МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

СТРАТЕГІЯ ІНТЕГРАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕРБЕЗПЕКИ

Монографія

Житомир
Вид. О.О. Євенок
2024

УДК 321:004.056(061.1ЄС)
С83

Рекомендовано до друку Вченою радою
Державного університету "Житомирська політехніка"
(протокол № 4 від 19.04.2024 р.)

Автори:
Євдокимов В. В., Грицишен Д. О., Свірко С. В., Дикий А. П., Сергієнко Л. В., Кіблик Д. В., Соха С. І., Сьомак О. М., Токарчук О. Й., Умрихіна І. О., Харченко О. А., Корзун С. В., Савчук С. О., Михаленко Д. Д., Бовсунівський С. І., Здибель Р. О., Порохнавець В. В., Соха А. І.

Рецензенти:

Олег Вікторович Кравчук
доктор наук з державного управління, професор
Хмельницький науково-дослідний експертно-криміналістичний центр МВС

Тетяна Василівна Барановська
доктор юридичних наук, доцент
Державний університет "Житомирська політехніка"

С83 Стратегія інтеграції державної політики протидії кіберзлочинності в європейську систему кібербезпеки : монографія / За загальною редакцією В. В. Євдокимова, Д. О. Грицишена. – Житомир : Вид. О. О. Євенок, 2024. – 300 с.
ISBN 978-966-995-298-1

Монографія присвячена комплексному аналізу формування та реалізації державної політики протидії кіберзлочинності в Україні в контексті інтеграції до європейської системи кібербезпеки. У виданні розглядаються теоретичні основи кіберзлочинності як об'єкта державної політики, сучасний стан кіберзагроз у світі та Україні, зокрема наслідки кібервійни росії. Окрему увагу приділено зарубіжному досвіду, зокрема країн ЄС (Польща, Болгарія, Чехія, Литва) та пострадянського простору, а також механізмам модернізації правового регулювання й інституційної структури в Україні. Запропоновано практичні рекомендації щодо інтеграції української політики протидії кіберзлочинності до європейського кіберпростору з урахуванням нормативно-правові бази ЄС.

Дане монографічне дослідження може бути корисним науковцям, здобувачам вищої освіти та усім, хто цікавиться питаннями державної політики протидії кіберзлочинності та євроінтеграції.

УДК 321:004.056(061.1ЄС)

ISBN 978-966-995-298-1

ЗМІСТ

ПЕРЕДМОВА

Інформаційне суспільство визначає ключові напрями соціально-економічних відносин, державної політики, трансформації правової та політичної систем, безпеки людини та громадянина. Важливим та небезпечним елементом інформаційного суспільства є кіберзлочинність, яка проникла в усі сфери суспільної діяльності та є загрозою функціонування як окремої інституції, так і держави в цілому. Кіберзлочинність є однією із найбільших загроз сьогодення, адже формування інформаційного суспільства визначило вплив інформаційних технологій на усі сфері суспільного життя. Кіберзлочини можуть становити загрозу не лише окремій особі, а й державним інституціям та міжнародним організаціям. Кіберзлочини можуть здійснюватися в різноманітних сферах суспільного життя й, відповідно, мати різноманітні наслідки, які неможливо ідентифікувати за окремими складовими та обсягами, адже вони можуть бути різного типу: матеріальними, фінансовими, природніми, репутаційними, а також носити загальнолюдський, особистісний характер. Натомість, обсяги скоєних злочинів можуть стосуватися не лише окремого індивіда, а й чинити вплив на цілі держави, їхні об'єднання та окремі регіони.

За даними Google TAG [112], кількість кібератак на українських користувачів у 2022 р. зросла на 200 %, а на користувачів країн НАТО – майже на 300 %. У 2024 році, за даними департаменту Кіберполіції України, було знешкоджено 57 організованих груп (з них 9 – злочинні організації), до складу яких входили 254 учасники, які вчинили понад 1 тис. кіберзлочинів. Відповідно до інформації оприлюдненої Держспецзв'язком[1] у 2023 р. кількість кібератак зросла на 15,9 % та становила 2543 інциденти, серед яких 347 – на уряд та урядові

[1] Жарикова А. Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. Економічна правда. URL: https://epravda.com.ua/news/2024/01/31/709355/

організації; 276 – органи місцевого самоврядування; 175 – суб'єктів безпекового та оборонного секторів; 127 – юридичні особи. За офіційними даними European Repository of Cyber Incidents (EuRepoC)[2] Україна увійшла до п'ятірки країн, що проводили найбільше кібератак у 2022-2024 рр. (2,6 % від загальної кількості), частину з яких можна пояснити воєнними діями та потребою протидії російській агресії.

Для забезпечення високого рівня кібербезпеки України є потреба в трансформації державної політики протидії кіберзлочинності. Це особливо актуалізується в умовах євроінтеграційних процесів та потребою трансформації інформаційної безпеки відповідно до вимог ЄС.

Ключові напрямки розвитку державної кримінально-правової політики з питань протидії кіберзлочинності викладено у працях вітчизняних вчених, зокрема: Т. В. Барановської, М. О. Будакового, О. М. Будонової, В. М. Бутузова, М. М. Галамбо, Д. О. Грицишена, А. П. Дикого, М. О. Думчикова, В. В. Євдокимова, Н. А. Загребельної, І. Д. Казанчук, Р. А. Калюжного, Н. В. Камінської, І. В. Каріх, К. О. Кислої, В. В. Коваленко, Я. Ю. Кондратьєва, Б. А. Кормичема, А. В. Котелевець, О. В. Кравчука, В. О. Кучменка, Ю. Є. Максименка, К. В. Малишева, А. І. Марущака, Г. В. Новицького, Т. М. Пушкарьової, С. О. Савчука, Т. С. Ярового, Т. П. Яцик та інших. Серед зарубіжних вчених зазначені питання піднімалися у дослідженнях: Т. Ахрам, А. М. Бослер, М. Брюс, Ф. Варезе, Дж. Ванг, Д. Варзанде, Н. Ванетик, С. Гордон, М. Давидян, Ф. Дінг, Дж. Донг, А. Ерола, Р. Кашьяп, М. Кіперберг, Х. Лаллі, Я. Люстхаус, Ф. Марбук, Д. Нерс, К. Фарахбод, Н. Фейр, Б.С. Фішер, Д. Форд, Т. М. Хао, Б. Хенсон, Дж. Холт, Д. Цзян, С. Чен, К. Шайо, Л. Шепард та інших.

Вказані вчені здійснили вагомий внесок у розвиток теоретичних та методологічних положень щодо формування і реалізації державної кримінально-правової політики у сфері протидії кіберзлочинності.

[2] Присяжнюк Н. Які країни проводять найбільше політизованих кібератак у світі: Україна увійшла до п'ятірки. Liga.net. URL: https://tech.liga.net/ua/other/article/yaki-krainy-provodiat-naibilshe-polityzovanykh-kiberatak-u-sviti-ukraina-uviishla-do-piatirky

Проте, зважаючи на динамічність розвитку віртуального простору та інформаційних технології, є потреба в постійному оновленні підходів. Зокрема, в межах наукових досліджень, уваги потребує певна сукупність проблемних питань. Невирішеними на сьогодні залишаються, власне, такі аспекти, як-от: розуміння сутності та властивостей кіберзлочинності як об'єкта державної кримінально-правової політики, що вимагає дослідження ключових дефініцій, дотичних до вище вказаного поняття, а також більш детальне вивчення його класифікацій, окреслених у різних літературних джерелах. Несформованими на сьогодні залишаються методологічні положення щодо формування та реалізації досліджуваної політики з позиції зростання та модифікації кіберзлочинів в Україні та світі.

Варто наголосити, що однією з особливостей, що значно ускладнює інструментальні механізми у сфері протидії кіберзлочинності, є неможливість ідентифікації територіальної приналежності і злочинця, і самої жертви, внаслідок чого унеможливлюється реалізація державної кримінально-правової політики відокремлено від міжнародної спільноти та країн-партнерів, що додатково вимагає вивчення міжнародного досвіду. Визначальним при трансформації підходів до протидії кіберзлочинності є модернізація суб'єктної структури державного управління, адже на сьогодні відсутнє інституційне забезпечення з питань протидії кіберзлочинності, яке дозволяє комплексно вирішити означену проблему. Зважаючи на зміни в міжнародному праві щодо протидії кіберзлочинності, євроінтеграційних процесах, та модернізації кримінального законодавства, є потреба у вдосконаленні підходів щодо кримінальної відповідальності за скоєні кіберзлочини.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ СТРАТЕГІЇ ІНТЕГРАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕРБЕЗПЕКИ

1.1. Кіберзлочини як об'єкт державної політики: поняття та класифікація

Кіберзлочинність є однією із найбільших загроз сьогодення, адже формування інформаційного суспільства визначило вплив інформаційних технологій на усі сфері суспільного життя. Кіберзлочини можуть становити загрозу не лише окремій особі, а й державним інституціям та міжнародним організаціям. Варто наголосити, що однією з особливостей, що значно ускладнює інструменти протидії кіберзлочинності є неможливість ідентифікувати територіальну приналежність і самого злочинця, і жертви. Адже, «Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти та обмінюватися інформацією та ідеями по всьому світу. Щоб кіберпростір залишався відкритим, вільним та безпечним, в Інтернеті повинні застосовуватися ті самі норми, принципи та цінності, що існують в офлайн-режимі. У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Однак, поряд із позитивними аспектами цифровізації зростає і рівень кіберзлочинності, яка стає

однією з найсерйозніших загроз для безпеки держав, організацій та окремих осіб. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень – від крадіжки особистих даних і фінансових шахрайств до атак на критичні інфраструктури» [2].

Крім того, наслідки кіберзлочинності також неможливо ідентифікувати за окремими складовими та обсягом, площиною ураження, адже вони можуть бути матеріальними, фінансовими, природніми, репутаційними, і навіть у форматі людських жертв. У свою чергу, їхні обсяги можуть носити не лише індивідуальний характер, а й завдавати впливу на цілі держави, їхні об'єднання та регіони: «Сьогодні ми живемо в епоху інформаційного суспільства, коли фактично електронно-обчислювані машини та телекомунікаційні системи охоплюють усі сфери життєдіяльності: і держави в цілому, і кожного громадянина зокрема. Разом з тим запровадження глобальної діджиталізації у суспільстві сформувало певні виклики щодо можливостей зловживання інформаційними та телекомунікаційними технологіями. Наразі жертвами зловмисників, які здійснюють свою діяльність у віртуальному просторі (кіберсередовищі), можуть стати не лише окремі громадяни, але й цілі держави. При цьому безпека десятків тисяч користувачів може виявитися залежною лише від декількох зловмисників. Варто зауважити, що кількість кримінальних правопорушень у кіберпросторі зростає пропорційно кількості користувачів мережі Інтернет та кількості телекомунікаційних систем» [48]. Все це визначає складність державної кримінально-правової політики з питань протидії кіберзлочинності, відтак диктує неможливість її реалізації відокремлено від міжнародної спільноти та країн-партнерів. Важливим залишається формування інструментів протидії, що носять правовий, організаційний, соціальний, економічний, технологічний та міжнародний характер.

Питання формування та реалізації державної кримінально-правової політики щодо протидії кіберзлочинам досліджено вітчизняними вченими, серед яких: Д. С. Азаров, О. Амелін, С. В. Бєлай, П. Д. Біленчук, В. М. Бутузов, В. О. Голубєв, Д. О. Грицишен, О. П. Дзьобань, О. Ю. Довженко, І. О. Драган, І. В. Європіна, М. В. Карчевський, М. О. Кравцова, В. В. Лісовий, О. В. Махницький, А. А. Музика, В. В. Пивоваров, В. Г. Пилипчук, Б. В. Романюк, С. О. Савчук, О. Столяр, К. В. Терещенко, В. С. Цимбалюк, К. В. Юртаєва та інші. Серед зарубіжних вчених зазначене проблемне питання піднімали у своїх працях: М. Брюс, Н. Ванетик, Ф. Варезе, Д. Варзанде, С. Гордон, М. Давидян, Ф. Дінг, Дж. Донг, А. Ерола, Р. Кашьяп, М. Кіперберг, Х. Лаллі, Я. Люстхаус, Ф. Марбук, Д. Нерс, К. Фарахбод, Н. Фейр, Д. Форд, М. Хао, Д. Цзян, С. Чен, К. Шайо, Л. Шепард та інші.

На шляху забезпечення високого рівня національної безпеки в цілому та інформаційної, економічної, воєнної, як її складових зокрема, є потреба в перегляді сучасних підходів щодо формування державно-кримінальної політики з питань протидії кіберзлочинності: «Сучасний стан розвитку інформаційних систем і технологій, рівень розвитку кіберзлочинності загострили наявні та спричинили виникнення нових проблем нормативно-правової регламентації організаційно-правових заходів протидії кіберзлочинності, захисту інформаційних ресурсів, інформаційно-телекомунікаційних систем, інформаційного простору держави загалом. Стала очевидною проблема відсутності системних підходів до політики кібернетичної безпеки держави» [173]. Кіберзлочинність має особливі властивості, які не характерні будь-яким іншим видам злочинів, а їхня результативність залежить від суспільної свідомості, обізнаності та грамотності, що має бути враховані при формуванні досліджуваної державної політики.

