DOI https://doi.org/10.30525/978-9934-26-686-7-15

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В ПРОЦЕСІ РОЗСЛІДУВАННЯ

Сироїд. Т. Л.

ВСТУП

Кіберзлочинність – це глобальне явище, що стосується всіх держав, і воно так само безмежне, як і сам Інтернет. Поверхня атаки продовжує зростати в міру того, як суспільство стає більш цифровим, і все більше громадян, підприємств, державних служб і пристроїв підключаються до Інтернету.

Складні злочинні мережі діють у всьому світі, координуючи складні атаки за лічені хвилини. Держави та їх правоохоронні органи повинні йти в ногу з новими технологіями, розуміти можливості, які вони відкривають для злочинців, і те, як їх можна використовувати в якості інструментів для боротьби з кіберзлочинністю[1].

Згідно з оцінкою загроз організованої злочинності в Інтернеті (IOCTA), кіберзлочинність стає все більш агресивною та конфронтаційною. Це можна побачити в різних формах кіберзлочинності, включаючи злочини у сфері високих технологій, витік даних та сексуальне насильство.

Кіберзлочинністю є будь-яка злочинна активність у віртуальному просторі (кіберпросторі). У деяких кіберзлочинах здійснюються прямі атаки на комп'ютери або інші пристрої для виведення їх з ладу. В інших кіберзлочинах комп'ютери використовуються правопорушниками для поширення шкідливих програмних кодів, отримання незаконної інформації, розкрадання особистих даних з метою шахрайства. Отже, кіберзлочини – це злочини, вчинені в кіберпросторі (з використанням мережі Інтернет чи іншої комп'ютерної мережі), як компонент злочину. Широкий спектр можливостей, які намагаються використати кіберзлочинці, вражає. До таких злочинів належать: використання ботнетів – мереж пристроїв, заражених шкідливими програмами без відома їх користувачів – для передачі вірусів, які незаконно отримують віддалений контроль над пристроями, крадуть паролі та відключають антивірусний захист; створення «чорних ходів» на скомпрометованих пристроях для крадіжки грошей та даних або віддалений доступ до пристроїв для створення ботнетів; створення онлайн-форумів обміну хакерським досвідом; абузостійкий хостинг та створення противірусних сервісів; відмивання традиційних та віртуальних валют; здійснення онлайн-шахрайства, наприклад через системи онлайн-платежів, кардинг та соціальну інженерію; різні форми сексуальної експлуатації дітей в Інтернеті, включаючи поширення в Інтернеті матеріалів про сексуальне насильство над дітьми та прямі трансляції такого насильства; онлайн-хостинг

[1] Cybercrime. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 20.02.2026).

операцій з продажу зброї, фальшивих паспортів, підроблених та клонованих кредитних карток, наркотиків, а також хакерські послуги.[2]

Встановлення ефективних норм, що регулюють поведінку в місці, яке всі відвідують, але яке нікому не належить, – дуже важке завдання. Однак наявність норм необхідна для забезпечення максимального рівня свободи і зниження ризиків, пов'язаних з перебуванням у кіберпросторі. Враховуючи ту обставину, що технології розвиваються швидше, ніж норми, що регулюють їх застосування, необхідно постійно знаходити шляхи вирішення нових завдань, частіше пов'язаних із такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних і обмін інформацією між державами-членами та приватними структурами.

1. Міжнародно-правова основа протидії кіберзлочинності

Питання правового регулювання інформаційного простору, захисту осіб у кіберпросторі, протидії злочинам, які вчиняються з використанням можливостей кіберпростору тощо є обговорюваними як на універсальному, так і на регіональному міжнародному рівнях. Зокрема, у межах Організації Об'єднаних Націй (далі – ООН, Організація) вони є центром уваги головних органів організації, інституцій, спеціалізованих структур, установ, форумів, які діють під її егідою (Генеральна Асамблея, Економічна і Соціальна Рада, Комісія із запобігання злочинності і кримінального правосуддя, Конгреси ООН із запобігання злочинності і кримінального правосуддя, Міжнародний союз електрозв'язку (МСЕ), Організація Об'єднаних Націй із питань освіти, науки і культури (ЮНЕСКО), Конференція ООН із торгівлі і розвитку (ЮНКТАД), Програма розвитку Організації Об'єднаних Націй (ПРООН), Управління ООН із наркотиків і злочинності (ЮНОДК), Міжнародна організація кримінальної поліції (Інтерпол) тощо, які акцентують увагу на тому, що кіберзлочинність є одним із нових політичних питань у сфері запобігання злочинності і кримінального правосуддя, яке потребує розроблення шляхів і засобів його вирішення.

Слід зазначити, що ООН ще в 1994 році опублікувала Керівництво із запобігання злочинності, пов'язаної із застосуванням комп'ютерів, і боротьби з нею, в якому зазначалось, що «потенційна сфера охоплення комп'ютерної злочинності така ж широка, як і сфера охоплення міжнародних телекомунікаційних систем». Хоча в Керівництві слово «Інтернет» згадується одноразово, а термін «кіберзлочинність» взагалі не використовується, висновки, які воно містить, є далекоглядними. Основну увагу приділено поняттю «комп'ютерний злочин», формулюванню терміна «кіберзлочинність»[3].

Рішучість щодо прийняття заходів задля того, щоб усі могли користуватися благами нових технологій, особливо інформаційних і комунікаційних, відповідно до рекомендацій, зазначених у Декларації міністрів на сесії

[2] Cybercrime. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (дата звернення:10.02.2026).

[3] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication. 1994). URL: https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF (дата звернення:11.02.2026).

ЕКОСОР 2000 р., була висловлена Декларацією тисячоліття ООН 2000 р. (ст. 20)[4], підтверджена Цілями сталого розвитку ООН (Ціль 9).[5]

