УДК 341.4:[343.346.8:004] DOI: https://doi.org/10.32631/pb.2025.4.05

МИКОЛА ВОЛОДИМИРОВИЧ МОРДВИНЦЕВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0002-7674-3164,
e-mail: lukoly@ukr.net;

ДМИТРО ВАЛЕНТИНОВИЧ ПАШНЄВ,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0001-8693-3802,
e-mail: dvpashnev@gmail.com;

ОЛЕКСІЙ ВОЛОДИМИРОВИЧ ХЛЄСТКОВ,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі;
https://orcid.org/0000-0001-8777-8269,
e-mail: Khliestkov.Oleksii@univd.edu.ua

МІЖНАРОДНІ МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ

У статті здійснено всебічний аналіз міжнародних моделей правового регулювання протидії кіберзлочинності, визначено їхні ключові елементи, тенденції розвитку та можливості впровадження в українське законодавство. Розкрито універсальні підходи, розроблені в межах Ради Європи й ООН, а також регіональні моделі Європейського Союзу, Сполучених Штатів Америки, країн Азії та НАТО. Особливу увагу приділено Конвенції Ради Європи про кіберзлочинність 2001 року, її додатковим протоколам і сучасним механізмам міжнародного співробітництва. Продемонстровано, що Конвенція стала основоположним документом у сфері уніфікації правових підходів до криміналізації діянь, пов'язаних із використанням інформаційних технологій, і створила основу для транскордонного обміну електронними доказами.

Метою дослідження є узагальнення міжнародного досвіду протидії кіберзлочинності та розроблення рекомендацій щодо його адаптації в Україні. Методологічною основою стали системний, порівняльно-правовий, історико-правовий і аналітичний методи, які дали змогу виявити закономірності формування сучасних моделей кібербезпеки. Проаналізовано нормативно-правові акти, міжнародні договори, наукові праці та практичні ініціативи держав у сфері кіберзахисту.

Висвітлено участь України в міжнародних програмах і проєктах, спрямованих на розвиток кіберстійкості, зокрема в межах співпраці з Європейським Союзом, НАТО й ООН. Обґрунтовано необхідність гармонізації українського законодавства з міжнародними стандартами, вдосконалення процедур збору та використання електронних доказів, а також посилення інституційної спроможності правоохоронних органів. Наголошено, що після початку повномасштабного вторгнення російської федерації 24 лютого 2022 року кіберзлочинність стала одним із ключових інструментів гібридної війни проти України.

Наукова новизна полягає у визначенні перспектив розвитку національної системи протидії кіберзлочинності на основі міжнародних практик. Отримані результати мають практичне значення для вдосконалення правового регулювання, посилення міжнародного співробітництва та забезпечення кіберстійкості держави в умовах сучасних загроз. Запропоновані висновки можуть бути використані для розроблення національної стратегії

кібербезпеки та підвищення ефективності міжвідомчої взаємодії у сфері протидії кіберзлочинності.

Ключові слова: *кіберзлочинність, кібербезпека, Будапештська конвенція, міжнародне співробітництво, правове регулювання, гібридна війна, кіберзахист, Україна.*

Оригінальна стаття

ВСТУП. Стрімкий розвиток інформаційних технологій у XXI столітті став підґрунтям для формування глобального цифрового середовища, яке відкриває нові можливості для економічного розвитку, комунікації та соціальної взаємодії. Водночас цифровізація суспільства породила нові виклики, серед яких особливе місце посідає кіберзлочинність. Її масштаби зростають кожного року, охоплюючи фінансову сферу, критичну інфраструктуру, комунікаційні системи та приватне життя громадян. За оцінками міжнародних експертів, збитки від кіберзлочинів щорічно вимірюються сотнями мільярдів доларів, а прогнозні тенденції свідчать про подальше зростання цієї цифри (Bartoli, 2024).

Кіберзлочинність має транснаціональний характер. Злочини, скоєні у віртуальному просторі, часто здійснюються групами, що діють із території різних держав, а потерпілі можуть перебувати в будь-якій точці світу. Це зумовлює необхідність пошуку ефективних механізмів міжнародної співпраці, гармонізації національних законодавств і вироблення єдиних підходів до протидії кіберзлочинності[1].

Нормативно-правове регулювання є ключовим елементом у боротьбі з кіберзлочинністю. Саме правові інструменти визначають межі допустимих дій держави у сфері кібербезпеки, встановлюють кримінальну відповідальність за відповідні діяння та створюють умови для взаємодії між державними органами, бізнесом і громадянським суспільством. Без належної правової основи неможливо забезпечити ефективне функціонування механізмів виявлення, розслідування та попередження кіберзлочинів. Як зазначають В. Романюк і С. Абламський (2024), розбудова системи цифрової доказової бази вимагає чіткого правового регламентування процедур збору та використання електронних доказів, що є одним із наріжних каменів у сучасній практиці протидії кіберзлочинності.

На окрему увагу заслуговує міжнародний вимір правового регулювання. Найбільш відомим міжнародним документом у цій сфері є Конвенція Ради Європи про кіберзлочинність (так звана Будапештська конвенція, далі – Конвенція)[2], яка стала базовим орієнтиром для багатьох країн світу, зокрема й України. Подальший розвиток цього документа відображено в Додатковому протоколі до Конвенції 2003 року[3], спрямованому на криміналізацію діянь расистського та ксенофобського характеру, а також у Другому додатковому протоколі 2022 року[4], який удосконалив механізми міжнародного співробітництва у сфері електронних доказів. Вагомий внесок у формування європейських стандартів кібербезпеки зробили такі акти Європейського Союзу, як Директива 2013/40/ЄС про атаки на інформаційні системи[5] та Директива (ЄС) 2022/2555 (NIS2 Directive)[6], що визначають межі захисту критичної інформаційної інфраструктури та взаємодії між державами-членами. На рівні національного законодавства на розвиток трансатлантичної співпраці у

1 Understanding cybercrime: Phenomena, challenges and legal response. September 2012 // ITU : сайт. https://www.itu.int/ITU-D/cyb/Cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (дата звернення: 15.10.2025).

2 Convention on Cybercrime. ETS No. 185. Budapest, 23.XI.2001 // Council of Europe : офіц. сайт. URL: https://rm.coe.int/1680081561 (дата звернення: 15.10.2025).