Властивостями кіберзлочинів та кіберзлочинності, що визначають її як особливий об'єкт державної кримінально-правової політики є наступні:

– *екстериторіальність*. Так, кіберзлочинність «носить транснаціональний характер, так як кіберзлочинці в силу своєї приналежності до комп'ютерного «андеграунду» для отримання злочинних доходів та спрощення вчинення злочинних діянь на території двох і більше держав змушені, незалежно від національності, об'єднуватися в міжнародні злочинні групи» [64]. «Відсутність чітко визначених кордонів у кіберпросторі створює безліч труднощів у притягнення винних до кримінальної відповідальності, і єдине вирішення проблеми транскордонності кіберзлочинів проти власності, на нашу думку, полягає в розвитку тісного міжнародного співробітництва» [110]. Саме це характеризує кіберзлочинність як транснаціональну злочинність, що, в свою чергу, визначає специфіку підходів до системи протидії таким видам злочинності. Вітчизняна дослідниця з проблем транснаціональної злочинності І. М. Леган вказує на наступне: «Нині кіберзлочинність – одна з найбільш розповсюджених і популярних форм транснаціональної злочинності. Складні кіберзагрози створюють нові проблеми для правоохоронних органів, включно з великими обсягами даних, міжнародні розслідування і нові знання у технічній галузі. З огляду на постійну еволюцію кіберзлочинності, правоохоронним організаціям та органам необхідно ділитися інформацією та знаннями зі своїми колегами в усьому світі щодо розробки своєчасних і дієвих заходів у відповідь на проведені та реалізовані розвідувальні дії» [78]. Зазначене вказує на неможливість прив'язати скоєний кіберзлочин до певної території, окремої особистості – виконавець та замовних злочину можуть навіть не бути знайомими та перебувати на різних кінцях планети.

– *інноваційна залежність*: «із першого дня існування всесвітнього віртуального простору в нього стали проникати різні правопорушники, зокрема й злісні злочинці. З'являються нові форми і види злочинних посягань у сфері високих технологій. Злочинці все частіше застосовують системних підхід до планування своїх дій, використовують сучасні технології та спеціальні засоби, створюють нові системи конспірації» [65]. «Кіберзлочинність є явищем новітньої, цифрової доби. Саме це й робить «кіберів» набагато небезпечнішими й ефективнішими за своїх «класичних» колег – шахраїв. Це люди, які працюють головою і роблять свої «справи», не відходячи від свого комп'ютера або сидячи на лавочці з ноутбуком і мобільним телефоном. Для сучасних «технарів» це часто ідеальний спосіб заробити і реалізувати себе. Злочинці не стоять на місці. Їхні методи вдосконалюються і стають дедалі складнішими» [52]. «Кіберзлочинність в Україні має високотехнологічний характер, що викликано використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп'ютерних пристроїв, носіїв комп'ютерної інформації та інше, які виступають знаряддями і засобами вчинення кримінальних правопорушень» [92]. Це характеризує злочинців як високоінтелектуальних осіб, а інструменти скоєння злочину як високотехнологічні;

– *багатопрофільність*. Микитчик А.В. вказує на ключові риси кіберзлочинності, які характеризують її як багатопрофільну, оскільки вона: «отримала риси економічної злочинності, так як більшість кіберзлочинів відбувається в банківсько-фінансовому або корпоративному секторі (інтернет-банкінг, банківський фішинг, кібервимагання та ін.), а діяльність злочинців спрямована на вилучення доходів (прибутку); трансформується в злочинність політичного характеру, що пов'язано з активізацією протиправної

діяльності в кіберпросторі серед представників хакерського руху, спецслужб і силових структур зарубіжних держав, міжнародних екстремістських і терористичних організацій (DDoSатаки на урядові сайти, кібершпіонаж щодо інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше» [92]. Так, наслідки можуть проявлятися в: а) економічній сфері – крадіжка коштів, або інших ресурсів, зменшення прибутків, банкрутство та інше; репутаційній сфері – оприлюднення особистої інформації, або інформації, що становить комерційну чи державну таємницю, що може нашкодити репутації особі, інституції, державі чи міжнародній організації; політичній сфері – кібератаки можуть призвести до повалення політичного режиму, недійсності виборчих процесів та інше; воєнній сфері – кібервійни стали новим видом загроз для держави та її територіальної цілісності і суверенітету. Відповідно, обсяги наслідків можуть стосуватися не лише втрати певних економічних ресурсів та репутаційного капіталу особи, організації, держави, міжнародної інституції, а й людських жертв, руйнування інфраструктури, припинення та призупинка функціонування певних інфраструктурних галузей, катастроф та інше;

– *латентність*, оскільки такі злочини «мають високий ступінь латентності, яка становить від декількох десятків до декількох тисяч відсотків з різних видів злочинних діянь, що обумовлено різними об'єктивними факторами (небажання жертв комп'ютерних злочинів звертатися до правоохоронних органів, неочевидність комп'ютерних злочинів для більшості населення в силу їх вчинення у віртуальному середовищі, складність виявлення комп'ютерних злочинів за відсутності необхідної кількості фахівців в правоохоронних органах та ін.)» [92]. Латентність є

великою проблемою для правоохоронної системи, адже небажання повідомляти про скоєні в кіберпросторі злочини призводить до безкарності та збільшенню можливостей для скоєння кіберзлочинів, які матимуть більш глобальні наслідки.

– *трансформаційність*. Кіберзлочинність модифікує інструменти скоєння злочинів в різних сферах суспільного життя. «Розвиток сучасних комп'ютерних технологій привносить у життя громадян не лише нові прогресивні можливості, але й ряд небезпечних аспектів, які знаходять своє відображення у кіберзлочинності. За допомогою доступу до мережі Інтернет були модифіковані раніше відомі злочини, як-от: крадіжки, онлайн-шахрайства, вимагання, розповсюдження дитячої порнографії; згодом з'явилися й абсолютно нові, раніше не відомі види злочинів – скімінг, фішинг, кардінг, вішинг, шимінг та інші. Зважаючи на те, що кіберзлочини можуть вчинятися на території однієї держави, так і інших держав, до злочинних угруповань можуть входити представники різних національностей, перед міжнародним співтовариством постало питання боротьби з кіберзлочинністю. Характеристика кіберзлочинів як соціальних явищ передбачає їхню актуальність для усього суспільства і потребує наявності стратегії держави в усіх сферах запобігання кіберзлочинності» [85]. Так, кіберзлочин, на відміну від інших видів злочину, може мати різносторонню мету та в більшості випадків виступає інструментом скоєння іншого виду злочину, зокрема політичного, економічного, терористичного, сексуального та іншого.

Зазначене вказує на необхідність формування державної кримінально-правової політики, що характеризується наступними властивостями:

– багатовекторність – характеризує державну кримінально-правову політику як таку, що охоплює різні методи та способи протидії кіберзлочинам у різних сферах суспільного життя;

– міжсистемність – визначає потреби у формуванні державно-кримінально-правової політики щодо взаємодії між різними суб'єктами реалізації державної кримінально-правової політики різних сфер.

У контексті формування методології та реалізації державної кримінально-правової політики будемо притримуватися думки вітчизняного вченого Д. О. Грицишена, який виділяє наступні етапи щодо реалізації державної політики у сфері протидії економічній злочинності, зміст якої можна адаптувати до державної кримінально-правової політики з питань протидії кіберзлочинності:

– ідентифікація та виявлення ключових проблем у суспільному житті щодо економічної злочинності та їхнього впливу на національну безпеку;

– визначення стейкхолдерів та ідентифікація їхніх інтересів щодо запобігання та протидії економічній злочинності;

– обґрунтування змісту кримінальної політики як системи та як процесу запобігання та протидії економічній злочинності;

– формування об'єктно-предметного поля державної кримінальної політики у сфері запобігання та протидії економічній злочинності;

– визначення мети та завдань державної кримінальної політики у сфері запобігання та протидії економічній злочинності;

– обґрунтування напрямів формування та реалізації державної кримінальної політики в сфері запобігання та протидії економічній злочинності;

– визначення суб'єктів формування та реалізації державної кримінальної політики в сфері запобігання та протидії економічній злочинності;

– визначення об'єктів державної кримінальної політики в сфері запобігання та протидії економічній злочинності;

– встановлення взаємозв'язків із іншими видами державної політики у сфері запобігання та протидії економічній злочинності;

– обґрунтування методів та принципів державної кримінальної політики у сфері запобігання та протидії економічній злочинності;

– встановлення механізмів державної кримінальної політики у сфері запобігання та протидії економічній злочинності [30].

Змістове наповнення зазначених етапів щодо формування та реалізації державної кримінально-правової політики з питань протидії кіберзлочинності представлено в табл. 1.1.

Розроблена методологія формування та реалізації державної кримінально-правової політики ґрунтується на визначених властивостях кіберзлочинності та тенденціях розвитку інформаційного суспільства та активізації діяльності людини та окремих інституцій у віртуальному просторі. Важливою складовою є визначення змісту проблеми, яку має вирішити державна політика. У цьому контексті означене проблемне питання пропонуємо розглядати як своєрідні: «динамічні тенденції розвитку інформаційного суспільства та активізація діяльності людини у віртуальному просторі, що зумовлює зростання кіберзлочинності, що становить загрозу національній безпеці та впливає на рівень глобальної безпеки».

Таблиця 1.1

Методологічні положення формування та реалізації державної кримінально-правової політики з питань протидії кіберзлочинності

<table>
<tr><td colspan="4">1. СУСПІЛЬНА ПРОБЛЕМ КІБЕРЗЛОЧИННОСТІ ЯК ОБ'ЄКТУ ДЕРЖАВНОЇ ПОЛІТИКИ</td></tr>
<tr><td colspan="4">ЗМІСТ ПРОБЛЕМИ
– динамічні тенденції розвитку інформаційного суспільства та активізація діяльності людини у віртуальному просторі, що зумовлює зростання кіберзлочинності, що становить загрозу національній безпеці та впливає на рівень глобальної безпеки</td></tr>
<tr><td colspan="4">ОЗНАКИ ПРОБЛЕМИ:</td></tr>
<tr><td colspan="4">що характеризують детермінантами розвитку кіберзлочинності</td></tr>
<tr><td>Геополітичні</td><td>Внутрішньополітичні</td><td>Економічні</td><td>Соціальні</td></tr>
<tr><td>Правові</td><td>Державно-управлінські</td><td>Технологічні</td><td>Віктимологічні</td></tr>
<tr><td colspan="4">що характеризують системні проблеми державної політики</td></tr>
<tr><td>– низька ефективність правоохоронної системи</td><td colspan="2">– невідповідність суб'єктної структури державного управління</td><td>– відсутність механізмів адаптації до міжнародної системи протидії</td></tr>
<tr><td colspan="4">наслідки, визначають вплив на рівень складових національної безпеки:</td></tr>
<tr><td>– інформаційна</td><td colspan="2">– економічна</td><td>– енергетична</td><td>– продовольча</td></tr>
<tr><td>– соціальна</td><td colspan="2">– воєнна</td><td>– екологічна</td><td>– політична</td></tr>
<tr><td colspan="4">2. СТЕЙКХОЛДЕРИ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</td></tr>
<tr><td colspan="4">виплаває на носіїв інтересів:</td></tr>
<tr><td>Публічних інтересів</td><td colspan="2">Суспільних інтересів</td><td>Приватних інтересів</td></tr>
<tr><td colspan="4">3. ВИХІДНІ ПОЛОЖЕННЯ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</td></tr>
<tr><td>Зміст державної кримінально-правової політики протидії кіберзлочинності</td><td colspan="3">– як процес: сукупність послідовних процесів організаційно-методологічного характеру, які полягають у розробці, формуванні, верифікації та реалізації та оцінки державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів у відповідності із визначеними принципами, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності її наслідкам;
– як система: система взаємодії суб'єктів законодавством, виконавчої та судової влади щодо формування та реалізації державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів, відповідно до визначених принципів, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності, зокрема її наслідкам</td></tr>
</table>