Знаковою подією стало прийняття у 2024 році першого всеохоплюючого глобального договору про кіберзлочинність – Конвенції Організації Об'єднаних Націй проти кіберзлочинності (резолюція Генеральної Асамблеї ООН 79/243).[6] Договір об'єднує держави-учасниці спільною метою: запобігання та боротьба з кіберзлочинністю, зокрема шляхом зміцнення міжнародної співпраці, а також сприяння технічній допомозі та розбудові потенціалу, зокрема для країн, що розвиваються. Містить норми щодо криміналізації найпоширеніших форм кіберзлочинності. Розділ Конвенції про криміналізацію вимагає, щоб держави-учасниці створили комплексну систему, спрямовану на злочини, скоєні через системи інформаційно-комунікаційних технологій (далі – ІКТ). Це включає криміналізацію «кіберзалежних злочинів» (широко відомих як «незаконний хакерський злом»), які спрямовані на конфіденційність, цілісність і доступність електронних даних та систем ІКТ, а також «злочинів, що сприяють кіберзлочинності», які є традиційними злочинами, масштаби, швидкість та обсяг яких значно зросли через неправильне використання систем ІКТ. Розділ про юрисдикцію встановлює чіткі та гнучкі правила, що запобігають злочинцям використовувати прогалини в юрисдикції для уникнення покарання, водночас окреслюючи правові сфери, які можуть регулювати держави-учасниці. Конвенція покладає на сторони надавати допомогу іншим державам-учасницям у кримінальних розслідуваннях, коли докази або підозрювані знаходяться на їхній території. Ця співпраця включає екстрадицію, взаємну допомогу у пошуку та збереженні даних, а також взаємну правову допомогу для сприяння збору та обміну доказами. Розділ про процесуальні заходи та правоохоронну діяльність надає державам-учасницям можливість вирішувати питання, пов'язані із забезпеченням електронних доказів, адаптуючи традиційні засоби та методи розслідування до середовища ІКТ. Ці заходи дозволяють ефективно збирати електронні докази, одночасно захищаючи права людини та підтримуючи як національні кримінальні провадження, так і міжнародну співпрацю. Договір покладає на правоохоронців зобов'язання під час розслідування та переслідування кіберзлочинів за допомогою цих процесуальних заходів поважати основні права людини. Розділ про міжнародну співпрацю встановлює глобальну систему, яка дозволяє сторонам договору допомагати одна одній у розслідуваннях, кримінальному переслідуванні, поверненні активів та судових провадженнях через кордони. Розділ про профілактичні заходи розроблений для сприяння

[4] Resolution adopted by the General Assembly [without reference to a Main Committee (A/55/L.2)] 55/2. United Nations Millennium Declaration. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf (дата звернення:09.02.2026).

[5] THE 17 GOALS. URL: https://sdgs.un.org/goals (дата звернення:08.02.2026).

[6] 79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. URL: https://docs.un.org/en/A/RES/79/243 (дата звернення 11.02.2026).

зменшенню та управлінню ризиками і загрозами кіберзлочинності. Він передбачає низку профілактичних заходів та акцентує на залученні й активній участі у цьому процесі всіх зацікавлених сторін – урядів, приватного сектору, наукових кіл, організацій громадянського суспільства та громадськості в цілому. Розділ про технічну допомогу та обмін інформацією встановлює широкі заходи щодо технічної допомоги, нарощування потенціалу та обміну інформацією між державами-учасницями, приділяючи особливу увагу потребам країн, що розвиваються. Договір засновує Конференцію держав-учасниць, яка служить основним механізмом нагляду за впровадженням Конвенції та покращенням потенціалу і співпраці між державами-учасницями для досягнення цілей Конвенції.

На міжнародному регіональному знаковим документом є Конвенція про кіберзлочинність 2001 р. Ради Європи (далі – Конвенція (ETS № 185)),[7] яка стала першим міжнародним договором про злочини, що вчиняються через Інтернет та інші комп'ютерні мережі, особливо щодо порушень авторських прав, комп'ютерного шахрайства, дитячої порнографії та порушень мережної безпеки. Вона також містить низку функцій та процедур, таких як пошук комп'ютерних мереж та перехоплення. Основну мету договору викладено у преамбулі і вона полягає у проведенні загальної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом ухвалення відповідного законодавства та розвитку міжнародного співробітництва.

Конвенцію спрямовано головним чином на гармонізацію елементів внутрішнього кримінального матеріального права щодо правопорушень та пов'язаних із ними положень у сфері кіберзлочинності; надання внутрішньо-державним органам кримінально-процесуальних повноважень, необхідних для розслідування та судового переслідування таких злочинів, а також інших злочинів, вчинених за допомогою комп'ютерної системи або пов'язаних із використанням електронних доказів та інших злочинів; встановлення швидкого та ефективного режиму міжнародного співробітництва.

Застосовуючи Конвенцію (ETS № 185), сторони дотримуються обов'язків урядів захищати людей від злочинів, вчинених онлайн або офлайн шляхом ефективного кримінального розслідування та судового переслідування. Деякі сторони Конвенції вважають, що вони пов'язані міжнародним зобов'язанням надавати засоби захисту від злочинів, вчинених за допомогою комп'ютерної системи (див.: К. У. проти Фінляндії, Європейський суд з прав людини (скарга № 2872/02, судове рішення від 2 березня 2009 р.)[8], з посиланням на процедури та повноваження для кримінальних розслідувань або розглядів, які сторони повинні встановити відповідно до Конвенції. Конвенцію відкрито для приєднання державами, які не є членами Ради Європи.

Конвенція про кіберзлочинність є впливовою міжнародною угодою, що регулює питання порушення закону через Інтернет або інші інформаційні мережі.

[7] Convention on Cybercrime. URL: ttps://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/convention_on_cybercrime_html/Budapest_Convention_on_Cybercrime.pdf (дата звернення:11.02.2026).

[8] Case of K.U. v. Finland (Application no. 2872/02). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964%22] (дата звернення:12.02.2026).

Вона вимагає від сторін модернізувати і гармонізувати своє кримінальне законодавство проти дій хакерів та інших порушень безпеки, включаючи порушення авторських прав, шахрайство за допомогою комп'ютера, дитячу порнографію та іншу протиправну кібердіяльність. Договір також передбачає процесуальні повноваження, що охоплюють обшук комп'ютерних мереж і перехоплення комунікацій у контексті боротьби з кіберзлочинністю; створює можливості для ефективного міжнародного співробітництва. Конвенція не є інструментом забезпечення захисту персональних даних, вона криміналізує діяльність, яка може порушувати право суб'єкта на захист особисти даних. Конвенція також зобов'язує договірні сторони передбачити при виконанні Конвенції адекватний рівень захисту прав і свобод людини, у тому числі прав, гарантованих Конвенцією про захист прав людини і основоположних свобод 1950 р., як право на захист персональних даних.

Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ETS № 189) 2003 р.[9], розширює сферу дії Конвенції про кіберзлочинність, включаючи її суттєві, процедурні та присвячені міжнародному співробітництву положення, охоплюючи також правопорушення, пов'язані з расистською та ксенофобською пропагандою. Таким чином, крім гармонізації суттєвих правових аспектів такої поведінки, Протокол спрямовано на розширення можливостей сторін щодо використання коштів і напрямків міжнародного співробітництва, передбачених Конвенцією (ETS № 185) у цій галузі.

Другий Додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття електронних доказів 2022 р. (CETS 224)[10] спрямовано на подальше зміцнення співпраці у боротьбі з кіберзлочинністю та розширення можливостей органів кримінального правосуддя щодо збирання доказів в електронній формі про кримінальний злочин для цілей конкретних кримінальних розслідувань або розглядів за допомогою додаткових інструментів, що стосуються більш ефективної взаємодії та інших форм співробітництва між компетентними органами; співробітництво у надзвичайних ситуаціях (тобто у ситуаціях, коли існує значний та безпосередній ризик для життя або безпеки будь-якої фізичної особи); та пряме співробітництво між компетентними органами і постачальниками послуг та іншими суб'єктами, які володіють відповідною інформацією або контролюють її.

