КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародного права,
європейської та євроатлантичної інтеграції

Спеціальність 293 «Міжнародне право»
Освітня програма 293.00.01 «Міжнародне право»

БАКАЛАВРСЬКА РОБОТА

на тему:

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ: ПРАВОВИЙ ДОСВІД ЄС ТА УКРАЇНИ

Здобувача 4 курсу
денної форми навчання
Балабанцевої Дарини Олександрівни

Науковий керівник
Шереметьєва О.Ю., кандидат юридичних наук, доцент, доцент кафедри
міжнародного права, європейської та євроатлантичної інтеграції

Київ - 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄС	Європейський Союз
ООН	Організація Об’єднаних Націй
EC3	European Cybercrime Centre
Europol	European Union Agency for Law Enforcement Cooperation
Eurojust	European Union Agency for Criminal Justice Cooperation
ENISA	European Union Agency for Cybersecurity
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU Institutions
GDPR	General Data Protection Regulation
NIS Directive	Network and Information Security Directive
NIS2	Directive on Measures for a High Common Level of Cybersecurity
DSA	Digital Services Act
DMA	Digital Markets Act
CJEU	Court of Justice of the European Union
IP	Internet Protocol
IT	Information Technology

ВСТУП

Стрімкий розвиток інформаційних технологій та активна цифровізація сучасного суспільства зумовили суттєві зміни у функціонуванні держав, економічних систем і суспільних відносин. Інформаційні технології сьогодні стали невід'ємною складовою діяльності органів державної влади, фінансових установ, підприємств та звичайних громадян. Водночас розширення використання цифрових технологій спричинило появу нових ризиків і загроз, пов'язаних із незаконним використанням комп'ютерних систем, мереж та інформаційних ресурсів. Однією з найбільш небезпечних серед таких загроз є кіберзлочинність.

Кіберзлочинність є складним соціально-правовим явищем, що охоплює широкий спектр правопорушень, пов'язаних із застосуванням інформаційно-комунікаційних технологій. До таких правопорушень належать незаконний доступ до комп'ютерних систем, втручання у функціонування інформаційних мереж, поширення шкідливого програмного забезпечення, кібершахрайство, незаконне використання персональних даних та інші злочини, що здійснюються у кіберпросторі [19; 23]. Характерною особливістю кіберзлочинів є їх транснаціональний характер, що суттєво ускладнює процес їх виявлення, розслідування та притягнення винних осіб до відповідальності.

Актуальність теми дослідження зумовлена тим, що кіберзлочинність становить серйозну загрозу для економічної, інформаційної та національної безпеки держав. У сучасних умовах кіберзлочини здатні спричиняти значні матеріальні збитки, порушувати функціонування критично важливої інфраструктури, а також створювати ризики для стабільності діяльності державних інституцій. У зв'язку з цим держави змушені розробляти ефективні механізми правового регулювання та розвивати міжнародне співробітництво у сфері протидії кіберзлочинності.

Важливу роль у формуванні міжнародної системи боротьби з кіберзлочинністю відіграють міжнародно-правові акти, зокрема Конвенція про кіберзлочинність Ради Європи 2001 року, яка визначає основні принципи криміналізації кіберзлочинів та

встановлює механізми міжнародної співпраці у цій сфері [2]. Значне місце у забезпеченні кібербезпеки посідає також законодавство Європейського Союзу, яке включає директиви та регламенти, спрямовані на підвищення рівня захисту інформаційних систем та мережевої інфраструктури [4; 7].

Проблеми протидії кіберзлочинності є предметом наукових досліджень багатьох учених як в Україні, так і за її межами. Вагомий внесок у вивчення правових аспектів кіберзлочинності зробили такі дослідники, як О. Баранов, О. Кузьменко, М. Швець, О. Литвинов, а також зарубіжні науковці Д. Волл, С. Бреннер, М. Яр, Дж. Клаф та інші [15; 16; 20; 22]. У своїх працях вони аналізують теоретичні та практичні аспекти протидії кіберзлочинності, особливості правового регулювання у різних державах, а також проблеми міжнародної співпраці у цій сфері.

Попри значну кількість наукових досліджень, питання правового регулювання боротьби з кіберзлочинністю залишаються актуальними та потребують подальшого наукового осмислення. Особливої уваги потребує вивчення особливостей правового регулювання кіберзлочинності у Європейському Союзі, а також можливостей використання європейського досвіду для вдосконалення законодавства України.

Метою дипломної роботи є на підставі комплексного аналізу міжнародно-правових та національно-правового механізмів протидії кіберзлочинності, особливостей правового регулювання боротьби з кіберзлочинністю у Європейському Союзі та Україні, визначити основні напрями удосконалення законодавства України у цій сфері з урахуванням досвіду ЄС.

Для досягнення поставленої мети необхідно вирішити такі завдання:

— охарактеризувати поняття та основні ознаки кіберзлочинності;
— визначити теоретико-правові підходи до класифікації кіберзлочинів;
— з’ясувати особливості міжнародно-правових механізмів протидії кіберзлочинності;
— розкрити особливості правового регулювання боротьби з кіберзлочинністю в Європейському Союзі;
— охарактеризувати інституційні механізми ЄС у сфері протидії кіберзлочинності;

— узагальнити практику застосування законодавства Європейського Союзу у сфері кібербезпеки;
— висвітлити особливості правового регулювання боротьби з кіберзлочинністю в Україні;
— здійснити порівняльно-правову характеристику законодавства Європейського Союзу та України;
— визначити основні напрями вдосконалення законодавства України у сфері протидії кіберзлочинності.

Об’єктом дослідження є суспільні відносини, що виникають у процесі протидії кіберзлочинності.

Предметом дослідження є правовий досвід, а також законодавство Європейського Союзу та України у галузі боротьби з кіберзлочинністю.

Методологічну основу дослідження становлять загальнонаукові та спеціально-юридичні методи наукового пізнання. У ході дослідження застосовувалися формально-юридичний метод - для аналізу нормативно-правових актів України, Європейського Союзу та міжнародних договорів у сфері протидії кіберзлочинності; порівняльно-правовий метод - з метою зіставлення законодавства України та ЄС у сфері кібербезпеки; системний метод - для дослідження механізмів функціонування міжнародної та національної систем протидії кіберзлочинності; метод аналізу та синтезу - під час опрацювання наукових підходів до визначення поняття та класифікації кіберзлочинів; історико-правовий метод - для дослідження процесу становлення міжнародно-правових механізмів боротьби з кіберзлочинністю; логіко-юридичний метод - при формулюванні висновків і узагальненні результатів проведеного дослідження. Використання зазначених методів дозволило комплексно дослідити особливості правового регулювання боротьби з кіберзлочинністю як на міжнародному, так і на національному рівнях.

Нормативну основу дослідження становлять Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», а також міжнародні договори та нормативно-правові акти

Європейського Союзу, зокрема Конвенція про кіберзлочинність, директиви та регламенти ЄС у сфері кібербезпеки [1; 2; 4; 9; 12].

Наукову основу дослідження становлять праці українських та зарубіжних учених, присвячені проблемам кіберзлочинності, інформаційної безпеки та міжнародного права.

Структура дипломної роботи зумовлена метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, що включають дев’ять підрозділів, висновків до кожного розділу, загальних висновків, а також списку використаних джерел. У першому розділі досліджуються теоретичні засади кіберзлочинності та міжнародно-правові механізми протидії цьому явищу. Другий розділ присвячений аналізу правового регулювання боротьби з кіберзлочинністю у Європейському Союзі та діяльності відповідних інституцій. У третьому розділі розглядаються особливості правового регулювання протидії кіберзлочинності в Україні, проводиться порівняльний аналіз законодавства України та ЄС, а також визначаються напрями вдосконалення національного законодавства у цій сфері.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

1.1. Поняття та ознаки кіберзлочинності в сучасному міжнародному праві

Сучасний етап розвитку суспільства характеризується надзвичайно швидким прогресом інформаційно-комунікаційних технологій, який суттєво впливає на функціонування практично всіх сфер суспільного життя. Упродовж останніх десятиліть спостерігається активна цифрова трансформація суспільних процесів, що проявляється у широкому використанні мережі Інтернет, цифрових платформ, електронних сервісів та різноманітних інформаційних систем. Такі технологічні зміни істотно трансформували способи взаємодії між людьми, державами та організаціями, а також значною мірою вплинули на розвиток економічних, політичних і соціальних процесів.

Сьогодні використання цифрових технологій стало невід'ємною складовою діяльності державних органів, міжнародних організацій, суб'єктів господарювання та громадян. Електронне урядування, цифрові фінансові послуги, онлайн-комунікації, електронна комерція та дистанційна освіта є лише окремими прикладами того, як інформаційно-комунікаційні технології інтегрувалися у повсякденне життя сучасного суспільства. Завдяки цьому значно спростився доступ до інформації, прискорилися процеси передачі даних і комунікації, а також активізувався розвиток міжнародних економічних та соціальних зв'язків [16].

Водночас необхідно зазначити, що поряд із численними позитивними наслідками цифровізації суспільства виникають і нові виклики, які пов'язані з безпекою інформаційного простору. Активне впровадження цифрових технологій створило передумови для появи нових форм протиправної діяльності, які

здійснюються у кіберпросторі. Сучасні технології можуть використовуватися не лише для законної діяльності, але й як інструмент для вчинення злочинів. Саме тому питання протидії кіберзлочинності набуває дедалі більшого значення як на національному, так і на міжнародному рівнях.

З огляду на це боротьба з кіберзлочинністю потребує комплексного підходу, який передбачає поєднання правових, організаційних та технічних заходів. Ефективна протидія таким правопорушенням неможлива без належного нормативно-правового регулювання, міжнародної співпраці, а також використання сучасних технологічних інструментів для виявлення, розслідування та попередження кіберзлочинів [18].

Кіберзлочинність у сучасній науковій та правовій доктрині розглядається як складне і багатовимірне явище, що поєднує правові, технічні та соціальні аспекти. Особливість цього феномена полягає у тому, що він виник безпосередньо в умовах формування інформаційного суспільства та стрімкого розвитку цифрових технологій. У науковій літературі відсутнє єдине універсальне визначення поняття «кіберзлочинність», що пояснюється значною різноманітністю форм і способів здійснення відповідних правопорушень.

Різні дослідники пропонують власні підходи до тлумачення цього поняття, однак більшість із них погоджується з тим, що кіберзлочинність охоплює широкий спектр злочинів, пов’язаних із використанням комп’ютерних систем, інформаційних мереж та інших цифрових технологій [15]. Узагальнюючи наукові підходи до визначення цього явища, можна зазначити, що кіберзлочинність включає як злочини, які здійснюються із використанням інформаційних технологій як інструменту, так і злочини, спрямовані безпосередньо проти комп’ютерних систем, мереж або інформаційних ресурсів [22].

Особливу роль у формуванні міжнародно-правового підходу до визначення та протидії кіберзлочинності відіграє Конвенція Ради Європи про кіберзлочинність 2001 року, більш відома як Будапештська конвенція. Цей міжнародно-правовий документ став першим універсальним актом, спрямованим на гармонізацію кримінального

законодавства держав у сфері боротьби з комп'ютерними злочинами, а також на розвиток міжнародного співробітництва у цій сфері [2].

Положення конвенції визначають основні категорії правопорушень, пов'язаних із використанням інформаційних технологій та комп'ютерних систем. До таких правопорушень належать, зокрема, незаконний доступ до комп'ютерних систем, незаконне перехоплення даних, втручання у функціонування інформаційних систем, комп'ютерне шахрайство, а також інші форми протиправної діяльності у цифровому середовищі [2]. Важливим аспектом цього міжнародного документа є також створення механізмів міжнародної співпраці між державами у сфері розслідування кіберзлочинів.

У наукових дослідженнях кіберзлочинність часто розглядається як особливий різновид злочинної діяльності, що характеризується використанням інформаційних технологій або як інструменту вчинення злочину, або як безпосереднього об'єкта злочинного посягання. У цьому контексті відповідні правопорушення можуть бути спрямовані як проти інформаційних систем і цифрових ресурсів, так і проти суспільних відносин, що реалізуються за допомогою сучасних технологій. Зокрема, це може стосуватися фінансових операцій, електронної комерції, цифрових комунікацій, обробки персональних даних або функціонування державних інформаційних систем [23].

Однією з найбільш характерних рис кіберзлочинності є її транснаціональний характер. На відміну від багатьох традиційних злочинів, кіберзлочини можуть здійснюватися незалежно від територіальних кордонів держав. Правопорушник може знаходитися в одній країні, використовувати сервери, розташовані в іншій державі, а наслідки його дій можуть проявлятися одночасно у кількох країнах світу. Така специфіка значно ускладнює процес виявлення правопорушень, проведення розслідування та притягнення винних осіб до відповідальності. Саме тому ефективна боротьба з кіберзлочинністю потребує активної міжнародної співпраці між державами, міжнародними організаціями та правоохоронними органами різних країн [19].

Кіберзлочинність має також низку характерних ознак, які відрізняють її від інших форм злочинної діяльності. Передусім слід відзначити використання інформаційно-комунікаційних технологій як основного інструменту здійснення правопорушень. У більшості випадків особи, які вчиняють такі злочини, застосовують комп'ютерні системи, мережі передачі даних, глобальну мережу Інтернет, а також інші цифрові інструменти для реалізації своїх протиправних намірів [20].

Іншою важливою характеристикою кіберзлочинності є можливість забезпечення високого рівня анонімності у кіберпросторі. Завдяки використанню сучасних технологій правопорушники можуть приховувати свою особу, застосовувати підроблені або анонімні облікові записи, використовувати спеціалізовані мережі та технічні засоби, що ускладнюють їх ідентифікацію. Це створює додаткові труднощі для правоохоронних органів і потребує застосування спеціальних методів розслідування, а також використання сучасних технічних засобів у сфері цифрової криміналістики [21].

Ще однією характерною рисою кіберзлочинності є високий рівень технологічності. Для здійснення багатьох кіберзлочинів необхідні спеціальні знання у сфері програмування, функціонування комп'ютерних мереж, інформаційної безпеки та інших технічних галузей. Водночас розвиток інформаційних технологій сприяє появі нових способів здійснення злочинів у кіберпросторі, що постійно ускладнює процес їх своєчасного виявлення та попередження [17].

Крім того, кіберзлочинність характеризується значним масштабом і швидкістю поширення. Завдяки глобальному характеру мережі Інтернет навіть один злочин може мати масштабні наслідки та одночасно впливати на велику кількість користувачів у різних країнах світу. Наприклад, поширення шкідливого програмного забезпечення, організація масових фішингових кампаній або здійснення атак на інформаційні системи можуть завдати значної шкоди державним установам, фінансовим організаціям, підприємствам та приватним особам [24].

Важливо також враховувати, що кіберзлочинність постійно трансформується відповідно до розвитку сучасних технологій. Поява нових цифрових платформ,

хмарних сервісів, технологій штучного інтелекту, криптовалют та інших інноваційних рішень створює не лише нові можливості для розвитку суспільства, але й нові інструменти для здійснення протиправної діяльності. У зв'язку з цим держави змушені постійно вдосконалювати національне законодавство, а також розробляти нові механізми протидії кіберзлочинності на національному та міжнародному рівнях [25].

Таким чином, кіберзлочинність слід розглядати як складне соціально-правове явище, яке виникло внаслідок стрімкого розвитку інформаційного суспільства та поширення цифрових технологій. Основними характеристиками цього явища є використання інформаційно-комунікаційних технологій, транснаціональний характер правопорушень, можливість забезпечення анонімності у цифровому середовищі, високий рівень технологічності та значний масштаб потенційних наслідків. Урахування цих особливостей має важливе значення для формування ефективних міжнародно-правових механізмів протидії кіберзлочинності та забезпечення належного рівня безпеки у сучасному цифровому середовищі [23].

