DOI https://doi.org/10.30525/978-9934-26-686-7-13

КОНВЕНЦІЯ РАДИ ЄВРОПИ ПРО КІБЕРЗЛОЧИННІСТЬ ЯК ОСНОВА КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ СУСПІЛЬНИХ ВІДНОСИН У КІБЕРПРОСТОРІ В УКРАЇНИ

Політова А. С.

ВСТУП

Відзначимо, що новинами про кіберзлочини вже нікого не дивують, а така інформація сприймається як звичайна. Правоохоронні органи адаптуються до нових викликів та розвивають нові механізми у сфері кіберзахисту. Захист відбувається на кількох рівнях – як на суто технічному й програмному, так і на рівні законодавства. Країни ЄС та США вже мають відповідну базу знань і процедур, які ефективно працюють у сфері кіберзахисту. Україна так само мало не щодня відповідає все новим і новим викликам і працює над запобіганням таким злочинам[1].

Досліджуючи світові тенденції деякі вчені відзначають, що кількість здійсненних кібератак щорічно зростає, а їх характер дедалі стає складнішим. Фішингові атаки є лідерами серед кіберзлочинів у світі, які демонструють тенденціюдо подальшого збільшення. У 2023р. кількість атак із використанням зловмисного програмного забезпечення становила 6,06 млрд випадків, що свідчить про масштабність проблеми. Глобальні фінансові втрати від кіберзлочинності у 2023 р. склали понад 7,1 трлн дол. США, а до 2029 р. можуть зрости до15,63 трлн дол. США. Основними наслідками для організацій від втрати конфіденційної інформації є: втрата доходу (56,6 %), погіршення репутації (38,9 %) та послаблення конкурентних позицій (35,8 %). Найбільш вразливими залишаються освітній сектор, урядові структури, сектор розваг та фінансові установи. У цих галузях є значна кількість інцидентів із використанням зловмисного програмного забезпечення. США, росія, Франція та Нідерланди є основними країнами-джерелами кібератак, тоді як Канада та Сінгапур демонструють найвищий рівень непокоєння щодо можливих загроз[2]. Окрім того, відповідно до світового рейтингу кіберзлочинності (*World Cybercrime Index*), який був розроблений авторами з Оксфордського університету та Університету Нового Південного Вельсу, найпершою в рейтингу кіберзлочинності стала Росія (58,39 бала), за нею з великим відривом ідуть Україна (36,44 бала), Китай (27,86 бала), США (25,01 бала),

[1] Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. *Mind.ua*. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu (дата звернення: 14.02.2026).

[2] Дикий, А., Савіцький, В., Савчук, С., & Соха, А. (2025). Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав. *Society and Security*, (1(7), 63–74. https://doi.org/10.26642/sas-2025-1(7)-63-74

Нігерія (21,28 бала) та Румунія (14,83 бала). Велика Британія посідає восьме місце у списку (9,01 бала)[3].

Реформа законодавства України, у тому числі й Кримінального кодексу, привертає увагу до питання імплементації у національне законодавство положень міжнародних актів, у тому числі й протидії злочинності. Враховуючи цей аспект, метою нашого дослідження є імплементація положень Конвенції Ради Європи про кіберзлочинність у Кримінальний кодекс України щодо кримінальної відповідальності за кіберзлочини.

1. Конвенція Ради Європи про кіберзлочинність: аналіз окремих положень

І. І. Нагорний вважає, що популярність використання цифрових платформ, перехід до електронного формату документообігу, а також віртуального простору в усіх сферах суспільного життя зумовило виникнення нових форм злочинної поведінки, які називають «кіберзлочини», що за своїм змістом відрізняються від традиційних кримінальних правопорушень за своїм масштабом, способами вчинення та наслідками. Злочини у сфері ІТ вчиняються дистанційно та виходять за межі юрисдикції держав, унаслідок чого національні правові й правоохоронні системи виявляються нездатними до оперативного реагування на нові виклики й загрози [4].

Відзначимо, що перші спроби уніфікувати правові підходи щодо протидії кіберзлочинам у країнах Європи відбувалися під егідою ради Європи. Одне з найбільш ґрунтовних діянь, зорієнтованих на регулювання цієї проблеми, є ухвалення Рекомендацією Європи 23 листопада 2001 р. Конвенції про кіберзлочинність (ратифікована 1 липня 2004 р.).

У преамбулі Конвенції про кіберзлочинність зазначено, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами та даними, шляхом установлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва[5].

---

[3] Крайня В. Світовий рейтинг кіберзлочинності очолила Росія. Україна посіла друге місце. *ms.detector.media*. URL: https://ms.detector.media/kiberbezpeka/post/34647/2024-04-11-svitovyy-reytyng-kiberzlochynnosti-ocholyla-rosiya-ukraina-posila-druge-mistse/ (дата звернення: 14 .02.2026).