3 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. ETS No. 189. Strasbourg, 28.I. 2003 // Council of Europe : офіц. сайт. URL: https://rm.coe.int/168008160f (дата звернення: 15.10.2025).

4 Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. ETS No. 224. Strasbourg, 12.V.2022 // Council of Europe : офіц. сайт. URL: https://rm.coe.int/1680a49dab (дата звернення: 15.10.2025).

5 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // EUR-Lex : офіц. сайт. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj (дата звернення: 15.10.2025).

6 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) // EUR-Lex : офіц. сайт. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 15.10.2025).

сфері кібербезпеки суттєво вплинув Закон про уточнення законного використання даних за межами Сполучених Штатів (CLOUD Act)[1] 2018 року, який регулює доступ до електронних даних, що розміщені за межами юрисдикції конкретної держави.

Україна, перебуваючи на етапі активної цифрової трансформації, стикається з низкою викликів, пов'язаних із забезпеченням кібербезпеки. Наявність постійних кіберзагроз, зокрема з боку держав-агресорів, робить питання адаптації міжнародного досвіду та вдосконалення національної правової бази вкрай актуальним. Особливої гостроти ця проблема набула після початку повномасштабного вторгнення російської федерації 24 лютого 2022 року. Кібератаки стали невід'ємною частиною збройної агресії, яка спрямована на дестабілізацію роботи органів державної влади, об'єктів критичної інфраструктури, фінансового сектору та медіа. Масове використання шкідливого програмного забезпечення, фішингових кампаній і деструктивних дій у кіберпросторі підтвердило, що інформаційна та кібербезпека є одним із ключових напрямів національної безпеки.

У цих умовах питання вдосконалення правових механізмів протидії кіберзлочинності та посилення міжнародного співробітництва для України стало не лише науково-теоретичним, а й життєво важливим. Таким чином, дослідження міжнародних моделей правового регулювання протидії кіберзлочинності та визначення можливостей їх упровадження в Україні є надзвичайно актуальним завданням сучасної юридичної науки і практики. Наше дослідження спрямоване на пошук оптимальних підходів до формування такої системи нормативно-правових засад, яка б одночасно відповідала національним інтересам і забезпечувала інтеграцію у світовий правовий простір.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є аналіз міжнародних моделей нормативно-правового регулювання протидії кіберзлочинності та визначення можливостей їх адаптації в українському правовому полі з урахуванням сучасних безпекових викликів.

Для досягнення цієї мети необхідно вирішити такі *завдання*:

1) визначити основні універсальні та регіональні міжнародні документи у сфері протидії кіберзлочинності;

2) охарактеризувати ключові підходи ЄС, США й інших провідних держав до правового забезпечення кібербезпеки;

3) проаналізувати участь України в міжнародних ініціативах і угодах у сфері кібербезпеки та протидії кіберзлочинності;

4) виявити проблемні аспекти імплементації міжнародних норм у національне законодавство;

5) сформулювати рекомендації щодо вдосконалення правових механізмів протидії кіберзлочинності в Україні на основі кращих світових практик.

ОГЛЯД ЛІТЕРАТУРИ. Проблематика протидії кіберзлочинності вже тривалий час перебуває в центрі наукових досліджень як в Україні, так і за кордоном. Вітчизняні науковці наголошують, що розвиток цифрових технологій призвів до появи нових форм злочинної діяльності, які вимагають належного правового реагування. Як наголошують О. Пунда та співавтори (2023), ефективна протидія кіберзлочинності в Україні залежить від організаційної спроможності кіберполіції та її здатності до міжнародної взаємодії, зокрема в умовах воєнного часу.

У міжнародних дослідженнях увага зосереджена на необхідності гармонізації законодавства та створення узгоджених процедур для розслідування кіберзлочинів. На думку Ф. Спізія (2022), прийняття Другого додаткового протоколу до Конвенції стало важливим кроком у посиленні транскордонного обміну електронними доказами та захисту потерпілих у кіберпросторі. Водночас А. Сашуліду (2024) зазначає, що запровадження нового пакета законодавчих актів ЄС щодо електронних доказів знаменує перехід до якісно нової парадигми судового співробітництва у цифровій сфері.

Питання узгодження процедур збору електронних доказів та їхнього використання у кримінальному процесі детально досліджує С. Тоша (2024), який звертає увагу на правові і технічні труднощі реалізації положень Другого додаткового протоколу до Конвенції. Він наголошує, що ефективність цих норм значною мірою залежить від рівня довіри між державами та здатності забезпечити захист персональних даних.

Проблема забезпечення прав людини в контексті міжнародних ініціатив із кібербезпеки розглядається у працях Т. Тропіної (2024), яка застерігає від надмірного розширення державного контролю під приводом кіберзахисту. Вона наголошує, що дотримання прав людини має залишатися фундаментальним принципом під час формування міжнародних угод у сфері цифрової безпеки.

[1] Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Public Law No. 115-141 // CONGRESS.GOV : офіц. сайт. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943 (дата звернення: 15.10.2025).

П. Г. К'яра (2024) акцентує увагу на формуванні права на кібербезпеку як окремого правового інституту в межах Європейського Союзу, що відображає нові тенденції у взаємодії між правом і технологіями. На його думку, поява такого права є логічним продовженням розвитку концепції «цифрових прав людини».

Значний внесок у розвиток теорії кіберстійкості зробили Й. Ріствей і співавтори (2025), які запропонували концептуальну модель реалізації стандартів Директиви (ЄС) 2022/2555 (NIS2) у державах – членах ЄС. Їхнє дослідження демонструє, що підвищення кіберстійкості вимагає інтегрованого підходу, який охоплює управління ризиками, реагування на інциденти та підготовку кадрів.

Еволюцію європейської нормативної бази розглядає Н. Вандезанде (2024), який зазначає, що Директива (ЄС) 2022/2555 (NIS2) стала важливим кроком до посилення єдиних стандартів захисту критичної інфраструктури та створення спільного простору кібербезпеки в Європі.