Проведений аналіз дає підстави стверджувати, що кіберзлочинність є одним із найдинамічніших видів сучасної злочинної діяльності, розвиток якого безпосередньо зумовлений процесами глобальної цифровізації та активним поширенням інформаційно-комунікаційних технологій. На відміну від традиційних правопорушень, кіберзлочини можуть вчинятися дистанційно, мати транскордонний характер і вирізнятися високим рівнем латентності, що суттєво ускладнює їх своєчасне виявлення та ефективне розслідування. Характерною особливістю таких правопорушень є також використання комп'ютерних систем і цифрових технологій як засобу вчинення злочину або безпосереднього об'єкта злочинного посягання. Сукупність наведених ознак свідчить про необхідність постійного вдосконалення правових та організаційних механізмів забезпечення кібербезпеки [15; 18].

1.2. Теоретико-правові підходи до класифікації кіберзлочинів

Однією з важливих складових наукового дослідження проблеми кіберзлочинності є визначення та аналіз підходів до її класифікації. У сучасній юридичній та кримінологічній літературі значна увага приділяється питанням систематизації правопорушень, що вчиняються із використанням інформаційних технологій, комп'ютерних систем та цифрових мереж [15; 18]. Така увага з боку науковців пояснюється тим, що кіберзлочинність є відносно новим, але надзвичайно динамічним явищем, яке швидко змінюється разом із розвитком технологій. У зв'язку з цим виникає необхідність чіткого визначення основних категорій та видів правопорушень у цифровому середовищі.

Класифікація кіберзлочинів має важливе значення не лише з теоретичної точки зору, але й у практичному вимірі. Насамперед вона сприяє глибшому науковому осмисленню природи кіберзлочинності як соціально-правового явища. Водночас систематизація відповідних правопорушень дозволяє державам формувати більш ефективну правову політику у сфері кібербезпеки, удосконалювати кримінальне законодавство та створювати дієві механізми протидії злочинам у цифровому середовищі. Крім того, чітке розмежування різних видів кіберзлочинів відіграє важливу роль у розвитку міжнародного співробітництва, оскільки сприяє гармонізації законодавства різних держав та створенню спільних підходів до боротьби з такими правопорушеннями [16].

Систематизація кіберзлочинів дозволяє визначити їх правову природу, встановити характерні особливості механізму їх вчинення, а також окреслити найбільш ефективні правові та організаційні інструменти протидії таким діянням. Завдяки цьому правоохоронні органи отримують можливість більш точно визначати кваліфікацію правопорушень, обирати відповідні методи розслідування та застосовувати необхідні заходи запобігання. У свою чергу, для міжнародного права така класифікація створює підґрунтя для розробки узгоджених стандартів

криміналізації кіберзлочинів та формування ефективної системи міжнародної взаємодії у цій сфері [16].

У сучасній юридичній науці сформувалося декілька підходів до класифікації кіберзлочинів. Це пояснюється тим, що кіберзлочинність є складним і багатогранним явищем, яке охоплює елементи різних галузей права, зокрема кримінального, інформаційного та міжнародного права [17; 22]. Крім того, розвиток інформаційних технологій постійно призводить до появи нових форм протиправної діяльності, що ускладнює створення єдиної універсальної класифікації.

Багато науковців пропонують власні критерії класифікації кіберзлочинів, спираючись на різні підходи до аналізу цього явища. Зокрема, дослідники пропонують класифікувати такі правопорушення залежно від об'єкта посягання, способу вчинення злочину, характеру використання інформаційних технологій, а також від суспільних відносин, яким може бути завдано шкоди внаслідок відповідних протиправних дій [23]. Така багатоваріантність наукових підходів свідчить про складність та багатовимірність феномена кіберзлочинності.

Одним із найбільш поширених і водночас найбільш зрозумілих підходів у науковій літературі є класифікація кіберзлочинів залежно від ролі комп'ютерних технологій у процесі вчинення правопорушення [19]. У межах цього підходу дослідники розрізняють злочини, у яких інформаційні технології виступають об'єктом посягання, а також злочини, у яких такі технології використовуються як інструмент або засіб реалізації злочинного наміру.

Згідно з цим підходом, усі кіберзлочини умовно поділяються на дві основні групи. До першої групи належать правопорушення, у яких комп'ютерні системи, інформаційні мережі або цифрові дані виступають безпосереднім об'єктом посягання. У таких випадках протиправні дії спрямовані саме на порушення нормального функціонування інформаційних систем або на незаконне втручання у їхню роботу. Це може проявлятися у несанкціонованому доступі до комп'ютерних систем, втручанні у функціонування інформаційних ресурсів, зміні або знищенні цифрових даних, а також у блокуванні доступу до інформаційних систем [12].

Такі правопорушення становлять особливу загрозу для функціонування сучасного інформаційного суспільства, оскільки інформаційні системи сьогодні використовуються у діяльності державних органів, фінансових установ, підприємств та інших важливих інституцій. Порушення їхньої роботи може призвести до значних економічних втрат, витоку конфіденційної інформації або навіть до порушення стабільності функціонування окремих секторів економіки.

До другої групи відносять правопорушення, у яких комп'ютерні технології виступають не об'єктом посягання, а засобом або інструментом вчинення інших злочинів [20]. У таких випадках інформаційні системи використовуються правопорушниками для реалізації протиправних намірів, однак самі по собі вони не є основною метою злочину.

Прикладами таких правопорушень можуть бути шахрайські дії з використанням електронних платіжних систем або банківських сервісів, незаконне отримання доступу до фінансових ресурсів, розповсюдження неправдивої інформації, а також незаконне поширення персональних даних громадян. Крім того, до цієї категорії можуть належати різноманітні форми фінансових махінацій у мережі Інтернет, включаючи фішинг, онлайн-шахрайство або маніпуляції з електронними транзакціями [21].

Важливу роль у формуванні міжнародного підходу до класифікації кіберзлочинів відіграє Конвенція Ради Європи про кіберзлочинність 2001 року [2]. Цей міжнародно-правовий акт став одним із ключових документів, що визначає основні напрями міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Він встановлює базову систему правопорушень у сфері використання інформаційних технологій та слугує орієнтиром для гармонізації кримінального законодавства держав.

Відповідно до положень цієї Конвенції кіберзлочини можна поділити на кілька основних категорій [2]. До першої категорії належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних систем і даних. У межах цієї категорії йдеться про такі правопорушення, як незаконний доступ до комп'ютерних систем, незаконне перехоплення інформації, втручання у

функціонування комп’ютерних систем, а також незаконне втручання у комп’ютерні дані.

Друга категорія включає злочини, пов’язані з використанням комп’ютерних систем для здійснення шахрайських дій або підробки інформації [2]. У таких випадках інформаційні технології використовуються для маніпуляцій з електронними даними, що здійснюються з метою отримання неправомірної матеріальної вигоди. До цієї групи можуть належати різні форми фінансових злочинів, зокрема комп’ютерне шахрайство, незаконні операції з електронними платежами або підробка електронних документів.

Окрему категорію становлять правопорушення, пов’язані з незаконним поширенням певних видів інформації, що можуть порушувати законодавство різних держав або становити загрозу суспільній безпеці [3]. У цьому контексті йдеться, зокрема, про незаконне розповсюдження шкідливого програмного забезпечення, яке може використовуватися для здійснення атак на інформаційні системи, викрадення даних або порушення функціонування комп’ютерних мереж. Також до цієї групи можуть належати інші форми протиправного використання цифрового контенту, які суперечать законодавству окремих держав.

Таким чином, класифікація кіберзлочинів відіграє важливу роль у формуванні ефективної системи міжнародно-правового регулювання у сфері боротьби з кіберзлочинністю [18]. Систематизація різних видів правопорушень, що вчиняються у цифровому середовищі, дозволяє більш чітко окреслити межі цього явища та визначити його основні характеристики. Завдяки такому підходу стає можливим не лише впорядкування великої кількості різнорідних протиправних дій, що здійснюються у кіберпросторі, але й більш глибоке розуміння їх правової природи та механізмів вчинення. Крім того, класифікація сприяє формуванню цілісного уявлення про масштаби поширення кіберзлочинності, а також про ті ризики і загрози, які вона створює для сучасного суспільства.

Особливо важливим є те, що систематизація кіберзлочинів створює передумови для більш ефективної координації дій держав у сфері протидії таким правопорушенням. Умови глобалізації та транснаціонального характеру

кіберзлочинності вимагають активної взаємодії між державами, міжнародними організаціями та правоохоронними структурами різних країн. Саме тому чітке визначення різних категорій кіберзлочинів дозволяє узгоджувати підходи до їх криміналізації, удосконалювати механізми міжнародного співробітництва та розробляти спільні стратегії боротьби з такими загрозами.

У наукових дослідженнях досить поширеним є підхід до класифікації кіберзлочинів залежно від об'єкта посягання [22]. Такий підхід ґрунтується на визначенні тих суспільних відносин, на які спрямована протиправна діяльність правопорушників. Іншими словами, головним критерієм класифікації у цьому випадку виступає сфера суспільних інтересів, які зазнають шкоди внаслідок вчинення кіберзлочину.

Застосування цього підходу дозволяє більш чітко визначити ступінь суспільної небезпечності конкретного правопорушення, а також оцінити можливі наслідки його вчинення для держави, суспільства або окремих громадян. Крім того, подібна класифікація сприяє більш точному визначенню об'єкта кримінально-правової охорони, що є важливим для правильної кваліфікації відповідних правопорушень.

До першої групи зазвичай відносять злочини, спрямовані безпосередньо проти інформаційних систем, комп'ютерних мереж та цифрових даних [12; 17]. У таких випадках основним об'єктом посягання виступає інформаційна безпека, а також стабільне та безперебійне функціонування комп'ютерних систем і цифрової інфраструктури. Подібні правопорушення можуть створювати значні загрози для діяльності державних органів, фінансових установ, підприємств та інших організацій, що використовують інформаційні технології у своїй повсякденній діяльності.

До цієї категорії, зокрема, належать незаконний доступ до комп'ютерних систем, створення або поширення шкідливого програмного забезпечення, втручання у роботу інформаційних систем, блокування доступу до електронних даних, а також інші дії, спрямовані на порушення цілісності або доступності інформації. Подібні правопорушення можуть призводити до витоку конфіденційної інформації, порушення роботи важливих інформаційних систем або завдання значної матеріальної шкоди.

Друга група охоплює правопорушення, що посягають на майнові права та економічні інтереси осіб із використанням інформаційних технологій [19; 21]. У цьому випадку кіберпростір виступає своєрідним середовищем, у якому здійснюється протиправна діяльність, а комп'ютерні системи та мережа Інтернет використовуються як інструменти реалізації злочинних намірів.

Прикладами таких правопорушень можуть бути різні форми інтернет-шахрайства, незаконне використання банківських карток, отримання доступу до рахунків користувачів електронних платіжних систем, фішингові атаки або інші способи отримання конфіденційної фінансової інформації. Внаслідок подібних дій правопорушники можуть незаконно заволодівати грошовими коштами або іншими матеріальними цінностями, що завдає значної шкоди як окремим особам, так і фінансовим установам.

Третю групу становлять правопорушення, спрямовані проти прав і свобод людини [8]. У сучасному цифровому середовищі досить поширеними є випадки незаконного збирання, використання або поширення персональних даних, порушення права на приватність, а також інші дії, що можуть негативно впливати на особисту безпеку та репутацію людини.

Розвиток соціальних мереж, онлайн-комунікацій та цифрових сервісів значно розширив можливості для обміну інформацією, однак водночас створив нові ризики для захисту особистих даних та приватного життя громадян. У цьому контексті особливої актуальності набувають питання забезпечення належного рівня захисту персональної інформації, а також розробки ефективних правових механізмів протидії правопорушенням, що посягають на права людини у цифровому середовищі.

Окрім зазначених підходів, деякі науковці пропонують класифікувати кіберзлочини залежно від способу їх вчинення [23]. Такий підхід передбачає аналіз технічних методів і засобів, які використовуються правопорушниками для реалізації злочинної діяльності у кіберпросторі. У межах цього підходу виділяють кілька основних груп правопорушень, що відрізняються за технологічними особливостями здійснення протиправних дій.

Одним із найбільш поширених способів вчинення кіберзлочинів є використання шкідливого програмного забезпечення [21]. До таких програм належать комп'ютерні віруси, троянські програми, програми-вимагачі (ransomware), шпигунське програмне забезпечення та інші види шкідливого програмного коду. Такі інструменти можуть застосовуватися для пошкодження комп'ютерних систем, викрадення конфіденційної інформації, отримання несанкціонованого доступу до електронних ресурсів або блокування доступу до цифрових даних.

Ще одним досить поширеним способом здійснення кіберзлочинів є використання методів соціальної інженерії [22]. У цьому випадку правопорушники не обов'язково використовують складні технічні засоби або програмне забезпечення. Натомість вони намагаються отримати необхідну інформацію шляхом психологічного впливу на користувачів. Наприклад, це може бути введення людини в оману шляхом надсилання підроблених електронних листів, створення фальшивих вебсайтів або використання інших маніпулятивних методів з метою отримання конфіденційних даних.

Окрему категорію становлять кіберзлочини, пов'язані з організацією масштабних кібератак на інформаційні системи державних органів, фінансових установ або великих компаній [29]. Подібні атаки можуть мати серйозні наслідки для функціонування важливих елементів державної інфраструктури. У деяких випадках вони можуть бути спрямовані на порушення роботи систем енергопостачання, транспорту, зв'язку або інших об'єктів критичної інфраструктури.

Такі дії можуть становити значну загрозу для національної безпеки держави, оскільки порушення роботи важливих інформаційних систем здатне призвести до масштабних економічних втрат, соціальної нестабільності або навіть до створення небезпечних ситуацій для життя і здоров'я людей.

Водночас розвиток сучасних технологій постійно змінює характер кіберзлочинності та сприяє появі нових форм протиправної діяльності у мережі Інтернет [30]. Поширення хмарних технологій, мобільних застосунків, цифрових платіжних систем та систем штучного інтелекту створює нові можливості для

розвитку цифрової економіки. Проте одночасно ці технології можуть використовуватися правопорушниками для здійснення нових видів кіберзлочинів.

Саме тому держави змушені постійно вдосконалювати законодавство у сфері кібербезпеки, розробляти нові механізми запобігання кіберзлочинності та активно розвивати міжнародне співробітництво у цій сфері.

Отже, у сучасній юридичній науці існує декілька підходів до класифікації кіберзлочинів, які базуються на різних критеріях [15; 23]. Найбільш поширеними є поділ правопорушень залежно від ролі інформаційних технологій у їх вчиненні, об’єкта посягання, а також способу реалізації злочинної діяльності. Використання таких підходів дозволяє більш глибоко дослідити природу кіберзлочинності, визначити її ключові характеристики та сформувати ефективні правові механізми протидії цьому явищу як на національному, так і на міжнародному рівнях.

Проведене дослідження показало, що у сучасній юридичній науці досі відсутній єдиний універсальний підхід до класифікації кіберзлочинів, що пояснюється складністю, багатовимірністю та постійною еволюцією цього явища. Водночас наявні наукові підходи дозволяють систематизувати кіберзлочини залежно від об’єкта посягання, способу вчинення правопорушення або характеру використання інформаційних технологій у кожному конкретному випадку. Така класифікація має суттєве практичне значення, оскільки сприяє вдосконаленню кримінального законодавства, більш точному формуванню складів правопорушень, а також розробленню дієвих і гнучких механізмів протидії кіберзлочинності в умовах сучасного цифрового середовища [19; 23].