[4] Нагірний І. П. Еволюція правової протидії злочинам у сфері інформаційних технологій: історичні витоки та сучасні виклики. *Європейський правничий часопис*. 2026. С. 141-147. URL: https://doi.org/10.36919/3041-1149(print).11.2025.141-147 (дата звернення: 14.02.2026).

[5] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

Отже, зупинимося більш детально на загальній характеристиці цієї Конвенції.

Розділ І. Використання термінів Конвенції включає лише одну статтю, де закріплено визначення термінів, що застосовуються, зокрема:

- «Комп'ютерна система» – будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

- «Комп'ютерні дані» – будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

- «Постачальник послуг» означає:

і. будь-яку державну або приватну установу, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та

іі. будь-яку іншу установу, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги;

- «Дані про рух інформації» – будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги[6].

Саме Розділ ІІ. Заходи, які мають здійснюватися на національному рівні Конвенції має велике значення для нашого дослідження, адже саме положення цього розділу при ратифікації Конвенції повинні бути імплементовані у національне законодавство – Закон України про кримінальну відповідальність та Кримінальний процесуальний кодекс України.

Зупинимося більш детально на основних аспектах Частини 1. Матеріальне кримінальне право Розділ ІІ Конвенції. Проведений аналіз дозволяє відзначити, що ця частина включає п'ять заголовків, а саме:

Заголовок 1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

- ст. 2. Незаконний доступ, тобто навмисний доступ до цілої комп'ютерної системи або її частини без права на це; таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою;

- ст. 3. Нелегальне перехоплення – навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані; таке правопорушення було вчинене з

[6] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою;

- ст. 4. Втручання у дані – навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

- ст. 5. Втручання у систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

- ст. 6. Зловживання пристроями – навмисне вчинення, без права на це:

a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином:

i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 вище;

ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та

b. володіння предметом, перерахованим у підпунктах a. і або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5;

Заголовок 2. Правопорушення, пов'язані з комп'ютерами:

- ст. 7. Підробка, пов'язана з комп'ютерами, тобто навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти;

- ст. 8. Шахрайство, пов'язане з комп'ютерами – навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом:

a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних,

b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи;

Заголовок 3. Правопорушення, пов'язані зі змістом:

- ст. 9. Правопорушення, пов'язані з дитячою порнографією, тобто навмисне вчинення, без права на це, наступних дій:

a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;

b. пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;

c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;

d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;

e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації;

Заголовок 4. Правопорушення, пов'язані з порушенням авторських та суміжних прав:

- ст. 10. Правопорушення, пов'язані з порушенням авторських та суміжних прав, яке полягає: «1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.

2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем»[7].

Окрім того, у Заголовку 5. Додаткова відповідальність і санкції передбачено:

- ст. 11. Спроба і допомога або співучасть, тобто навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів, перерахованих у статтях 2-10 цієї Конвенції, з метою вчинення такого злочину; навмисну спробу вчинити будь-який зі злочинів, перерахованих у статтях 3-5, 7, 8, 9.1.a та 9.1.c цієї Конвенції;

- ст. 12. Корпоративна відповідальність, тобто юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи.

Окрім того, така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

a. повноважень представляти цю юридичну особу;

b. повноважень приймати рішення від імені цієї юридичної особи;

c. повноважень здійснювати контроль в рамках цієї юридичної особи[8].

- ст. 13. Санкції і заходи – звернута увага на два аспекти:

По-перше, кримінальні правопорушення, встановлені відповідно до статей 2-11, каралися ефективними, пропорційними і переконливими санкціями, включаючи позбавлення волі;

[7] Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

[8] Там само.

По-друге, юридичні особи, які несуть відповідальність відповідно до статті 12, каралися ефективними, пропорційними і переконливими кримінальними або некримінальними санкціями або заходами, включаючи грошові санкції.

Таким чином, можна відзначити, що у Частині 1. Матеріальне кримінальне право Конвенції визначено діяння, за повинна наставати кримінальна відповідальність. Окрім того, визначено особливості кримінальної відповідальності у співучасті за такі діяння, покарання для фізичних та юридичних осіб. Також ми погоджуємося з тим, що рівень можливостей, які отримують зловмисники, й тенденція до збільшення кількості злочинів у сфері комп'ютерних інформаційних технологій становлять загрозу не лише демократичним перетворенням та розвитку інформаційного суспільства в Україні, а й національній безпеці загалом[9].

2. Кіберзлочини: поняття та види кримінальних правопорушень

Аналізуючи положення Кримінального кодексу України зауважимо, що поняття «кіберзлочини», «кіберзлочинність», «комп'ютерні кримінальні правопорушення» або «кримінальні правопорушення у сфері інформаційних технологій» не врегульовано. Окрім того, ці дефініції не знайшли однозначного формулювання й у працях вчених, які також пропонуються різні критерії класифікації таких кримінально протиправних діянь.