Негативною ознакою сьогодення стало використання ІКТ у вчиненні терористичних злочинів[11]. У 2015 році Парламентська асамблея Ради Європи (ПАРЄ) прийняла рекомендацію № 2070 щодо зміцнення співробітництва

[9] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. URL: https://rm.coe.int/168008160f (дата звернення:14.02.2026).

[10] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (дата звернення:14.02.2026).

[11] Сироїд Т. Л., Гавриленко О. А. Внесок Ради Європи у забезпечення інформаційної безпеки та протидію кіберзлочинності. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2020. Вип. 61, т. 2. С. 149–154. DOI https://doi.org/10.32782/2307-3322.61-2.33

у боротьбі з кібертероризмом та іншими масовими атаками в мережі Інтернет[12]. Рекомендація підкреслює роль Ради Європи у вирішенні глобального виклику, пов'язаного з безпекою комп'ютерних мереж у зв'язку з появою кібертероризму та інших масових атак, що діють на/через комп'ютерні системи, являючи собою серйозну загрозу національній безпеці, громадській безпеці та добробуту країн.

Кіберзлочинність також є одним із пріоритетів Європейського Союзу (далі – ЄС, Союз) у боротьбі з серйозною та організованою злочинністю в рамках EMPACT 2022–2025. Кіберзлочинність – проблема, що зростає, для таких країн, як держави-члени ЄС, у більшості яких добре розвинено Інтернет-інфраструктуру і платіжні системи знаходяться в режимі онлайн. Але не лише фінансові дані, а й дані загалом є ключовою мішенню для кіберзлочинців. Кількість та частота витоків даних зростають, що, своєю чергою, призводить до збільшення кількості випадків шахрайства та вимагання.

ЄС докладає суттєвих зусиль до розробки й узгодження законодавства щодо кіберзлочинності, яке діє на території держав-членів, серд таких нормативів слід зазначити: Директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких як електронна торгівля на внутрішньому ринку (в редакції від 17.02.2024); Повідомлення Європейського парламенту, Ради та Комітету регіонів: Загальна політика боротьби з кіберзлочинністю (COM(2007) 267 final); Директива 2011/93/ЄС Європейського парламенту та Ради про боротьбу із сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією, яка замінює Рамкове рішення Ради 2004/68/ЈНА (в редакції від 17.12.2011); Повідомлення Комісії Раді та Європейському парламенту: Боротьба зі злочинністю в наш цифровий вік: створення Європейського центру кіберзлочинності (COM(2012) 140 final); Директива 2013/40/ЄС Європейського парламенту та Ради про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/ЈНА; Рішення (CFSP) 2019/797 – обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам (в редакції від 14.05.2025); Регламент (ЄС) 2019/796 – обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам (в редакції від 14.05.2025); Регламент (ЄС) 2019/881 Європейського парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, що скасовує Регламент (ЄС) № 526/2013 (Закон про кібербезпеку) (Текст, що стосується ЄЕЗ) (в редакції від 04.02.2025); Регламент (ЄС) 2021/1149 про створення Фонду внутрішньої безпеки (спрямований на забезпечення високого рівня безпеки в Європейському Союзі, зокрема шляхом запобігання та протидії тероризму і радикалізації, серйозній і організованій злочинності та кіберзлочинності); Регламент (ЄС) 2021/887 про створення Європейського промислового, технологічного та науково-дослідного центру кібербезпеки

[12] Increasing co-operation against cyberterrorism and other largescale attacks on the Internet. URL: http://www.europeanrights.eu/public/atti/2070_ing.pdf (дата звернення: 13.02.2026).

та мережі національних координаційних центрів,; Директива (ЄС) 2024/1385 про боротьбу з насильством щодо жінок та домашнім насильством, яка спрямована на введення цільових мінімальних правил щодо прав цієї групи жертв злочинів і криміналізації найбільш важких форм насилля стосовно жінок і кібернасилля; Регламент (ЄС) 2024/2847 (в редакції від 20.11.2024), який встановлює горизонтальні вимоги до кібербезпеки для продуктів із цифровими елементами; Регламент (ЄС) 2024/1689, що встановлює гармонізовані правила щодо штучного інтелекту.

Перш за все слід зазначити, що прийняті ЄС акти мають за мету унормувати діяльність, пов'язану з використанням ІКТ у різних сферах відносин. Так, Директива 2000/31/ЄС[13] встановлює стандартні правила ЄС із різних питань, пов'язаних з електронною торгівлею. Вона спрямована на сприяння належному функціонуванню внутрішнього ринку шляхом забезпечення вільного переміщення послуг інформаційного суспільства між державами-членами. Документ наближає деякі національні положення про послуги інформаційного суспільства, що стосуються: внутрішнього ринку, постачальників послуг, комерційного зв'язку, електронних контрактів, відповідальності посередників, кодексів поведінки, позасудового врегулювання спорів, судових позовів та співробітництва між державами-членами. Директива доповнює законодавство Союзу, що застосовується до послуг інформаційного суспільства, без шкоди для рівня захисту, зокрема, громадської охорони здоров'я та інтересів споживачів, встановленого актами Союзу та національним законодавством, що їх реалізує, тією мірою, якою це не обмежує свободу надання послуг інформаційного суспільства.

Директиву 2013/40/ЄС[14] спрямовано на боротьбу з кіберзлочинністю та забезпечення інформаційної безпеки завдяки суворішому державному законодавству, суворішим кримінальним покаранням та більш тісній співпраці між надмірними податками. Директива запроваджує нові правила, що гармонізують криміналізацію та покарання за низку правопорушень, спрямованих проти інформаційних систем. Ці правила включають заборону використання ботнетів – шкідливого програмного забезпечення, призначеного для віддаленого управління мережею комп'ютерів. Основними видами кримінальних злочинів, що охоплюються Директивою, є атаки на інформаційні системи, починаючи від атак типу «відмова в обслуговуванні», призначених для виведення із ладу сервера, і закінчуючи перехопленням даних та атаками ботнетів. Директива зобов'язує держави-члени криміналізувати означені правопорушення; розширювати співпрацю правоохоронних органів. Директива передбачає зближення систем кримінального законодавства країн ЄС та розширення співробітництва

[13] Consolidated text: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0031-20240217 (дата звернення:12.02.2026).

[14] 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. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (дата звернення: 12.02.2026).

між судовими органами щодо незаконного доступу до інформаційних систем, незаконного втручання у систему, незаконного втручання в дані, незаконного перехоплення. Документ містить норми щодо запровадження ефективних, пропорційних та стримуючих санкцій. Покладає зобов'язання на держави-члени щодо вжиття необхідних заходів для забезпечення того, щоб такі діяння, як незаконний доступ до інформаційних систем, незаконне втручання у систему, незаконне втручання в дані, незаконне перехоплення, засоби, що використовуються для вчинення правопорушень, а також підбурювання, пособництво та підбурювання і спроба скоєння означених злочинів (статті 3–8), каралися ефективними, пропорційними і кримінальними покараннями.

