативна платформа, що забезпечує єдність у визначенні складів кіберзлочинів, процедур слідства та механізмів правової допомоги. Конвенція передбачає криміналізацію низки діянь, які становлять загрозу для цифрової безпеки, зокрема незаконного доступу до комп'ютерних систем, несанкціонованого перехоплення даних, втручання в роботу інформаційних систем, зловживання спеціальними пристроями, комп'ютерного шахрайства, фальсифікації цифрових документів та злочинів, пов'язаних із дитячою порнографією. Такий перелік охоплює як технічно складні правопорушення, так і соціально небезпечні прояви цифрової злочинності. Ці положення формують основу для уніфікованого підходу до кваліфікації кіберзлочинів, що дозволяє забезпечити їх ефективне переслідування у транскордонному вимірі, з урахуванням швидкоплинності цифрових слідів, складності юрисдикційних питань та необхідності оперативного реагування. Для України, яка стикається з системними кібератаками в умовах гібридної війни, така уніфікація є не лише правовою потребою, а й елементом національної безпеки.

У процесуальному аспекті Конвенція встановлює низку спеціалізованих механізмів, які дозволяють ефективно збирати, зберігати та використовувати електронні докази в умовах цифрового середовища. Ці механізми враховують особливості кіберпростору, де інформація може бути змінена або знищена за лічені секунди, а сліди злочину – розпорошені між різними юрисдикціями. Зокрема, Конвенція передбачає можливість негайного збереження комп'ютерних даних (ст. 16–17), що дозволяє упередити їх втрату до початку формального слідства. Обшук і вилучення цифрової інформації (ст. 19) забезпечують доступ до комп'ютерних систем, носіїв та хмарних сервісів, із можливістю копіювання, блокування або вилучення даних. Перехоплення трафіку та доступ до переданих даних (ст. 20–21) дозволяють здійснювати моніторинг мережевої активності в реальному часі, що є критично важливим для виявлення та документування злочинної діяльності. Ці інструменти не лише розширюють технічні можливості слідчих органів, а й вимагають дотримання чітких правових процедур, які гарантують захист прав людини, зокрема права на приватність, недоторканність кореспонденції та захист персональних даних. Конвенція наголошує на необхідності забезпечення судового контролю, чіткого визначення меж повноважень та процедурної прозорості. Окрему увагу приділено міжнародному виміру: документ закладає інституційні засади транскордонної взаємодії, включаючи механізми правової допомоги (ст. 25–34), екстрадиції (ст. 24) та створення мережі контактних пунктів 24/7 (ст. 35), які забезпечують оперативний обмін інформацією між правоохоронними органами різних країн. Така інфраструктура дозволяє державам координувати дії у режимі реального часу, долати бар'єри юрисдикції та забезпечувати ефективне переслідування кіберзлочинців. У сукупності ці положення сприяють формуванню єдиного правового поля, яке зміцнює глобальну кіберстійкість, підвищує рівень правової довіри між державами та забезпечує оперативну сумісність процесуальних дій у боротьбі з транснаціональними цифровими загрозами.

У 2003 році Конвенцію було доповнено Додатковим протоколом, який передбачає криміналізацію дій расистського та ксенофобського характеру, вчинених із використанням комп'ютерних систем. Цей документ розширює сферу дії Конвенції, визнаючи, що цифрове середовище може бути використане для поширення ненависті,

дискримінації та підбурювання до насильства.

Україна ратифікувала Будапештську конвенцію про кіберзлочинність у 2005 році, підтвердивши свою прихильність до міжнародних стандартів у сфері цифрової безпеки та правосуддя. Водночас держава скористалася правом на застереження, передбаченим самою Конвенцією, і офіційно заявила про обмеження застосування окремих її положень. Зокрема, це стосувалося статті 6, яка передбачає криміналізацію зловживання пристроями, що можуть бути використані для вчинення кіберзлочинів. Українська сторона обґрунтувала це застереження необхідністю узгодження міжнародних норм із принципами національного кримінального права, зокрема щодо чіткого визначення складу злочину, меж кримінальної відповідальності та допустимості використання технічних засобів як об'єкта правового регулювання. Такий підхід дозволив зберегти гнучкість у формуванні внутрішньої правової політики у сфері кібербезпеки, водночас не порушуючи загальної логіки співпраці в межах Конвенції. Україна продовжує активно брати участь у роботі Кіберкомітету Ради Європи (T-CY), долучається до розробки директивних записок та бере участь у міжнародних навчаннях і тренінгах, спрямованих на підвищення ефективності боротьби з кіберзлочинністю. Така позиція свідчить про прагнення держави не лише адаптувати міжнародні стандарти до національного контексту, а й бути активним учасником глобального процесу формування правової архітектури цифрової епохи.