Так, наприклад, під кіберзлочинністю пропонується розуміти сукупність правопорушень, скоєних у «кіберпросторі» за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж та комп'ютерних даних[10]. Натомість інші вчені стверджує, що кіберзлочинність – це сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [11]. І. І. Васильковський відзначає, що кіберзлочинність (або «злочин з використанням комп'ютерних технологій») – це економічний злочин, скоєний з використанням обчислювальної техніки та мережі Інтернет. Приклади кіберзлочинності можуть бути різними: розповсюдження вірусів, незаконне вивантаження інформації, фішинг і фармінг, а також розкрадання особистої інформації (наприклад, реквізитів банківських рахунків). До цієї категорії відносять тільки ті економічні злочини, в яких основним (а не допоміжним або

[9] Dulepa V. P. Criminological characteristics of cybercrime. *Juridical scientific and electronic journal*. 2021. No. 11. P. 592–595. DOI: https://doi.org/10.32782/2524-0374/2021-11/147 (date of access: 17.02.2026).

[10] Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

[11] Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посібн. Харків : Право, 2014. 284 с.

супутнім) інструментом скоєння злочину є комп'ютер, Інтернет або електронні носії інформації та пристрої[12].

Саме тому можна погодитися із С. В. Корзун, яка відзначає, що поняття «кіберзлочинність» має багатовекторне розуміння, що обумовлено його поширеністю в різних сферах суспільних відносин (економічна система, політична система, міжнародні відносини, соціальна сфера), різноманітними наслідками (економічні, соціальні, людські жертви, психологічні та інші) та впливом на національну безпеку (інформаційну, безпеку державного кордону, політичну, економічну, енергетичну, продовольчу та інші)[13].

Що ж нормативного визначення, то, зокрема, у Законі України від 5 жовтня 2017 р. № 2163-VIII «Про основні засади забезпечення кібербезпеки України» відзначено, під кіберзлочином (комп'ютерним злочином) слід розуміти суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [14]. Такий підхід законодавця свідчить про використання термінів «кіберзлочини» та «комп'ютерні злочини» як синонімів. Але, як вважає О. І. Денькович, недоліком вказаного законодавчого визначення кіберзлочинності (так само як і визначення злочинності в межах статистичного підходу) є те, що воно відображає НЕ сутність та зміст поняття (тобто сукупність його істотних, необхідних і достатніх ознак), а його обсяг (тобто вказує на об'єкти, як за методологічними підходами доктринальні кримінологічні визначення кіберзлочинності виходять з того, що цей вид злочинності є сукупністю кримінальних правопорушень, їх арифметичною сумою. Різняться вони у тому, які саме кримінальні правопорушення потрібно включати в обсяг цього поняття, тобто якими ознаками характеризується кіберзлочин як одиничний елемент вказаної суми, чим він відрізняється від інших видів кримінальних правопорушень [15].

М. Ю. Яцишин виокремлює такі критерії, які дозволяють вченому узагальнити основні кваліфікаційні ознаки кібернетичних злочинів як основи їх класифікації:

---

[12] Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2 (10-11). С. 276–28.

[13] Корзун С. В. Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам. *Економіка, управління та адміністрування*. 2025. № 1(111). С. 131–145. DOI: https://doi.org/10.26642/ema-2025-1(111)-131-145 (дата звернення: 17.02.2026).

[14] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.02.2026).

[15] Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 17.02.2026).

1. Кіберзлочини, що виникли в результаті створення і поширення ІКТ, та завдають шкоду учасникам кіберпростору шляхом порушення конфіденційності, цілісності та доступності ІКТ. До цього виду злочинних діянь відносяться: незаконний доступ; нелегальне перехоплення; втручання в дані; втручання в систему; зловживання пристроями.

2. Традиційні злочини, вчинені з використанням ІКТ: тероризм; підробка; шахрайство; переслідування, вимагання, порушення права інтелектуальної власності та ін.

3. Кіберзлочини, що пов'язані зі створенням та розповсюдженням нелегального контенту за допомогою ІКТ. До цієї групи злочинних діянь відносимо будь-які цифрові операції із забороненою інформацією, яку становить дитяча порнографія, расистський та ксенофобний матеріал тощо[16].

Але А. В. Боровик та І. М. Копотун вважають, що основною сутнісною ознакою кіберзлочину є те, що це діяння, сама можливість вчинення якого випливає з особливих можливостей інформаційно-телекомунікаційних технологій, які використовуються для завдання шкоди суспільним відносинам[17].