Продовження табл. 1.1

<table>
<tr><td colspan="4">Об’єктно-предметне поле державної кримінально-правової політики протидії кіберзлочинності</td></tr>
<tr><td colspan="2">Об’єкт державної політики</td><td colspan="2">Предмет державної політики</td></tr>
<tr><td colspan="2">– діяльність суспільних інститутів на різних рівням соціально-економічної системи, що реалізується у віртуальному просторі або з використанням інформаційно-комп’ютерних технологій із порушенням встановлених національним або міжнародним законодавством параметрів через кібернетичну злочинність та становлять загрозу національній безпеці держави в цілому та її окремим складовим зокрема</td><td colspan="2">– сукупність організаційно-методологічних положень правового, організаційного, інформаційного та економічного характеру щодо протидії кіберзлочинності, що полягає в порушенні встановлених національним або міжнародним законодавством параметрів діяльності суспільних інститутів, що реалізується у віртуальному просторі або з використанням інформаційно-комп’ютерних технологій</td></tr>
<tr><td colspan="4">Мета та завдання державної кримінально-правової політики протидії кіберзлочинності</td></tr>
<tr><td>Мета</td><td colspan="3">– розробка, формування, верифікація та впровадження державно-управлінських рішень та механізмів їх реалізації щодо протидії кіберзлочинності для забезпечення відповідного рівня національної безпеки в цілому та її складових зокрема</td></tr>
<tr><td colspan="4">Завдання</td></tr>
<tr><td>1. Модернізація суб’єктної структури системи державного управління в сфері протидії кіберзлочинності</td><td>2. Налагодження інформаційно-комунікаційної системи між суб’єктами реалізації державної кримінально-правової політики</td><td>3. Адаптація вітчизняного законодавства в сфері кіберзахисту та протидії кіберзлочинності до вимог ЄС</td><td>4. Налагодження інформаційно-комунікаційної системи з правоохоронними органами зарубіжних країн</td></tr>
<tr><td>5. Налагодження інформаційно-комунікаційної системи з міжнародними урядовими та неурядовими організаціями</td><td>6. Налагодження інформаційно-комунікаційної системи з міжнародними поліцейськими організаціями</td><td>7. Реформування кримінального законодавства щодо встановлення відповідальності та протидії кіберзлочинам</td><td>8. Розробка та реалізація превентивних заходів щодо протидії кіберзлочинності серед населення</td></tr>
<tr><td>9. Розробка заходів із забезпечення інформаційної та іншої видів безпеки суб’єктів реалізації державної політики</td><td>10. Ратифікація міжнародних нормативно-правових актів щодо протидії кіберзлочинності та забезпечення кіберзахисту</td><td>11. Оптимізація фінансового забезпечення суб’єктів реалізації державної кримінально-правової полі-тики протидії кіберзлочинності</td><td>12. Підвищення рівня кадрового потенціалу правоохоронної системи щодо протидії кіберзлочинності</td></tr>
<tr><td colspan="4">4. НАПРЯМИ РОЗВИТКУ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ</td></tr>
<tr><td colspan="2">– реформування кримінального законодавства щодо протидії кіберзлочинності</td><td>– трансформація суб’єктної структури системи державного управління в сфері протидії кіберзлочинності</td><td>– розширення міжнародно-правового механізму реалізації державної кримінально-правової політики</td></tr>
</table>

Продовження табл. 1.1

5. ОБ'ЄКТИ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ			
– регулювання суспільних відносин щодо використання інформаційно-комп'ютерних технологій	– регулювання діяльності суспільних інституцій в віртуальному просторі	– функціонування правоохоронної системи (діяльність правоохоронних органів) щодо протидії кіберзлочинності	– міжнародні відносини щодо протидії кіберзлочинам та забезпечення інформаційної безпеки держави
6. СУБ'ЄКТИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
Центральні органи виконавчої влади, що реалізують державну кримінально-правову політику протидії кіберзлочинності		*Суб'єкти правоохоронної діяльності на які покладаються функції з протидії кіберзлочинності*	
Міністерство цифрової трансформації України	Міністерство внутрішніх справ України	*прямо пов'язані із протидією кіберзлочинності*	
		Служба безпеки України	Національна поліція України
Міністерство закордонних справ	Міністерство оборони України		
Міністерство юстиції України	Міністерство фінансів України	Державне бюро розслідувань	
Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів		Адміністрація Державної служби спеціального зв'язку та захисту інформації України	
		опосередковано пов'язані із протидією кіберзлочинності	
Національне агентство з питань запобігання корупції	Державна служба фінансового моніторингу України	Національне антикорупційне бюро України	Бюро економічної безпеки України
7. ВЗАЄМОЗВ'ЯЗКИ ІНШИМИ ВИДАМИ ДЕРЖАВНОЇ ПОЛІТИКИ			
– політика в сфері правоохоронної діяльності	– політика в сфері митної діяльності	– політика в сфері охорони державного кордону	– інноваційна політика
– економічна політика	– інформаційна політика	– оборонна політика	– фінансова політика
– антикорупційна політика	– монетарна політика	– антитерористична політика	– зовнішня політика
8. МЕТОДОЛОГІЯ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
Методи прямого впливу		*Методи непрямого впливу*	
– укази	– постанови	– соціально-психологічні	– інформаційні
– рішення	– розпоряджень	– стимулюючі	– профілактичні
Принципи			
– обґрунтованості	– аналітичності	– системності	– прозорості	– ефективності
– комплексності	– послідовності	– аполітичності	– правомочності	– гуманізму
9. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
– кримінально-правовий	– міжнародно-правовий	– фінансово-економічний	– організаційний

Ця проблема характеризується сукупністю ознак, які пропонуємо згрупувати наступним чином:

– ті ознаки, які характеризуються детермінантами розвитку кіберзлочинності;

– ті ознаки, яким властивий системний погляд на проблеми державної політики.

У наукові літературі, яка досліджує питання розвитку державної кримінально-правової політики щодо протидії кіберзлочинності досить часто дослідники визначають саме ті фактори, які призводять до поширення та розвитку явища кіберзлочинності. Комплексне бачення, що визначає правові і кримінологічні, економічні, політичні, державно-управлінські аспекти детермінант розвитку кіберзлочинності представлено у дослідженні Б. Головкіна [25]. Погоджуємося із результатами вказаного дослідження та вважаємо, що такий підхід має стати підґрунтям у розробці методології формування та реалізації державної кримінально-правової політики з питань протидії кіберзлочинам (табл. 1.2).

Щодо системних проблем розвитку державної кримінально-правової політики, то в більші мірі вони стосуються власне правоохоронної системи. З цього приводу у науковій літературі існують різні точки зору.

Никончук Н. С., Маслова О. О. визначають наступні ознаки, або ж симптоми проблеми, що є загрозою поширення кіберзлочинності:

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

Таблиця 1.2

Характеристика детермінант запобігання кіберзлочинності, за Б. Головкіним [25]

ПОЛІТИЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ	
зовнішньополітичні або геополітичні	
розгортання в кіберпросторі шкідливого програмного забезпечення та проведення широкомасштабних кампаній з викрадення у політичних, економічних або військових цілях чутливої інформації	мілітаризація кіберпростору, використання його для проведення розвідувальної, терористичної, диверсійної та іншої підривної діяльності
недостатній рівень кібернетичної стійкості мереж, інформаційних систем та об'єктів критичної інфраструктури	недотримання організаціями державного і приватного сектору різних держав міжнародних норм і стандартів кібербезпеки
декларативність політики та недостатність координації превентивних заходів	перетворення кіберпростору на середовище геополітичного суперництва за технологічне домінування у цифровому світі
нестабільність кіберпростору, постійне збільшення кількості та зміна характеру глобальних викликів і загроз для сталого функціонування національної інформаційної інфраструктури	фінансування та використання в геополітичних інтересах спеціальними службами і розвідувальними органами держав, що претендують на домінування у кіберпросторі
широкі можливості для проведення у кіберпросторі глобальних дезінформаційних компаній	
Внутрішньополітичні	
нерозвинений механізм комунікацій у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю, спрямованої на поширення достовірної інформації	непідкріплення політичної волі вищого керівництва держави щодо сталого розвитку інформаційного суспільства та створення безпечного комунікативного середовища
недостатній рівень гармонізації міжнародних стандартів кібербезпеки із законодавством України	незавершеність реформування системи захисту інформації з обмеженим доступом
недоліки в організації та проведення просвітницької роботи серед населення з питань безпечної поведінки у кіберпросторі	недоліки концепції державної політики у сфері забезпечення кібербезпеки та протидії кіберзлочинності
неефективна система підготовки кваліфікованих фахівців з кібербезпеки	нерозвинена міжнародна співпраця з ключовими іноземними партнерами

Продовження табл. 1.2

ЕКОНОМІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
недостатній обсяг державного фінансування цифрового сектору, у тому числі заходів з кібербезпеки	функціонування аутсорсингової моделі організованого злочинного бізнесу в кіберпросторі	низький внутрішній попит на високотехнологічні програмні продукти, технічні рішення і проривні технології
велика пропозиція в темній мережі, закритих групах зловмисного програмного забезпечення	розвинений у темній мережі кіберпростору незаконний обіг цифрових технологій, продуктів та послуг	інтенсивні темпи цифровізації фінансового сектору економіки і перехід на електронні платіжні системи
широкі можливості здійснення конфіденційних платежів, приховування коштів та легалізації доходів, одержаних від кіберзлочинів	інноваційна відсталість економіки та її низька конкурентоспроможність, експортна орієнтованість інформаційно-комунікаційних технологій	
заощадження витрат державними і приватними структурами на купівлі та експлуатації комп'ютерної техніки й обладнання	високий комерційний попит серед користувачів на зловмисне програмне забезпечення, кримінальні послуги операторів таких продуктів і хакерів	функціонування в національному сегменті мережі Інтернет незаконного обігу контрафактного програмного забезпечення
відсутність конкурентного ринку телекомунікаційних послуг	низькозатратність, малоризикованість та високодохідність кіберзлочинної діяльності	збільшення обсягів трудової зайнятості в IT-секторі
СОЦІАЛЬНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
психологічна залежність значної частини суспільства від використання мобільних пристроїв, застосунків, соціальних мереж	функціонування у кіберпросторі великої кількості закритих соціальних груп криміногенної спрямованості	зловживання користувачами у кіберпросторі цифровими правами та свободами у протиправних цілях
використання технологій соціальної інженерії для зміни способу мислення і характеру поведінки людей та їхніх об'єднань у кіберпросторі	зумовлені цифровізацією держави і суспільства зміни соціальної поведінки, що виражаються у переході на віртуальну модель комунікацій замість фізичної взаємодії	деформації моральної і правової свідомості користувачів під цілеспрямованим інформаційно-психологічним деструктивним впливом
зростання аудиторії користувачів та збільшення часу перебування у кіберпросторі	розмивання меж між реальним і віртуальним життям, що створює ілюзію безпеки	низький рівень цифрової грамотності користувачів Інтернету, Е-сервісів

Продовження табл. 1.2

НОРМАТИВНО-ПРАВОВІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
несформованість цілісної нормативно-правової бази у сфері забезпечення кібербезпеки і боротьби з кіберзлочинністю	нормативна неврегульованість питань щодо електронних комунікацій, використання штучного інтелекту, Інтернету речей	повільні темпи наближення національного законодавства у сфері захисту персональних даних до законодавства ЄС
неврегульованість в Законі України «Про телекомунікації» порядку взаємодії між суб'єктами забезпечення кібербезпеки та операторами, провайдерами телекомунікацій	недосконаліть нормативно-правової бази у сфері електронних довірчих послуг, зумовлена неповною імплементацією Регламенту ЄС 910/214	недостатній рівень гармонізації національного законодавства про критичну інфраструктуру та її захист із нормами Директиви (ЄС)
низька ефективність захисту прав громадян та суб'єктів господарювання у кіберпросторі, зумовлена неповною імплементацією в національне законодавство Директиви 2002/58/ЄС	неврегульованість на законодавчому рівні питання запровадження ризик-орієнтованого підходу та механізму його реалізації в систему забезпечення кібербезпеки	нечітка правова регламентація форм і механізму участі операторів, провайдерів телекомунікаційних послуг та інших суб'єктів приватного сектору
недосконалий організаційно-правовий механізм державно-приватної взаємодії у сфері забезпечення кібербезпеки	неповна імплементація Конвенції про кіберзлочинність у КК України	
ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ		
організаційна незавершеність архітектури національної системи забезпечення кібербезпеки	недостатня інституційна спроможність суб'єктів протидії кіберзлочинності	
недостатнє для розвитку національної системи кіберзахисту і протидії кіберзагрозам державне фінансування	низький рівень підготовки і підвищення кваліфікації фахівців з інформаційної і кібернетичної безпеки	
недостатній рівень технічної захищеності державних інформаційних ресурсів	недостатньо розвинена міжнародна співпраця з питань кібербезпеки	
відсутність у значної частини державних органів, органів місцевого самоврядування, суб'єктів господарювання, віднесених до об'єктів критичної інфраструктури	нерозробленість механізму громадського контролю за законністю та ефективністю діяльності суб'єктів забезпечення кібербезпеки	
відсутність загальнодержавної програми цифрової грамотності населення	нездійснення аудиту стану кібербезпеки	

Продовження табл. 1.2

ТЕХНОЛОГІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ	
висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій	забюрократизованість порядку сертифікації й експертизи Комплексної системи захисту інформації
можливість проникати в локальні мережі підприємств, організацій, установ шляхом підключення за протоколом віддаленого робочого столу	порушення загальних вимог до кіберзахисту об'єктів критичної інфраструктури власниками або керівниками
використання застарілого антивірусного програмного забезпечення, ненадійних паролів, невпровадження інноваційних технологічних рішень	недотримання суб'єктами господарювання, які працюють на ринку ЄС, вимог Регламенту щодо захисту персональних даних
технологічна застарілість і неефективність програмно-апаратних засобів криптографічного і технічного захисту інформації з обмеженим доступом	відсутність у багатьох власників і користувачів державних інформаційних ресурсів служби захисту інформації та системних адміністраторів
використання неліцензованого і несертифікованого програмного забезпечення	технологічна і технічна відсталість цифрової інфраструктури України
використання у системах реєстрації та контролю доступу до інформаційних систем технологічно несумісних механізмів, алгоритмів та протоколів електронної ідентифікації та впізнання	ненадійна система кіберзахисту інформації з обмеженим доступом в юридичних осіб державної і приватної форми власності
незахищеність каналів зв'язку, електронної пошти, телекомунікаційних мереж, серверів і баз даних	відсутність Єдиного реєстру оцінки ризиків і загроз на різних рівнях і об'єктах кіберзахисту
відсутність безпечного DNS-сервера	відсутність захищеного обміну ідентифікаційними даними
ВІКТИМОЛОГІЧНІ ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ	
інтенсивний розвиток електронних послуг, зумовлений переходом на віддалений режим роботи під час світової пандемії	збільшення в рази кількості пристроїв підключених до глобальної мережі Інтернет та інших локальних мереж
високі ризики віктимізації державних службовців, які не дотримуються основ кібергігієни	заняття нелегальною електронною комерцією, а також надання нелегальних платних послуг користувачам мережі Інтернет
створення і самопоширення неповнолітніми компрометуючих матеріалів інтимного характеру та особистих даних у кіберпростір	відвідування маловідомих сайтів і веб-сторінок інтернет-магазинів, переходи на вкладки спливаючої реклами
професійна віктимність окремих категорій користувачів, які надають послуги та здійснюють господарську діяльність у кіберпросторі	нерозбірливі знайомства в Інтернеті, вступ до різних груп, відверте спілкування
надмірна довірливість при використанні послуг Інтернет-банкінгу	економія витрат на системах програмного і технічного захисту інформації

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації усіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту» [97].