1.3. Міжнародно-правові механізми протидії кіберзлочинності

Стрімкий розвиток цифрових технологій, а також активні процеси глобалізації інформаційного простору упродовж останніх десятиліть суттєво вплинули на характер суспільних відносин. Інформаційні технології стали невід'ємною складовою функціонування сучасного суспільства, охоплюючи практично всі сфери діяльності людини – економіку, фінанси, державне управління, освіту, науку, міжнародну торгівлю та повсякденну комунікацію між людьми. Водночас поряд із численними перевагами цифровізації виникають і нові ризики, пов'язані з можливістю використання сучасних технологій для здійснення протиправної діяльності. У зв'язку з цим спостерігається поступове, але досить відчутне зростання кількості правопорушень, що здійснюються у кіберпросторі [2; 3].

Однією з ключових особливостей кіберзлочинів є їхня здатність виходити за межі юрисдикції однієї держави. На відміну від багатьох традиційних видів злочинів, які здебільшого пов'язані з певною територією, правопорушення у кіберпросторі можуть здійснюватися дистанційно, з використанням комп'ютерних мереж та глобальної мережі Інтернет. Це означає, що особа, яка вчиняє кіберзлочин, може перебувати в одній державі, тоді як сервери або інформаційні системи, на які спрямована атака, можуть знаходитися в іншій країні, а потерпілі - ще в кількох державах одночасно. У результаті такі правопорушення набувають вираженого транскордонного характеру та можуть охоплювати території кількох держав одночасно [5].

За таких умов традиційні механізми протидії злочинності, що функціонують виключно в межах національної правової системи, виявляються недостатньо ефективними. Національні правоохоронні органи часто стикаються з труднощами під час встановлення місця вчинення правопорушення, ідентифікації осіб, причетних до злочину, або отримання необхідних доказів, які можуть зберігатися на серверах, розташованих у різних юрисдикціях. Крім того, відмінності у національному законодавстві різних держав інколи ускладнюють процес притягнення

правопорушників до відповідальності. У зв’язку з цим дедалі більшої актуальності набуває розвиток міжнародно-правових механізмів, спрямованих на координацію зусиль держав, гармонізацію національного законодавства та зміцнення міжнародного співробітництва у сфері протидії кіберзлочинності [4; 6].

Одним із ключових міжнародних документів у цій сфері є Конвенція Ради Європи про кіберзлочинність 2001 року, яка більш відома під назвою Будапештська конвенція [1]. Цей міжнародно-правовий акт вважається першим комплексним міжнародним договором, що був спеціально розроблений для врегулювання питань протидії злочинам, пов’язаним із використанням комп’ютерних систем та інформаційних технологій. Прийняття цього документа стало важливим етапом у формуванні міжнародної системи боротьби з кіберзлочинністю, оскільки він заклав основи для вироблення узгоджених підходів до криміналізації відповідних правопорушень, а також створив правові механізми для розвитку міжнародного співробітництва у сфері розслідування кіберзлочинів [1].

Будапештська конвенція визначає основні категорії правопорушень, які повинні бути криміналізовані у національному законодавстві держав-учасниць [1]. До таких правопорушень, зокрема, належать незаконний доступ до комп’ютерних систем, незаконне перехоплення даних, втручання у функціонування комп’ютерних систем, втручання у комп’ютерні дані, а також зловживання технічними пристроями, які можуть використовуватися для вчинення кіберзлочинів. Окрім цього, документ передбачає необхідність криміналізації таких правопорушень, як комп’ютерне шахрайство та комп’ютерна підробка, що здійснюються з використанням інформаційних технологій [1].

Важливо зазначити, що Конвенція також приділяє увагу правопорушенням, пов’язаним із незаконним поширенням певних видів інформації через комп’ютерні мережі. Зокрема, мова йде про матеріали, що містять дитячу порнографію, розповсюдження яких становить серйозну загрозу для суспільної безпеки та прав людини. У цьому контексті держави-учасниці зобов’язуються вживати відповідних законодавчих та організаційних заходів для запобігання таким правопорушенням та притягнення винних осіб до відповідальності [1].

Важливим елементом Будапештської конвенції є також встановлення спеціальних процесуальних механізмів, які дозволяють правоохоронним органам більш ефективно здійснювати розслідування злочинів у кіберпросторі [1; 7]. Оскільки цифрові докази мають специфічний характер і можуть бути швидко змінені або знищені, документ передбачає застосування спеціальних інструментів, спрямованих на оперативне отримання та збереження електронної інформації.

Зокрема, Конвенція передбачає можливість оперативного збереження комп'ютерних даних, отримання доступу до інформаційних систем, вилучення електронної інформації та перехоплення мережевого трафіку в межах кримінального провадження. Використання таких процесуальних механізмів значно підвищує ефективність діяльності правоохоронних органів під час розслідування правопорушень, пов'язаних із використанням інформаційних технологій, а також сприяє більш швидкому збиранню доказової бази у справах про кіберзлочини [1; 7].

Окрему увагу у положеннях Конвенції приділено питанням міжнародної правової допомоги між державами [1]. У зв'язку з тим, що кіберзлочини часто мають транскордонний характер, ефективна боротьба з ними неможлива без налагодження тісної співпраці між правоохоронними органами різних країн. Саме тому держави-учасниці Конвенції зобов'язуються активно взаємодіяти між собою з метою встановлення осіб, причетних до вчинення кіберзлочинів, збору доказів, а також притягнення винних до кримінальної відповідальності [6].

У цьому контексті Конвенція передбачає створення ефективної системи взаємної правової допомоги між державами, що включає можливість обміну інформацією, проведення спільних розслідувань та надання допомоги у збиранні доказів. Крім того, документ передбачає механізм оперативного обміну інформацією між компетентними органами різних держав, що дозволяє швидко реагувати на кіберінциденти та координувати дії у процесі розслідування таких правопорушень [1].

Поряд із Будапештською конвенцією важливу роль у формуванні міжнародної системи протидії кіберзлочинності відіграють також міжнародні організації [3]. Їхня діяльність спрямована на розробку міжнародних стандартів у сфері кібербезпеки,

координацію зусиль держав та сприяння розвитку міжнародного співробітництва у боротьбі з кіберзлочинами.

Значний внесок у координацію діяльності держав у цій сфері здійснює Організація Об'єднаних Націй [8]. У межах діяльності ООН регулярно проводяться міжнародні конференції, експертні зустрічі та наукові обговорення, присвячені проблемам кібербезпеки та протидії злочинам у цифровому середовищі. Під час таких заходів держави мають можливість обмінюватися досвідом, обговорювати актуальні виклики та розробляти рекомендації щодо вдосконалення національного законодавства у сфері боротьби з кіберзлочинністю.

Крім того, Генеральна Асамблея Організації Об'єднаних Націй неодноразово ухвалювала резолюції, спрямовані на зміцнення міжнародного співробітництва у сфері кібербезпеки та протидії злочинам у цифровому середовищі. У відповідних документах підкреслюється необхідність консолідації зусиль держав для забезпечення безпеки глобального інформаційного простору, а також наголошується на важливості формування ефективних міжнародно-правових механізмів реагування на новітні виклики у сфері кібербезпеки. Такі резолюції мають значний вплив на формування сучасної міжнародної політики у сфері боротьби з кіберзлочинністю, оскільки вони визначають основні напрями співробітництва держав та сприяють виробленню узгоджених підходів до забезпечення безпеки у кіберпросторі. Крім того, зазначені документи стимулюють розвиток міжнародного діалогу між державами, міжнародними організаціями та експертною спільнотою з питань протидії кіберзагрозам та забезпечення стабільності цифрового середовища [8].

Важливе місце у системі міжнародної протидії кіберзлочинності посідає також Міжнародна організація кримінальної поліції – Інтерпол [9]. Діяльність цієї організації спрямована на забезпечення ефективної взаємодії між правоохоронними органами різних держав з метою запобігання та розслідування злочинів міжнародного характеру. У сучасних умовах, коли значна частина правопорушень пов'язана з використанням інформаційних технологій, роль Інтерполу у сфері боротьби з кіберзлочинністю постійно зростає. Організація забезпечує оперативний обмін інформацією між правоохоронними структурами різних країн, координує проведення

міжнародних розслідувань та сприяє організації спільних операцій, спрямованих на викриття транснаціональних злочинних угруповань, які здійснюють діяльність у кіберпросторі [9].

У структурі Інтерполу функціонують спеціалізовані підрозділи, діяльність яких безпосередньо спрямована на боротьбу з кіберзлочинністю. Ці підрозділи здійснюють аналітичну роботу, досліджують новітні тенденції розвитку кіберзлочинної діяльності та надають державам-членам організації методичну й експертну підтримку у розслідуванні складних правопорушень, пов'язаних із використанням цифрових технологій. Крім того, Інтерпол активно сприяє підвищенню професійної підготовки співробітників правоохоронних органів, організовуючи спеціалізовані навчальні програми, тренінги та міжнародні конференції з питань боротьби з кіберзлочинністю. Така діяльність сприяє формуванню єдиного професійного підходу до розслідування кіберзлочинів та підвищує ефективність міжнародної взаємодії у цій сфері [9].

Не менш важливим елементом міжнародної системи протидії кіберзлочинності є діяльність Європолу [10]. Ця організація відіграє важливу роль у забезпеченні координації співпраці правоохоронних органів держав Європейського Союзу у боротьбі з різними видами організованої злочинності, зокрема й злочинами, що здійснюються у кіберпросторі. Європол виступає своєрідною платформою для обміну інформацією, аналітичними даними та практичним досвідом між правоохоронними органами держав-членів Європейського Союзу. Завдяки цьому забезпечується більш ефективна координація спільних дій у процесі виявлення, розслідування та попередження кіберзлочинів [10].

У структурі Європолу функціонує спеціалізований підрозділ — Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre). Основною метою діяльності цього центру є підтримка розслідувань, пов'язаних із кіберзлочинами, а також аналіз сучасних тенденцій розвитку кіберзагроз у цифровому середовищі. Центр здійснює аналітичну роботу, досліджує нові форми та методи вчинення кіберзлочинів, а також надає експертну підтримку державам-членам Європейського Союзу під час проведення складних міжнародних розслідувань. Крім того, діяльність

цього підрозділу спрямована на підвищення ефективності боротьби з такими видами правопорушень, як кіберфінансові злочини, атаки на інформаційні системи, незаконне використання персональних даних та інші форми злочинної діяльності у цифровому середовищі [10].

Слід також зазначити, що поряд із діяльністю міжнародних організацій важливим інструментом протидії кіберзлочинності є укладення двосторонніх та багатосторонніх міжнародних договорів між державами [6]. Такі міжнародні угоди створюють правову основу для співробітництва держав у сфері розслідування кіберзлочинів та сприяють формуванню ефективних механізмів взаємодії між компетентними органами різних країн. Зокрема, такі договори спрямовані на спрощення процедур надання взаємної правової допомоги, забезпечення можливості екстрадиції осіб, підозрюваних у вчиненні кіберзлочинів, а також на розвиток співпраці у сфері обміну інформацією та проведення спільних міжнародних розслідувань [6].

Важливим напрямом розвитку міжнародних механізмів боротьби з кіберзлочинністю є гармонізація національного законодавства різних держав [3; 4]. Як відомо, правові системи різних країн можуть суттєво відрізнятися за своїми принципами, структурою та підходами до криміналізації певних видів правопорушень. У разі відсутності узгоджених правових стандартів це може створювати значні труднощі під час проведення міжнародних розслідувань та притягнення винних осіб до відповідальності. Саме тому міжнародні організації та міждержавні об’єднання приділяють значну увагу розробці спільних підходів до криміналізації кіберзлочинів, а також до формування єдиних процедур їх розслідування та судового переслідування [3; 6].

Водночас слід підкреслити, що міжнародне співробітництво у сфері боротьби з кіберзлочинністю постійно розвивається у відповідь на нові технологічні виклики, які виникають у сучасному цифровому середовищі [2]. Стрімке поширення хмарних технологій, використання криптовалют, розвиток систем штучного інтелекту, а також поява нових цифрових сервісів і платформ створюють не лише додаткові можливості для розвитку цифрової економіки, але й нові ризики, пов’язані з можливістю

використання цих технологій у протиправних цілях. У зв'язку з цим міжнародна спільнота змушена постійно вдосконалювати існуючі правові механізми та розробляти нові інструменти, які дозволять ефективно протидіяти кіберзлочинам у сучасних умовах [2; 6].

Таким чином, міжнародно-правові механізми протидії кіберзлочинності формують складну і багаторівневу систему правових норм, інституцій та форм співробітництва, спрямованих на боротьбу з правопорушеннями у кіберпросторі [3; 6]. До основних елементів цієї системи належать міжнародні договори, діяльність міжнародних організацій, механізми взаємної правової допомоги між державами, а також процеси гармонізації національного законодавства у сфері протидії кіберзлочинності [6]. Ефективне функціонування таких механізмів є важливою передумовою забезпечення належного рівня кібербезпеки, стабільності інформаційного середовища та захисту інтересів держав, суспільства і окремих громадян у глобальному цифровому просторі [2].

Аналіз міжнародно-правових механізмів протидії кіберзлочинності дозволяє зробити висновок, що ефективна боротьба з такими правопорушеннями є можливою лише за умов системної та активної міжнародної співпраці між державами. Транскордонний характер значної частини кіберзлочинів вимагає узгоджених дій правоохоронних органів різних країн, гармонізації правових підходів, а також постійного розвитку механізмів міжнародної правової допомоги. Особливе значення у цьому контексті має Конвенція Ради Європи про кіберзлочинність 2001 року, яка фактично заклала базові міжнародні стандарти криміналізації кіберзлочинів і визначила ключові принципи співробітництва держав у сфері їх розслідування [2]. Важливу роль у формуванні глобальної системи протидії кіберзлочинності також відіграють міжнародні організації, зокрема ООН та Інтерпол, діяльність яких сприяє координації зусиль держав та розвитку спільних підходів до боротьби з кіберзагрозами [33; 54].

РОЗДІЛ 2

ПРАВОВИЙ ДОСВІД ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1. Правове регулювання боротьби з кіберзлочинністю в ЄС

Європейський Союз протягом останніх десятиліть активно формує та вдосконалює власну систему правового регулювання у сфері протидії кіберзлочинності. Посилена увага до цієї проблематики зумовлена насамперед швидким розвитком інформаційно-комунікаційних технологій, а також масштабними процесами цифровізації, які сьогодні охоплюють практично всі сфери суспільного життя. Цифрові технології стали невід'ємною складовою функціонування економіки, державного управління, міжнародної торгівлі, фінансової системи, банківського сектору, сфери надання послуг та повсякденної діяльності громадян. Водночас активне впровадження цифрових інструментів і мережевих технологій створює не лише нові можливості для розвитку держав та суспільства, але й формує значну кількість ризиків, пов'язаних із безпекою інформаційних систем, захистом цифрової інфраструктури та охороною персональних даних користувачів [17; 27].

У сучасних умовах цифровий простір став одним із ключових елементів функціонування суспільства, а тому будь-які загрози у сфері кібербезпеки можуть мати серйозні наслідки як для окремих держав, так і для міжнародної спільноти загалом. Кібератаки здатні порушувати роботу державних установ, фінансових систем, об'єктів критичної інфраструктури, а також завдавати значних матеріальних збитків. Саме тому питання забезпечення належного рівня кібербезпеки поступово перетворилося на один із пріоритетних напрямів політики Європейського Союзу. У межах ЄС кібербезпека розглядається не лише як технічна проблема, але і як

важливий елемент забезпечення економічної стабільності, національної безпеки та захисту прав і свобод людини у цифровому середовищі [14; 28].