Такі різні підходи щодо визначення ознак кіберзлочинів дозволяють відзначити, що до основними їх властивостями, на нашу думку, є: вчинення діяння у кіберпросторі або із застосуванням інформаційно-комунікаційних технологій; використання специфічних способів реалізації кримінально протиправного наміру (несанкціонованого доступу, втручання в роботу систем, шкідливе програмне забезпечення, маніпулювання даними, соціальна інженерія); спрямованість посягання на інформацію, цифрові ресурси та інфраструктуру; анонімність або псевдоанонімність суб'єкта; транснаціональний організований характер таких кримінальних правопорушень; високий рівень латентності та складність їх виявлення і доказування у кримінальному провадженні.

Окрім того, звернемо увагу й на те, що в основу класифікації кібезлочинів вчені пропонують різні критерії, враховуючи, у тому числі, й положення міжнародного кримінального права. Так, наприклад, Д. Ю. Дрижакова, О. О. Горішній та М. М.Тараненко досліджуючи питання ефективності правових механізмів запобігання кіберзлочинності в Україні відзначають, що відповідно до міжнародних підходів кіберзлочини поділяються на кілька основних категорій:

- злочини проти комп'ютерних систем (наприклад, несанкціонований доступ до інформації, її знищення чи модифікація);
- злочини з використанням інформаційних технологій (шахрайство, розповсюдження шкідливого програмного забезпечення, викрадення персональної інформації);

[16] Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

[17] Боровик А. В. Кіберзлочини в Україні (кримінально-правово характеристика) : навч. посіб. Луцьк : ВолиньПоліграф, 2019. 304 с.

- злочини, пов'язані з контентом (кібертероризм, розповсюдження незаконної інформації, зокрема пропаганди насильства або дитячої порнографії)[18].

Натомість В. Г. Кундеус пропонує класифікувати за такими видами залежно від об'єкту посягання кіберзлочини (комп'ютерні злочини):

1) Злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами КК України. Такі злочини посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об'єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки. Наприклад: викрадення реквізитів платіжних карток (фішинг, вішинг, шиммінг, скимінг); незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардінг); заволодіння коштами через фіктивні Інтернет-магазини, Інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн-шахрайство); порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо.

2) Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України. Ознакою віднесення цих злочинів до комп'ютерних є те, що вони посягають на відносини, що виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку[19].

Але є дослідники, які не виокремлюючи критеріїв (підстав) для класифікації кіберзлочинів, просто надають їх перелік. Так, наприклад, Н. В. Савчук наводить рейтинг найбільш суттєвих кіберзлочинів:

- фальшиві рахунки на оплату із Інтернет-магазину (підроблені рахунки, які розсилаються електронною поштою, містять посилання на шкідливі програми);
- фальшиві повідомлення про доставку товару (злочинці часто видають себе за популярні поштові служби та розсилають листи, які під прикриттям повідомлення містять віруси);
- фішинг – заволодіння платіжними особистими даними користувачів шляхом обману на шахрайське їх використання, що пов'язано із електронною комерцією;

[18] Дрижакова Д. Ю., Горішній О. О., Тараненко М. М. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні. 2025. URL: https://doi.org/10.5281/zenodo.15074665 (дата звернення: 14.02.2026).

[19] Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

- крадіжка особистих даних через фальшиве анкетування (користувачі, які люблять заповнювати різного роду анкети в обмін на різні подарунки, потрапляють до групи ризику);

- компроментування популярних веб-сайтів (кіберзлочинці атакують ті сайти, які відвідує найбільша кількість користувачів);

- відправлення результатів пошукових запитів (користувачам розсилаються посилання на веб-сайти при використанні яких комп'ютер отримує вірус, що призводить значних збитків);

- вірусна реклама;

- небезпечні привітальні листівки;

- підроблені сайти благодійних фондів;

- шахрайство на розпродажу (відвідавши сайт користувачі, клікнушви по банерній рекламі дешевого мобільного телефону, стають жертвами програми – троянський кінь)[20].

У дослідженні «Cyber crime: A review of the evidence» Dr. Mike McGuire (University of Surrey) та Samantha Dowling (Home Office Science) виокремлюють:

- Кіберзалежні злочини – це правопорушення, які можуть бути вчинені лише за допомогою комп'ютера, комп'ютерних мереж або іншої форми ІКТ. Ці діяння включають поширення вірусів та іншого шкідливого програмного забезпечення, хакерство та розподілені атаки типу «відмова в обслуговуванні» (DDoS), тобто перевантаження Інтернет-серверів для виведення з ладу мережевої інфраструктури або веб-сайтів. Кіберзалежні злочини – це, перш за все, діяння, спрямовані проти комп'ютерів або мережевих ресурсів, хоча атаки можуть мати й вторинні наслідки, такі як шахрайство.

- Кіберзлочини – це традиційні злочини, масштаб або охоплення яких збільшуються завдяки використанню комп'ютерів, комп'ютерних мереж або інших ІКТ. На відміну від кіберзалежних злочинів, їх все ще можна вчиняти без використання ІКТ. Такими типами кіберзлочинів є:

шахрайство (включаючи масовий маркетинг, фішингові електронні листи та інші види шахрайства; шахрайство в онлайн-банкінгу та електронній комерції);

крадіжка (включаючи крадіжку особистої інформації та даних, пов'язаних із ідентифікацією);

сексуальні злочини проти дітей (включаючи ґрумінг і створення та/або розповсюдження сексуальних зображень) [21].