Рішення (CFSP) 2019/797[15] та Регламент (ЄС) 2019/796[16], запроваджують структуру, яка дозволяє ЄС вводити санкції для стримування та реагування на кібератаки, які становлять зовнішню загрозу для ЄС чи країн ЄС. Такі протиправні дії включають атаки, що стосуються інформаційних систем, а також: критичної інфраструктури, необхідної для життєдіяльності суспільства чи здоров'я громадян, безпеки, захисту та економічного чи соціального благополуччя; послуг, необхідних для основної соціальної та економічної діяльності, зокрема енергетика, транспорт, банківська справа; фінансів, охорони здоров'я, питної води, цифрової інфраструктури; найважливіших державних функцій, зокрема оборони, управління та функціонування інститутів, публічних виборів, економічної та громадянської інфраструктури, внутрішньої безпеки і зовнішніх зв'язків, включаючи дипломатичні місії; зберігання чи обробка секретної інформації; або урядових аварійно-рятувальних загонів. Ці кібератаки включають атаки на країни, які не є членами ЄС, або міжнародні організації, коли дії вважаються необхідними для досягнення спільних цілей зовнішньої та безпекової політики ЄС.

Означені нормативи дозволяють ЄС накладати санкції на осіб чи організації, які відповідальні за кібератаки чи спроби кібератак, надають фінансову, технічну чи матеріальну підтримку таким атакам, чи беруть участь у них в інший спосіб. Санкції можуть також застосовуватись до пов'язаних з ними осіб або організацій. Обмежувальні заходи включають заборону на в'їзд до ЄС та заморожування активів. На країни ЄС покладено зобов'язання щодо встановлення мір покарання за ці правопорушення.

Регламентом (ЄС) 2024/2847[17] встановлено горизонтальні вимоги щодо кібербезпеки для продуктів із цифровими елементами. Документ визначає правила допуску на ринок продуктів із цифровими елементами для забезпечення кібербезпеки таких продуктів; основні вимоги до кібербезпеки

[15] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng (дата звернення: 12.02.2026).

[16] Там само.

[17] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (дата звернення: 12.02.2026).

для проектування, розробки та виробництва продуктів, а також зобов'язання для економічних операторів щодо кібербезпеки цієї продукції; основні вимоги до кібербезпеки для процесів обробки вразливостей, застосовних виробниками, і пов'язані з ними зобов'язання; правила нагляду за ринком, включаючи моніторинг і забезпечення дотримання вимог.

Регламент (ЄС) 2024/1689[18] встановлює гармонізовані правила розміщення на ринку, введення в експлуатацію та використання систем штучного інтелекту (ШІ) в ЄС. Він забороняє певні практики та запроваджує особливі вимоги для систем ШІ з високим ризиком, а також зобов'язання для операторів таких систем; включає гармонізовані правила прозорості для певних систем ШІ, гармонізовані правила розміщення на ринку моделей ШІ загального призначення, правила моніторингу ринку, нагляду за ринком, управління та забезпечення дотримання; запроваджує заходи, спрямовані на підтримку інновацій. Метою Регламенту є покращення функціонування єдиного ринку ЄС та сприяння впровадженню орієнтованого на людину та надійного ШІ, забезпечуючи при цьому високий рівень захисту здоров'я, безпеки та основних прав, закріплених Хартією ЄС про основні права, від негативного впливу систем ШІ в ЄС.

Директива (ЄС) 2024/1385 про боротьбу з насильством щодо жінок та домашнім насильством[19] визначає в якості кримінальних правопорушень кіберпереслідування (ст. 6), кібердомагання (ст. 7) та кіберпідбурювання до насильства чи ненависті (с. 8) тощо.

Організація з безпеки і співробітництва в Європі (далі – ОБСЄ) також відіграє важливу роль у підвищенні кібер- / ІКТ-безпеки, зокрема за рахунок зниження ризиків конфліктів між державами, що виникають унаслідок використання ІКТ. Ключовим завданням щодо цього є введення в дію відповідних вказівок ООН з боку груп урядових експертів на регіональному рівні.

Багато держав інвестують у наступальні та оборонні можливості ІКТ, додаючи складний вимір міждержавним відносинам. Такі можливості можуть змінюватись від розвідувальних та інформаційних операцій до порушення критично важливих мереж і служб або можливостей управління та командування.

Унікальні характеристики ІКТ значно збільшили ймовірність неправильного сприйняття, прорахунків та навіть напруженості між державами, коли вони стикаються з питаннями намірів, атрибуції, правил та норм. У відповідь держави-учасниці ОБСЄ працюють над заходами зміцнення довіри (далі – ЗД) для зниження ризиків конфліктів, що виникають унаслідок використання ІКТ. Вони покликані зробити кіберпростір більш передбачуваним і пропонують конкретні інструменти та механізми, щоб уникнути непорозумінь, зокрема такі: механізм об'єднання держав для консультацій з приводу можливих інцидентів у сфері

[18] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 12.02.2026).

[19] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення:12.02.2026).

кібер- / ІКТ-безпеки з метою зниження напруженості, що зростає; платформу для обміну думками, національною політикою та підходами в галузі безпеки і сфері кібер/ІКТ, що дозволяє державам краще «читати» наміри одна одної в кіберпросторі; конкретні напрямки роботи, наприклад захист критично важливої інфраструктури з використанням ІКТ, що дозволяють державам-учасницям колективно підвищувати кіберстійкість у регіоні ОБСЄ на благо всіх.

На додаток до ЗД безпеки, кібер / ІКТ, ОБСЄ та її інститути також зосереджені на протидії загрозам безпеці кібер/ІКТ з боку недержавних суб'єктів, таких як організована злочинність і терористи. Ключовий акцент тут робиться на заохоченні адекватних і своєчасних заходів у відповідь з боку національних органів влади на ці мінливі загрози, починаючи від більш якісної судової експертизи і закінчуючи інноваційними підходами, що дозволяють запобігти перетворенню ІКТ на тактичних помічників терористів.

Заходи з правової протидії кіберзлочинності запроваджуються і на рівні Ліги арабських держав, в межах якої прийнято Арабську конвенцію про боротьбу зі злочинами, пов'язаними з технологіями, яку спрямовано на покращання співпраці між арабськими державами в боротьбі з правопорушеннями у сфері інформаційних технологій для захисту безпеки та інтересів арабських держав, а також безпеки їхніх спільнот і окремих осіб (2010 р.). Договір містить визначення злочинів, пов'язаних із використанням інформаційних технологій, процесуальні положення та механізми правової і судової співпраці між державами-учасницями у цій сфері[20].