Головкін Б. вказує на наступні «симптоми» проблеми державної кримінально-правової політики щодо протидії кіберзлочинам, які визначаються станом функціонування правоохоронної системи:

– невизначеність державної політики щодо боротьби із кіберзлочинністю, нерозробленість концепції запобігання і протидії кіберзлочинності, відсутність загальнодержавних та регіональних

програм із протидії кіберзлочинності, несформованість стратегічних пріоритетів та відповідного їм комплексу заходів із запобігання найбільш поширеним видам кіберзлочинів;

– недостатня спроможність суб'єктів боротьби з кіберзлочинністю задля ефективного здійснення кроків щодо запобігання і протидії кіберзлочинам (недостатньо сил, засобів, матеріально-технічних ресурсів, кадрового потенціалу, бюджетного фінансування);

– відсутність центрального органу, відповідального за боротьбу з кіберзлочинністю в Україні, який здійснював би координацію діяльності усіх суб'єктів на загальнодержавному рівні, забезпечував би міжвідомчу взаємодію та міжнародну співпрацю;

– брак кіберекспертів, оперативних працівників, слідчих, прокурорів, що спеціалізуються на запобіганні, виявленні, розслідуванні, припиненні кіберзлочинів;

– недостатня забезпеченість правоохоронних органів спеціальними технічними засобами виявлення та реагування на кіберпосягання, що містять ознаки кіберзлочинів» [25].

Колектив авторів монографічного дослідження, за редакцією Д. О. Грицишена та В. В. Євдокимова, зазначає ключові системні проблеми, зокрема:

– заполітизованість правоохоронної системи держави, що у результаті призводить до низького рівня управління її функціональними та операційними процесами;

– низький рівень інформованості суспільства про реформування правоохоронної системи;

– відсутність комунікації між правоохоронними органами;

– мінливість правового механізму щодо політичних сил, що, як наслідок, призводить до значних змін у законодавстві та прийнятті недосконалих початкових законів;

– відсутність комплексності у реформуванні;

– відсутність комунікації між центральними органами виконавчої влади, що реалізують політику у різних сферах суспільного життя, які є суміжними до правоохоронної системи;

– недосконаліть структури правоохоронної системи;

– проблема фінансового забезпечення правоохоронної системи [69].

Підсумовуючи вище зазначене, вбачаємо необхідність у групуванні системних «симптомів» проблеми державної кримінально-правової політики протидії кіберзлочинності:

– низька ефективність правоохоронної системи, що визначається недостанім фінансуванням, низьким рівнем кадрового потенціалу, недосконалою матеріально-технічною базою, прогалинами у правовому забезпеченні у контексті реалізації положень кримінального законодавства щодо протидії кіберзлочинності, відсутністю комунікації між різними учасниками реалізації державної політики;

– невідповідність суб'єктної структури державного управління, адже питання кібербезпеки та протидії кіберзлочинам наявне в системі Національної поліції, яка має обмеженні функції;

– відсутність механізмів адаптації щодо міжнародної системи протидії; зокрема на сьогодні законодавство України у сфері протидії кіберзлочинності має бути гармонізованим із директивами Європейського союзу, а також є необхідність повної ратифікації міжнародних нормативно-правових актів та налагодження тісної співпраці не лише з правоохоронними органами зарубіжних країн, а й міжнародними поліцейськими організаціями.

Ефективність реалізації державної кримінально-правової політики з питань протидії кіберзлочинності залежить від якості врегулювання публічних, приватних та суспільних інтересів: «Право опиняється в епіцентрі проблеми інтересів у плані їх виявлення, нормативного закріплення та захисту. Складні суспільні явища, що підлягають регулюванню правом, постають поєднанням різних

інтересів – економічних, соціальних, політичних, тощо. Інтенсивний розвиток і диференціація соціальних інтересів висунули в розряд першочергових завдання адекватного правового їх вираження, забезпечення та захисту від посягань. Успішне виконання правом його функцій соціального регулювальника та засобу організації суспільного життя можливе лише при правильному поєднанні юридичних механізмів із соціальними інтересами людей, оскільки будь-яка норма права, так чи інакше, пов'язана із конкретним інтересом» [170].

Вперше питання вивчення правоохоронної системи як системи реалізації державної кримінально-правової політики протидії злочинності у контексті врегулювання інтересів було представлено у дослідженні К. В. Малишева [86], зокрема автор вивчає правоохоронну систему на перетині приватних публічних та суспільних інтересів:

– «правоохоронна система, як система забезпечення дотримання інтересів учасників суспільних відносин. Основною метою правоохоронної системи є забезпечення дотримання інтересів учасників суспільних відносин;

– правоохоронна система, як складова сукупності інтересів учасників суспільної взаємодії. При формуванні та реалізації державної політики у сфері трансформації правоохоронної системи різні суспільні групи намагаються сформувати власний інтерес до її розвитку. Відповідно, кожен механізм має бути спрямований на подолання конфлікту інтересів;

– правоохоронна система як інструмент порушення інтересів учасників суспільних відносин у контексті професійної діяльності. Під час виконання професійних завдань у правоохоронній діяльності, в окремих випадках, для забезпечення національних та публічних інтересів, суб'єкти правоохоронної системи можуть нехтувати приватними інтересами» [86].

Вбачаємо, що врегулювання інтересів стейкхолдерів має відбуватися наступним чином:

– по-перше, при формуванні державної кримінально-правової політики протидії кіберзлочинності, зокрема на етапі визначення її мети, завдань та цілей;

– по-друге, при реалізації державної кримінально-правової політики протидії кіберзлочинності. Це стосується вивчення впливу механізмів реалізації державної політики на різних учасників суспільних відносин;

– по-третє, державна політика має сформувати таку сукупність інструментів, щоб врегулювати інтереси, а також захистити їх в інформаційному суспільстві та віртуальному просторі.

Представлені вихідні положення з державної кримінально-правової політики протидії кіберзлочинності визначають два підходи до змісту, зокрема:

– як процес: сукупність послідовних кроків організаційно-методологічного характеру, які полягають у розробці, формуванні, верифікації, реалізації та оцінці державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів, відповідно до визначених принципів, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності та її наслідків;

– як система: взаємодія суб'єктів законодавства, а також виконавчої та судової влади щодо формування та реалізації державно-управлінських рішень, що передбачають застосування сукупності інструментів та методів, відповідно до визначених принципів, що є складовими правового, організаційного, інформаційного та економічного механізмів протидії кіберзлочинності та її наслідків.

У цьому контексті визначено зміст об'єкта, предмета та мети досліджуваної політики. Об'єктом державної політики є діяльність суспільних інститутів на різних рівнях соціально-економічної системи, що реалізується у віртуальному просторі або з використанням інформаційно-комп'ютерних технологій із порушенням встановлених національним або міжнародним законодавством параметрів через

кібернетичну злочинність та становлять загрозу національній безпеці держави в цілому та її окремим складовим зокрема. Під предметом запропоновано розуміти сукупність організаційно-методологічних положень правового, організаційного, інформаційного та економічного характеру щодо протидії кіберзлочинності, що полягає у порушенні встановлених національним або міжнародним законодавством параметрів діяльності суспільних інститутів, зміст яких реалізується у віртуальному просторі або з використанням інформаційно-комп'ютерних технологій. Мета полягає у розробці, формуванні, верифікації та впровадженні державно-управлінських рішень та механізмів їхньої реалізації щодо протидії кіберзлочинності для забезпечення відповідного рівня національної безпеки в цілому та її складових зокрема. Відповідно до об'єктно-предметного поля та визначеної мети, а також зважаючи на складові проблеми, пропонуємо виділити наступні завдання щодо розвитку державної кримінально-правової політики:

– модернізація суб'єктної структури системи державного управління у сфері протидії кіберзлочинності;

– налагодження інформаційно-комунікаційної системи між суб'єктами реалізації державної кримінально-правової політики;

– адаптація вітчизняного законодавства у сфері кіберзахисту та протидії кіберзлочинності до вимог ЄС;

– налагодження інформаційно-комунікаційної системи з правоохоронними органами зарубіжних країн;

– налагодження інформаційно-комунікаційної системи з міжнародними урядовими та неурядовими організаціями;

– налагодження інформаційно-комунікаційної системи з міжнародними поліцейськими організаціями;

– реформування кримінального законодавства щодо встановлення відповідальності та протидії кіберзлочинам;

– розробка та реалізація превентивних заходів щодо протидії кіберзлочинності серед населення;

– розробка заходів із забезпечення інформаційної та іншої видів безпеки суб'єктів реалізації державної політики;

– ратифікація міжнародних нормативно-правових актів щодо протидії кіберзлочинності та забезпечення кіберзахисту;

– оптимізація фінансового забезпечення суб'єктів реалізації державної кримінально-правової політики протидії кіберзлочинності;

– підвищення рівня кадрового потенціалу правоохоронної системи щодо протидії кіберзлочинності.

Зазначені завдання характеризують такі напрямки розвитку державної політики, як: реформування кримінального законодавства щодо протидії кіберзлочинності; трансформація суб'єктної структури системи державного управління у сфері протидії кіберзлочинності; розширення міжнародно-правового механізму реалізації державної кримінально-правової політики. Відповідно, визначено наступні об'єкти державної політики: регулювання суспільних відносин щодо використання інформаційно-комп'ютерних технологій; регулювання діяльності суспільних інституцій у віртуальному просторі; функціонування правоохоронної системи (діяльність правоохоронних органів) щодо протидії кіберзлочинності; міжнародні відносини щодо протидії кіберзлочинам та забезпечення інформаційної безпеки держави.

Сучасна суб'єктна структура державного управління у сфері протидії кіберзлочинам, представлена: 1) центральними органами виконавчої влади, що реалізують державну кримінально-правову політику з питань протидії кіберзлочинності (Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Міністерство оборони України, Міністерство юстиції України, Міністерство фінансів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших видів злочинів, Національне агентство з питань запобігання корупції, Державна

служба фінансового моніторингу України); 2) суб'єкти правоохоронної діяльності, на які покладаються функції з протидії кіберзлочинності, що прямо пов'язані із протидією кіберзлочинності (Служба безпеки України, Національна поліція України, Державне бюро розслідувань, Служба зовнішньої розвідки України); 2) суб'єкти правоохоронної діяльності, на які покладаються функції з протидії кіберзлочинності, що опосередковано пов'язані із протидією кіберзлочинності (Національне антикорупційне бюро України, Бюро економічної безпеки України, Державна прикордонна служба України, Національна гвардія України, Державна митна служба України, Управління державної охорони України). Така суб'єктна структура визначає взаємодію із різними видами державної політики.

Методологія реалізації державно-кримінальної політики ґрунтується на методах прямого (укази, постанови, рішення, розпорядження) та непрямого впливу (соціально-психологічні, інформаційні, стимулюючі, профілактичні), а також принципах (обґрунтованості, аналітичності, системності, прозорості, ефективності, комплексності, послідовності, аполітичності, правомочності, гуманізму).