Отже, проведений нами аналіз щодо поняття «кіберзлочинів» та видів кримінальних правопорушень, дозволяють зробити висновок, що поняття «кіберправопорушення» відображає широкий спектр суспільно небезпечних діянь, що здійснюються в кіберпросторі за допомогою комп'ютерних систем та мереж. Сучасне розуміння кіберзлочинності становить не лише традиційні

[20] Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. URL: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf (дата звернення: 18.02.2026).

[21] Dr. Mike McGuire, Samantha Dowling. Cyber crime: A review of the evidence / Summary of key findings and implications. Home Office Research Report 75. October 2013. URL: https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf (дата звернення: 18.02.2026).

правопорушення, адаптовані до цифрового середовища, але й злочинні дії, які стали можливими завдяки новітнім технологіям. Ці правопорушення мають різноманітний характер і об'єкт впливу, охоплюючи від порушень інформаційної безпеки до шахрайств та кібератак. Науковці та правозахисники вживають різні терміни для опису цих правопорушень, зокрема «комп'ютерні правопорушення», «кіберправопорушення» та інші, кожен з яких має свою специфіку та значення залежно від контексту. Відмінності у трактуванні цих понять негативно впливають на законодавчі та практичні аспекти протидії кіберправопорушенням [22].

Окрім того, на підставі проведеного аналізу існуючих підходів щодо дефініції «кіберзлочинів», пропонуємо під кіберзлочинами розуміти суспільно небезпечні діяння, що вчиняються у цифровому середовищі або з використанням інформаційно-комунікаційних мереж, хмарних сервісів чи інших елементів кіберпростору, та спрямованих на порушення конфіденційності, цілісності або доступності інформації, цифрових ресурсів і технологічної інфраструктури, а також на завдання майнової чи немайнової шкоди фізичним і юридичним особам, суспільстві або державі. У сучасних проявах кіберзлочинності характеризується активним використанням автоматизованих атак, штучного інтелекту, технологій соціальної інженерії, криптовалюти, уразливого програмного забезпечення, що зумовлює трансформацію як спосіб вчинення таких кримінальних правопорушень, так і механізмів їх протидії.

3. Імплементація положень Конвенції Ради Європи про кіберзлочинність в Кримінальний кодекс України

Як стверджує В. Г. Кундеус, політика в сфері протидії кіберзлочинності здійснюється різноманітними засобами. Найбільш ефективними у системи її протидії залишаються засоби кримінально-правового впливу. Діяльність з протидії кіберзлочинам засобами кримінально-правового впливу ґрунтується на їх криміналізації. Хоча поняття «кіберзлочинність», «кіберзлочини» використовується як у міжнародному, так і у національному законодавстві, Кримінальний кодекс (далі – КК України) не містить визначення поняття кіберзлочину[23].

Аналіз наукових публікацій щодо імплементації положень міжнародно-правових актів щодо протидії кіберзлочинам вказує на те, що дискусійним питанням залишається визначення переліку міжнародно-правових актів, які регулюють це питання. Так, наприклад, О. М. Жеребець стверджує, що центральне місце на національному рівні в механізмі правового регулювання

[22] Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

[23] Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

боротьби з такими злочинами займають норми: Європейської Конвенції про взаємну правову допомогу у кримінальних справах 1959 р. (ратифікована із застереженнями і заявами Законом України від 16.01.98 р. № 4498-ВР), Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 р. (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV), Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 р. (ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV), загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору [24]. Натомість інші вказують, що до цих міжнародних актів відносяться: 1) Конвенція про кіберзлочинність Ради Європи, прийнята 21.11.2001 р. та Додатковий протокол від 28.01.2003 р. (далі – Будапештська конвенція); 2) Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. (далі – Конвенція ЛАД); 3) Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (далі – Угода ШОС); 4) Конвенція про кібербезпеку і захист персональних даних Африканського Союзу від 27.06.2014 р. (далі – Конвенція АС) [25]. Також М. І. Саєнко, Є. А. Савела та Ю. Ю. Тополянський вважають, що до таких міжнародно-правових актів відносяться: конвенція «Про кіберзлочинність», ратифікована у 2005 р. державами Ради Європи та іншими державами; Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 р.; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 р.; Мінімальний список правопорушень у боротьбі з кіберзлочинністю цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 р. [26]. Окрім того, висловлюється й така думка, що найбільш відомим міжнародним документом у цій сфері є Конвенція Ради Європи про кіберзлочинність (так звана Будапештська конвенція, далі – Конвенція), яка стала базовим орієнтиром для багатьох країн світу, зокрема й України. Подальший розвиток цього документа відображено в Додатковому протоколі до Конвенції 2003 р., спрямованому на криміналізацію діянь расистського та ксенофобського характеру, а також у Другому додатковому протоколі 2022 р., 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 та Директива (ЄС)

[24] Zherebets O. Implementation of state policy in the field of combating cyber crime: legislative aspect. *INFORMATION AND LAW*. 2021. No. 4(39). P. 129–134. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248834 (date of access: 14.02.2026).