Як узагальнює Т. Тропіна (2024), ефективна система протидії кіберзлочинності має базуватися на поєднанні правових, організаційних і технологічних інструментів, а також на партнерстві між державним та приватним сектором. Проведений аналіз наукових джерел свідчить, що гармонізація національних законодавств і посилення міжнародного співробітництва є ключовими умовами забезпечення кібербезпеки.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологічною основою дослідження є комплекс наукових підходів і методів, які дозволили здійснити системний аналіз міжнародних моделей правового регулювання протидії кіберзлочинності та визначити можливості їх упровадження в Україні.

По-перше, застосовано загальнонаукові методи аналізу та синтезу, за допомогою яких досліджено сутність і зміст правових механізмів протидії кіберзлочинності в міжнародному та національному вимірах. Метод індукції дозволив узагальнити окремі приклади регіональних і національних правових систем, тоді як дедукція сприяла формулюванню загальних висновків щодо тенденцій розвитку міжнародного правового регулювання в цій сфері.

По-друге, використано системний підхід, що дозволив розглядати правове забезпечення кібербезпеки як багатокомпонентне явище, в якому взаємодіють міжнародні норми, національні законодавства та практика їх застосування. Це дало змогу виявити як сильні сторони сучасних моделей, так і проблемні аспекти їх реалізації.

По-третє, застосовано порівняльно-правовий метод, який дав змогу дослідити особливості регулювання кіберзлочинності в різних правових системах світу. Порівняння підходів Європейського Союзу, США та інших держав дозволило виокремити універсальні елементи, що можуть бути адаптовані до українського законодавства.

По-четверте, використано метод аналізу нормативно-правових актів і міжнародних договорів, що дало можливість визначити основні універсальні та регіональні документи у сфері протидії кіберзлочинності, а також простежити їхній вплив на формування національних правових систем, зокрема правової системи України.

Крім того, застосовано історико-правовий метод, завдяки якому простежено еволюцію міжнародних підходів до протидії кіберзлочинності – від перших спроб міжнародного правового врегулювання до сучасних ініціатив, включаючи додаткові протоколи до Конвенції.

Значну увагу приділено також методу узагальнення наукових досліджень, що дозволило інтегрувати здобутки зарубіжної та української науки у сфері кібербезпеки і виявити білі плями, які потребують подальшого дослідження.

Таким чином, комплексне поєднання зазначених методів забезпечило об'єктивність, повноту і достовірність отриманих результатів, а також дозволило розробити практичні рекомендації щодо вдосконалення українського законодавства у сфері протидії кіберзлочинності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ

1. Міжнародні універсальні підходи до боротьби з кіберзлочинністю

Розвиток глобального цифрового простору зумовив потребу у виробленні єдиних міжнародних стандартів. Сьогодні універсальні підходи формуються переважно в межах Ради Європи й ООН, що стало основою для більшості національних законодавств у цій сфері.

Найважливішим і найбільш визнаним міжнародним інструментом є Конвенція Ради Європи про кіберзлочинність 2001 року, відома як Будапештська конвенція. Це перший міжнародний договір, який комплексно врегулював питання криміналізації діянь, пов'язаних із використанням інформаційних технологій. Конвенція встановила уніфіковані підходи до визначення складів злочинів: незаконного доступу до комп'ютерних систем, перехоплення даних, втручання в роботу мереж, поширення шкідливого програмного забезпечення, комп'ютерного шахрайства тощо.

Особливе значення має те, що документ не лише формує матеріально-правову базу, а й містить процесуальні положення: вимоги щодо збереження даних, доступу до трафіку, вилучення інформації та співпраці компетентних органів різних держав у сфері розслідування кіберзлочинів.

Конвенція стала еталоном для національних законодавств: більшість її положень імплементовані у кримінальні кодекси країн-учасниць, включаючи Україну. При цьому Конвенція відкрита для приєднання не лише для членів Ради Європи, а й для будь-якої держави світу, що значно підвищує її універсальність.

Подальший розвиток цього міжнародного інструмента знайшов відображення у двох додаткових протоколах. Перший додатковий протокол 2003 року зосереджений на криміналізації діянь, пов'язаних із поширенням через комп'ютерні системи матеріалів расистського та ксенофобського характеру. Цей документ розширив сферу дії Конвенції, врахувавши нові загрози, що поширилися в цифровому середовищі.

Новітнім етапом став Другий додатковий протокол до Конвенції, ухвалений у 2022 році. Він суттєво посилює можливості транскордонної співпраці у сфері кримінального переслідування кіберзлочинців. Особливу увагу в ньому приділено процедурі доступу до електронних доказів, що часто зберігаються на серверах за межами юрисдикції конкретної держави. Протокол передбачає нові механізми взаємодії між правоохоронними органами, включаючи прямі запити про надання інформації постачальникам послуг, що є критично важливим у сучасному середовищі хмарних технологій. Таким чином, документ адаптує міжнародне співробітництво до реалій цифрової епохи.

Не менш важливим чинником у формуванні універсальних підходів є діяльність Організації Об'єднаних Націй. Упродовж останніх двох десятиліть Генеральна Асамблея та спеціалізовані робочі групи ухвалили низку резолюцій, присвячених питанням безпеки у кіберпросторі. Хоча більшість цих документів має рекомендаційний характер, вони відображають глобальний консенсус щодо необхідності вироблення правил поведінки держав у цифровому середовищі. На особливу увагу заслуговує діяльність Групи урядових експертів ООН і Відкритої робочої групи з питань розробки глобальної конвенції про кіберзлочинність (Hakmeh, 2024). Нині триває активна дискусія щодо створення нового універсального договору під егідою ООН, який би доповнив або навіть частково замінив чинні міжнародні акти.

Універсальні підходи, вироблені на рівні Ради Європи й ООН, мають не лише юридичне, а й політичне значення. Вони забезпечують єдність у визначенні базових категорій кіберзлочинів, формують механізми міжнародної правової допомоги та задають стандарти для розроблення національних законодавств. Для України, яка є учасницею Конвенції та бере участь у роботі ООН у сфері кібербезпеки, ці документи створюють правову основу для протидії кіберзлочинності.

Особливої актуальності універсальні інструменти набули після 24 лютого 2022 року, коли кіберзагрози стали невід'ємною частиною повномасштабної збройної агресії проти України. Участь у міжнародних ініціативах дозволяє нашій державі отримувати доступ до сучасних механізмів обміну інформацією та правової допомоги, що має критичне значення в умовах кібервоєн нового покоління.