Таким чином, проведене дослідження дозволило розробити комплексну теоретико-методологічну конструкцію державної кримінально-правової політики, що складається з наступних послідовних етапів: 1) визначення суспільної проблеми та її ключових ознак, які згруповано за детермінантами розвитку кіберзлочинності, системними проблемами правоохоронної діяльності та за механізмом впливу кіберзлочинності на складові національної безпеки); 2) ідентифікація стейкхолдерів, здійснена на основі обґрунтування впливу на носіїв публічних, приватних та суспільних інтересів; 3) вихідні положення державної кримінально-правової політики з питань протидії кіберзлочинності; 4) визначення напрямів розвитку державної політики (реформування кримінального законодавства щодо протидії кіберзлочинності; трансформація суб'єктної структури

системи державного управління у сфері протидії кіберзлочинності; розширення міжнародно-правового механізму реалізації державної кримінально-правової політики); 5) визначення об'єктів державної політики; 6) обґрунтування суб'єктного складу; 7) визначення методів та принципів реалізації державної політики із наданням пропозиції щодо ключових механізмів її реалізації.

1.2. Сучасний стан наукових досліджень з проблем державної політики протидії кіберзлочинності

У сучасному світі кібербезпека та боротьба із кіберзлочинністю стають ключовими пріоритетами і для держави, і для приватного сектору. Із розвитком цифрових технологій зростає кількість кіберзагроз, що вимагає не лише вирішення питань технічного характеру, а й передбачає здійснення глибокого наукового аналізу. У цьому контексті важливим інструментом виступає бібліометричний аналіз.

Бібліометричний аналіз дозволяє систематизувати наукові знання у сфері кібербезпеки, визначити основні напрями досліджень, виокремити авторів, які найбільш активно порушували окреслену тему, означити провідні установи та виокремити ключові тенденції щодо подальшого розвитку означеної галузі. Завдяки цьому методу, можна швидко оцінити, які аспекти кіберзлочинності досліджуються найінтенсивніше, а які залишаються поза увагою. Це допомагає сформулювати актуальні теми для подальших досліджень. Крім того, бібліометричний аналіз є корисним для розробки ефективної державної політики в галузі безпеки. Він дозволяє виявити науково-обґрунтовані підходи щодо проблеми боротьби з кіберзлочинністю, сприяє орієнтації на міжнародний досвід та дає змогу адаптувати кращі практики. Використання бібліометричного методу сприяє більш

глибокому розумінню проблеми цифрової безпеки та покращує рівень захисту інформаційного простору.

Бібліометричний аналіз будемо проводити у рамках даних наукометричних баз даних, як-от: Scopus та Web of Science. Це дві найбільш авторитетні світові платформи з пошуку наукової інформації, де доволі чисельно представлено пошуковий запит терміну «cybercrime» (кіберзлочинність). Ми проаналізуємо кількість публікацій за роками, визначимо, які аспекти кіберзлочинності (наприклад, фінансове шахрайство, хакерство, кібертероризм тощо) є найбільш вивченими, а також дослідимо співпрацю між авторами та відповідними установами. Окрему увагу буде приділено аналізу найбільш цитованих публікацій, що дозволить виявити наукові роботи, які справили найбільший вплив на окреслення означеної проблеми.

Загалом у базі даних Scopus нараховується 6648 документів, що містять термін «cybercrime», натомість у базі Web of Science – 4567 наукових робіт. Ці цифри свідчать про активну наукову зацікавленість проблемою кіберзлочинності.

Графік відображає динаміку зростання кількості наукових публікацій, присвячених темі «cybercrime» у базах даних Scopus та Web of Science у період з 1999 по 2025 рік. До 2010 року наукова активність у цій галузі залишалася незначною, однак, починаючи з 2011 року, спостерігається стабільне зростання кількості публікацій в обох базах, що свідчить про посилення інтересу науковців до проблем кіберзлочинності. Особливо стрімке зростання кількості публікацій спостерігається з 2015 року, що збігається зі збільшенням глобальних кіберзагроз та активізацією цифрової трансформації суспільства. Найвищий пік публікацій у Scopus фіксується у 2023 році – майже 1000 документів. У базі Web of Science кількість публікацій зростала більш поступово і досягла свого піку у 2021–2023 роках, коли щорічно фіксувалося у публікаційному полі понад 400 робіт.

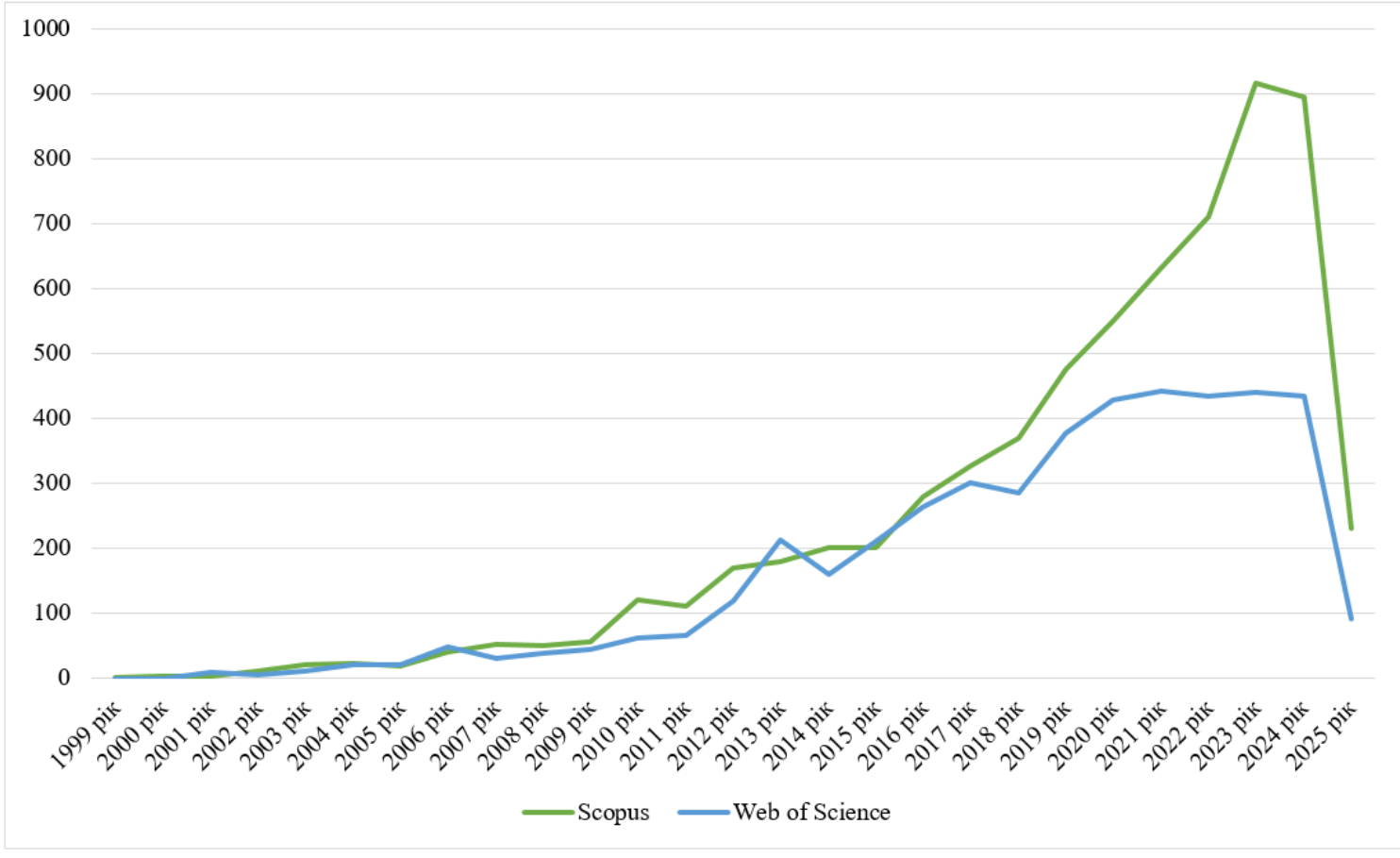

Рис. 1.1. Динаміка кількості публікацій за пошуковим запитом «cybercrime» у БД Scopus та Web of Science

У базі даних (далі по тексту – БД) Scopus у 1999 році було опубліковано дві роботи, які були присвячені дослідженню кіберзлочинності. Однією з таких праць є дослідження П. Джонстона «Фінансові злочини: Запобігання та регулювання у нематеріальному середовищі» (Financial Crime: Prevention and Regulation in the Intangible Environment). У своїй роботі П. Джонстон наголошує на глибокій трансформації глобальної фінансової індустрії під впливом цифровізації, зокрема на тлі переходу у нове тисячоліття. Автор звертає увагу на те, що технологічні виклики, як-от: синдром помилки 2000 року (Y2K) – змусили політиків та експертів з інформаційних технологій консолідувати зусилля задля запобігання можливим збоям у фінансовій системі. Водночас він підкреслює, що реакція на значно серйознішу проблему – кіберзлочинність – залишається дещо хаотичною та невиразною. Автор критично оцінює рівень готовності урядів і регуляторів до загроз, що постають у новому цифровому середовищі, вказуючи на нестачу скоординованих дій [228]. Ця робота стала однією із перших спроб осмислення кіберзлочинності у контексті глобального фінансового простору, а також підняла важливу проблему: швидкого розвитку цифрових технологій, який значно випереджає реалізацію механізмів правового та безпекового характеру та їхню здатність максимально швидко адаптуватися до нових форм загроз.

Ще однією знаковою публікацією 1999 року, яка була включена до бази Scopus за темою «cybercrime», стала стаття Дж. Хейнса та П. Джонстона «Глобальна кіберзлочинність: нові іграшки для відмивачів грошей» (Global Cybercrime: New Toys for Money Launderers), опублікована в журналі Journal of Money Laundering Control. У ній автори акцентують увагу на нових можливостях, які відкриває цифровий світ для підвищення рівня транснаціональної злочинності, зокрема для реалізації схем

відмивання грошей. Стаття показує, наскільки швидкий розвиток електронної комерції та цифрових фінансових інструментів (як-от: електронні перекази, кредитні/дебетові картки, смарт-картки) суттєво ускладнюють роботу правоохоронних органів, адже більшість транзакцій не залишає жодного паперового або аудиторського сліду. Автори метафорично описують Інтернет як «всесвітню кіберкондитерську», де транснаціональний злочинець вільно переміщується між інструментами для незаконних фінансових операцій, не виходячи з кіберкафе». У публікації підкреслюється, що кіберзлочинність руйнує традиційні географічні межі, а технологічний прогрес у сфері комунікацій і цифрових систем лише посилює це явище [220].

Таким чином, уже наприкінці 1990-х автори попереджають про глобальний характер цифрових загроз і необхідність перегляду підходів до фінансового моніторингу та міжнародного правового співробітництва.

На зображенні представлена тематична мапа, яка демонструє основні напрямки досліджень у сфері кіберзлочинності на основі співзгадуваності ключових слів у наукових публікаціях. Горизонтальна вісь відображає ступінь релевантності тем: чим далі тема розташована праворуч, тим вона важливіша для загального поля дослідження. Вертикальна вісь показує ступінь «розробленості» теми: чим вищий показник, тим краще опрацьована тема у науковій літературі.

У нижньому правому квадраті знаходяться так звані базові теми-поняття – у нашому випадку це «*computer crime*», «*cyber-crimes*», «*crime*». Вони є високо релевантними, тобто центральними для наукового поля, однак ще не мають достатньої глибини опрацювання. Це означає, що поняття кіберзлочинності лежить в основі більшості досліджень, але потребує подальшої деталізації та розгляду у контексті окремо взятих до уваги підтем.