Африканський союз докладає зусиль щодо розробки правової основи у протидії кіберзлочинності, яка має тенденції до зростання в регіоні. Це підтверджується статистичними даними, згідно яких африканський континент демонструє один із найшвидших темпів зростання проникнення Інтернету у світі, а цифрове підключення майже потроїлося за останні п'ять років. У той самий період як уряди, так і приватні структури в Африці стикаються зі зростаючою тенденцією кібератак, що відповідає тому, що було зафіксовано також на глобальному рівні. Масштабні крадіжки персональних даних, комп'ютерні втручання, цькування, переслідування та інші форми кібернасилля або сексуального насильства щодо дітей в Інтернеті є нападами на права людини. Мова ненависті, ксенофобія та расизм сприяють радикалізації, що призводить до насильницького екстремізму. Атаки на комп'ютери та дезінформація, що використовуються на виборах і передвиборчих кампаніях, є атаками на функціонування фундаментальних інституцій та політичну стабільність. Щоденні атаки на критичну інформаційну інфраструктуру впливають на національну безпеку, економічні та інші національні інтереси, а також на міжнародний мир і стабільність[21].

[20] Arab Convention on Combating Information Technology Offences. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/arab_convention_on_combating_information_technology_offences__html/Arab_Convention_on_Combating_Information_Technology_Offences.pdf (дата звернення:12.02.2026).

[21] African Forum on cybercrime. URL: https://au.int/fr/node/34897 (дата звернення: 13.02.2026).

Серед правових актів слід вказати Конвенцію Африканського Союзу про кібербезпеку та захист особистих даних (2014 р.), яку спрямовано на створення законодавчої бази для забезпечення кібербезпеки та захисту персональних даних. Договір покладає на держави-учасниці зобов'язання щодо розробки національної політики кібербезпеки та відповідного інституційного механізму управління; розробки законодавства та створення інститутів у сфері протидії кіберзлочинності; забезпечення моніторингу та реагування на інциденти і попередження; здійснення національної і транскордонної координації та глобальної співпраці[22].

У межах АС розроблено Стратегію AFRIPOL щодо боротьби з кіберзлочинністю 2020-2024 рр.[23]. Вона є гнучким документом, який підлягає періодичному перегляду з метою забезпечення його актуальності, подальшого реагування на нові загрози у динамічному середовищі, в якому діють сили безпеки, та відповідність очікуванням держав-членів. Документ, головним чином, має на меті розробити дорожню карту боротьби з кіберзлочинністю, тобто основні напрямки дій для розробки заходів контролю за злочинами, спрямованими на комп'ютери та інформаційні системи, у спробах отримати несанкціонований доступ до пристроїв або запобігти доступу законних користувачів до цих пристроїв (часто за допомогою шкідливого програмного забезпечення).

Стратегія зосереджена на чотирьох напрямках дій зі спільною метою допомогти державам розробити узгоджені методології контролю та таким чином забезпечити плідний обмін інформацією. Ці напрямки полягають у наступному: зміцнення можливостей центральної групи AFRIPOL з боротьби з кіберзлочинністю, а також команд держав-членів, шляхом надання ресурсів та механізмів для збору доказів, необхідних для цифрових розслідувань; спеціалізована підготовка фахівців у боротьбі з кіберзлочинністю; розробка гармонійного та узгодженого регулювання, а також широка співпраця між державами-членами Африканського Союзу; забезпечення постійної оцінки загроз щодо кіберзлочинності на рівні суспільства/членства.

Ключовою частиною інтеграційних пріоритетів АС є Стратегія цифрової трансформації АС на 2020–30 рр.[24] Ктім того, Порядок денний 2063[25] – довгостроковий план розвитку Африканського Союзу, який відповідає глобальній рамковій програмі Цілей сталого розвитку ООН, зазначає науку, технології, інновації та охорону здоров'я як ключові цілі, що є пріоритетами для трансформації Африки.

---

[22] African Union Convention on Cyber Security and Personal Data Protection. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/african_union_convention_on_cyber_security_and_personal_data_protection__html/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата звернення: 11.02.2026).

[23] AFRIPOL Cybercrime Strategy. URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/ (дата звернення: 13.02.2026).

[24] The Digital Transformation Strategy for Africa (2020-2030). URL: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.p (дата звернення: 13.02.2026).

[25] Documents Agenda 2063. URL: https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf (дата звернення: 13.02.2026).

2. Міжнародна інституційна основа протидії кіберзлочинності

Найбільший обсяг роботи у справі боротьби з міжнародною злочинністю на інституційному універсальному рівні здійснюється в межах Міжнародної організації кримінальної поліції (Інтерпол).[26] Невід'ємною складовою діяльності Інтерполу є протидія комп'ютерній злочинності, на нього покладено функцію збирання, обробки й аналізу інформації, яка поступає з мережі Інтернет із метою надання допомоги у виявленні протиправних діянь, вчинення яких полегшується завдяки Інтернету. Крім того, Цільовою групою по здійсненню контртерористичних операцій створено Робочу групу по боротьбі з використанням Інтернету в терористичних цілях. До завдань якої віднесено: виявлення і об'єднання зусиль зацікавлених сторін і партнерів з метою обміну інформацією, а також визначення можливих шляхів протидії цій загрозі на національному, регіональному і глобальному рівнях; вивчення питання щодо ролі ООН у координації дій держав-членів.

Зважаючи на ту особливість, що негативною ознакою сьогодення стало використання ІКТ у скоєнні терористичних злочинів, безперечно, значну роль в організаційній співпраці протидії злочинності відіграє Контртерористичний комітет (КТК) (резолюція Ради Безпеки ООН 1373 (2001))[27], створений з метою сприяння зміцненню потенціалу держав-членів ООН щодо запобігання терористичним актам як на національному, так і на міжрегіональному рівні. Резолюція 1373 (2001) закликає держави-члени здійснити низку заходів, спрямованих на зміцнення їхніх правових та інституційних можливостей у галузі боротьби з тероризмом, у тому числі криміналізувати фінансування тероризму; невідкладно заблокувати будь-які засоби, пов'язані з особами, причетними до терористичних актів; не надавати ні в якій формі фінансову підтримку терористичним групам; здійснювати обмін інформацією з іншими урядами щодо будь-яких груп, які вчиняють чи які планують здійснити терористичні акти; співпрацювати з іншими урядами в розслідуванні, виявленні, арешті, видачі та переслідуванні осіб, причетних до таких актів тощо.

Спеціалізована установа ООН Міжнародний союз електрозв'язку (далі – МСЕ) сприяє інноваціям у сфері інформаційно-комунікаційних технологій, а також у питаннях кіберзлочинності. Для прийняття конкретних заходів, спрямованих на обмеження комп'ютерних загроз, МСЕ розробив Глобальну програму кібербезпеки, яка забезпечує рамки для координації зусиль щодо задоволення юридичних, технічних, організаційних і навчальних потреб у всьому світі. Програма визначила основні принципи, цілі та стратегії розробки моделей законодавства у сфері боротьби з кіберзлочинністю та базується на п'яти стратегічних принципах, а саме: правові заходи; технічні та

[26] Constitution of the International CriminaL Police Organization-INTERPOL. URL: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents (дата звернення: 10.02.2026).