Висновки. Українські правоохоронні органи, судова система та профільні міністерства вже здійснюють практичні кроки у напрямку адаптації процесуальних механізмів, передбачених Будапештською конвенцією, зокрема щодо збору електронних доказів, реагування на кіберінциденти та взаємодії з міжнародними контактними пунктами. Важливим напрямом є також розбудова національної експертизи у сфері цифрової криміналістики, удосконалення нормативно-правових актів та впровадження спеціалізованих навчальних програм для слідчих, прокурорів і суддів. Водночас Україна активно бере участь у глобальних ініціативах, спрямованих на протидію кіберзлочинності, обмін досвідом, навчання фахівців та розробку спільних стандартів кіберзахисту. Співпраця з Європолом, INTERPOL, ENISA та іншими міжнародними структурами дозволяє інтегруватися в європейську систему цифрової безпеки та оперативно реагувати на транснаціональні загрози.

Окрему роль у зміцненні кіберстійкості держави відіграють підрозділи кібербезпеки в системі сектору безпеки і оборони, зокрема кібервійська, створення яких стало відповіддю на зростання інтенсивності та складності кібератак у межах гібридної війни. Ці підрозділи виконують завдання з виявлення, нейтралізації та попередження кіберзагроз, захисту критичної інфраструк тури, а також участі в інформаційній протидії агресору. Їхня діяльність тісно пов'язана з положеннями Будапештської конвенції, зокрема в частині міжнародного співробітництва, обміну інформацією та дотримання стандартів прав людини у сфері кібероперацій. Таким чином, для України Будапештська конвенція є не лише юридичним документом, а інструментом цифрової стійкості, міжнародної солідарності та стратегічного розвитку. Її положення – це дорожня карта для формування сучасної, адаптивної та правозахищеної системи кібербезпеки, здатної протистояти викликам XXI століття як у цивільному, так і у військовому вимірі.

Бібліографічні посилання

1. Філіпенко Н.Є., Лукашевич С.Ю. (2023) Діяльність судово-експертних установ щодо запобігання злочинності з використанням прогресивних інформаційних методик та технологій. Журнал «Наукові інновації та передові технології» № 14(28) 2023 (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»). С. 487-496.

2. Council of Europe. Convention on Cybercrime (ETS No. 185), Budapest, 23 November 2001. Strasbourg: Council of Europe. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

3. Конвенція про кіберзлочинність. Додатковий протокол від 28.01.2003 до Конвенції. Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

O. Onopriienko, S. Onopriienko

Council of Europe convention on cybercrime: conclusions for Ukraine.

Abstract. The report's theses examine the significance of the Council of Europe Convention on Cybercrime (CETS No. 185) and the specifics of its adaptation to the Ukrainian legal field. The key provisions of the document, as well as the mechanisms of international cooperation arising from its implementation, are considered. The relevance of the Convention for Ukraine in the context of growing cyber threats and digital security challenges is assessed. Attention is focused on the need to harmonize national legislation, establish interdepartmental coordination, and integrate into the European cyberspace.

Keywords: cybercrime, cybersecurity, Budapest Convention, international cooperation, legal regulation, cyberspace, national security, standards.

Зразок для цитування:

Онопрієнко О., Онопрієнко С. Конвенція Ради Європи про кіберзлочинність: висновки для України. Пропілеї права та безпеки, 2025. №8. С 257-259. DOI: https://doi.org/10.32620/pls.2025.8.66.