[25] Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

[26] Saenko M. I., Savela E. A., Topolyansky Y. Y. International experience against cyber crime and cyber crime. *Uzhhorod National University Herald. Series: Law*. 2021. No. 64. P. 386–391. DOI: https://doi.org/10.24144/2307-3322.2021.64.71 (date of access: 14.02.2026).

2022/2555 (NIS2 Directive), що визначають межі захисту критичної інформаційної інфраструктури та взаємодії між державами-членами.

Саме тому можна погодитися із Р. В. Захаревичем, який стверджує, що успішна боротьба з кіберзлочинами вимагає від українського законодавства не тільки оперативного реагування на нові виклики, але й запозичення найкращих практик міжнародного права та досвіду провідних країн у сфері кібербезпеки. Імплементація зарубіжного досвіду дозволяє не лише модернізувати національну правову систему, а й гармонізувати її з міжнародними стандартами, що є необхідною умовою для ефективної співпраці в боротьбі з транскордонною кіберзлочинністю[27].

Так, беззаперечно, що в умовах повномасштабного вторгнення Російської Федерації на територію України, важливе значення має саме захист інформаційної безпеки. У Стратегії кібербезпеки України зазначено, що «Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури» [28]. Окрім того, це пов'язано також з необхідністю гармонізації українського законодавства з міжнародними стандартами, зокрема, й адаптацією до вимог Європейського Союзу та Конвенції про кіберзлочинність.

У першому підрозділі нашого дослідження нами проаналізовано окремі положення Конвенції Ради Європи про кіберзлочинність та визначено перелік діянь, за які за національним законодавством повинна бути передбачена відповідальність. Вважаємо, що такий аналіз щодо імплементації положень Конвенції у Кримінальний кодекс України найкраще відобразити у формі Таблиці 1.

Разом з тим, враховуючи положення Конвенції Ради Європи про кіберзлочинність, В. Г. Хахановський та В. Д. Гавловський, до кіберзлочинів також пропонують відносити: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України); посягання на територіальну цілісність і недоторканність України (ст. 110); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145); надання неправдивих відомостей до органу ведення Державного

[27] Zakharevych R. V. Implementation of foreign experience into Ukrainian legislation on combating cybercrime. *Analytical and Comparative Jurisprudence*. 2025. Vol. 2, no. 3. P. 372–376. URL: https://doi.org/10.24144/2788-6018.2025.03.2.60 (date of access: 14.02.2026).

[28] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.02.2026).

Таблиця 1

Імплементація положень Конвенції Ради Європи про кіберзлочинність у Кримінальний кодекс України

№ з/п	Конвенція Ради Європи про кіберзлочинність	Кримінальний кодекс України
1.	*Стаття 2 – Незаконний доступ* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисний доступ до цілої комп'ютерної системи або її частини без права на це. Сторона може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою.	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер*
2.	*Стаття 3 – Нелегальне перехоплення* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані. Сторона може вимагати, щоб таке правопорушення було вчинене з недобросовісною метою або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації*

Продовження таблиці 1

3.	*Стаття 4 – Втручання у дані* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. 2. Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду.	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації* *Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*
4.	*Стаття 5 – Втручання у систему* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це	*Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* *Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї*

Продовження таблиці 1

5.	*Стаття 6 – Зловживання пристроями* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це: a. виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: i. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у статтях 2-5 вище; ii. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5; та b. володіння предметом, перерахованим у підпунктах a. і або ii вище, з наміром його використання для вчинення будь-якого зі злочинів, перерахованих у статтях 2-5. Сторона може передбачити у законодавстві, що для встановлення кримінальної відповідальності необхідно володіти певною кількістю таких предметів	*Стаття 361-1. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут*
6.	*Стаття 7 – Підробка, пов'язана з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних,	*Стаття 190. Шахрайство* 4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки

	яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти. Сторона може вимагати наявність наміру обману або подібної нечесної поведінки для встановлення кримінальної відповідальності	
7.	*Стаття 8 – Шахрайство, пов'язане з комп'ютерами* Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: a. будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, b. будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи	*Стаття 190. Шахрайство* 4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки
8.	*Стаття 9 – Правопорушення, пов'язані з дитячою порнографією* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, наступних дій: a. вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем; b. пропонування або надання доступу до дитячої порнографії за допомогою	*Стаття 301. Ввезення, виготовлення, збут і розповсюдження порнографічних предметів* 2. Ті самі дії, вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру

	комп'ютерних систем; c. розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем; d. здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; e. володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації	*Стаття 301-2. Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи* 1. Проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу
9.	*Стаття 10 – Правопорушення, пов'язані з порушенням авторських та суміжних прав* 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення авторських прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Паризьким Актом від 24 липня 1971 р. щодо Бернської Конвенції про захист літературних та художніх творів, Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про авторське право, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем. 2. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за порушення суміжних прав, як це визначено законодавством такої Сторони відповідно до її зобов'язань за Міжнародною Конвенцією про захист виконавців, виробників	*Стаття 176. Порушення авторського права і суміжних прав*

	фонограм і організацій мовлення (Римська конвенція), Угодою про торгівельні аспекти прав інтелектуальної власності і Угодою ВОІВ про виконання і фонограми, за винятком будь-яких моральних прав, які надаються такими Конвенціями, у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем.	

реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158); порушення таємниці голосування (ст. 159); порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (ст. 161); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення таємниці усиновлення (удочеріння) (ст. 168); порушення недоторканності приватного життя (ст. 182); розголошення комерційної або банківської таємниці (ст. 232); завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259); незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (в частині збуту через Інтернет) (ст. 263); заклики до вчинення дій, що загрожують громадському порядку (ст. 295); ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300); сутенерство або втягнення особи в заняття проституцією (ст. 303); незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307); викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (ст. 312); викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (в частині збуту через Інтернет) (ст. 313); розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330); погроза або насильство щодо працівника правоохоронного органу (ст. 345); погроза або насильство щодо журналіста (ст. 345-1); погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346); погроза

або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350); незаконне втручання в роботу автоматизованої системи документообігу суду (ч. 1 ст. 376); розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381); розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398); розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422); пропаганда війни (ст. 436); виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1)[29].

Вважаємо, що деякі з таких кримінально протиправних діянь вчиняються з використанням комп'ютерів або комп'ютерних систем, програмного забезпечення тощо, проте серед цього переліку є також кримінальні правопорушення, в які протягом останніх років було внесено зміни та доповнення або викладено в новій редакції. Окрім того, відповідно до п. 7 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р, передбачено завершення імплементації в законодавство України положень Конвенції про кіберзлочинність щодо імплементація в законодавство України положення Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних з терміном виконання IV квартал 2025 р.[30]. Це вказує на те, що робота в цьому аспектів продовжується.

ВИСНОВКИ

За результати проведеного дослідження щодо Конвенції Ради Європи про кіберзлочинність як основи кримінально-правової охорони суспільних відносин у кіберпросторі в України, можна зробити такі висновки:

1. Конвенція Ради Європи про кіберзлочинність є фундаментальним міжнародним документом, спрямованих на криміналізацію діянь, пов'язаних з із використанням інформаційно-комунікаційних технологій, а також на забезпечення ефективного міжнародного співробітництва у сфері запобігання та протидії кіберзлочинності.

2. Для України Конвенція Ради Європи про кіберзлочинність має велике значення, оскільки: по-перше, визначає міжнародно-правові зобов'язання держави у сфері криміналізації кіберзлочинів та напрями міжнародного співробітництва; по-друге, є фундаментом для удосконалення Закону України про кримінальну відповідальність та адаптації його до європейських стандартів.

[29] Хахановський В. Г., Гавловський В. Д. Interpretation and classification of criminal offenses as cybercrimes. *INFORMATION AND LAW*. 2020. No. 2(33). P. 99–109. DOI: https://doi.org/10.37750/2616-6798.2020.2(33).208101 (date of access: 18.02.2026).

[30] Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядж. Каб. Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text (дата звернення: 18.02.2026).

3. Сучасні тенденції розвитку кіберзлочинності, зокрема, активне використання штучного інтелекту, ринку криптовалют, хмарних сервісів, автоматизованих кібератак, атак на критичну інфраструктуру, стають поштовхом для удосконалення нормативно-правових актів з питань протидії кіберзлочинності та розширення напрямів міжнародного співробітництва у протидії злочинності. Разом з тим, ефективність такого механізму залежить від імплементації положень Конвенції Ради Європи про кіберзлочинність у національне законодавство, у тому числі й Кримінальний кодекс України.

АНОТАЦІЯ

Актуальність теми пов'язана з тим, що в сучасних умовах кіберзлочинність набула ознак глобального явища, що посягає не лише на майнові права, конфіденційність та інформаційну безпеку окремих осіб, але й на стабільність функціонування державних інституцій, об'єктів критичної інфраструктури, фінансових систем та механізмів публічного управління. Особливої актуальності ці питання набувають для України в умовах збройної агресії та гібридних загроз, коли кібератаки виступають елементом дестабілізації державного управління, інформаційного впливу та підриву національної безпеки.