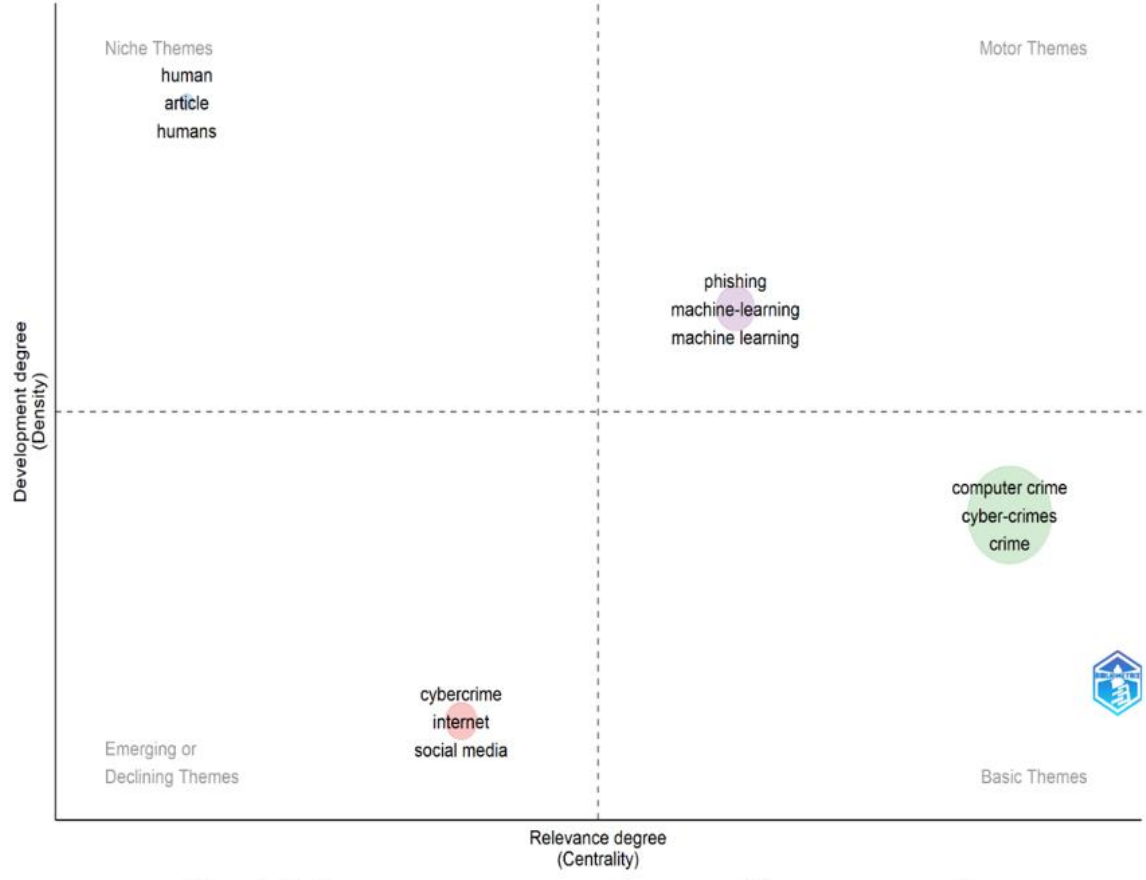

Рис. 1.2. Тематична мапа досліджень кіберзлочинності

(Джерело: розроблено за допомогою Biblioshiny та Scopus)

У верхньому правому квадранті представлено ключові дефініції – «*phishing*», «*machine learning*», «*machine-learning*». Вони вирізняються і високою релевантністю, і водночас високим рівнем наукового інтересу. Це свідчить про інтенсивність вивчення означеної проблеми, яка, насамперед, пов'язана з використанням машинного навчання, з метою виявлення кіберзагроз, зокрема фішингу. Ці напрями активно розвиваються та формують сучасну технічну парадигму кібербезпеки.

Нижній лівий квадрант охоплює ті проблемні тематики, які перебувають на етапі формування дослідницького інтересу, або ж навпаки – втраті наукової актуальності – «*cybercrime*», «*internet*», «*social media*». Незважаючи на те, що ці ключові поняття є важливими, вони мають порівняно низькі показники за релевантністю та щільністю. Це може свідчити про те, що ці теми або потребують оновлення змісту та більш глибшого переосмислення, або вони ще не набули повного «наукового розгортання» у конкретному дослідницькому контексті.

У верхньому лівому квадраті представлено так звані нішеві теми – «*human*», «*article*», «*humans*». Вони досить добре опрацьовані з точки зору глибини, але мають низьку релевантність щодо основного наукового ядра дослідження. Це може свідчити про їхню міждисциплінарність або вторинну роль у дослідженнях з питань кіберзлочинності.

Загалом тематична мапа демонструє, що наука про кіберзлочинність активно розвивається у напрямку застосування штучного інтелекту, натомість загальні поняття залишаються поза увагою, відтак можуть стати основою для нових, більш вузьких дослідницьких напрямків.

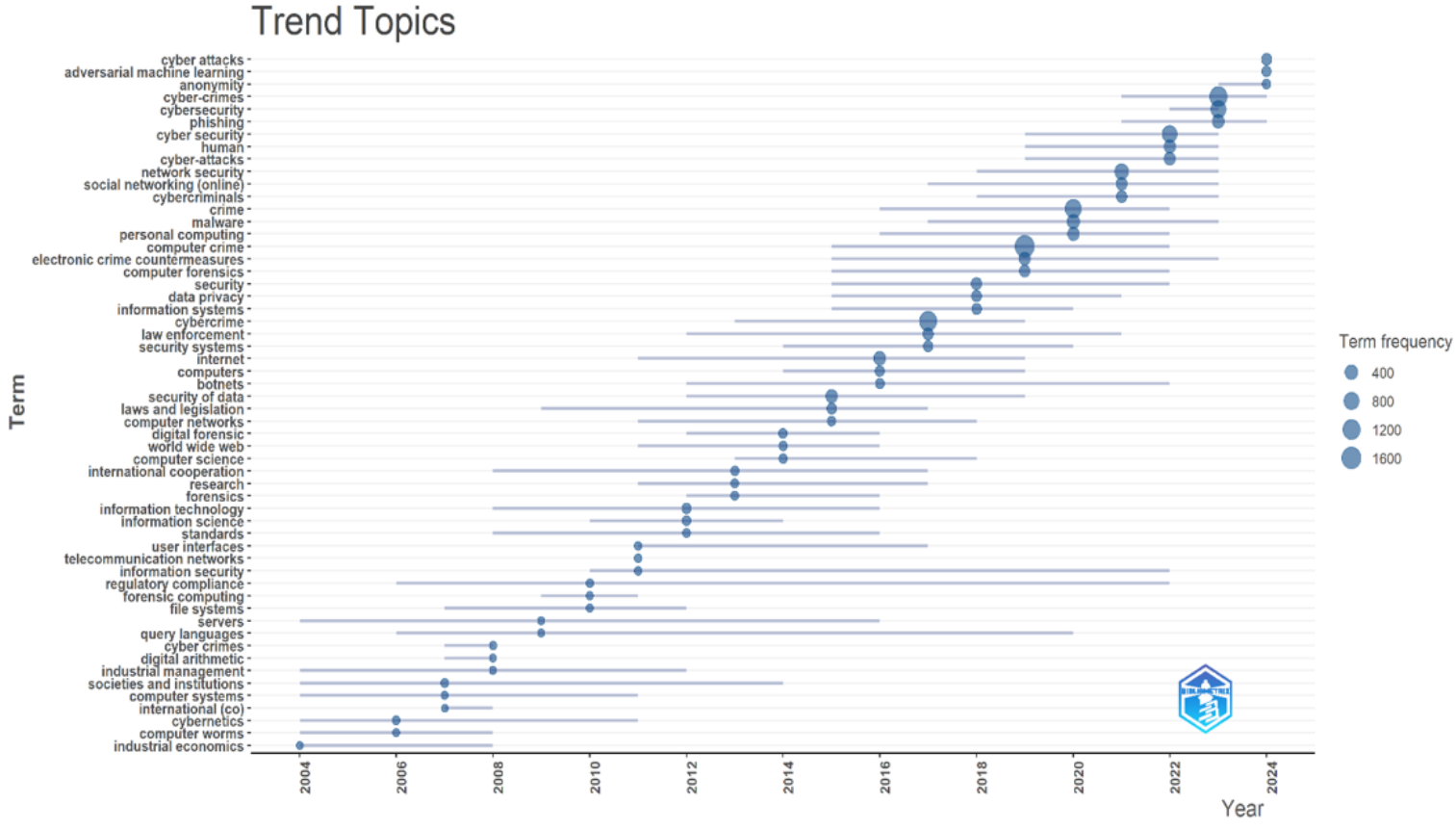

Рис. 1.3. Трендові теми у дослідженнях кіберзлочинності (2003–2024): еволюція та частотність термінів

(Джерело: розроблено за допомогою Biblioshiny та Scopus)

На діаграмі відображено динаміку появи й популярності ключових термінів у наукових дослідженнях, пов'язаних із кіберзлочинністю, упродовж 2003–2024 років. За вертикальною віссю розміщено перелік термінів, що використовувались у публікаціях, а за горизонтальною – роки. Розмір кожної точки відповідає частоті використання терміну у відповідному році (чим більша точка, тим частіше термін зустрічався).

У 2003–2010 рр. дослідження переважно зосереджувалися на фундаментальних темах, як-от: *computer science*, *information security*, *forensics*, *cybernetics*, *servers*, *file systems* та *internet*. Це свідчить про технічне підґрунтя становлення дисципліни.

З 2010-х років починають активно з'являтися більш прикладні теми: *cybercrime*, *computer forensics*, *law enforcement*, *security systems*, *personal computing* та *data privacy*. Також фіксується зростання інтересу до правового регулювання (*laws and legislation*), що відображає потребу у нормативному забезпеченні боротьби з кіберзлочинністю.

Період з 2016 по 2023 роки спостерігаємо стрімке зростання термінів, пов'язаних з інноваційними технологіями та соціальними чинниками, зокрема: *phishing*, *cybercriminals*, *social networking*, *machine learning*, *cyber-attacks*, *network security*, *adversarial machine learning*. Це вказує на зростання рівня складності кіберзагроз та свідчить про зміщення фокусу досліджень у напрямку прогнозування, виявлення загроз та аналізу поведінки зловмисників у цифровому середовищі.

В останні роки (2022–2024) прослідковується поява таких запитів, як: *cyber attacks*, *cybersecurity*, *security*, *anonymity* та *adversarial machine learning*, що свідчить про посилений інтерес до тем штучного інтелекту, зокрема з використанням автоматизованих алгоритмів та збереження анонімності в мережі.

Діаграма показує, що сфера досліджень кіберзлочинності еволюціонувала від загально-інформаційних та інфраструктурних тем до складних і спеціалізованих, які охоплюють машинне навчання, соціальні мережі, фішинг та анонімність. Це свідчить не лише про технічний прогрес, а й ілюструє зростання рівня загроз, що потребує міждисциплінарного підходу у низці досліджень, які піднімають питання реалізації найбільш ефективних заходів з питань кібербезпеки.

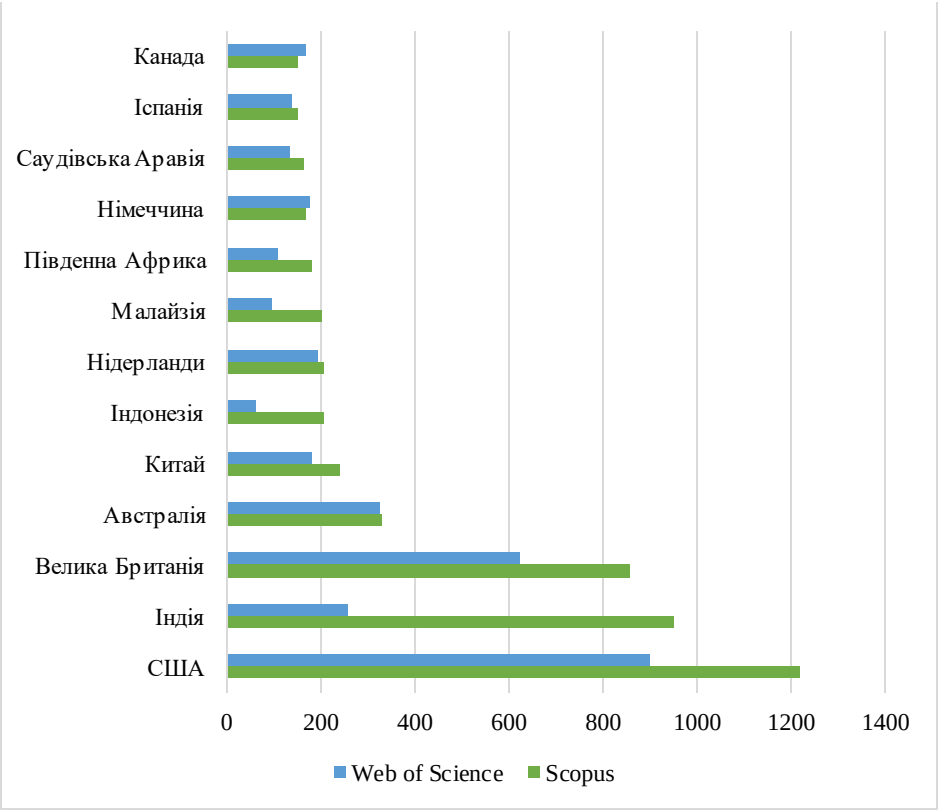

Рис. 1.4. Кількість публікацій за пошуковим терміном «cybercrime» у БД Scopus та Web of Science за географічним критерієм
(Джерело: побудовано авторами)

На діаграмі зображено порівняння кількості наукових публікацій з теми кіберзлочинності у базах даних Scopus та Web of Science, відповідно до вказаної країни. Вибрано 13 держав, які є найбільш активними у цьому напрямку досліджень. Очевидним

лідером є США, які мають найвищі показники в обох базах: понад 1200 публікацій у Scopus і близько 950 у Web of Science. Це свідчить про систематичну наукову активність та пріоритетність теми кіберзлочинності для американських дослідників.

На другому місці – Індія, яка демонструє значну кількість публікацій у Scopus (понад 900), але значно менше – у Web of Science. Велика Британія зберігає високу позицію за обома базами, що свідчить про стабільну якість і обсяг наукових публікацій. Подібна тенденція простежується і для Австралії, хоча її показники дещо нижчі. Інші країни, як-от: Китай, Нідерланди, Німеччина, Саудівська Аравія та Іспанія, мають помірні, але стабільні результати в обох базах. Водночас деякі держави – зокрема Малайзія, Індонезія та Південна Африка – демонструють вищу публікативну активність у базі Scopus. Загалом, діаграма свідчить про домінування США, Індії та Великої Британії у сфері дослідження з питань кіберзлочинності. Спостерігається значна перевага Scopus над Web of Science за кількістю публікацій у більшості країн.