[27] Resolution 1373 (2001). URL: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (дата звернення: 12.02.2026).

процедурні заходи; організаційні структури; створення потенціалу; міжнародне співробітництво (с. 506)[28].

У межах регіональних міжнародних організацій також функціонує низка структур, інституцій та агенств що сприяють підвищенню кібербезпеки, серед яких слід вказати Європейське поліцейське агентство (Європол), правовим підґрунтям функціонування якого є Регламент (ЄС) 2016/794 (в редакції від 28.06.2022). Серед завдань Європолу, означених статею 88 Договору про функціонування Європейського Союзу (ДФЄС), віднесено такі: підтримка та зміцнення діяльності поліцейських органів та інших правоохоронних служб держав-членів, їхньої взаємної співпраці щодо запобігання та протидії тяжким злочинам, що впливають на дві або більше держав-членів, тероризму та тим формам злочинів, що впливають на спільні інтереси, охоплені політикою ЄС[29], зокрема ... комп'ютерній злочинності, виготовленню контрафактної і піратської продукції тощо.

Регламент (ЄС) 2016/794 уповноважив Європол на виконання таких задач: збирання, збереження, обробка, аналіз інформації і даних, а також обмін інформацією і даними; безвідкладне повідомлення компетентним органам держав-членів через спеціальний відділ про факти, які їх зачіпають, і сповіщення про зв'язок, який констатовано між злочинами; сприяння розслідуванням у державах-членах, особливо шляхом передачі національним відділам усієї необхідної інформації з цього приводу; звернення до компетентних органів відповідних держав-членів із запитами про порушення, проведення та координацію розслідувань і висунення пропозицій щодо створення сумісних слідчих бригад у визначених справах; надання державам-членам інформації та допомоги в аналізі при проведенні масштабних заходів («зустрічі у верхах», міжнародні спортивні змагання) тощо[30].

Заслуговують на увагу практичні інноваційні підходи Європолу щодо запобігання кіберзлочинам, серед яких слід вказати програму «Кіберзахисники», яка має за мету підвищення обізнаності про кіберзлочини[31].

Агентство Європейського союзу з кібербезпеки (ENISA) займається досягненням високого загального рівня кібербезпеки в Європі (створене в 2004 р.

---

[28] Сироїд Т.Л. Міжнародно-правове регулювання сфери інформаційно-комунікаційних технологій і протидія кіберзлочинності // Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменского: моногр. / авт. кол.; за ред. В. М. Репецького, В. В. Гутника. Львів; Одеса: Фенікс, 2017. 564 с. С. 495-521. ISBN 978-966-928-118-0

[29] Consolidated version of the Treaty on the Functioning of the European Union. URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (дата звернення:10.02.2026).

[30] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. https://eur-lex.europa.eu/eli/reg/2016/794/oj/eng (дата звернення: 13.02.2026).

[31] Cyber Defenders. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders (дата звернення: 13.02.2026).

та посилене Регламентом (ЄС) 2019/881 (в редакції 04.02.2025)[32]. ENISA робить свій внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг та процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами й органами ЄС та допомагає Європі підготуватися до кібервикликів у майбутньому. За допомогою обміну знаннями, нарощування потенціалу та підвищення обізнаності Агентство працює разом зі своїми ключовими зацікавленими сторонами над зміцненням довіри до підключеної економіки, підвищенням стійкості інфраструктури ЄС та, зрештою, для забезпечення цифрової безпеки європейського суспільства і громадян.

З 2013 року функціонує Європейський центр боротьби з кіберзлочинністю (ЕС3)[33] – підрозділ Європолу покликаного відігравати провідну роль у боротьбі з кіберзлочинністю на території ЄС. ЕС3 займається створенням оперативних і аналітичних потужностей, необхідних для забезпечення швидкого реагування на кіберзлочини, а також організацією взаємодії офіційних відомств ЄС і країн-членів з міжнародними партнерами. Мандат ЕС3 охоплює такі сфери відповідальності: боротьба зі злочинами, які вчиняються організованими злочинними групами та тягнуть за собою отримання незаконних доходів в особливо великих розмірах (шахрайство з кредитними картками або банківськими операціями); боротьба зі злочинами, що завдають серйозної шкоди жертві, зокрема розбещення малолітніх; боротьба з діями, спрямованими на спричинення шкоди або виведення з ладу інфраструктури та інформаційних систем ЄС. ЕС3 також відповідальний за збір та обробку даних, надання інформаційної, технічної та криміналістичної підтримки відповідним підрозділам правоохоронних органів країн – членів ЄС, координацію спільних розслідувань, навчання й підготовку фахівців (у співпраці із CEPOL). Центр сприяє проведенню необхідних досліджень і створенню програмного забезпечення, опікується оцінкою й аналізом наявних і потенційних загроз, складанням прогнозів і випуском завчасних попереджень. Сфера його діяльності також охоплює надання допомоги суддям і прокурорам[34].

Щороку ЕС3 публікує оцінку загрози організованої злочинності в Інтернеті (IOCTA) – флагманський стратегічний звіт про ключові результати, нові загрози та події в кіберзлочинності. IOCTA демонструє, наскільки широкою і різноманітною є кіберзлочинність і як ЕС3 є ключовою частиною Європолу та відповідних заходів ЄС. ЕС3 використовує тристоронній підхід до боротьби з кіберзлочинністю: криміналістика, стратегія та операції. Ці заходи також

[32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (дата звернення: 13.02.2026).

[33] Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0140 (дата звернення: 12.02.2026).

[34] European Cybercrime Centre URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення:12.02.2026).

підтримуються Групою кіберрозвідки (CIT), аналітики якої збирають та обробляють інформацію, пов'язану з кіберзлочинністю, з державних, приватних та відкритих джерел і визначають загрози та моделі, що виникають.

Сумісно з ЕС3 працює Спільна цільова група боротьби з кіберзлочинністю (J-CAT) (створена у 2014 р.), яка надає допомогу у протидії кіберзлочинності всередині та за межами ЄС. Цільова група має за мету стимулювати та координувати дії, засновані на інтелекті, з ключовими загрозами та цілями кіберзлочинності, полегшуючи спільну ідентифікацію, встановлення пріоритетів, підготовку та початок транскордонних розслідувань та операцій з боку своїх партнерів. Її компетенція J-CAT охоплює: високотехнологічні злочини (зокрема шкідливе програмне забезпечення, вторгнення); сприяння вчиненню злочинів (куленепробивний хостинг, контр-антивірусні послуги, лізинг та оренда інфраструктури, відмивання грошей, включаючи віртуальні валюти); онлайн-шахрайство (онлайн-платіжні системи, кардинг, соціальна інженерія).[35]

Кіберзлочинність – це зростаюча та швидкорозвинена сфера злочинності, яка становить значну частку загальної роботи Євроюсту – Агентства Європейського Союзу з питань співробітництва у сфері кримінального правосуддя, – це унікальний центр де національні судові органи тісно співпрацюють у боротьбі з серйозною організованою транскордонною злочинністю. Роль Євроюсту полягає в тому, щоб допомогти зробити Європу безпечнішим місцем шляхом координації роботи національних органів влади-держав-членів ЄС, а також третіх держав – у розслідуванні та переслідуванні транснаціональної злочинності[36]. Євроюст підтримує національні органи влади у співпраці та використанні доступних інструментів транскордонного розслідування кіберзлочинності та пов'язаної з нею злочинності.