На відміну від традиційних моделей правового регулювання, які існують у межах окремих держав, у Європейському Союзі сформувалася багаторівнева система правового забезпечення боротьби з кіберзлочинністю. Така система передбачає поєднання наднаціонального рівня правового регулювання, представленого актами права Європейського Союзу, та національного рівня, який охоплює законодавство держав-членів. Правові акти ЄС визначають загальні стандарти, базові принципи та мінімальні вимоги щодо забезпечення кібербезпеки і протидії кіберзлочинності, тоді як держави-члени забезпечують їх імплементацію у власні правові системи [18].

Подібний механізм дозволяє поєднати єдині європейські стандарти із особливостями національних правових систем держав-членів. У результаті формується комплексна модель правового забезпечення кібербезпеки, яка забезпечує координацію дій між державами Європейського Союзу та сприяє більш ефективній протидії сучасним кіберзагрозам. Крім того, така система дозволяє забезпечити більш узгоджену правову політику у сфері цифрової безпеки, а також створює сприятливі умови для розвитку міжнародного співробітництва між державами-членами у сфері боротьби з кіберзлочинністю [27; 28].

Правову основу регулювання боротьби з кіберзлочинністю в Європейському Союзі становлять численні нормативно-правові акти, серед яких особливе місце займають директиви та регламенти ЄС. Саме ці правові інструменти визначають загальні правила, стандарти та вимоги, яких повинні дотримуватися держави-члени під час формування національної політики у сфері кібербезпеки. Директиви встановлюють мінімальні вимоги щодо криміналізації певних діянь, пов’язаних із використанням інформаційних технологій, а також покладають на держави-члени обов’язок привести національне законодавство у відповідність до визначених стандартів. Завдяки цьому забезпечується поступова гармонізація правових систем держав Європейського Союзу у сфері боротьби з кіберзлочинністю [4; 28].

Одним із ключових нормативно-правових актів Європейського Союзу у сфері протидії кіберзлочинності є Директива 2013/40/ЄС щодо атак на інформаційні

системи [4]. Зазначений документ визначає основні правові підходи до криміналізації низки діянь, пов'язаних із незаконним втручанням у функціонування комп'ютерних систем та інформаційних мереж. Зокрема, директива передбачає кримінальну відповідальність за несанкціонований доступ до комп'ютерних систем, втручання у роботу інформаційних мереж, незаконне пошкодження, зміну або видалення комп'ютерних даних. Крім того, у положеннях цього нормативного акта закріплено відповідальність за створення, придбання, використання або поширення шкідливого програмного забезпечення, яке може застосовуватися для здійснення кібератак або інших протиправних дій у цифровому середовищі.

Варто зазначити, що положення Директиви 2013/40/ЄС значною мірою базуються на принципах, закріплених у Конвенції Ради Європи про кіберзлочинність, більш відомій як Будапештська конвенція. Водночас директива не лише відтворює положення цього міжнародного документа, а й деталізує їх з урахуванням особливостей правової системи Європейського Союзу та сучасних викликів у сфері кібербезпеки [2; 31]. Таким чином, Директива 2013/40/ЄС відіграє важливу роль у формуванні єдиного підходу держав-членів до криміналізації кіберзлочинів та створенні узгоджених механізмів правового реагування на кіберзагрози.

Важливим елементом європейської системи забезпечення кібербезпеки є також Директива (EU) 2016/1148, більш відома як NIS Directive [6]. Основною метою цього нормативно-правового акта є підвищення загального рівня безпеки мережевих та інформаційних систем на території Європейського Союзу. Директива визначає базові стандарти безпеки для критично важливої інфраструктури, яка забезпечує функціонування ключових секторів економіки та суспільного життя [37].

Зокрема, дія NIS Directive поширюється на такі стратегічно важливі сфери, як енергетика, транспорт, банківський і фінансовий сектор, охорона здоров'я, водопостачання, а також цифрові послуги. Відповідно до положень директиви держави-члени зобов'язані розробляти національні стратегії кібербезпеки, визначати операторів критично важливих послуг та забезпечувати належний рівень захисту інформаційних систем, що використовуються у відповідних секторах [6].

Крім цього, директива передбачає створення спеціальних механізмів реагування на кіберінциденти, а також розвиток співпраці між державами-членами у сфері обміну інформацією про кіберзагрози. Такий підхід свідчить про те, що ефективна протидія кіберзлочинності не може обмежуватися лише кримінально-правовими заходами. Важливе значення мають також превентивні механізми, розвиток технічних засобів захисту інформаційних систем та активне міжнародне співробітництво у сфері кібербезпеки [35].

Подальший розвиток правового регулювання у сфері кібербезпеки пов'язаний із прийняттям Директиви NIS2, яка суттєво розширила сферу правового регулювання та встановила більш жорсткі вимоги щодо забезпечення кіберзахисту в державах-членах Європейського Союзу [7; 38]. Зокрема, нова директива посилила вимоги щодо управління кіберризиками, обов'язкового повідомлення про кіберінциденти, а також відповідальності суб'єктів, які забезпечують функціонування критично важливих секторів економіки та цифрової інфраструктури.

Значну роль у забезпеченні безпеки цифрового середовища в межах Європейського Союзу відіграє також Регламент (ЄС) 2016/679 — Загальний регламент про захист даних (GDPR) [8]. Цей нормативний акт встановлює комплексну систему правового захисту персональних даних громадян Європейського Союзу та визначає основні принципи обробки такої інформації [39].

GDPR регулює порядок збору, зберігання, використання, обробки та передачі персональних даних, а також закріплює права громадян щодо контролю за використанням їхньої особистої інформації. Однією з ключових особливостей цього регламенту є встановлення суворих вимог до організацій та компаній, які здійснюють обробку персональних даних. У разі порушення положень GDPR передбачено застосування значних фінансових санкцій, розмір яких може сягати значних сум. Такий підхід стимулює компанії, установи та інші організації впроваджувати сучасні технічні й організаційні механізми захисту інформації та приділяти більше уваги питанням інформаційної безпеки [8; 39].

Таким чином, у межах правової системи Європейського Союзу формується комплексна модель забезпечення кібербезпеки, яка поєднує кримінально-правові,

адміністративні та організаційні механізми. Така система дозволяє не лише реагувати на вже вчинені кіберзлочини, але й запобігати їх виникненню шляхом підвищення рівня захисту інформаційних систем, розвитку міжнародного співробітництва та гармонізації законодавства держав-членів у сфері цифрової безпеки [25; 26].

Однією з ключових особливостей правового регулювання у межах Європейського Союзу є гармонізація кримінального законодавства держав-членів. Така гармонізація спрямована на забезпечення узгодженості правових підходів різних країн до криміналізації діянь, пов'язаних із використанням інформаційно-комунікаційних технологій, а також на створення ефективних механізмів спільної протидії кіберзлочинності. Важливу роль у цьому процесі відіграють директиви Європейського Союзу, які встановлюють мінімальні стандарти правового регулювання, обов'язкові для імплементації у національне законодавство держав-членів [4; 28].

Такі директиви визначають загальні вимоги щодо криміналізації окремих видів правопорушень, які можуть бути вчинені з використанням комп'ютерних систем, мережі Інтернет або інших цифрових технологій. Наприклад, у сфері протидії комп'ютерному шахрайству, незаконному доступу до інформаційних систем або втручанню у роботу комп'ютерних мереж директиви визначають перелік конкретних діянь, що мають визнаватися кримінальними правопорушеннями у законодавстві держав-членів. У свою чергу, національні правові системи повинні передбачати механізми притягнення винних осіб до кримінальної відповідальності, а також ефективні процедури розслідування і правозастосування [18].

Подібний підхід має важливе практичне значення, оскільки дозволяє зменшити розбіжності між національними правовими системами держав-членів та забезпечити більш узгоджену правову політику у сфері боротьби з кіберзлочинністю. Крім того, гармонізація законодавства значно полегшує міжнародну співпрацю між правоохоронними органами різних держав, що має особливе значення під час розслідування транскордонних кіберзлочинів. Завдяки єдиним правовим стандартам держави-члени можуть ефективніше здійснювати обмін інформацією, координувати

проведення спільних слідчих дій та забезпечувати притягнення правопорушників до відповідальності [53].

У правовій політиці Європейського Союзу значна увага приділяється не лише криміналізації кіберзлочинів, але й заходам їх запобігання. Профілактика кіберзлочинності розглядається як один із ключових напрямів сучасної політики у сфері кібербезпеки. Реалізація таких превентивних заходів здійснюється через спеціальні програми, стратегічні документи та комплексні політичні ініціативи, спрямовані на зміцнення безпеки цифрового середовища [35].

Одним із таких документів є Європейська стратегія кібербезпеки (Cybersecurity Strategy 2020), яка визначає основні напрями розвитку політики Європейського Союзу у сфері забезпечення кібербезпеки [14; 35]. У цьому документі сформульовано низку стратегічних пріоритетів, спрямованих на підвищення рівня стійкості цифрової інфраструктури Європи до сучасних кіберзагроз. Значна увага приділяється захисту критично важливих інформаційних систем, які забезпечують функціонування ключових секторів економіки та суспільного життя.

Крім того, стратегія передбачає розвиток сучасних технологій кіберзахисту, удосконалення систем моніторингу кіберзагроз та підвищення ефективності реагування на кіберінциденти. Важливим напрямом також є підготовка висококваліфікованих фахівців у сфері кібербезпеки, оскільки дефіцит професійних кадрів у цій сфері залишається однією з актуальних проблем сучасного цифрового суспільства. Окремо стратегія наголошує на необхідності координації дій між державами-членами Європейського Союзу, що дозволяє оперативно реагувати на масштабні кіберінциденти та мінімізувати їх негативні наслідки для економіки й суспільства [40].

Таким чином, Європейська стратегія кібербезпеки підкреслює, що ефективна боротьба з кіберзлочинністю потребує комплексного підходу. Такий підхід має включати не лише формування сучасної нормативно-правової бази, але й розвиток інституційного потенціалу, підвищення рівня технічної підготовки фахівців та активне міжнародне співробітництво у сфері кібербезпеки [26].

Окреме місце у правовій системі Європейського Союзу займає законодавство, спрямоване на регулювання діяльності цифрових платформ та онлайн-сервісів. У сучасних умовах такі платформи відіграють важливу роль у формуванні цифрового середовища, оскільки забезпечують обмін інформацією, здійснення електронної комерції та комунікацію між мільйонами користувачів у різних країнах світу. Саме тому ефективне регулювання діяльності цифрових сервісів є важливим елементом загальної системи забезпечення кібербезпеки [55].

У цьому контексті особливе значення мають Регламент про цифрові послуги (Digital Services Act, DSA) та Регламент про цифрові ринки (Digital Markets Act, DMA) [56; 57]. Зазначені нормативно-правові акти спрямовані на формування більш безпечного, прозорого та контрольованого цифрового середовища у межах Європейського Союзу.

Зокрема, Регламент DSA встановлює низку обов'язків для онлайн-платформ та інших постачальників цифрових послуг. До таких обов'язків належать оперативне реагування на повідомлення про незаконний контент, запобігання поширенню шахрайських схем у мережі Інтернет, а також забезпечення належного рівня захисту користувачів від різних видів кіберзагроз. Важливою складовою цього регламенту є також підвищення прозорості діяльності цифрових платформ та запровадження механізмів контролю за їхньою діяльністю [56].

Водночас Регламент про цифрові ринки (DMA) спрямований на регулювання діяльності великих технологічних компаній, які займають домінуюче становище у цифровій економіці. Основною метою цього документа є забезпечення справедливої конкуренції на цифрових ринках, а також запобігання можливим зловживанням з боку великих цифрових платформ. Одним із важливих аспектів цього регламенту є підвищення прозорості алгоритмів та механізмів обробки даних, що сприяє зменшенню ризиків маніпулювання інформацією або неправомірного використання персональних даних користувачів [57].

У сукупності зазначені нормативно-правові акти формують додатковий правовий механізм захисту користувачів, інформаційних систем та цифрової інфраструктури у межах Європейського Союзу. Вони сприяють підвищенню рівня

безпеки цифрового середовища та створюють правові умови для більш відповідальної діяльності цифрових платформ і постачальників цифрових послуг [53].

Варто також зазначити, що правове регулювання у сфері кібербезпеки в Європейському Союзі передбачає поєднання різних видів юридичної відповідальності. У багатьох випадках законодавство передбачає не лише кримінальну відповідальність за вчинення кіберзлочинів, але й адміністративну або цивільно-правову відповідальність. Подібний підхід дозволяє застосовувати більш гнучкі механізми реагування на правопорушення у цифровому середовищі [8; 15].

Зокрема, поряд із кримінальними санкціями можуть застосовуватися адміністративні штрафи, обмеження діяльності компаній або інші заходи правового впливу. Водночас потерпілі особи отримують право вимагати відшкодування матеріальної або моральної шкоди у цивільно-правовому порядку. Така система відповідальності сприяє підвищенню превентивного ефекту правових норм та стимулює суб'єктів господарювання приділяти більше уваги питанням кібербезпеки й захисту інформаційних систем [8; 39].

Проведений аналіз дозволяє зробити висновок, що правове регулювання Європейського Союзу у сфері кіберзлочинності загалом орієнтоване на поступову та системну гармонізацію національних законодавств держав-членів, а також на формування єдиних мінімальних стандартів криміналізації кіберзлочинів. Такий підхід не обмежується лише формальним зближенням правових норм, а передбачає глибшу інтеграцію правових механізмів реагування на кіберзагрози в межах усього ЄС.

Завдяки цьому забезпечується більша узгодженість кримінально-правових систем різних держав, зменшуються правові розбіжності у кваліфікації кіберзлочинів та підвищується передбачуваність правозастосовної практики. У практичному вимірі це сприяє підвищенню ефективності розслідування транскордонних правопорушень, оскільки правоохоронні органи держав-членів діють у більш уніфікованому правовому полі та використовують подібні підходи до кваліфікації діянь.

Крім того, така модель правового регулювання створює більш стабільне та узгоджене правове середовище для протидії кіберзагрозам на рівні всього

Європейського Союзу, що є особливо важливим з огляду на постійне зростання складності та масштабів кіберзлочинної діяльності [4; 28].

2.2. Інституційні механізми Європейського Союзу у сфері протидії кіберзлочинності

Створення ефективної системи інституційної протидії кіберзлочинності стало одним із ключових завдань сучасної правової політики у зв'язку зі стрімким розвитком інформаційно-комунікаційних технологій та активною цифровізацією суспільних процесів [6; 15]. Масштабне поширення цифрових платформ, глобальних інформаційних мереж, електронних сервісів і сучасних засобів комунікації суттєво змінило характер сучасної злочинності. Якщо раніше значна частина правопорушень була пов'язана переважно з фізичним простором, то сьогодні дедалі більше злочинних дій здійснюється саме у цифровому середовищі. З одного боку, технологічний розвиток сприяє економічному зростанню, розширенню міжнародної співпраці та підвищенню доступності інформації, однак з іншого — створює нові можливості для вчинення протиправних дій у кіберпросторі.