Таким чином, універсальні підходи у сфері протидії кіберзлочинності створюють фундамент для побудови глобальної системи кібербезпеки. Їхнє значення полягає в поєднанні обов'язкових норм міжнародного права та рекомендаційних актів, які разом формують багаторівневу правову основу для боротьби з кіберзлочинністю. Для України ці інструменти мають не лише теоретичну, а й практичну вагу, оскільки визначають вектор інтеграції у світовий правовий простір та сприяють підвищенню стійкості до кіберзагроз.

2. Регіональні моделі боротьби з кіберзлочинністю

Поряд з універсальними міжнародними підходами важливу роль у боротьбі з кіберзлочинністю відіграють регіональні системи правового регулювання, які враховують особливості правових традицій, рівень розвитку інформаційних технологій і стратегічні пріоритети держав певного регіону. Найбільш показовими прикладами є моделі, сформовані в межах ЄС, США, а також окремих регіональних об'єднань в Азії та в межах НАТО.

2.1. Європейський Союз

У межах ЄС боротьба з кіберзлочинністю інтегрована в ширший контекст забезпечення кібербезпеки. Важливим етапом стало ухвалення Директиви 2013/40/ЄС про атаки на інформаційні системи, яка гармонізувала криміналізацію низки кіберзлочинів у державах-членах. Директива зобов'язала країни ЄС забезпечити ефективні санкції за незаконний доступ до систем, втручання в роботу мереж, перехоплення даних та використання шкідливого програмного забезпечення.

Подальший розвиток цієї політики відбувався через упровадження Директиви (ЄС) 2022/2555 (NIS2). Цей документ визначає вимоги до захисту критичної інфраструктури та зобов'язує держави-члени створювати національні органи кібербезпеки, а також забезпечувати взаємодію на європейському рівні. Як зазначають А. Ющак та Е. Сасон (2023), прийняття пакету законів ЄС щодо електронних доказів (*e-evidence*) стало фундаментальним кроком до створення спільного європейського правового простору у сфері кримінальної юстиції.

Крім того, в межах Директиви (ЄС) 2022/2555 (NIS2) посилюється роль Агентства ЄС з кібербезпеки (ENISA), яке координує обмін інформацією та розроблення стандартів. На думку Г. Кучинської (2024), імплементація цих положень у національні правові системи, зокрема в Польщі, продемонструвала потребу в системному оновленні підходів до управління кіберризиками та правового статусу електронних доказів.

Важливим чинником у діяльності ЄС є також Європол, у структурі якого функціонує Європейський центр кіберзлочинності (EC3). Цей центр координує міжнародні розслідування, надає аналітичну підтримку та сприяє обміну електронними доказами між правоохоронними органами країн-членів. Як наголошує С. Шміц-Берндт (2023), одним із викликів у реалізації положень Директиви (ЄС) 2022/2555 (NIS2) є визначення чітких критеріїв повідомлення про кіберінциденти, що суттєво впливає на правозастосовну практику в державах – членах ЄС.

2.2. Сполучені Штати Америки

У Сполучених Штатах Америки боротьба з кіберзлочинністю розглядається як складова національної безпеки. Основу правового регулювання становить Закон про комп'ютерне шахрайство і зловживання (CFAA, 1986)[1], який визначає кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем, викрадення інформації та пошкодження даних. Подальший розвиток законодавства відбувся завдяки ухваленню низки актів, зокрема Закону про об'єднання та зміцнення Америки шляхом надання відповідних інструментів, необхідних для перехоплення та протидії тероризму (USA PATRIOT Act, 2001)[2], що розширив повноваження правоохоронних органів у сфері електронного спостереження, та Закону про уточнення законного використання даних за межами Сполучених Штатів (CLOUD Act, 2018), який встановив нові механізми доступу до даних, що зберігаються за кордоном.

Важливу роль відіграють також інституційні механізми. Чільне місце в розслідуванні кіберзлочинів посідає Федеральне бюро розслідувань, у складі якого діє відділ з кіберзлочинності. Крім цього, до боротьби з кіберзагрозами залучений Департамент внутрішньої безпеки США, який координує діяльність різних відомств і приватного сектору. У структурі Департаменту внутрішньої безпеки США функціонує Агентство з кібербезпеки та інфраструктурної безпеки, що здійснює моніторинг загроз і надає рекомендації для захисту критичних об'єктів.

Американська модель акцентує увагу на партнерстві із приватним сектором, оскільки більшість інфраструктури належить комерційним компаніям. Тому США активно впроваджують програми обміну інформацією про загрози між державними та приватними структурами, що забезпечує оперативне реагування на кібератаки.

2.3. Інші регіональні приклади

У країнах Азії також активно формується власна правова база. Наприклад, Сінгапур ухвалив Закон про кібербезпеку (Cybersecurity Act, 2018)[3], який встановив вимоги до операторів критичної інформаційної інфраструктури та передбачив повноваження національного агентства у сфері кіберзахисту. Японія ще у 2014 році створила Національний центр реагування на інциденти в галузі комп'ютерної безпеки (NISC), що координує дії уряду та бізнесу. Китай має власну комплексну модель, в основі якої лежить Закон про кібербезпеку Китайської Народної Республіки (2017)[4], що

[1] Computer Fraud and Abuse Act (CFAA), Public Law No. 99-474 // CONGRESS.GOV : офіц. сайт. URL: https://www.congress.gov/bill/99th-congress/house-bill/4718/text (дата звернення: 15.10.2025).

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law No. 107-56 // CONGRESS.GOV : офіц. сайт. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm (дата звернення: 15.10.2025).

[3] Cybersecurity Act 2018 (No. 9 of 2018) // Singapore Statuses Online : офіц. сайт. URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/ (дата звернення: 15.10.2025).

[4] 2016 Cybersecurity Law : adopted on 7 November 2016 // China Law Translate : сайт. URL: https://www.chinalawtranslate.com/en/2016-cybersecurity-law/#gsc.tab=0 (дата звернення: 15.10.2025).

поєднує суворе державне регулювання з розвитком національної індустрії кіберзахисту.