Звернута увага на Частину 1. Матеріальне кримінальне право Конвенції Ради Європи про кіберзлочинність, де закріплено перелік діянь, за які повинна наставати кримінальна відповідальність. Визначено особливості кримінальної відповідальності у співучасті за такі діяння, види покарань для фізичних та юридичних осіб за Конвенцією Ради Європи про кіберзлочинність. Проаналізовано існуючі підходи до поняття «кіберзлочини», «кіберзлочинність», «комп'ютерні злочини» та запропоновано авторське визначення поняття «кіберзлочинів». Зауважено, що у сучасних проявах кіберзлочинності характеризується активним використанням автоматизованих атак, штучного інтелекту, технологій соціальної інженерії, криптовалюти, уразливого програмного забезпечення, що зумовлює трансформацію як спосіб вчинення таких кримінальних правопорушень, так і механізмів їх протидії. Відзначено, що п. 7 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р, імплементації в законодавство України положень Конвенції про кіберзлочинність продовжується.

Література

1. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. *Mind.ua*. URL: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu (дата звернення: 14.02.2026).

2. Дикий, А., Савіцький, В., Савчук, С., & Соха, А. (2025). Світові тенденції кіберзлочинності та загрози інформаційній безпеці держав. *Society and Security*, (1(7), 63–74. DOI: https://doi.org/10.26642/sas-2025-1(7)-63-74

3. Крайня В. Світовий рейтинг кіберзлочинності очолила Росія. Україна посіла друге місце. *ms.detector.media*. URL: https://ms.detector.media/

kiberbezpeka/post/34647/2024-04-11-svitovyy-reytyng-kiberzlochynnosti-ocholyla-rosiya-ukraina-posila-druge-mistse/ (дата звернення: 14.02.2026).

4. Нагірний І. П. Еволюція правової протидії злочинам у сфері інформаційних технологій: історичні витоки та сучасні виклики. *Європейський правничий часопис*. 2026. С. 141-147. DOI: https://doi.org/10.36919/3041-1149 (print).11.2025.141-147 (дата звернення: 14.02.2026).

5. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 15.02.2026).

6. Dulepa V. P. Criminological characteristics of cybercrime. *Juridical scientific and electronic journal*. 2021. No. 11. P. 592–595. DOI: https://doi.org/10.32782/2524-0374/2021-11/147 (date of access: 17.02.2026).

7. Shak R. Concepts and Types of Cyber Offenses in Criminal Law. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 44. P. 325–335. DOI: https://doi.org/10.23939/law2024.44.325 (date of access: 14.02.2026).

8. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посібник. Харків : Право, 2014. 284 с.

9. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1-2 (10-11). С. 276–28.

10. Корзун С. В. Понятійно-категоріальний апарат державної кримінально-правової політики протидії кіберзлочинам. *Економіка, управління та адміністрування*. 2025. № 1(111). С. 131–145. DOI: https://doi.org/10.26642/ema-2025-1(111)-131-145 (дата звернення: 17.02.2026).

11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.02.2026).

12. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 17.02.2026).

13. Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум права*. 2018. Т. 53, № 5. С. 92–99. DOI: https://doi.org/10.5281/zenodo.2009191 (дата звернення: 14.02.2026).

14. Боровик А. В. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посібник. Луцьк : ВолиньПоліграф, 2019. 304 с.

15. Дрижакова Д. Ю., Горішній О. О., Тараненко М. М. Оцінка ефективності правових механізмів запобігання кіберзлочинності в Україні. 2025. DOI: https://doi.org/10.5281/zenodo.15074665 (дата звернення: 14.02.2026).

16. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. URL: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf (дата звернення: 18.02.2026).

17. Dr. Mike McGuire, Samantha Dowling. Cyber crime: A review of the evidence / Summary of key findings and implications. Home Office Research Report 75. October 2013. URL: https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf (дата звернення: 18.02.2026).

18. Кундеус, В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора О.М. Литвака (м. Харків, 23 квіт. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 44-45.

19. Zherebets O. Implementation of state policy in the field of combating cyber crime: legislative aspect. *INFORMATION AND LAW*. 2021. No. 4(39). P. 129–134. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248834 (date of access: 14.02.2026).

20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 18.02.2026).

21. Хахановський В. Г., Гавловський В. Д. Interpretation and classification of criminal offenses as cybercrimes. *INFORMATION AND LAW*. 2020. No. 2(33). P. 99–109. DOI: https://doi.org/10.37750/2616-6798.2020.2(33).208101 (date of access: 18.02.2026).

22. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : Розпорядж. Каб. Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-р#Text (дата звернення: 18.02.2026).

Information about the author:
Politova Anna Serhiivna,
Candidate of Legal Sciences, Associate Professor,
Associate Professor of Department of Law
Mariupol State University
6, Preobrazhenska, Kyiv, Ukraine, 3037, Ukraine