На рис. 1.5, створеному за допомогою VOSviewer, зображено мережу міжнародної наукової співпраці у сфері досліджень з питань кіберзлочинності. Кожен круг позначає окрему країну, а його розмір свідчить про кількість публікацій; лінії між країнами демонструють наукові зв’язки, вибудовані на основі співавторства. Товщина лінії вказує на активність взаємодії між двома країнами.

Центральне місце займають США, які не лише мають найбільшу кількість публікацій, але й є ключовим вузлом міжнародного співробітництва. Вони тісно пов’язані із науковими спільнотами країн Європи, Азії, Африки та Північної Америки. США формують потужну наукову платформу, об’єднуючи навколо себе партнерів із Нідерландів, Німеччини, Канади, Китаю, Малайзії, Нігерії та інших країн.

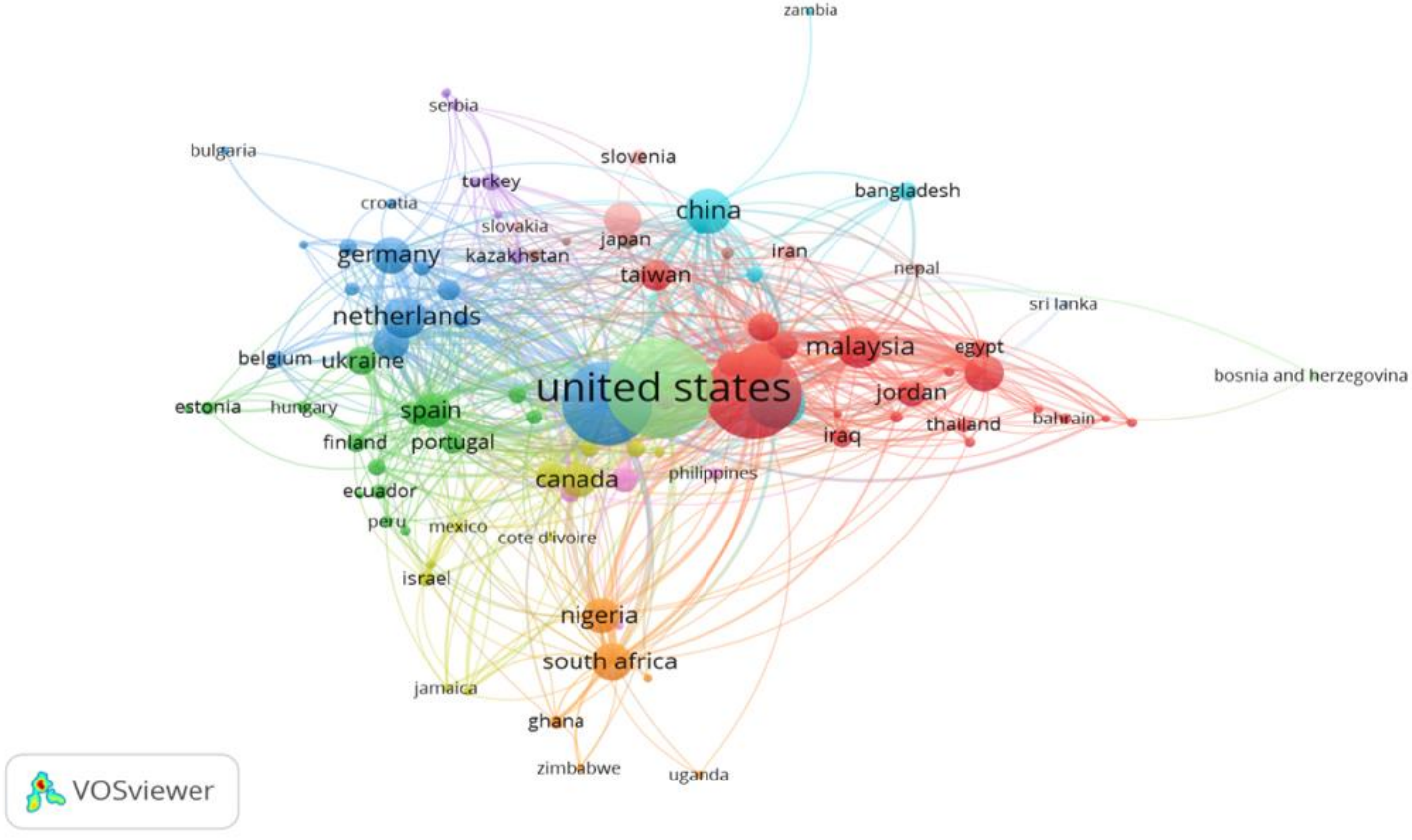

Рис. 1.5. Міжнародна наукова співпраця у сфері кіберзлочинності: мережевий аналіз, відповідно до країни
(Джерело: побудовано за допомогою інструментарію VOSviewer)

На мапі чітко виокремлюються регіональні кластери. Один із найбільш насичених – це азійсько-середземноморський кластер (червоний), до якого входять: Малайзія, Йорданія, Ірак, Єгипет, Таїланд. Тут лідерство належить Малайзії, яка демонструє високу наукову активність і водночас співпрацю із різними державами. Інший важливий кластер формують країни Європи (синій): Німеччина, Нідерланди, Бельгія, Хорватія, Україна. Також виокремлюється африканський кластер (помаранчевий), очолюваний Південною Африкою та Нігерією, які активно інтегруються у глобальні наукові процеси.

Таким чином, карта яскраво показує, що дослідження в галузі кіберзлочинності мають чітко виражену глобальну кооперацію. Попри домінування США, спостерігається також посилення регіональної активності з боку країн Азії, Африки та Європи. Це свідчить про те, що проблема кіберзлочинності є спільним викликом, який об'єднує науковців різних країн і потребує міждержавної співпраці для ефективного вивчення та реагування.

На рис. 1.6. представлено карту ключових понять у сфері кіберзлочинності, створену за допомогою VOSviewer. У центрі зображення – термін «cybercrime», який є найчастішим і має найтісніші зв'язки з іншими поняттями. Поруч розташовані такі ключові слова, як: *cybersecurity, cyber security, digital forensics, cyber-attacks, machine learning* та *social media.* Це свідчить про те, що сучасне вивчення кіберзлочинності є міждисциплінарним і охоплює не лише технічні аспекти захисту, а й враховує соціальні виклики, пов'язані з цифровими загрозами.

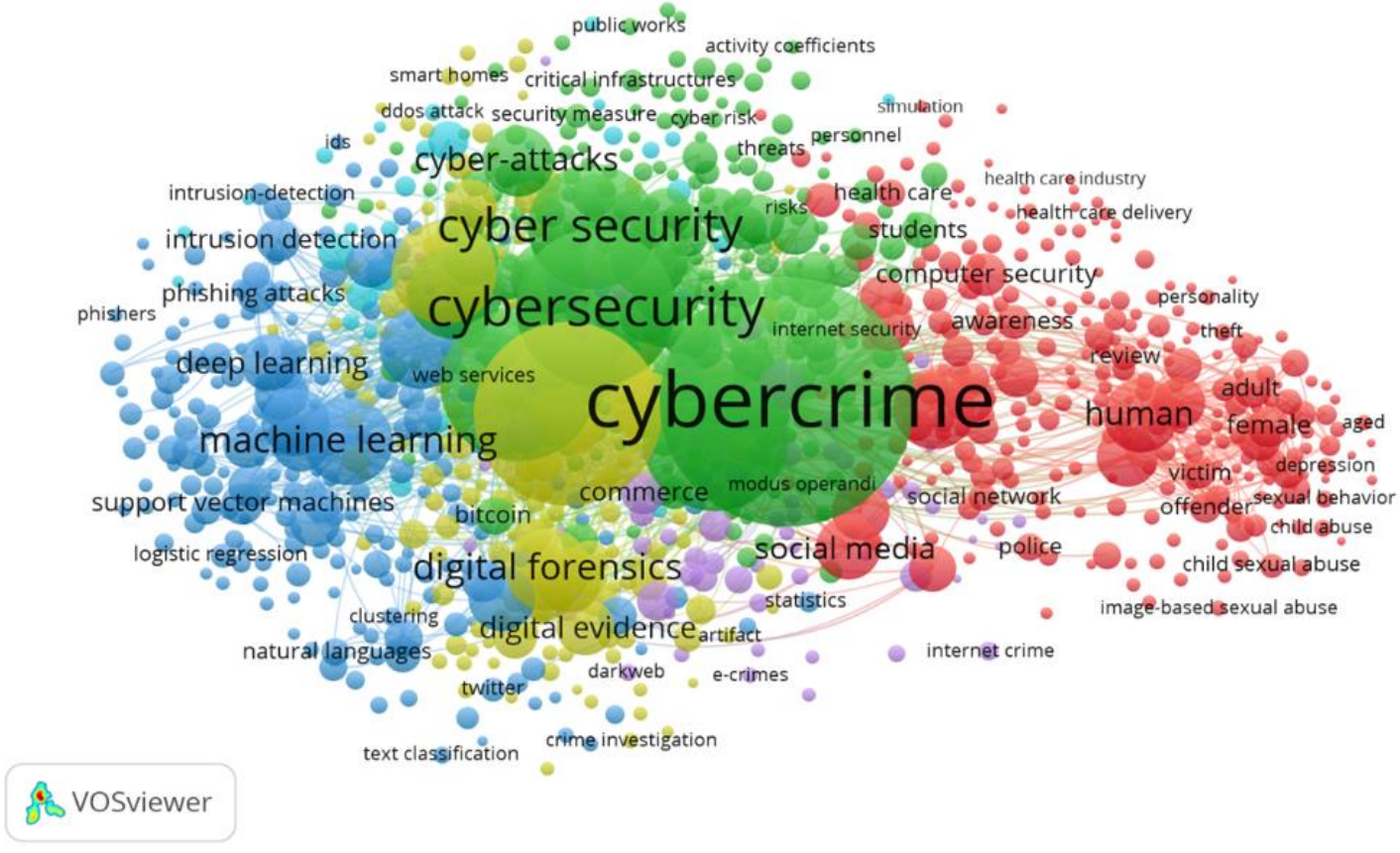

Рис. 1.6. Карта візуалізації ключових слів у сфері кіберзлочинності

Джерело: побудовано за допомогою інструментарію VOSviewer

Серед основних кластерів варто виокремити синій, у якому зосереджені технічні терміни, як-от: *machine learning, deep learning, intrusion detection, phishing attacks.* Це свідчить про активізацію досліджень у сфері застосування штучного інтелекту для виявлення кіберзагроз. Зелений кластер включає теми, пов'язані з управлінням ризиками, безпекою та критичною інфраструктурою: *cyber-attacks, threats, risks, cyber risk*. Жовтий кластер охоплює цифрову криміналістику, електронні докази, тіньову мережу та цифрову комерцію.

Окремо виділено червоний кластер, пов'язаний із соціальними та психологічними аспектами: *human, awareness, victim, offender, female, child abuse, depression.* Він підкреслює гуманітарний вимір кіберзлочинності, зміст якого полягає у вивченні психології особистостей жертви та злочинця, відповідно і механізмів психологічних наслідків, соціальних реакцій на відповідні кіберзлочини.

Таким чином, ця візуалізація відображає складну структуру наукового поля, де кіберзлочинність постає як багатогранне явище, що вимагає інтеграції технічних, правових і соціальних підходів. Вона може слугувати орієнтиром для дослідників, які шукають актуальні напрями для подальших наукових розвідок.

На рис. 1.7 представлено порівняльну характеристику наукової активності провідних університетів світу, відображену у певних дослідженнях. Найбільш виразну активність у науковому просторі демонструє Мічиганський державний університет, який очолює рейтинг в обох базах.