Особливу увагу заслуговують ініціативи НАТО. У 2008 році Альянс визнав кіберпростір окремим операційним середовищем, а у 2014 році було створено Центр передового досвіду з кібероборони в Таллінні (CCDCOE), який розробляє стратегії, проводить навчання та моделює сценарії кіберконфліктів. Альянс послідовно підтримує партнерів, зокрема Україну, у зміцненні їхньої кіберстійкості. У цьому контексті, як зазначають С. Снейл ка Мтузе та М. Мусоні (2023), розвиток регіонального співробітництва на кшталт африканської моделі правового регулювання кібербезпеки може слугувати прикладом для адаптації локальних правових систем до міжнародних стандартів.

Регіональні моделі демонструють різноманітність підходів до боротьби з кіберзлочинністю. Європейський Союз робить акцент на гармонізації законодавства та створенні єдиних стандартів для держав-членів; США – на криміналізації та посиленні повноважень правоохоронних органів у поєднанні з партнерством із приватним сектором; країни Азії – на поєднанні державного контролю з розвитком інституційної спроможності; НАТО – на колективній обороні та спільних практиках реагування.

Для України вивчення цих моделей має особливе значення, адже вони демонструють різні інструменти і механізми, що можуть бути адаптовані у вітчизняному правовому полі для підвищення ефективності протидії кіберзлочинності.

3. Україна в міжнародному правовому полі

Україна є активним учасником міжнародних ініціатив у сфері протидії кіберзлочинності та кібербезпеки. Вступивши до Конвенції у 2006 році, наша держава фактично інтегрувалася у глобальну систему боротьби з кіберзлочинністю. Це зобов'язало Україну гармонізувати національне кримінальне законодавство з положеннями Конвенції та забезпечити механізми міжнародного співробітництва. Зокрема, у Кримінальному кодексі України були закріплені склади злочинів, аналогічні передбаченим у Конвенції, що дозволило створити базові умови для взаємодії з іншими державами.

Участь у Конвенції надала українським правоохоронним органам можливість отримувати міжнародну правову допомогу в розслідуванні кіберзлочинів і долучатися до глобальних механізмів обміну електронними доказами. Це набуло особливого значення після ухвалення Другого додаткового протоколу 2022 року до Конвенції, який спрощує доступ до цифрових даних, розташованих за межами національної юрисдикції.

Важливим напрямом міжнародної діяльності України є співпраця з ЄС. У межах Угоди про асоціацію між Україною та ЄС передбачено гармонізацію українського законодавства у сфері кібербезпеки та захисту інформаційних систем з європейськими нормами. Україна бере участь у програмах ЄС з кібербезпеки, зокрема CyberEast, яка спрямована на розвиток потенціалу правоохоронних органів у країнах Східного партнерства. У межах цієї співпраці здійснюється підготовка кадрів, удосконалення нормативної бази та створення механізмів реагування на кіберінциденти.

Вагому роль відіграє і взаємодія з НАТО. Україна з 2014 року отримує підтримку від Альянсу у сфері кібербезпеки, а після 2022 року ця співпраця істотно активізувалася. У межах Трастового фонду НАТО з кібербезпеки надано технічну допомогу, обладнання, а також проведено низку спільних навчань для українських фахівців. Партнерство із Центром передового досвіду з кібероборони в Таллінні дало змогу інтегрувати українських експертів у міжнародні дослідницькі проєкти та практику відпрацювання сценаріїв кіберконфліктів.

Не менш важливим є співробітництво України з Організацією Об'єднаних Націй. Наша держава бере активну участь у засіданнях Відкритої робочої групи ООН з розробки глобальної конвенції про кіберзлочинність, що спирається на Резолюцію 77/194 (2022)[1]. Україна послідовно відстоює позицію щодо необхідності створення універсального інструмента, який не лише враховуватиме специфіку сучасних кіберзагроз, а й забезпечуватиме ефективну правову допомогу між державами. Участь України у глобальних форумах з кібербезпеки сприяє її інтеграції у міжнародні структури цифрової безпеки[2].

Варто наголосити, що після початку повномасштабної збройної агресії російської федерації 24 лютого 2022 року питання кібербезпеки для України набуло виняткової актуальності. Кібератаки стали одним з основних інструментів

[1] Resolution adopted by the General Assembly on 15 December 2022 (A/RES/77/194) // United Nations : офіц. сайт. URL: https://undocs.org/en/A/RES/77/194 (дата звернення: 15.10.2025).

[2] Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816) // United Nations : офіц. сайт. URL: https://docs.un.org/en/A/75/816 (дата звернення: 15.10.2025).

гібридної війни. Вони спрямовані проти державних інформаційних систем, об'єктів критичної інфраструктури, фінансового сектору та медіа. У цих умовах міжнародне співробітництво дозволяє не лише підвищити стійкість до атак, а й забезпечує політичну підтримку з боку партнерів.

Водночас Україна стикається з низкою проблем. Попри приєднання до Конвенції та тісну співпрацю з ЄС і НАТО, національне законодавство потребує подальшого вдосконалення. Зокрема, існують колізії у визначенні окремих складів кіберзлочинів, недостатньо врегульовані процедури збирання та використання електронних доказів, а також є проблеми з імплементацією директив ЄС. Актуальним також залишається питання кадрового і технічного забезпечення підрозділів кіберполіції та інших органів, відповідальних за боротьбу з кіберзлочинністю.

Таким чином, Україна є частиною глобальної та регіональної системи протидії кіберзлочинності, активно співпрацює з міжнародними організаціями і партнерами. Однак ефективність цієї співпраці значною мірою залежить від здатності держави адаптувати міжнародні стандарти до власних умов, а також від подальшого вдосконалення національної правової бази й інституційної спроможності.

4. Проблеми та виклики для України

Попри активний розвиток міжнародного правового регулювання та участь України у ключових міжнародних і регіональних ініціативах, залишається низка проблем і викликів, які обмежують ефективність протидії кіберзлочинності. Вони мають як глобальний, так і національний характер.