Особливістю сучасних кіберзлочинів є їх виражений транснаціональний характер. У багатьох випадках кіберзлочини вчиняються із використанням інфраструктури, яка розташована у різних державах, а самі правопорушники можуть одночасно діяти з території кількох юрисдикцій [18, с. 94]. Це значно ускладнює процес виявлення, розслідування та притягнення винних осіб до відповідальності, оскільки традиційні національні механізми боротьби зі злочинністю не завжди здатні ефективно реагувати на подібні виклики. Крім того, цифровий характер таких злочинів дозволяє злочинцям приховувати власну особу, використовувати анонімні мережі та швидко змінювати місце здійснення протиправної діяльності. У зв'язку з цим виникла необхідність створення комплексної системи міждержавної взаємодії та спеціалізованих інституцій, здатних координувати діяльність різних держав у сфері протидії кіберзлочинності.

Саме з метою подолання зазначених проблем у межах Європейського Союзу було сформовано розгалужену систему спеціалізованих органів та інституцій, діяльність яких спрямована на координацію дій держав-членів, обмін оперативною

інформацією, організацію спільних розслідувань, а також формування стратегічних підходів до забезпечення кібербезпеки [27; 28]. Функціонування таких інституцій дозволяє значно підвищити ефективність реагування на сучасні кіберзагрози та забезпечити більш узгоджене застосування правових механізмів боротьби з кіберзлочинністю у межах Європейського Союзу. Важливою особливістю цієї системи є поєднання правоохоронних, аналітичних, консультативних та координаційних функцій, що забезпечує комплексний підхід до вирішення проблем кібербезпеки.

Однією з ключових інституцій у цій системі є Європейське поліцейське управління (Europol) [41]. Основним завданням Europol є сприяння співробітництву між правоохоронними органами держав-членів Європейського Союзу з метою запобігання, виявлення та розслідування тяжких міжнародних злочинів, серед яких важливе місце займають кіберзлочини [41; 53]. У сучасних умовах Europol фактично виконує роль центральної координаційної платформи, яка забезпечує взаємодію між державами у сфері боротьби з транснаціональною злочинністю.

Однією з найважливіших функцій Europol є забезпечення оперативного та ефективного обміну інформацією між правоохоронними органами різних держав-членів. Організація також здійснює аналітичну обробку значних обсягів інформації, що дозволяє виявляти нові тенденції розвитку кіберзлочинності, прогнозувати потенційні загрози та формувати рекомендації щодо реагування на них. Як зазначає L. Hansen, «ефективна координація між державами-членами є необхідною умовою протидії транснаціональним кіберзагрозам» [27, с. 84]. Завдяки такій діяльності Europol сприяє більш оперативному реагуванню на сучасні кіберзагрози та забезпечує підвищення ефективності міжнародних розслідувань.

Особливе місце у структурі Europol займає Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre — EC3), створений у 2013 році [42]. Створення цього центру стало важливим етапом розвитку інституційної системи протидії кіберзлочинності у Європейському Союзі. Основною місією EC3 є підтримка держав-членів під час розслідування складних кіберзлочинів, координація

міжнародних операцій, а також забезпечення аналітичної та технічної підтримки у сфері боротьби з кіберзлочинністю [41; 42].

ЕС3 здійснює діяльність у кількох основних напрямах. Центр займається протидією кібершахрайству, атакам на інформаційні системи, поширенню шкідливого програмного забезпечення, незаконному обігу викрадених даних, а також злочинам, пов'язаним із сексуальною експлуатацією дітей у мережі Інтернет [42]. Окрім безпосередньої участі у розслідуваннях, ЕС3 активно проводить аналітичну та дослідницьку роботу. Фахівці центру систематично аналізують новітні тенденції розвитку кіберзлочинності, вивчають методи та інструменти, які використовують кіберзлочинці, а також розробляють рекомендації для правоохоронних органів держав-членів щодо підвищення ефективності боротьби з такими правопорушеннями.

Варто зазначити, що діяльність Europol та ЕС3 має важливе практичне значення для міжнародної координації боротьби з кіберзлочинністю. Зокрема, ЕС3 бере участь у проведенні масштабних міжнародних операцій, спрямованих проти кіберзлочинних мереж, які займаються поширенням програм-вимагачів, фінансовим шахрайством, незаконною торгівлею персональними даними та іншими формами злочинної діяльності у цифровому середовищі [41]. Така діяльність підтверджує важливість існування спеціалізованих інституцій, здатних забезпечити швидку взаємодію між державами у випадках розслідування транснаціональних кіберзлочинів.

Не менш важливу роль у системі забезпечення кібербезпеки відіграє Агентство Європейського Союзу з кібербезпеки (ENISA) [5]. Діяльність цього агентства спрямована на підвищення загального рівня кібербезпеки у Європейському Союзі та надання державам-членам експертної підтримки у формуванні ефективної політики захисту інформаційних систем і цифрової інфраструктури [36; 40].

ENISA здійснює широкий спектр функцій, які охоплюють аналітичну, дослідницьку, консультативну та координаційну діяльність. Агентство бере участь у розробленні стандартів кіберзахисту, підготовці методичних рекомендацій для державних органів та приватного сектору, а також у формуванні стратегічних підходів до управління кіберризиками. Важливим напрямом діяльності ENISA є

сприяння розвитку співпраці між урядовими структурами, бізнесом, науковими установами та експертним середовищем у сфері кібербезпеки [40].

Окрім цього, ENISA відіграє важливу роль у підготовці фахівців у сфері кібербезпеки. Агентство організовує навчальні програми, спеціалізовані тренінги, конференції та симуляційні вправи, спрямовані на підвищення рівня готовності держав-членів до реагування на масштабні кіберінциденти. Такі заходи дозволяють не лише оцінити ефективність існуючих механізмів реагування, але й формувати єдиний підхід до управління кіберризиками у межах Європейського Союзу. У звіті ENISA Threat Landscape Report підкреслюється, що розвиток спільної системи кіберстійкості є одним із ключових факторів забезпечення безпеки цифрового простору ЄС [40].

Ще однією важливою інституцією у системі боротьби з кіберзлочинністю є Євроюст (Eurojust), який відповідає за розвиток судового співробітництва між державами-членами Європейського Союзу у кримінальних справах [53]. Значення діяльності Eurojust особливо зростає у випадках розслідування транснаціональних злочинів, коли злочинні групи здійснюють свою діяльність на території кількох держав одночасно [18; 53].

Eurojust забезпечує координацію процесуальних дій між національними органами прокуратури та слідчими органами різних держав. Крім того, ця інституція сприяє створенню спільних слідчих груп, допомагає вирішувати питання юрисдикції, а також забезпечує ефективний обмін інформацією між правоохоронними органами різних країн. Завдяки цьому значно підвищується ефективність міжнародних розслідувань, спрямованих на протидію організованим кіберзлочинним угрупованням та іншим формам транснаціональної злочинності.

Важливим елементом інституційної системи кібербезпеки Європейського Союзу є також мережа команд реагування на комп’ютерні інциденти (CERT) [35]. Такі команди відіграють ключову роль у виявленні, аналізі та оперативному реагуванні на кіберінциденти, які можуть становити загрозу для інформаційних систем, цифрової інфраструктури та функціонування державних установ.

У структурі Європейського Союзу функціонує CERT-EU, який відповідає за забезпечення кібербезпеки інституцій, органів та агентств ЄС [35]. Основними завданнями CERT-EU є моніторинг кіберзагроз, аналіз потенційно небезпечної активності у цифровому середовищі, а також реагування на інциденти, пов'язані з порушенням безпеки інформаційних систем [35; 40].

Крім безпосереднього реагування на кіберінциденти, CERT-EU проводить дослідження шкідливого програмного забезпечення, аналізує нові типи кібератак та розробляє рекомендації щодо підвищення рівня захисту цифрової інфраструктури. Організація також активно співпрацює з національними CERT-командами держав-членів, що дозволяє забезпечувати швидкий обмін інформацією та координацію спільних дій у випадках масштабних кібератак або інших кризових ситуацій у цифровому середовищі.

Важливо зазначити, що ефективність інституційної системи Європейського Союзу значною мірою залежить від рівня взаємодії між різними структурами та органами. Для цього у ЄС активно використовуються механізми координації та обміну інформацією між правоохоронними органами, судовими установами, урядовими структурами та представниками приватного сектору [27; 28]. Спеціалізовані платформи співпраці дозволяють оперативно обмінюватися інформацією про нові кіберзагрози, методи їх здійснення та можливі способи протидії.

Крім внутрішньої співпраці у межах Європейського Союзу, важливе значення має взаємодія з міжнародними організаціями. Зокрема, держави-члени активно співпрацюють з Інтерполом, Радою Європи та іншими міжнародними структурами, діяльність яких спрямована на протидію кіберзлочинності [31; 54]. Така взаємодія дозволяє формувати більш широку глобальну систему боротьби з кіберзлочинністю та забезпечує узгодженість дій між різними державами і міжнародними організаціями.

Таким чином, інституційні механізми Європейського Союзу відіграють ключову роль у формуванні ефективної системи боротьби з кіберзлочинністю. Створення спеціалізованих органів, таких як Europol, EC3, ENISA, Eurojust та CERT-

EU, дозволило сформувати комплексну багаторівневу систему координації діяльності держав-членів у сфері кібербезпеки [40; 41; 42; 53]. Діяльність цих інституцій сприяє не лише підвищенню ефективності розслідування кіберзлочинів, але й зміцненню міжнародного співробітництва, розвитку аналітичних та профілактичних механізмів, а також забезпеченню належного рівня захисту інформаційного простору Європейського Союзу.

Інституційна система Європейського Союзу у сфері кібербезпеки забезпечує не лише формальне впровадження правових норм, але й їхню реальну практичну реалізацію, відіграючи ключову роль у координації дій держав-членів у протидії кіберзлочинності. Вона формує багаторівневий механізм взаємодії, у межах якого кожна інституція виконує чітко визначену функцію, доповнюючи діяльність інших структур.

Взаємодія між Europol, зокрема його кіберпідрозділом EC3, Eurojust, ENISA та національними CERT-структурами дозволяє створювати комплексний та узгоджений механізм реагування на кіберзлочини. У цьому механізмі поєднуються аналітичні можливості, технічна експертиза, оперативно-розшукова діяльність та судово-правова координація, що забезпечує більш повне охоплення всіх етапів протидії кіберзлочинності - від виявлення загрози до притягнення винних осіб до відповідальності.

Така багаторівнева модель суттєво підвищує ефективність боротьби з транснаціональною кіберзлочинністю, оскільки дозволяє оперативно реагувати на інциденти, швидко обмінюватися інформацією між державами-членами та забезпечувати узгодженість дій у межах усього Європейського Союзу [27; 41; 53].

2.3. Практика застосування законодавства ЄС щодо кіберзлочинів

Практичне застосування законодавства Європейського Союзу у сфері протидії кіберзлочинності має надзвичайно важливе значення для забезпечення реальної ефективності правового регулювання в умовах стрімкого розвитку інформаційних технологій та постійного розширення цифрового середовища. Слід зазначити, що саме по собі ухвалення нормативно-правових актів не може автоматично гарантувати високий рівень кібербезпеки. Наявність відповідних законодавчих норм є лише необхідною передумовою для ефективної боротьби з кіберзлочинами. Водночас визначальне значення має належна імплементація таких норм у національні правові системи держав-членів, а також їх практичне застосування правоохоронними органами, судами та іншими компетентними інституціями [23].

Крім цього, важливим аспектом ефективного функціонування механізму протидії кіберзлочинності є узгодженість дій держав-членів Європейського Союзу та налагоджена система взаємодії між їхніми правоохоронними структурами. У сучасних умовах кіберзлочини досить часто виходять за межі юрисдикції однієї держави, що суттєво ускладнює процес їх виявлення та розслідування. Саме тому досягнення ефективних результатів у цій сфері можливе лише за умови комплексного та системного підходу, який поєднує ефективне правове регулювання, інституційну співпрацю та дієві механізми реалізації законодавчих норм на практиці [21].

Одним із ключових напрямів практичного застосування законодавства Європейського Союзу у сфері боротьби з кіберзлочинністю є гармонізація кримінального законодавства держав-членів. Така гармонізація спрямована на забезпечення більшої узгодженості правових підходів до визначення складів кіберзлочинів, а також процедур їх розслідування та притягнення винних осіб до відповідальності. У цьому контексті особливо важливе значення має Директива 2013/40/ЄС про атаки на інформаційні системи [4], яка встановлює мінімальні стандарти криміналізації діянь, пов’язаних із незаконним втручанням у комп’ютерні системи та інформаційні мережі.

Прийняття цієї директиви стало важливим етапом у формуванні більш узгодженої та ефективної правової політики Європейського Союзу у сфері боротьби з кіберзлочинами. Вона створила правову основу для уніфікації підходів до криміналізації окремих видів протиправної діяльності у цифровому середовищі та сприяла підвищенню ефективності правозастосовної практики в державах-членах [22]. Відповідно до положень цього нормативно-правового акта держави-члени Європейського Союзу були зобов'язані привести своє національне законодавство у відповідність до встановлених вимог. Така адаптація дозволила сформувати більш узгоджений правовий простір, що значною мірою полегшує процес кримінального переслідування осіб, причетних до вчинення кіберзлочинів [23].

Практика застосування зазначених правових норм свідчить про те, що уніфікація законодавства держав-членів істотно підвищує ефективність міжнародної співпраці між правоохоронними органами. Особливо важливою така взаємодія є з огляду на специфіку кіберзлочинів, які у більшості випадків мають транскордонний характер [24]. У сучасних умовах правопорушники можуть здійснювати незаконну діяльність з території однієї держави, використовуючи серверну інфраструктуру, розташовану в іншій країні, тоді як шкода завдається користувачам або організаціям, що перебувають у третій державі.

За таких обставин ефективність розслідування подібних правопорушень значною мірою залежить від можливості оперативної взаємодії між державами. Наявність узгоджених правових механізмів дозволяє правоохоронним органам швидко обмінюватися необхідною інформацією, координувати проведення слідчих дій та забезпечувати притягнення винних осіб до відповідальності незалежно від місця вчинення злочину [25]. Саме тому важливо, щоб правові системи держав-членів Європейського Союзу мали схожі підходи до визначення складів кіберзлочинів, а також до процедур їх виявлення, розслідування та процесуального переслідування.

Важливе місце у практичній реалізації законодавства Європейського Союзу у сфері боротьби з кіберзлочинністю займає діяльність спеціалізованих європейських інституцій та агентств. До таких органів належать, зокрема, Європол та Євроюст, які

виконують важливу координаційну функцію у забезпеченні співпраці між правоохоронними органами держав-членів [41].

Завдяки діяльності цих інституцій створюються ефективні механізми обміну оперативною та аналітичною інформацією між компетентними органами різних держав. Крім того, вони сприяють організації спільних міжнародних операцій, спрямованих на боротьбу з транснаціональними злочинними угрупованнями, що здійснюють свою діяльність у кіберпросторі. Не менш важливим напрямом їхньої діяльності є надання експертної підтримки під час проведення складних кримінальних розслідувань, які охоплюють території кількох держав та потребують високого рівня координації між різними правоохоронними структурами [42].

Особливе місце у цій системі посідає Європейський центр боротьби з кіберзлочинністю (ЕС3), який функціонує у структурі Європолу [42]. Створення цього центру стало важливим етапом у розвитку інституційної системи протидії кіберзлочинності в Європейському Союзі. Основною метою діяльності ЕС3 є надання державам-членам комплексної підтримки під час розслідування кіберінцидентів та боротьби з різними формами кіберзлочинності.