Європейська судова мережа з питань кіберзлочинності (EJCN)[37], створена у 2016 році для сприяння контактам між фахівцями, які спеціалізуються на протидії викликам, що виникають у зв'язку з кіберзлочинністю, кібер-злочинністю та розслідуваннями в кіберпросторі, а також для підвищення ефективності розслідувань і кримінального переслідування. EJCN посилює співпрацю між компетентними судовими органами, забезпечуючи обмін досвідом, передовим досвідом та іншими відповідними знаннями щодо розслідування та кримінального переслідування кіберзлочинності.

Євроюст є ключовим партнером EJCN, особливо в ситуаціях, коли Мережа має справу з численними викликами, пов'язаними з дійсно безкордонним характером кіберзлочинності. Крім того, Євроюст проводить регулярні зустрічі Мережі та підтримує обмін інформацією між членами EJCN та іншими

[35] Joint Cybercrime Action Taskforce. URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (дата звернення:08.02.2026).

[36] Consolidated text: Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. URL: https://eur-lex.europa.eu/eli/reg/2018/1727/2025-11-04/eng (дата звернення: 13.02.2026).

[37] European Judicial Cybercrime Network. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (дата звернення: 12.02.2026).

зацікавленими сторонами, які відіграють роль у забезпеченні верховенства права в кіберпросторі.

Серед регіональних структур слід зазначити Механізм співробітництва поліції Африканського Союзу (AFRIPOL) – це технічна установа АС, яка має за завдання зміцнювати та гармонізувати можливості правоохоронних органів у державах-членах. Його місія полягає в підтримці африканських поліцейських служб у запобіганні та боротьбі з транснаціональною організованою злочинністю, тероризмом, кіберзлочинністю та іншими новими загрозами континентальній безпеці.

На виконання свого мандату AFRIPOL надає комплексний спектр механізмів підтримки, серед яких: очне та онлайн-навчання, включаючи спеціалізовані курси через спеціалізовану платформу електронного навчання; навчання тренерів для забезпечення національної стійкості навичок; проведення семінарів для обміну досвідом та передовим досвідом між державами-членами; доступ до судово-медичних та слідчих інструментів; підтримка спільних операцій та транскордонних розслідувань; сприяння державно-приватному партнерству для вдосконалення стратегій запобігання злочинності; сприяння співпраці через безпечну систему зв'язку та спільні бази даних; стажування та можливості отримання стипендій для розвитку майбутніх лідерів правоохоронних органів[38].

Контртерористичний центр Африканського Союзу (AUCTC) – спеціалізована установа, створена для зміцнення потенціалу держав-членів АС у сфері реагування на боротьбу з тероризмом та насильницьким екстремізмом. Працюючи у тісній співпраці з регіональними економічними співтовариствами і регіональними механізмами, AUCTC надає технічну, оперативну та стратегічну підтримку. Він розробляє інструменти та програми для запобігання, аналізу та ефективного реагування на терористичні загрози на африканському континенті[39].

ВИСНОВОК

Підсумовуючи вищеозначене слід констатувати, що кіберзлочини є складними не лише за своїми юридичними ознаками, але й тому, що вони часто мають транснаціональний характер, тобто це діяння, ініціювання, запобігання чи наслідки яких зачіпають більш ніж одну країну, і вони мають багатонаціональний характер. Крім того, вони є видом професійної діяльності організованих злочинних груп. Кіберзлочини охоплюють широкий спектр об'єктів посягання. Вони послаблюють економіку держав, впливаючи (прямо та опосередковано) на економічні витрати урядів і тягнуть за собою кримінальну діяльність, яка може загрожувати стабільності держав, особливо у випадку поєднання з транснаціональною злочинністю, включаючи відмивання грошей, контрабанду зброї, торгівлю наркотичними речовинами. Крім того, вони посягають на права і свободи людини (крадіжка особистих даних фізичних осіб, насилля щодо неповнолітніх, насилля стосовно жінок).

[38] About AFRIPOL. URL: https://afripol.africa-union.org/about (дата звернення: 13.02.2026).

[39] African Union Counter Terrorism Centre. ABOUT US. URL: https://caert.org.dz/about-us/мм(дата звернення: 13.02.2026).

Подолання цього негативного явища потребує сумісних активних дій з боку держав і міжнародного співтовариства та вирішення спільних проблем, серед яких: 1. Втрата даних: електронні дані є ключем до успішних розслідувань у всіх сферах кіберзлочинності, але можливості отримання таких даних значно обмежені. 2. Втрата місцезнаходження: останні тенденції призвели до ситуації, коли правоохоронні органи більше не можуть встановити фізичне місцезнаходження злочинця, злочинну інфраструктуру чи електронні докази. 3. Проблеми, пов'язані з національними правовими рамками: відмінності у національних правових базах держав. 4. Перешкоди для міжнародної співпраці: у міжнародному контексті не існує спільної правової бази для прискореного обміну доказами (як і для їх збереження). Існує також очевидна потреба в кращому механізмі транскордонної комунікації та швидкого обміну інформацією. 5. Проблеми державно-приватного партнерства: співпраця з приватним сектором є життєво важливою для боротьби з кіберзлочинністю, проте стандартизованих правил взаємодії немає, і таким чином розслідування можуть бути ускладнені[40].

Міжнародне співтовариство докладає зусиль щодо розробки правової основи протидії кіберзлочиннності та криміналізації протиправних дій про що свідчать акти, прийняті на рівні ООН та регіональних міжнародних організацій (РЄ, ЄС, ОБСЄ, ЛАД, АС), згідно з якими кіберзлочини віднесено до окремого виду міжнародних правопорушень. Важливим є імплементація існуючих міжнародних норм у національне законодавство; криміналізація кіберзлочинів; посилення співпраці держав з міжнародними спеціалізованими інституційними органами (структурами, агентствами) універсального і регіонального характеру задля попередження розповсюдження злочинів та притягнення до відповідальності винних осіб.