4.1. Глобальні проблеми

Насамперед слід відмітити відсутність єдиного універсального міжнародного договору, який охоплював би всі аспекти кіберзлочинності. Хоча Конвенція є найбільш визнаним документом у цій сфері, частина держав, зокрема Китай, російська федерація та низка країн, що розвиваються, не приєдналися до неї, поставивши під сумнів її універсальність. Це створює правові бар'єри для міжнародного співробітництва, оскільки держави часто керуються різними підходами до визначення складів кіберзлочинів і процедур обміну інформацією.

Іншою глобальною проблемою є транскордонний характер кіберзлочинів. Злочини, пов'язані з використанням інформаційних технологій, майже завжди виходять за межі однієї юрисдикції, що потребує швидкого обміну електронними доказами й ефективної взаємодії між правоохоронними органами. Проте чинні механізми міжнародної правової допомоги часто є занадто повільними та бюрократичними, що ускладнює оперативне реагування на кіберзагрози.

Ще одним викликом є баланс між безпекою та правами людини. Розширення повноважень державних органів у сфері доступу до даних та електронного спостереження викликає занепокоєння щодо можливих порушень права на приватність, свободу слова і захист персональної інформації. Це особливо актуально в умовах, коли держави ухвалюють закони, що передбачають масове зберігання та аналіз електронних даних.

4.2. Національні виклики для України

Для України, яка перебуває в умовах воєнного стану та стикається з безпрецедентним рівнем кіберзагроз, ці проблеми мають особливий характер. Одним із ключових викликів є неповна імплементація міжнародних стандартів у національне законодавство. Хоча більшість положень Конвенції вже знайшли відображення в українському праві, окремі питання залишаються неврегульованими або реалізовані частково. Це стосується, зокрема, процедур збирання та використання електронних доказів, а також співвідношення національних норм із положеннями директив ЄС.

Серйозною проблемою є кадровий і технічний дефіцит у підрозділах, відповідальних за боротьбу з кіберзлочинністю. Кіберполіція України та інші органи мають недостатнє фінансування, обмежений доступ до сучасних технологій і потребу в постійному підвищенні кваліфікації персоналу.

Додатковим викликом є інституційна координація. Попри створення низки органів, відповідальних за забезпечення кібербезпеки, існує проблема дублювання їхніх повноважень і недостатньо ефективної взаємодії між ними. Це знижує загальну ефективність системи протидії кіберзлочинності.

Важливою проблемою залишається масштабність і системність кібератак з боку російської федерації. Вони спрямовані на підрив державного управління, дестабілізацію критичної інфраструктури, поширення дезінформації та створення панічних настроїв у суспільстві. Протидія таким атакам вимагає не лише правових, а й технологічних та організаційних рішень, які виходять за межі традиційного кримінально-правового підходу.

Отже, головними проблемами сучасної системи протидії кіберзлочинності є фрагментарність міжнародного правового регулювання, складність транскордонної взаємодії,

виклики у сфері дотримання прав людини, а також внутрішні недоліки національної системи України, що посилюються в умовах збройної агресії. Подолання цих проблем потребує комплексних рішень, які мають включати вдосконалення законодавства, розвиток інституційної спроможності й активізацію міжнародної співпраці.

5. Рекомендації для України

Аналіз універсальних і регіональних моделей правового регулювання протидії кіберзлочинності дає змогу сформулювати низку висновків і рекомендацій, які мають практичне значення для України.

5.1. Гармонізація законодавства

Насамперед очевидною є необхідність подальшої гармонізації українського законодавства з міжнародними та європейськими стандартами. Конвенція та додаткові протоколи до неї, директиви ЄС і рекомендації міжнародних організацій мають стати орієнтирами для вдосконалення Кримінального кодексу України та кримінального процесуального законодавства. Особливу увагу слід приділити процедурі збирання, зберігання та використання електронних доказів, щоб забезпечити їхню допустимість у судових процесах.

5.2. Інституційна спроможність

Другою ключовою рекомендацією є посилення інституційної спроможності органів, що відповідають за кібербезпеку. Досвід ЄС і США показує, що ефективна протидія кіберзлочинності неможлива без належно підготовленого персоналу, сучасного технічного забезпечення та стабільного фінансування. Україні необхідно продовжувати інвестувати в розвиток кіберполіції, створення національних і галузевих центрів реагування на інциденти, а також підготовку кадрів.

5.3. Міжнародне співробітництво

Третьою рекомендацією є важливість поглиблення міжнародного співробітництва. Приклад співпраці в межах ЄС, НАТО й ООН доводить, що транскордонний характер кіберзлочинності вимагає колективних дій. Для України критично важливо зберігати активну участь у цих ініціативах, розширювати співпрацю у сфері обміну електронними доказами, брати участь у спільних розслідуваннях і тренінгах. Це не лише підвищить ефективність національної системи кібербезпеки, а й сприятиме політичній інтеграції в євроатлантичний простір.

5.4. Баланс безпеки та прав людини

Ще однією важливою рекомендацією є необхідність забезпечення балансу між захистом національної безпеки та дотриманням прав людини. Зарубіжний досвід свідчить, що надмірне розширення повноважень державних органів у сфері контролю за даними може призвести до порушення прав на приватність і свободу слова. Україна, прагнучи інтегруватися в європейську правову систему, має враховувати ці ризики та будувати систему кібербезпеки на засадах верховенства права і захисту прав людини.

5.5. Кіберстійкість у воєнних умовах

Особливого значення для України набуває рекомендація щодо формування кіберстійкості в умовах збройної агресії. Кібератаки, що стали складовою російської гібридної війни, вимагають комплексної відповіді, яка виходить за межі кримінально-правових заходів. Це вимагає поєднання правових, організаційних, технічних і дипломатичних інструментів. Україна має продовжувати розбудову системи національної кіберстійкості, інтегрованої з міжнародними структурами безпеки.

Таким чином, головні рекомендації для України можна звести до п’яти ключових напрямів: гармонізація законодавства, посилення інституційної спроможності, активізація міжнародного співробітництва, забезпечення балансу між безпекою та правами людини, а також розвиток кіберстійкості в умовах воєнних загроз. Їх реалізація сприятиме підвищенню ефективності протидії кіберзлочинності та зміцненню позицій України у глобальному кіберпросторі.