Центр забезпечує аналітичну, технічну та оперативну підтримку правоохоронним органам держав-членів у процесі проведення розслідувань, пов’язаних із використанням інформаційних технологій. Його діяльність також спрямована на виявлення нових кіберзагроз, аналіз сучасних тенденцій розвитку кіберзлочинності та розроблення рекомендацій щодо підвищення ефективності протидії таким правопорушенням. Крім цього, ЕС3 виконує важливу координаційну функцію, сприяючи організації спільних дій правоохоронних органів різних держав у боротьбі з кіберзлочинами та забезпечуючи більш ефективне використання наявних ресурсів у цій сфері [29].

Практичний досвід діяльності ЕС3 переконливо свідчить про те, що ефективна протидія кіберзлочинності не може бути забезпечена виключно за рахунок правових інструментів або ізольованих заходів окремих держав. Натомість вона потребує комплексної багаторівневої моделі реагування, яка одночасно охоплює правовий, технічний та організаційний рівні забезпечення кібербезпеки [30]. У межах такої

моделі особливо важливе значення має своєчасне виявлення кіберінцидентів, їх детальний технічний аналіз, а також оперативна координація дій між усіма залученими суб'єктами.

Діяльність Центру демонструє, що ефективність розслідувань значною мірою залежить від рівня взаємодії між різними учасниками системи кібербезпеки. ЕС3 активно співпрацює не лише з національними правоохоронними органами держав-членів ЄС, але й з міжнародними структурами, а також із представниками приватного сектору [41]. Така взаємодія має особливе значення, оскільки саме приватні компанії — зокрема провайдери цифрових послуг, фінансові установи та оператори онлайн-платформ — найчастіше першими фіксують ознаки кіберінцидентів у власних системах. Це дозволяє оперативно отримувати інформацію про нові загрози та швидше реагувати на них.

Практика також підтверджує, що кіберзлочинці постійно вдосконалюють свої методи, використовуючи різноманітні форми атак, серед яких фішингові кампанії, шкідливе програмне забезпечення, несанкціонований доступ до баз даних, а також складні схеми фінансового шахрайства в онлайн-середовищі [48]. У цьому контексті обмін інформацією між державними органами та приватним сектором дозволяє не лише реагувати на вже вчинені злочини, але й здійснювати превентивне виявлення потенційних загроз на ранніх етапах їх розвитку.

Окремої уваги потребує проблема кіберзлочинів, пов'язаних із діяльністю організованих злочинних угруповань [54]. Такі структури характеризуються високим рівнем організації, чітким розподілом ролей між учасниками та використанням сучасних технологічних засобів для забезпечення анонімності. Вони активно застосовують криптовалюти для здійснення фінансових операцій, використовують зашифровані канали зв'язку, а також спеціальні програмні засоби для приховування слідів своєї діяльності. У зв'язку з цим розслідування подібних злочинів потребує особливо складної координації між державами та міжнародними організаціями.

Практичний досвід Європейського Союзу також демонструє важливість застосування законодавства у судовій практиці. Одним із відомих прикладів є справа щодо діяльності міжнародної мережі шкідливого програмного забезпечення Emotet,

яку правоохоронні органи кількох держав ЄС ліквідували за координації Europol та Eurojust у 2021 році [41]. У межах цієї операції було проведено масштабне вилучення серверної інфраструктури, що використовувалася для розповсюдження шкідливого програмного забезпечення та викрадення персональних даних користувачів. Результати цієї справи продемонстрували ефективність практичного застосування механізмів міжнародного співробітництва та узгоджених правових процедур між державами-членами ЄС.

Ще одним важливим прикладом є справа EncroChat, пов'язана з використанням зашифрованої комунікаційної платформи організованими злочинними угрупованнями [42]. У результаті спільної операції правоохоронних органів Франції, Нідерландів та Europol було отримано доступ до зашифрованих повідомлень, що дозволило виявити численні факти незаконного обігу наркотиків, відмивання коштів та інших форм організованої злочинної діяльності. Надалі зібрані цифрові докази активно використовувалися у кримінальних провадженнях та судових процесах у різних державах Європейського Союзу.

Важливе значення для формування практики застосування законодавства ЄС має також судова практика Суду Європейського Союзу (Court of Justice of the European Union). Зокрема, у своїх рішеннях Суд неодноразово наголошував на необхідності дотримання балансу між забезпеченням кібербезпеки та захистом фундаментальних прав людини, насамперед права на приватність і захист персональних даних [39]. Такий підхід має особливе значення в умовах розвитку цифрових технологій та розширення повноважень державних органів у сфері моніторингу електронних комунікацій.

Практика Європейського суду з прав людини також істотно впливає на формування правових стандартів у сфері кібербезпеки та цифрових прав. У низці справ Суд підкреслював, що втручання держави у сферу приватного цифрового спілкування повинно бути законним, пропорційним та здійснюватися виключно за наявності достатніх правових підстав [33]. Це сприяє формуванню більш збалансованого підходу до застосування законодавства у сфері кібербезпеки.

Практичний досвід Європейського Союзу також переконливо демонструє критичну важливість співпраці з приватним сектором у сфері кібербезпеки [51]. Оскільки значна частина цифрової інфраструктури перебуває у приватній власності, саме компанії відіграють ключову роль у забезпеченні стабільності та безпеки інформаційних систем. У зв'язку з цим у ЄС активно розвивається модель публічно-приватного партнерства, яка передбачає регулярний обмін інформацією про кіберзагрози, спільну розробку стандартів безпеки та координацію дій у разі виникнення масштабних інцидентів [34].

У межах цієї моделі компанії не лише повідомляють про зафіксовані інциденти, але й беруть участь у формуванні практичних підходів до запобігання новим видам атак. Такий підхід дозволяє підвищити загальний рівень кіберстійкості як на рівні окремих організацій, так і на рівні всього Європейського Союзу.

Ще одним важливим елементом практичного застосування законодавства ЄС є розвиток та вдосконалення системи реагування на кіберінциденти. У державах-членах функціонують спеціалізовані команди CERT, які виконують завдання з моніторингу, виявлення, аналізу та ліквідації наслідків кібератак [40]. Їхня діяльність охоплює як технічний аналіз шкідливого програмного забезпечення, так і координацію заходів реагування на національному рівні.

Координація роботи CERT-команд на рівні Європейського Союзу має принципове значення, оскільки дозволяє забезпечити швидкий обмін технічною інформацією про нові вектори атак, індикатори компрометації та методи протидії [36]. У результаті держави-члени отримують можливість оперативно реагувати навіть на масштабні транскордонні кібератаки, мінімізуючи їх негативні наслідки для критичної інфраструктури та користувачів.

Разом із тим практика застосування законодавства Європейського Союзу у сфері протидії кіберзлочинності демонструє наявність низки суттєвих викликів. Одним із найбільш актуальних є надзвичайно швидкий темп розвитку інформаційних технологій, який постійно породжує нові форми та методи кіберзлочинної діяльності [37]. Це створює ситуацію, за якої правове регулювання об'єктивно не завжди встигає

адаптуватися до технологічних змін, що вимагає постійного оновлення нормативної бази та вдосконалення механізмів її практичного застосування.

Окремою проблемою залишається нерівномірність розвитку технічних та інституційних можливостей держав-членів ЄС [38]. Рівень забезпечення кібербезпеки суттєво відрізняється залежно від країни: одні держави мають розвинену цифрову інфраструктуру, сучасні технологічні рішення та достатню кількість кваліфікованих спеціалістів, тоді як інші стикаються з браком ресурсів і кадрового потенціалу. У зв'язку з цим на рівні Європейського Союзу особлива увага приділяється програмам підготовки фахівців, підвищенню цифрової компетентності та розвитку спільних освітніх ініціатив у сфері кібербезпеки [55].

Таким чином, практика застосування законодавства Європейського Союзу у сфері протидії кіберзлочинності свідчить про необхідність системного та комплексного підходу до вирішення цієї проблематики. Ефективна протидія сучасним кіберзагрозам можлива лише за умови одночасного поєднання правових механізмів, інституційної взаємодії, міжнародного співробітництва та активного залучення приватного сектору [40]. Саме така багаторівнева модель дозволяє Європейському Союзу забезпечувати більш стійку систему кібербезпеки та ефективно реагувати на постійно змінюваний характер кіберзлочинності.

Практика застосування законодавства Європейського Союзу у сфері протидії кіберзлочинності чітко демонструє важливість тісної координації між державами-членами, подальшого розвитку механізмів міжнародного співробітництва та активного залучення приватного сектору до системи кібербезпеки. Саме поєднання цих елементів забезпечує реальну ефективність правових норм у практичній площині.

Особливо значущим є впровадження моделей публічно-приватного партнерства, які дозволяють значно розширити можливості обміну інформацією про кіберзагрози, підвищити швидкість реагування на кіберінциденти та покращити якість аналітичної оцінки нових видів кіберзлочинної діяльності. Участь приватних компаній у цих процесах є критично важливою, оскільки саме вони володіють значною частиною цифрової інфраструктури та першими стикаються з наслідками кібератак.

У сукупності зазначені елементи формують ефективну та практично орієнтовану модель протидії кіберзлочинності в межах Європейського Союзу, яка поєднує правові, інституційні та організаційні інструменти, забезпечуючи більш високий рівень кіберстійкості та захисту цифрового середовища [34; 40; 51].

РОЗДІЛ 3

ПРАВОВИЙ ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

3.1. Правове регулювання боротьби з кіберзлочинністю в Україні

Стрімкий розвиток інформаційних технологій, а також активна цифровізація практично всіх сфер суспільного життя істотно змінили характер сучасних загроз у сфері безпеки. Цифрові технології створили широкі можливості для розвитку економіки, державного управління, комунікацій та обміну інформацією, однак водночас вони стали підґрунтям для виникнення нових форм протиправної діяльності. Однією з найбільш небезпечних таких форм є кіберзлочинність, яка становить серйозну загрозу для стабільного функціонування інформаційної інфраструктури держави, безпеки економічних процесів, а також для реалізації прав і свобод громадян у цифровому середовищі. У зв'язку з цим особливого значення набуває формування ефективної та системної моделі правового регулювання протидії кіберзлочинності в Україні, здатної відповідати сучасним технологічним викликам.

Правову основу регулювання відповідних відносин становлять положення Конституції України, які закріплюють базові принципи забезпечення прав і свобод людини та громадянина. Конституція визначає фундаментальні гарантії захисту інформації, забезпечення недоторканності приватного життя, а також охорони персональних даних. Такі положення формують загальні конституційні засади функціонування інформаційних відносин у державі та створюють правову основу для розвитку національної системи кібербезпеки. Саме на цих принципах базується подальше формування галузевого законодавства, спрямованого на захист інформаційних ресурсів та протидію злочинам у цифровому середовищі [1].

Важливим чинником формування національної системи правового регулювання у сфері боротьби з кіберзлочинністю є міжнародні зобов'язання

України. У сучасних умовах кіберзлочини часто мають транснаціональний характер, що потребує узгоджених дій різних держав та використання спільних міжнародно-правових стандартів. Одним із ключових міжнародних документів у цій сфері є Конвенція про кіберзлочинність 2001 року, відома як Будапештська конвенція. Приєднання України до цього міжнародного договору стало важливим кроком на шляху інтеграції до глобальної системи боротьби з кіберзлочинністю. Ратифікація Конвенції передбачає зобов'язання держави адаптувати національне законодавство до міжнародних стандартів, що стосуються криміналізації незаконного доступу до комп'ютерних систем, втручання у роботу інформаційних мереж, незаконного перехоплення комп'ютерних даних та інших форм протиправної діяльності у кіберпросторі [2].

Крім основного тексту Конвенції, важливе значення має також Додатковий протокол до неї, який передбачає криміналізацію поширення расистських і ксенофобських матеріалів через комп'ютерні системи. Приєднання України до цього протоколу дозволило розширити правові механізми реагування на злочини, що здійснюються у цифровому середовищі та пов'язані з поширенням дискримінаційного або екстремістського контенту. Це сприяло посиленню правового захисту суспільства від небезпечних проявів інформаційної агресії та незаконної діяльності в мережі Інтернет [3].

Центральне місце у системі національного законодавства, спрямованого на боротьбу з кіберзлочинністю, займає Кримінальний кодекс України. У його структурі передбачено спеціальний розділ, який присвячений злочинам у сфері використання електронно-обчислювальних машин, комп'ютерних систем і мереж. У межах цього розділу встановлено кримінальну відповідальність за низку діянь, пов'язаних із неправомірним втручанням у функціонування інформаційних ресурсів. Зокрема, до таких діянь належать несанкціонований доступ до інформаційних систем, створення та розповсюдження шкідливого програмного забезпечення, незаконне використання або копіювання комп'ютерної інформації, а також інші дії, що можуть порушувати нормальну роботу комп'ютерних мереж і систем [12].

Наявність таких норм у кримінальному законодавстві має принципове значення для формування ефективної системи протидії кіберзлочинності. Вони дозволяють чітко визначити коло діянь, які визнаються кримінальними правопорушеннями, а також встановлюють відповідні санкції за їх вчинення. Водночас практика застосування цих норм показує, що ефективність боротьби з кіберзлочинами значною мірою залежить від технічних можливостей правоохоронних органів, рівня підготовки спеціалістів та ефективності міжнародного співробітництва. Багато кіберзлочинів мають складний технічний характер і здійснюються із використанням серверів або мережевої інфраструктури, що розташована за межами держави, що істотно ускладнює процес їх розслідування [18].

Важливим елементом правового регулювання у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України». Цей нормативно-правовий акт визначає основні принципи державної політики у сфері кібербезпеки, встановлює правові та організаційні засади функціонування національної системи кіберзахисту, а також визначає коло суб’єктів, відповідальних за реалізацію державної політики у цій сфері. До таких суб’єктів належать, зокрема, Служба безпеки України, Державна служба спеціального зв’язку та захисту інформації, Національна поліція України, Міністерство оборони України, розвідувальні органи та інші державні інституції [9].

Зазначений закон передбачає створення національної системи кібербезпеки, основною метою якої є забезпечення ефективної координації діяльності різних державних органів у сфері захисту інформаційної інфраструктури. До ключових завдань цієї системи належать запобігання кіберінцидентам, своєчасне виявлення кіберзагроз, реагування на кібератаки, а також мінімізація їх негативних наслідків для державних органів, підприємств і громадян.

Важливим стратегічним документом у цій сфері є також Стратегія кібербезпеки України, яка визначає основні напрями розвитку державної політики у сфері захисту інформаційного простору. У цьому документі окреслено ключові пріоритети держави, серед яких — посилення інституційної спроможності органів державної влади, підвищення рівня захисту критичної інформаційної інфраструктури, розвиток

міжнародного співробітництва у сфері кібербезпеки та удосконалення національного законодавства відповідно до сучасних викликів цифрового середовища [13].

Окрім спеціалізованих нормативно-правових актів, важливу роль у регулюванні інформаційних відносин відіграє Закон України «Про інформацію». Він визначає основні принципи державної інформаційної політики, встановлює порядок доступу до інформації, а також регулює питання її використання, поширення та захисту. Норми цього закону створюють загальні правові засади функціонування інформаційного простору та забезпечують правові гарантії захисту інформаційних ресурсів [10].

Ще одним важливим елементом законодавчого регулювання є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Його положення спрямовані на забезпечення технічного та криптографічного захисту інформації, яка обробляється в електронних системах. Закон встановлює вимоги до створення систем захисту інформації, визначає правила їх функціонування, а також регулює питання сертифікації засобів захисту інформаційних ресурсів [11].

Попри наявність значної кількості нормативно-правових актів, що регулюють сферу кібербезпеки, система правового регулювання протидії кіберзлочинності в Україні продовжує активно розвиватися. Це пов’язано насамперед із надзвичайно швидким розвитком інформаційних технологій, який постійно породжує нові форми кіберзагроз і злочинної діяльності у цифровому середовищі. У таких умовах законодавство потребує регулярного оновлення та вдосконалення, щоб ефективно реагувати на нові виклики.