АНОТАЦІЯ

Стаття присвячена дослідженню міжнародно-правової та інституційної складової протидії кіберзлочинності. Проаналізовано положення міжнародних універсальних актів, акцентовано увагу на першому глобальному договорі про кіберзлочинність – Конвенції Організації Об'єднаних Націй проти кіберзлочинності (резолюція Генеральної Асамблї ООН 79/243). Розкрито сутність та особливості актів, прийнятих на рівні Ради Європи (Конвенція про кіберзлочинність 2001 р та додаткові протоколи до Конвенції, рекомендації тощо), Європейського Союзу (установчі акти, директиви, рішення, регламенти, повідомлення), Африканського Союзу (договірні та стратегічні акти); означено роль ОБСЄ у підвищенні кібер- / ІКТ-безпеки тощо. Зосереджено увагу на діяльності органів, інституцій, агентств, створених на міжнародному універсальному рівні (Міжнародна організація кримінальної поліції (Інтерпол), Контртерористичний комітет ООН, Міжнародний союз електрозв'язку тощо) та на регіональному рівні (Європейське поліцейське агентство (Європол),

[40] Common challenges in combating cybercrime As identified by Eurojust and Europol June 2019. URL: https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf (дата звернення: 13.02.2026).

Агентство Європейського Союзу з питань співробітництва у сфері кримінального правосуддя (Євроюст), Агентство Європейського союзу з кібербезпеки, Європейський центр боротьби з кіберзлочинністю, Механізм поліцейського співробітництва Африканського Союзу (AFRIPOL), Контр-терористичний центр Африканського Союзу (AUCTC) тощо) та їх ролі у протидії кіберзлочинності. Зроблено відповідні висновки і рекомендації.

Ключові слова: безпекові виклики, електронна торгівля, злочини, імплементація, криміналізація, міжнародні інституції, міжнародне співробітництво, особисті дані, права людини, Цілі сталого розвитку, штучний інтелект.

Література

1. About AFRIPOL. URL: https://afripol.africa-union.org/about (дата звернення: 13.02.2026).
2. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. URL: https://rm.coe.int/168008160f (дата звернення: 14.02.2026).
3. African Forum on cybercrime. URL: https://au.int/fr/node/34897 (дата звернення: 13.02.2026).
4. African Union Counter Terrorism Centre. ABOUT US. https://caert.org.dz/about-us/мм (дата звернення: 13.02.2026).
5. African Union Convention on Cyber Security and Personal Data Protection. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/african_union_convention_on_cyber_security_and_personal_data_protection__html/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (дата звернення:11.02.2026).
6. AFRIPOL Cybercrime Strategy. URL: https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/ (дата звернення: 13.02.2026).
7. Arab Convention on Combating Information Technology Offences. URL: https://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/arab_convention_on_combating_information_technology_offences__html/Arab_Convention_on_Combating_Information_Technology_Offences.pdf (дата звернення:12.02.2026).
8. Case of K.U. v. Finland (Application no. 2872/02). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964%22] (дата зверненн:12.02.2026).
9. Communication from the Commission to the Council and the European Parliament Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0140 (дата звернення: 12.02.2026).
10. Common challenges in combating cybercrime As identified by Eurojust and Europol June 2019. URL: https://www.eurojust.europa.eu/sites/default/files/assets/2019-06-joint-eurojust-europol-report-common-challenges-in-combating-cybercrime-en.pdf (дата звернення: 13.02.2026).
11. Consolidated text: Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services,

in particular electronic commerce, in the Internal Market (Directive on electronic commerce). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02000L0031-20240217 (дата звернення:12.02.2026).

12. Convention on Cybercrime. URL: ttps://sherloc.unodc.org/cld/uploads/res//treaties/definitions/treaty/convention_on_cybercrime_html/Budapest_Convention_on_Cybercrime.pdf (дата звернення:11.02.2026).

13. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/dec/2019/797/oj/eng (дата звернення: 12.02.2026).

14. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. URL: https://eur-lex.europa.eu/eli/reg/2019/796/oj/eng (дата звернення: 12.02.2026).

15. Consolidated version of the Treaty on the Functioning of the European Union. URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (дата звернення: 10.02.2026).

16. Consolidated text: Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA. URL: https://eur-lex.europa.eu/eli/reg/2018/1727/2025-11-04/eng (дата звернення: 13.02.2026).

17. Constitution of the International CriminaL Police Organization-INTERPOL. URL: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents (дата звернення: 10.02.2026).

18. Cyber Defenders. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders (дата звернення: 13.02.2026).

19. Cybercrime. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (дата звернення: 10.02.2026).

20. Cybercrime. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 10.02.2026).

21. Сироїд Т. Л., Гавриленко О. А. Внесок Ради Європи у забезпечення інформаційної безпеки та протидію кіберзлочинності. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2020. Вип. 61, т. 2. С. 149–154. DOI https://doi.org/ 10.32782/2307-3322.61-2.33

22. Сироїд Т.Л. Міжнародно-правове регулювання сфери інформаційно-комунікаційних технологій і протидія кіберзлочинності // Сучасні проблеми міжнародного права. Liber Amicorum до 60-річчя проф. М. В. Буроменского: моногр. / авт. кол.; за ред. В. М. Репецького, В. В. Гутника. Львів; Одеса: Фенікс, 2017. 564 с. С. 495-521. ISBN 978-966-928-118-0

23. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення: 12.02.2026).

24. 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. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (дата звернення:12.02.2026).

25. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. URL: https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng (дата звернення:12.02.2026).

26. Documents Agenda 2063. URL: https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf (дата звернення: 13.02.2026).

27. European Cybercrime Centre URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення:12.02.2026).

28. European Judicial Cybercrime Network. URL: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network (дата звернення: 12.02.2026).

29. Increasing co-operation against cyberterrorism and other largescale attacks on the Internet. URL: http://www.europeanrights.eu/public/atti/2070_ing.pdf (дата звернення:13.02.2026).

30. Joint Cybercrime Action Taskforce. URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (дата звернення:08.02.2026).

31. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (дата звернення: 12.02.2026).

32. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 12.02.2026).

33. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. https://eur-lex.europa.eu/eli/reg/2016/794/oj/eng (дата звернення: 13.02.2026).

34. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG (дата звернення: 13.02.2026).

35. Resolution adopted by the General Assembly [without reference to a Main Committee (A/55/L.2)] 55/2. United Nations Millennium Declaration. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_55_2.pdf (дата звернення:09.02.2026).

36. Resolution 1373 (2001). URL: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (дата звернення: 12.02.2026).

37. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (дата звернення:14.02.2026).

38. The Digital Transformation Strategy for Africa (2020-2030). URL: https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.p (дата звернення: 13.02.2026).

39. THE 17 GOALS. URL: https://sdgs.un.org/goals (дата звернення: 08.02.2026).

40. 79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes. URL: https://docs.un.org/en/A/RES/79/243 (дата звернення 11.02.2026).

41. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication. 1994). URL: https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF (дата звернення:11.02.2026).

Information about the author:
Syroid Tetiana Leonidivna,
DSc(Law), Professor,
Head of the Department of International and European Law
V.N. KarazinKharkivNational University Kharkiv,
4, Svobody square, Kharkiv, 61022, Ukraine