ВИСНОВКИ. Дослідження підтвердило, що боротьба з кіберзлочинністю є одним із ключових викликів сучасній системі міжнародної безпеки та правопорядку. Транснаціональний характер кіберзлочинів, їхня висока динаміка та постійне ускладнення способів їх учинення зумовлюють потребу в пошуку ефективних правових механізмів протидії на глобальному і національному рівнях.

Універсальні міжнародні підходи, сформовані Радою Європи й ООН, створили базову основу для уніфікації криміналізації кіберзлочинів і налагодження механізмів транскордонного співробітництва. Конвенція Ради Європи про кіберзлочинність і додаткові протоколи до неї залишаються основним правовим орієнтиром у цій сфері, у той час як ініціативи ООН відображають глобальний консенсус щодо необхідності міжнародної співпраці у протидії кіберзлочинності.

Регіональні моделі (ЄС, США, країни Азії, НАТО) продемонстрували різноманітні підходи до побудови систем кібербезпеки. Європейський Союз зосереджений на гармонізації законодавства та формуванні єдиних стандартів,

США – на кримінально-правовій відповідальності і партнерстві з приватним сектором, країни Азії – на поєднанні державного контролю з технологічним розвитком, країни НАТО – на колективній обороні та кіберстійкості. Порівняння цих моделей дає змогу виокремити найефективніші практики для адаптації в Україні.

Україна як учасниця Будапештської конвенції про кіберзлочинність та активний партнер ЄС, НАТО й ООН інтегрована у світову систему протидії кіберзлочинності. Водночас національне законодавство ще не повністю узгоджене з міжнародними стандартами, а кадрові і технічні ресурси у сфері кібербезпеки залишаються обмеженими. Ці виклики набули особливої гостроти після початку повномасштабної агресії російської федерації у 2022 році, коли кібератаки стали системною складовою гібридної війни проти України.

На основі проведеного аналізу можна сформулювати такі узагальнені висновки та рекомендації.

1. Необхідно продовжити гармонізацію кримінального та процесуального законодавства України з міжнародними стандартами, зокрема Будапештською конвенцією про кіберзлочинність і директивами ЄС.

2. Потрібно посилити інституційну спроможність органів кібербезпеки, зокрема через належне фінансування, технічне переоснащення та підвищення кваліфікації кадрів.

3. Необхідно розвивати міжнародне співробітництво в обміні електронними доказами, спільних розслідуваннях і навчаннях, активно використовуючи інструменти ЄС, НАТО й ООН.

4. Важливо забезпечити баланс між національною безпекою та правами людини, уникаючи надмірного розширення повноважень державних органів щодо контролю інформаційного простору.

5. Україна має створювати систему кіберстійкості, здатну ефективно протидіяти загрозам у воєнний час, поєднуючи правові, організаційні, технічні та дипломатичні інструменти.

Отже, досвід міжнародних і регіональних систем протидії кіберзлочинності може стати основою для вдосконалення національної моделі, що забезпечить інтеграцію України у глобальний правовий простір та підвищить її здатність протидіяти сучасним кіберзагрозам. Реалізація запропонованих заходів сприятиме зміцненню правопорядку, національної безпеки та стійкості держави в умовах гібридної війни.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право і безпека*. 2024. № 2 (93). С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13.

2. Bartoli L. Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*. 2024. Vol. 16, Iss. 2. Pp. 498–513. DOI: https://doi.org/10.1017/err.2025.31.

3. Chiara P. G. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*. 2024. Vol. 53. DOI: https://doi.org/10.1016/j.clsr.2024.105961.

4. Hakmeh J. The UN convention on cybercrime: a milestone in cybercrime cooperation? *Journal of Cyber Policy*. 2024. Vol. 9, Iss. 2. Pp. 125–130. DOI: https://doi.org/10.1080/23738871.2024.2441549.

5. Juszczak A., Sason E. The use of electronic evidence in the Area of Freedom, Security and Justice: An introduction to the new EU package on e-evidence. *EUCRIM*. 2023. Iss. 2. Pp. 182–200. DOI: https://doi.org/10.30709/eucrim-2023-014.

6. Kuczyńska H. The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change. *Studia Iuridica Lublinensia*. 2024. Vol. 33, No. 5. Pp. 9–28. DOI: https://doi.org/10.17951/sil.2024.33.5.125-153.

7. Punda O., Vavrynchuk M., Kohut O., Kravchuk S., Prysiazhniuk M. The Legal Status and Capabilities of Cyber Police in Ukraine: The Reasons for the Existence of Frauds with the Use of IT Technologies. *Pakistan Journal of Criminology*. 2023. Vol. 15, No. 2. Pp. 85–97.

8. Ristvej J., Tonhauser M., Chovanec D., Kubás J., Kollár B., Zamiar Z. Cyber resilience conceptual model for the European Union NIS2 standards implementation in Slovakia. *Scientific Reports*. 2025. Vol. 15. DOI: https://doi.org/10.1038/s41598-025-12829-3.

9. Sachoulidou A. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation. *New Journal of European Criminal Law*. 2024. Vol. 15, Iss. 3. Pp. 256–274. DOI: https://doi.org/10.1177/20322844241258649.

10. Schmitz-Berndt S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*. 2023. Vol. 9, Iss. 1. DOI: https://doi.org/10.1093/cybsec/tyad009.

11. Snail ka Mtuze S., Musoni M. An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*. 2023. Vol. 4. Pp. 299–232. DOI: https://doi.org/10.1365/s43439-023-00089-8.

12. Spiezia F. International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum*. 2022. Vol. 23. Pp. 101–108. DOI: https://doi.org/10.1007/s12027-022-00707-8.

13. Tosza S. Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems. *Studia Iuridica Lublinensia*. 2024. Vol. 33, No. 5. Pp. 237–252. DOI: https://doi.org/10.17951/sil.2024.33.5.237-260.

14. Tropina T. "This is not a human rights convention!": The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*. 2024. Vol. 9, Iss. 2. Pp. 200–220. DOI: https://doi.org/10.1080/23738871.2024.2419517.

15. Vandezande N. Cybersecurity in the EU: How the NIS2 – directive stacks up against its predecessor. *Computer Law & Security Review*. 2024. Vol. 52. DOI: https://doi.org/10.1016/j.clsr.2023.105890.