Окремого значення набуває процес гармонізації українського законодавства з правовими стандартами Європейського Союзу. У межах реалізації євроінтеграційного курсу України важливим завданням є адаптація національних нормативно-правових актів до європейських стандартів у сфері кібербезпеки. Такий процес сприяє підвищенню ефективності боротьби з кіберзлочинністю, зміцненню міжнародної співпраці та інтеграції України до спільного європейського простору безпеки [27].

Отже, правове регулювання боротьби з кіберзлочинністю в Україні формується на основі поєднання конституційних норм, міжнародних зобов'язань, положень кримінального законодавства та спеціалізованих нормативно-правових актів у сфері кібербезпеки. Така система створює необхідні передумови для забезпечення захисту інформаційної інфраструктури держави та протидії сучасним кіберзагрозам. Водночас подальший розвиток цифрових технологій і зростання масштабів кіберзлочинності обумовлюють необхідність постійного вдосконалення правових механізмів, розвитку інституційної спроможності держави та розширення міжнародного співробітництва у цій сфері.

Проведений аналіз свідчить, що нормативно-правова база України у сфері кібербезпеки вже в цілому сформована та охоплює основні напрями регулювання відносин у цифровому середовищі. Водночас вона потребує подальшого системного вдосконалення з урахуванням стрімкого розвитку інформаційно-комунікаційних технологій, а також постійної появи нових, більш складних форм кіберзлочинності.

Ефективність національного законодавства значною мірою залежить не лише від наявності відповідних нормативних актів, але й від його здатності оперативно адаптуватися до сучасних цифрових викликів. Йдеться, зокрема, про необхідність своєчасного оновлення правових норм, удосконалення механізмів їх реалізації та забезпечення належного рівня захисту інформаційних систем, державних реєстрів і критичної цифрової інфраструктури. У цьому контексті особливого значення набуває узгодженість національного законодавства з міжнародними стандартами кібербезпеки [9; 12].

3.2. Порівняльний аналіз правового досвіду ЄС та України в галузі боротьби з кіберзлочинністю

Розвиток інформаційних технологій та стрімка цифровізація економічних і соціальних процесів у глобальному масштабі зумовили суттєве зростання кількості кіберзлочинів. Такі трансформації сучасного суспільства створили принципово нове середовище, у якому традиційні підходи до забезпечення безпеки вже не є достатньо ефективними. У зв'язку з цим держави змушені не лише реагувати на нові загрози, а й формувати комплексні правові та інституційні механізми протидії кіберзлочинності, які враховують специфіку цифрового простору. Особливо важливим у цьому контексті є досвід Європейського Союзу, який вибудував досить розвинену та багаторівневу систему кібербезпеки, що поєднує нормативно-правове регулювання, діяльність спеціалізованих інституцій та інструменти міжнародної співпраці. Україна, зі свого боку, також поступово розвиває власну модель протидії кіберзлочинності, орієнтуючись на європейські підходи та міжнародні стандарти у цій сфері.

Передусім слід підкреслити, що одним із базових міжнародно-правових документів, який визначає загальні підходи до боротьби з кіберзлочинністю, є Конвенція Ради Європи про кіберзлочинність 2001 року. Україна приєдналася до цього документа, тим самим взявши на себе зобов'язання щодо гармонізації національного законодавства з його положеннями та принципами. У межах цієї Конвенції сформульовано ключові категорії кіберзлочинів, які держави повинні криміналізувати на національному рівні. Зокрема, йдеться про незаконний доступ до комп'ютерних систем, втручання у функціонування комп'ютерних мереж і даних, комп'ютерне шахрайство, а також створення, використання та поширення шкідливого програмного забезпечення, що становить загрозу для інформаційної безпеки [31].

У правовій системі Європейського Союзу регулювання кібербезпеки характеризується значно вищим рівнем системності та деталізації, оскільки воно

охоплює широкий спектр нормативно-правових актів, спрямованих на різні аспекти цифрової безпеки. Одним із ключових документів у цій сфері є Директива про безпеку мережевих та інформаційних систем, яка закладає основи загальноєвропейського підходу до забезпечення кіберстійкості. Відповідно до її положень, держави-члени зобов'язані формувати національні стратегії кібербезпеки, визначати уповноважені компетентні органи, а також забезпечувати функціонування ефективних механізмів реагування на кіберінциденти та кібератаки [37].

Подальший розвиток нормативної бази ЄС у цій сфері був пов'язаний із прийняттям Директиви NIS2, яка істотно розширила сферу регулювання та коло суб'єктів, що підпадають під вимоги кібербезпеки. Окрім цього, було підвищено стандарти управління кіберризиками, а також посилено вимоги щодо обов'язкового інформування про кіберінциденти. Такий підхід свідчить про поступовий перехід Європейського Союзу до моделі більш жорсткої та уніфікованої системи кіберзахисту, яка спрямована на забезпечення єдиного високого рівня безпеки в усіх державах-членах [38].

В Україні правове регулювання кібербезпеки базується насамперед на Законі України «Про основні засади забезпечення кібербезпеки України». Цей нормативно-правовий акт визначає ключові принципи державної політики у сфері кібербезпеки, а також встановлює систему суб'єктів, відповідальних за її реалізацію. До таких суб'єктів віднесено Службу безпеки України, Національну поліцію України, Державну службу спеціального зв'язку та захисту інформації, а також інші органи державної влади, що виконують функції у сфері захисту інформаційної інфраструктури.

Важливою складовою національної системи протидії кіберзлочинності є також кримінально-правове регулювання. Зокрема, Кримінальний кодекс України містить норми, які передбачають відповідальність за злочини у сфері використання комп'ютерних систем і мереж. Особливе значення має стаття 361 Кримінального кодексу України, яка встановлює відповідальність за несанкціоноване втручання у роботу електронно-обчислювальних машин, комп'ютерних мереж або телекомунікаційних систем. У науковій літературі справедливо зазначається, що

«криміналізація таких діянь є необхідною умовою ефективної боротьби з кіберзлочинністю» [45, с. 87].

Водночас, якщо порівнювати Україну з Європейським Союзом, можна констатувати, що національна система правового регулювання кібербезпеки все ще перебуває на етапі активного становлення та розвитку. Однією з ключових відмінностей є рівень інституційної координації. У ЄС функціонує розгалужена мережа спеціалізованих органів, які забезпечують комплексну протидію кіберзлочинності. Зокрема, важливу роль відіграє Європейський центр боротьби з кіберзлочинністю, що функціонує у структурі Європолу. Його діяльність спрямована на координацію розслідувань, підтримку держав-членів та організацію спільних операцій проти кіберзлочинних угруповань [42].

Крім того, значну роль у системі кібербезпеки ЄС відіграє Агентство Європейського Союзу з кібербезпеки (ENISA), яке здійснює аналітичну, методичну та експертну діяльність. Воно займається оцінкою кіберзагроз, розробкою рекомендацій для держав-членів та сприяє формуванню єдиних підходів до управління кіберризиками. Як підкреслюється у звітах агентства, сучасні кіберзагрози мають чітко виражений транскордонний характер, що обумовлює необхідність тісної міжнародної співпраці та оперативного обміну інформацією [40].

В Україні також функціонують спеціалізовані інституції у сфері кібербезпеки. Зокрема, у структурі Національної поліції діє Департамент кіберполіції, основними завданнями якого є виявлення, припинення та розслідування кіберзлочинів, а також взаємодія з міжнародними правоохоронними структурами. Водночас науковці наголошують, що ефективність діяльності таких органів значною мірою залежить від рівня технічного забезпечення, кадрового потенціалу та розвитку міжнародного співробітництва [46, с. 102].

Ще однією суттєвою відмінністю між Європейським Союзом та Україною є ступінь інтеграції кібербезпеки у загальну стратегію цифрового розвитку. У ЄС кібербезпека розглядається як невід’ємний елемент функціонування цифрової економіки та внутрішнього ринку. У Стратегії кібербезпеки Європейського Союзу

наголошується, що забезпечення безпечного цифрового середовища є ключовою передумовою сталого розвитку інформаційного суспільства [34].

В Україні також формується стратегічний підхід до розвитку кібербезпеки, однак рівень його інституційної та практичної реалізації поки що є менш системним порівняно з Європейським Союзом. Серед основних проблем можна виділити недостатню координацію між державними органами, обмежене фінансування, а також дефіцит висококваліфікованих спеціалістів у сфері кіберзахисту.

Разом з тим, Україна активно розвиває міжнародне співробітництво у сфері протидії кіберзлочинності. Особливо важливим є партнерство з Європейським Союзом, НАТО та іншими міжнародними організаціями, яке дозволяє отримувати технічну допомогу, обмінюватися досвідом та впроваджувати сучасні стандарти кібербезпеки [52].

Таким чином, результати порівняльного аналізу свідчать про те, що система правового регулювання протидії кіберзлочинності в Європейському Союзі є більш комплексною, структурованою та інституційно розвиненою. Водночас Україна вже сформувала базові правові та організаційні засади у цій сфері та поступово наближає своє законодавство до європейських стандартів. Подальший розвиток національної системи кібербезпеки потребує посилення інституційної координації, модернізації законодавства та розширення міжнародної співпраці з урахуванням найкращих практик ЄС.

Порівняльний аналіз законодавства України та Європейського Союзу дозволяє зробити висновок, що правова система ЄС загалом характеризується більш системним, структурованим та комплексним підходом до регулювання сфери кібербезпеки. Вона поєднує уніфіковані нормативно-правові акти, які встановлюють загальні стандарти для всіх держав-членів, із розвиненими інституційними механізмами, що забезпечують практичну координацію дій у сфері протидії кіберзлочинності.

Завдяки такій моделі в Європейському Союзі досягається вищий рівень узгодженості правозастосування, оперативності реагування на кіберзагрози та ефективності міжнародного співробітництва між правоохоронними органами. У

цьому контексті для України особливо актуальним є продовження процесу гармонізації національного законодавства з європейськими правовими стандартами, що є важливою умовою подальшої інтеграції до спільного європейського правового простору у сфері кібербезпеки [4; 7; 28].

3.3. Шляхи вдосконалення національного законодавства України в галузі боротьби з кіберзлочинністю з урахуванням досвіду ЄС

Стрімкий розвиток інформаційних технологій, цифровізація суспільних процесів та глобалізація інформаційного простору призводять до суттєвих змін у характері сучасної злочинності. Одним із найбільш помітних проявів цих трансформацій стало значне зростання кількості правопорушень, що вчиняються у кіберпросторі. Кіберзлочинність поступово перетворюється на один із найбільш динамічних і технологічно складних видів злочинної діяльності, що становить серйозну загрозу для функціонування державних інституцій, економічної стабільності та безпеки громадян. У зв'язку з цим питання вдосконалення законодавства у сфері протидії кіберзлочинності набуває особливої актуальності для України.

Одним із ключових напрямів удосконалення законодавства України є гармонізація національних правових норм із міжнародними стандартами та законодавством Європейського Союзу. У контексті європейської інтеграції це питання набуває особливого значення, оскільки адаптація національного законодавства до європейських стандартів сприяє підвищенню ефективності боротьби з кіберзлочинністю та зміцненню міжнародного співробітництва у цій сфері. Україна є учасником Конвенції Ради Європи про кіберзлочинність, яка визначає основні принципи криміналізації діянь у сфері інформаційних технологій, а також встановлює механізми міжнародної взаємодії під час розслідування кіберзлочинів [31].

Разом з тим, на практиці імплементація положень цієї Конвенції в українське законодавство потребує подальшого вдосконалення. Зокрема, виникає необхідність більш детального врегулювання процедур збору та збереження електронних доказів, забезпечення оперативного доступу до цифрових даних, а також розширення механізмів міжнародної правової допомоги у сфері розслідування кіберзлочинів.

Важливим кроком у цьому напрямі може стати приведення українського законодавства у відповідність до сучасних європейських стандартів кібербезпеки. У Європейському Союзі сформовано досить комплексну систему нормативно-правових актів, які регулюють різні аспекти цифрової безпеки. Одним із ключових документів є Директива про безпеку мережевих та інформаційних систем, яка встановлює єдині підходи до управління кіберризиками, реагування на кіберінциденти та організації обміну інформацією між державами-членами [37].

Запровадження подібних підходів в Україні дозволило б суттєво підвищити ефективність функціонування національної системи кібербезпеки. Крім того, це сприяло б більш тісній інтеграції України до європейського цифрового простору та створило б передумови для поглиблення співпраці з європейськими структурами у сфері кіберзахисту.

Ще одним важливим напрямом удосконалення законодавства є подальший розвиток кримінально-правових норм, спрямованих на протидію кіберзлочинності. У Кримінальному кодексі України вже передбачено відповідальність за низку злочинів у сфері використання комп'ютерних систем і мереж. Зокрема, кримінально караними є несанкціоноване втручання у роботу комп'ютерних систем, створення та поширення шкідливого програмного забезпечення, незаконне використання інформації та інші правопорушення, пов'язані з функціонуванням інформаційних технологій [44].

Однак швидкий розвиток цифрових технологій постійно породжує нові форми кіберзлочинності, які не завжди охоплюються чинними нормами кримінального законодавства. Як зазначають дослідники, «правове регулювання у сфері інформаційної безпеки повинно постійно адаптуватися до нових технологічних умов та нових форм злочинної діяльності» [47, с. 134].

Зокрема, потребують більш детального правового врегулювання питання, пов'язані з використанням криптовалют у злочинних схемах, шахрайством у сфері електронної комерції, незаконним обігом цифрових активів, а також правопорушеннями, пов'язаними із застосуванням технологій штучного інтелекту та автоматизованих систем.

Не менш важливим напрямом удосконалення законодавства є розвиток ефективних механізмів розслідування кіберзлочинів. Особливістю таких правопорушень є їх транснаціональний характер, що суттєво ускладнює діяльність правоохоронних органів. У багатьох випадках злочинні дії можуть здійснюватися з території однієї держави, тоді як технічна інфраструктура або сервери розташовані в іншій країні.

У зв'язку з цим надзвичайно важливим є розширення можливостей міжнародного співробітництва у сфері кримінального правосуддя. Конвенція про кіберзлочинність передбачає створення ефективних механізмів оперативної взаємодії між державами, включаючи обмін інформацією, надання взаємної правової допомоги, а також проведення спільних міжнародних розслідувань [31].

Крім того, значну роль у підвищенні ефективності боротьби з кіберзлочинністю відіграє вдосконалення системи інституційного забезпечення кібербезпеки. У Європейському Союзі координація діяльності у цій сфері здійснюється за участю спеціалізованих органів та агентств. Зокрема, важливу роль відіграють Європейський центр боротьби з кіберзлочинністю, який функціонує у структурі Європолу, а також Агентство Європейського Союзу з кібербезпеки (ENISA) [40].

Ці інституції здійснюють аналіз сучасних кіберзагроз, координують діяльність правоохоронних органів держав-членів, організовують спільні міжнародні операції та сприяють розвитку стратегічної співпраці у сфері кібербезпеки.

В Україні також функціонують спеціалізовані підрозділи, які займаються протидією кіберзлочинності. Зокрема, важливу роль відіграє Департамент кіберполіції Національної поліції України, основним завданням якого є запобігання, виявлення та розслідування кіберзлочинів. Водночас, як зазначається у наукових дослідженнях, ефективність діяльності таких підрозділів значною мірою залежить від рівня технічного забезпечення, доступу до сучасних інформаційних технологій та підготовки висококваліфікованих фахівців у сфері цифрової криміналістики [48, с. 91].

У зв'язку з цим важливим напрямом удосконалення законодавства має стати розвиток системи підготовки спеціалістів у сфері кібербезпеки та кіберрозслідувань.

Це передбачає створення спеціалізованих освітніх програм у закладах вищої освіти, підвищення кваліфікації працівників правоохоронних органів, а також активне залучення експертів з інформаційних технологій до процесу розслідування кіберзлочинів.

Ще одним перспективним напрямом є розвиток державно-приватного партнерства у сфері кібербезпеки. Значна частина об'єктів критичної інформаційної інфраструктури перебуває у власності або управлінні приватних компаній, що обумовлює необхідність їх активної участі у системі кіберзахисту. У країнах Європейського Союзу така співпраця є важливою складовою національних стратегій кібербезпеки та дозволяє оперативно реагувати на нові кіберзагрози [34].

В Україні також поступово формується практика взаємодії між державними органами та приватним сектором у сфері кібербезпеки. Проте для підвищення ефективності такої співпраці необхідно створити чіткі правові механізми обміну інформацією про кіберзагрози, визначити порядок взаємодії між суб'єктами кібербезпеки та забезпечити належний рівень захисту конфіденційних даних.

Таким чином, удосконалення законодавства України у сфері протидії кіберзлочинності має здійснюватися за кількома взаємопов'язаними напрямами. До них належать гармонізація національного законодавства з європейськими стандартами, розширення кримінально-правових норм щодо нових форм кіберзлочинності, розвиток міжнародного співробітництва, вдосконалення інституційної системи кібербезпеки, підготовка висококваліфікованих фахівців, а також розвиток державно-приватного партнерства у сфері кіберзахисту.

Реалізація зазначених заходів сприятиме формуванню більш ефективної національної системи протидії кіберзлочинності, підвищенню рівня захищеності інформаційної інфраструктури держави та забезпеченню належного рівня безпеки цифрового простору України.

Удосконалення законодавства України у сфері протидії кіберзлочинності має здійснюватися на комплексній та системній основі, із врахуванням сучасних міжнародних підходів і практики провідних держав. Такий процес повинен охоплювати гармонізацію національного законодавства з міжнародними та

європейськими стандартами, розвиток інституційної спроможності відповідних органів, а також підвищення ефективності діяльності правоохоронних структур у сфері виявлення, розслідування та запобігання кіберзлочинам.

Важливим напрямом є також активізація міжнародного співробітництва, зокрема в частині обміну інформацією, спільного розслідування транснаціональних кіберзлочинів та участі у міжнародних програмах кібербезпеки. Окрему увагу слід приділити посиленню взаємодії між державним і приватним секторами, оскільки саме приватні компанії часто виступають ключовими суб'єктами цифрової інфраструктури.

Крім того, перспективним напрямом є впровадження сучасних технологічних рішень у сфері кіберзахисту, що дозволить підвищити загальний рівень кіберстійкості держави та забезпечити більш ефективну протидію новітнім формам кіберзагроз [31; 47].

ВИСНОВКИ

У сучасних умовах швидкого розвитку інформаційних технологій та активної цифровізації суспільства кіберзлочинність перетворилася на одну з найбільш небезпечних форм сучасної злочинної діяльності. Глобалізація інформаційного простору, широке поширення мережевих технологій, а також зростаюча залежність державних інституцій, економічних процесів і суспільних відносин від цифрових систем спричиняють появу нових загроз, пов’язаних із неправомірним використанням інформаційних технологій. У зв’язку з цим питання формування ефективної системи правового регулювання та розвитку міжнародного співробітництва у сфері протидії кіберзлочинності набуває особливої актуальності.

У ході проведеного дослідження було проаналізовано теоретичні, міжнародно-правові та національні аспекти протидії кіберзлочинності, а також визначено ключові напрями вдосконалення правового регулювання у зазначеній сфері.

У першому розділі дипломної роботи розглянуто теоретичні засади дослідження кіберзлочинності. Зокрема, проаналізовано поняття та основні ознаки кіберзлочинності, що дозволяють відмежувати її від інших форм протиправної діяльності. У результаті встановлено, що кіберзлочинність являє собою сукупність злочинів, які вчиняються із використанням інформаційно-комунікаційних технологій або спрямовані проти комп’ютерних систем, мереж чи інформаційних ресурсів [19; 23]. До характерних особливостей кіберзлочинів належать їх транснаціональний характер, високий рівень латентності, застосування складних технологічних засобів, а також значні труднощі, що виникають у процесі їх виявлення та розслідування.

У межах дослідження також розглянуто основні підходи до класифікації кіберзлочинів. У науковій літературі пропонуються різні критерії їх класифікації, серед яких найбільш поширеними є поділ залежно від об’єкта посягання, способу вчинення правопорушення або використаних технологій [21; 22]. Зокрема, до основних видів кіберзлочинів відносять незаконний доступ до комп’ютерних систем, втручання у функціонування інформаційних систем, неправомірне використання

персональних даних, кібершахрайство, розповсюдження шкідливого програмного забезпечення та інші правопорушення, що здійснюються у кіберпросторі.

Окрему увагу в роботі приділено міжнародно-правовим механізмам протидії кіберзлочинності. У результаті дослідження встановлено, що ключову роль у формуванні міжнародної системи боротьби з кіберзлочинами відіграє Конвенція про кіберзлочинність Ради Європи 2001 року, яка визначає основні напрями криміналізації кіберзлочинів та встановлює механізми міжнародного співробітництва у цій сфері [2]. Важливе значення мають також додаткові протоколи до цієї Конвенції та інші міжнародні документи, спрямовані на гармонізацію законодавства різних держав і формування ефективних механізмів взаємодії між правоохоронними органами.

У другому розділі дипломної роботи досліджено особливості правового регулювання боротьби з кіберзлочинністю в Європейському Союзі. Аналіз нормативно-правової бази ЄС засвідчив, що у Союзі сформована комплексна система правового регулювання у сфері кібербезпеки. Значну роль у цьому відіграють директиви та регламенти Європейського Союзу, спрямовані на забезпечення захисту інформаційних систем та безпеки мережевої інфраструктури, зокрема Директива щодо атак на інформаційні системи, Директива NIS та Регламент про кібербезпеку [4; 5; 6; 7].

Характерною рисою правового регулювання у Європейському Союзі є поєднання нормативно-правових механізмів із ефективною інституційною системою забезпечення кібербезпеки. У межах ЄС функціонує низка спеціалізованих органів, діяльність яких спрямована на координацію боротьби з кіберзлочинністю, обмін інформацією між державами-членами та проведення спільних розслідувань. Серед таких інституцій важливу роль відіграють Europol, Європейський центр боротьби з кіберзлочинністю (ЕС3), Агентство ЄС з кібербезпеки (ENISA), а також Євроюст, який забезпечує координацію судового співробітництва між державами-членами [27; 28].

Крім того, у Європейському Союзі активно розвивається практика міжнародної взаємодії у сфері протидії кіберзлочинності. Це проявляється у створенні спільних

слідчих груп, проведенні міжнародних операцій проти кіберзлочинних угруповань, а також у регулярному обміні інформацією між правоохоронними органами різних держав.

Важливим аспектом дослідження також є практичне застосування законодавства Європейського Союзу у сфері протидії кіберзлочинності, оскільки саме на рівні правозастосовної практики найбільш чітко проявляється реальна ефективність нормативно-правових рішень. Установлено, що дієвість правових норм значною мірою підтверджується їх безпосередньою реалізацією у діяльності правоохоронних органів та спеціалізованих інституцій ЄС, зокрема під час проведення спільних розслідувань, організації міжнародних операцій, а також здійснення оперативного обміну інформацією між компетентними структурами держав-членів.

Практика застосування законодавства ЄС загалом демонструє високий рівень координації між державами-членами, а також відносно ефективне функціонування інституційного механізму боротьби з кіберзлочинністю, який поєднує аналітичні, оперативні та технічні ресурси. Водночас слід зазначити, що попри досягнутий рівень інтеграції, у цій сфері все ще зберігаються окремі виклики, насамперед пов’язані з транскордонним характером кіберзлочинів, їх високою динамічністю та постійною еволюцією методів їх вчинення, що потребує подальшого вдосконалення механізмів реагування та координації на рівні ЄС.

У третьому розділі роботи досліджено правове регулювання протидії кіберзлочинності в Україні та здійснено порівняльний аналіз українського та європейського законодавства. Установлено, що в Україні сформована певна система нормативно-правових актів, спрямованих на забезпечення кібербезпеки та боротьбу з кіберзлочинністю. Основу цієї системи становлять Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», а також інші нормативні акти, що регулюють питання інформаційної безпеки [1; 9; 12].

Водночас проведений аналіз показав, що національне законодавство у сфері кібербезпеки потребує подальшого вдосконалення. Зокрема, існує необхідність у

більш чіткому визначенні складів кіберзлочинів, удосконаленні механізмів міжнародного співробітництва, а також гармонізації українського законодавства з правом Європейського Союзу.

Порівняльний аналіз законодавства України та ЄС дозволив встановити, що європейська система протидії кіберзлочинності є більш комплексною та інституційно розвиненою. У Європейському Союзі функціонує розгалужена система органів, які забезпечують координацію діяльності держав-членів у сфері кібербезпеки, тоді як в Україні відповідна інституційна система ще перебуває на етапі формування.

У зв’язку з цим одним із ключових напрямів удосконалення законодавства України має стати подальша гармонізація національних правових норм із міжнародними та європейськими стандартами у сфері кібербезпеки. Важливим є також розвиток міжнародного співробітництва у сфері розслідування кіберзлочинів, удосконалення діяльності правоохоронних органів та впровадження сучасних технологічних засобів захисту інформаційних систем.

Отже, результати проведеного дослідження свідчать про те, що ефективна протидія кіберзлочинності потребує комплексного підходу, який поєднує вдосконалення законодавства, розвиток інституційних механізмів, зміцнення міжнародного співробітництва та підвищення рівня кібербезпеки держави. Реалізація зазначених напрямів сприятиме формуванню ефективної системи захисту інформаційного простору та забезпеченню належного рівня безпеки в умовах сучасного цифрового суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативні джерела та судова практика

1. Конституція України : Закон України від 28.06.1996 р. // Верховна Рада України : [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 10.05.2026).
2. Конвенція про кіберзлочинність (Budapest Convention on Cybercrime) від 23.11.2001 р. // Council of Europe : [Веб-сайт]. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата звернення: 10.05.2026).
3. Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації актів расистського та ксенофобського характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. // Council of Europe : [Веб-сайт]. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (дата звернення: 10.05.2026).
4. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040 (дата звернення: 10.05.2026).
5. Regulation (EU) 2019/881 of the European Parliament and of the Council (Cybersecurity Act) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата звернення: 10.05.2026).
6. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата звернення: 10.05.2026).

7. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 10.05.2026).

8. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 10.05.2026).

9. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. // Верховна Рада України : [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.05.2026).

10. Закон України «Про інформацію» від 02.10.1992 р. // Верховна Рада України : [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 10.05.2026).

11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Верховна Рада України : [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 10.05.2026).

12. Кримінальний кодекс України від 05.04.2001 р. // Верховна Рада України : [Веб-сайт]. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 10.05.2026).

13. Стратегія кібербезпеки України 2021 // Президент України : [Веб-сайт]. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 10.05.2026).

14. National Cybersecurity Strategy of the European Union 2020 // European Commission : [Веб-сайт]. URL: https://digital-strategy.ec.europa.eu/en/library/eu-cybersecurity-strategy-digital-decade (дата звернення: 10.05.2026).

Наукові джерела

15. Кузьменко О. В. Кіберзлочинність: кримінально-правова характеристика. Київ : Юрінком Інтер, 2020. 320 с.

16. Баранов О. А. Інформаційне право України. Київ : Юрінком Інтер, 2019. 456 с.

17. Швець М. Я. Кібербезпека та правове забезпечення інформаційної безпеки. Київ, 2021. 287 с.

18. Литвинов О. М. Протидія кіберзлочинності: міжнародно-правові аспекти. Харків : Право, 2018. 312 с.

19. Cybercrime: The Transformation of Crime in the Information Age. Cambridge : Polity Press, 2017. 240 p.

20. Cybercrime and the Law. Boston : Northeastern University Press, 2018. 368 p.

21. Cybercrime. New York : Routledge, 2016. 184 p.

22. Cybercrime and Society. London : Sage Publications, 2018. 304 p.

23. Principles of Cybercrime. Cambridge : Cambridge University Press, 2019. 538 p.

24. Cybercrime in Asia. Springer, 2017. 295 p.

25. IT Governance and Cybersecurity. London : Kogan Page, 2020. 432 p.

26. Cybersecurity and Global Politics. London : Routledge, 2019. 210 p.

27. Cybersecurity and the European Union. London : Routledge, 2018. 278 p.

28. Robinson N. Cybersecurity Governance in the EU // European Journal of Security Research. 2021. № 6. P. 115–132.

29. The Darkening Web: The War for Cyberspace. New York : Penguin Press, 2017. 432 p.

30. Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan, 2021. 351 p.

31. Council of Europe. Convention on Cybercrime (Budapest Convention). Budapest, 2001. 45 p.

32. Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 2003. 12 p.

33. United Nations. Comprehensive Study on Cybercrime. New York : United Nations Office on Drugs and Crime, 2013. 320 p.

34. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 2013. 20 p.

35. European Commission. The EU's Cybersecurity Strategy for the Digital Decade. Brussels, 2020. 24 p.

36. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата звернення: 10.05.2026).

37. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата звернення: 10.05.2026).

38. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 10.05.2026).

39. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 10.05.2026).

40. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. Athens, 2023. 128 p.

41. Europol. Internet Organised Crime Threat Assessment (IOCTA). The Hague : Europol, 2023. 96 p.

42. Europol. European Cybercrime Centre (EC3). Annual Report. The Hague, 2022. 74 p.

43. Cybercrime: The Transformation of Crime in the Information Age. Cambridge : Polity Press, 2007. 224 p.

44. Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston : Northeastern University Press, 2012. 389 p.

45. Cybercrime and Society. London : Sage Publications, 2018. 304 p.

46. Principles of Cybercrime. Cambridge : Cambridge University Press, 2015. 520 p.

47. Broadhurst R., Grabosky P. Cybercrime: The Challenge in Asia. Hong Kong : Hong Kong University Press, 2010. 276 p.

48. Future Crimes: Everything Is Connected, Everyone Is Vulnerable. New York : Anchor Books, 2016. 464 p.

49. Brenner S., Clarke L. Distributed Security: Preventing Cybercrime // Journal of International Law. 2005. № 11. P. 45–63.

50. UNODC. Cybercrime Repository // United Nations Office on Drugs and Crime : [Веб-сайт]. URL: https://www.unodc.org/cybercrime/en/cybercrime-repository.html (дата звернення: 10.05.2026).

51. OECD. Cybersecurity Policy Framework. Paris : OECD Publishing, 2019. 98 p.

52. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Defence Manual (Tallinn Manual 2.0). Cambridge : Cambridge University Press, 2017. 638 p.

53. European Parliament. Cybersecurity and Cybercrime: Legal and Policy Framework. Brussels, 2021. 44 p.

54. INTERPOL. Global Cybercrime Strategy. Lyon, 2022. 36 p.

55. World Economic Forum. Global Cybersecurity Outlook. Geneva, 2023. 76 p.

56. Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (дата звернення: 10.05.2026).

57. Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act) // EUR-Lex : [Веб-сайт]. URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (дата звернення: 10.05.2026).