Надійшла до редакції: 20.10.2025

Прийнята до опублікування: 10.12.2025

REFERENCES

1. Bartoli, L. (2024). Cybersecurity and the Fight against Cybercrime: Partners or Competitors? *European Journal of Risk Regulation*, *16*(2), 498–513. https://doi.org/10.1017/err.2025.31.

2. Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, *53*. https://doi.org/10.1016/j.clsr.2024.105961.

3. Hakmeh, J. (2024). The UN convention on cybercrime: a milestone in cybercrime cooperation? *Journal of Cyber Policy*, *9*(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549.

4. Juszczak, A., & Sason, E. (2023). The use of electronic evidence in the Area of Freedom, Security and Justice: An introduction to the new EU package on e-evidence. *EUCRIM*, *2*, 182–200. https://doi.org/10.30709/eucrim-2023-014.

5. Kuczyńska, H. (2024). The EU E-evidence Package from the Polish Perspective: High Time for a Systemic Change. *Studia Iuridica Lublinensia*, *33*(5), 9–28. https://doi.org/10.17951/sil.2024.33.5.125-153.

6. Punda, O., Vavrynchuk, M., Kohut, O., Kravchuk, S., & Prysiazhniuk, M. (2023). The Legal Status and Capabilities of Cyber Police in Ukraine: The Reasons for the Existence of Frauds with the Use of IT Technologies. *Pakistan Journal of Criminology*, *15*(2), 85–97.

7. Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B., & Zamiar, Z. (2025). Cyber resilience conceptual model for the European Union NIS2 standards implementation in Slovakia. *Scientific Reports*, *15*. https://doi.org/10.1038/s41598-025-12829-3.

8. Romaniuk, V. V., & Ablamskyi, S. Ye. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*, *2*(93), 140–150. https://doi.org/10.32631/pb.2024.2.13.

9. Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation. *New Journal of European Criminal Law*, *15*(3), 256–274. https://doi.org/10.1177/20322844241258649.

10. Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad009.

11. Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*, 299–232. https://doi.org/10.1365/s43439-023-00089-8.

12. Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. *ERA Forum*, *23*, 101–108. https://doi.org/10.1007/s12027-022-00707-8.

13. Tosza, S. (2024). Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems. *Studia Iuridica Lublinensia*, *33*(5), 237–252. https://doi.org/10.17951/sil.2024.33.5.237-260.

14. Tropina, T. (2024). "This is not a human rights convention!": The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*, *9*(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517.

15. Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2 – directive stacks up against its predecessor. *Computer Law & Security Review*, *52*. https://doi.org/10.1016/j.clsr.2023.105890.

Received the editorial office: 20 October 2025

Accepted for publication: 12 December 2025

MYKOLA VOLODYMYROVYCH MORDVYNTSEV,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 4,
Research Laboratory on the Problems of Information Technologies and Combating Crime in Cyberspace;
ORCID: https://orcid.org/0000-0002-7674-3164,
e-mail: lukoly@ukr.net;

DMYTRO VALENTYNOVYCH PASHNIEV,
Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 4,
Research Laboratory on the Problems of Information Technologies and Combating Crime in Cyberspace;
ORCID: https://orcid.org/0000-0001-8693-3802,
e-mail: dvpashnev@gmail.com;

OLEKSII VOLODYMYROVYCH KHLIESTKOV,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 4,
Research Laboratory on the Problems of Information Technologies and Combating Crime in Cyberspace;
ORCID: https://orcid.org/0000-0001-8777-8269,
e-mail: Khliestkov.Oleksii@univd.edu.ua

INTERNATIONAL MODELS OF LEGAL REGULATION FOR COMBATING CYBERCRIME: RECOMMENDATIONS FOR UKRAINE

This article provides a comprehensive analysis of international models of legal regulation for combating cybercrime, identifying their key elements, development trends, and possibilities for implementation in Ukrainian legislation. It reveals universal approaches developed within the Council of Europe and the UN, as well as regional models of the European Union, the United States of America, Asian countries and NATO. Particular attention is paid to the 2001 Council of Europe Convention on Cybercrime, its additional protocols and modern mechanisms of international cooperation. It is demonstrated that the Convention has become a fundamental document in the field of unifying legal approaches to the criminalisation of acts related to the use of information technologies and has created a basis for the cross-border exchange of electronic evidence.

The aim of the study is to summarise international experience in combating cybercrime and to develop recommendations for its adaptation in Ukraine. The methodological basis is based on systematic, comparative legal, historical legal and analytical methods, which made it possible to identify patterns in the formation of modern cybersecurity models. Regulatory and legal acts, international treaties, scientific works and practical initiatives of states in the field of cyber defence are analysed.

Ukraine's participation in international programmes and projects aimed at developing cyber resilience, in particular within the framework of cooperation with the European Union, NATO and the UN, is highlighted. The need to harmonise Ukrainian legislation with international standards, improve procedures for the collection and use of electronic evidence, and strengthen the institutional capacity of law enforcement agencies is substantiated. It is emphasised that after the start of the full-scale invasion by the Russian Federation on 24 February 2022, cybercrime has become one of the key instruments of hybrid warfare against Ukraine.

The scientific novelty lies in identifying the prospects for the development of a national system to combat cybercrime based on international practices. The results obtained are of practical importance for improving legal regulation, strengthening international cooperation, and ensuring the cyber resilience of the state in the face of modern threats. The proposed conclusions can be used to develop a national cybersecurity strategy and improve the effectiveness of interagency cooperation in the field of combating cybercrime.

Keywords: *cybercrime, cybersecurity, Budapest Convention, international cooperation, legal regulation, hybrid warfare, cyber defence, Ukraine.*

Цитування (ДСТУ 8302:2015): Мордвинцев М. В., Пашнєв Д. В., Хлєстков О. В. Міжнародні моделі правового регулювання протидії кіберзлочинності: рекомендації для України. *Право і безпека*. 2025. № 4 (99). С. 59–71. DOI: https://doi.org/10.32631/pb.2025.4.05.

Citation (APA): Mordvyntsev, M. V., Pashniev, D. V., & Khliestkov, O. V. (2025). International Models of Legal Regulation for Combating Cybercrime: Recommendations for Ukraine. *Law and Safety, 4*(99), 59–71. https://doi.org/10.32631/pb.2025.4.05.