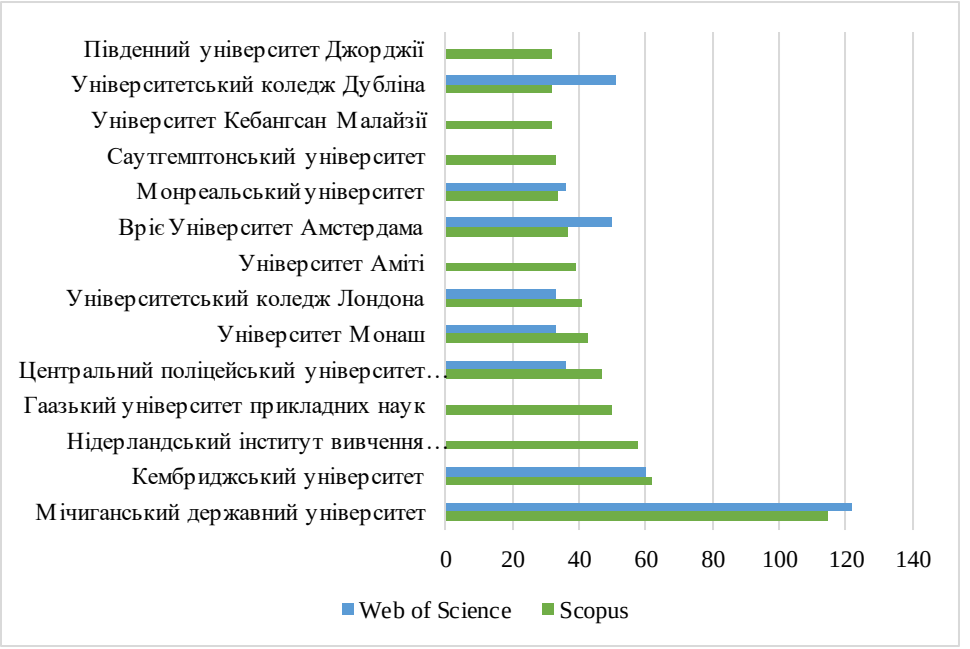

Рис. 1.7. Кількість публікацій за пошуковим терміном «cybercrime» у БД Scopus та Web of Science за приналежністю

(Джерело – побудовано авторами)

Високі показники також спостерігаються у Кембриджського університету, Нідерландського інституту вивчення злочинності, Монреальського університету та Університетського коледжу Лондона. Деякі університети, зокрема Врієуніверситет Амстердама та Університетський коледж Дубліна, мають більший показник саме у Web of Science. Цікавим є той факт, що деякі установи (наприклад, Університет Аміті, Університет Кебангсан Малайзії, Саутгемптонський університет) демонструють помітну активність лише у базі Scopus, а в Web of Science наукові публікації фактично відсутні. Це може бути пов’язано з фокусом на регіональні або прикладні видання, які частіше індексуються саме в Scopus. Окремо увагу привертають ті установи, які публікують свої дослідження переважно у Web of Science. Скажімо, Масарик

Університет у Брно (Чехія), який постає абсолютним лідером за кількістю публікацій у цій базі (166 робіт). Він навіть випереджає Мічиганський і Лондонський університети, які також демонструють значні результати. Примітно, що до переліку увійшло і Міністерство освіти і науки України, що свідчить про наявність українських дослідницьких ініціатив у сфері кібербезпеки на міжнародному рівні.

Таким чином, аналіз показує, що дослідження кіберзлочинності активно проводяться у багатьох країнах світу, а окремі університети відіграють ключову роль у формуванні глобального наукового простору цієї галузі.

На рис. 1.8 зображено 10 найрелевантніших джерел, у яких найчастіше публікуються наукові роботи, пов'язані з тематикою кіберзлочинності. Дані отримані з бази Scopus. Безперечним лідером за кількістю публікацій є «Lecture Notes in Computer Science (LNCS)», де було індексовано 103 документи.

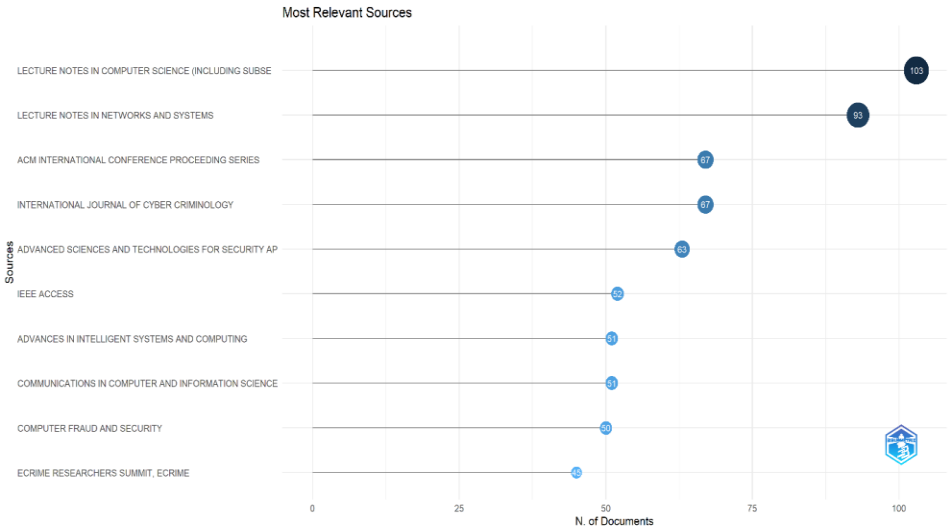

Рис. 1.8. Наукові джерела, що публікують дослідження з кіберзлочинності

(Джерело: розроблено за допомогою Biblioshiny та Scopus)

Це серія конференційних матеріалів, яка охоплює широкий спектр комп'ютерних наук, включно з темами інформаційної безпеки, штучного інтелекту, машинного навчання, тощо. На другому місці – «Lecture Notes in Networks and Systems», де зафіксовано 93 документи, що вказує на значну роль мережевих технологій у контексті кіберзлочинності. Також високі позиції займають «ACM International Conference Proceedings Series» та «International Journal of Cyber Criminology»; кожне із зазначених джерел містить по 67 публікацій. Перше видання є репрезентативним для комп'ютерних наук загалом, натомість друге спеціалізується безпосередньо на кримінологічних аспектах кіберзлочинів, демонструючи баланс між технічним і соціальним підходами до зазначеної теми. Серед інших помітних джерел – «IEEE Access», «Advanced Sciences and Technologies for Security Applications» та «Advances in Intelligent Systems and Computing», де публікуються роботи з питань цифрової безпеки, аналітики даних, машинного навчання й прикладних досліджень. Їхня поява у рейтингу свідчить про стрімкий розвиток міждисциплінарних досліджень у сфері кібербезпеки. Завершують список видання «Computer Fraud and Security» (50 публікацій) та «ECRIME Researchers Summit, eCrime» (45 публікацій), що свідчить про спеціалізовану спрямованість на теми кіберзлочинності, актуалізовані у бізнес-середовищі, фінансовому секторі та правоохоронній діяльності.

На рис. 1.9 представлено мережу наукової співпраці між дослідниками, які спеціалізуються на проблематиці кіберзлочинності. У центрі мапи найбільшим і найвпливовішим вузлом є Thomas J. Holt, що свідчить про його провідну роль у дослідженнях проблеми кіберзлочинності. У тісному науковому зв'язку з ним перебуває Adam M. Bossler. Цей червоний кластер зосереджує увагу на соціальних і поведінкових аспектах злочинності у віртуальному середовищі.

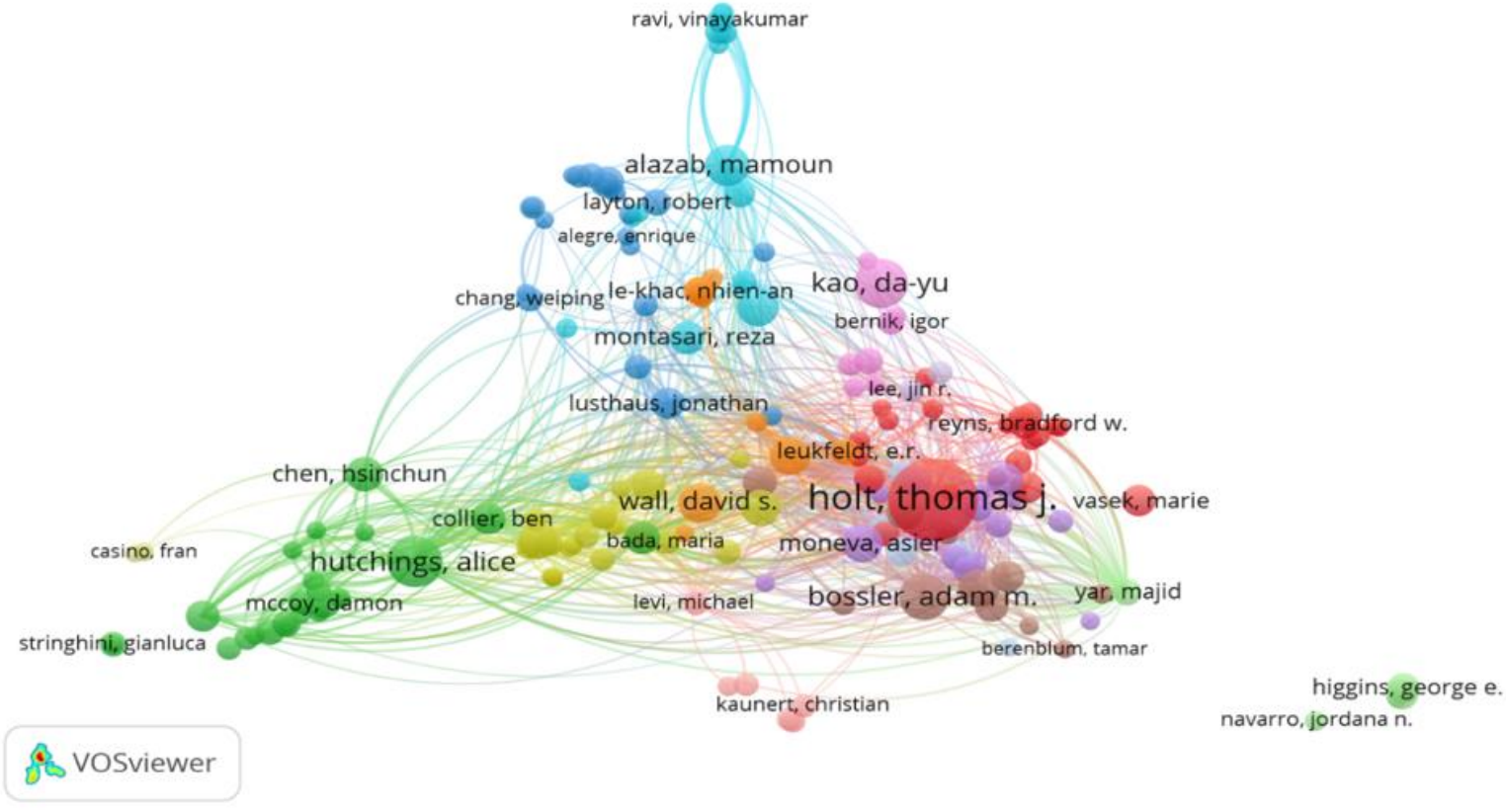

Рис. 1.9. Візуалізація співпраці між провідними дослідниками у галузі кіберзлочинності

(Джерело: побудовано за допомогою інструментарію VOSviewer)

Інший кластер (синій) формується навколо Mamoun Alazab і Vinayakumar Ravi, які, разом із співавторами, активно публікуються у сфері застосування штучного інтелекту, глибокого навчання та систем виявлення загроз. Їхні дослідження мають переважно технічне спрямування і публікуються у журналах інженерного та комп'ютерного профілю.

Зелений кластер зосереджено навколо Alice Hutchings і Ben Collier, які працюють на перетині кримінології, соціології та аналізу цифрових ризиків. Вони часто здійснюють співпрацю із Hsinchun Chen – одним із найбільш сучасних центрів у сфері цифрової криміналістики та інтелектуального аналізу даних (data mining).

Пурпуровий і жовтий кластери (із такими авторами як Kaunert Christian, Levi Michael, Wall David S., Yar Majid) стосуються регулювання, нормативно-правових механізмів та державної політики у сфері кіберпростору.

Важливо також відзначити, що мапа ілюструє високу щільність наукових контактів – майже всі автори мають кілька міжкластерних зв'язків, що підтверджує глобальний, міждисциплінарний характери досліджень у сфері кіберзлочинності.

Наступним кроком постає аналіз найбільш цитованих публікацій у БД Scopus та Web of Science.

Серед лідерів обох баз віднаходимо статтю «Deep Learning Approach for Intelligent Intrusion Detection System» (За авторства R. Vinayakumar та кола співавторів),яка була опублікована у журналі IEEE Access. У Scopus вона має 1282 цитування, у Web of Science – 804. Така кількість цитувань свідчить про її вагомість, особливо у технічному контексті, адже дослідження присвячено застосуванню глибинного навчання, з метою виявлення кіберзагроз – однієї із найактуальніших проблем сучасної кібербезпеки.

Таблиця 1.3

Топ-5 найбільш цитованих публікацій, присвячених кіберзлочинності у БД Scopus

Назва	Автор	Джерело	Кількість цитувань
Deep Learning Approach for Intelligent Intrusion Detection System [204]	R. Vinayakumar; Mamoun Alazab; K. P. Soman; Prabaharan Poornachandran; Ameer Al-Nemrat; Sitalakshmi Venkatraman	IEEE Access	1282
Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization [221]	Holt T. J., Bossler A. M.	Deviant Behavior	484
User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection [225]	Isaak J., Hanna M. J.	Computer	443
Robust Intelligent Malware Detection Using Deep Learning [244]	R. Vinayakumar et al.	IEEE Access	405
The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory [264]	Yar M.	European Journal of Criminology	395

Таблиця 1.4

Топ-5 найбільш цитованих публікацій, присвячених кіберзлочинності у БД Web of Science

Назва	Автор	Джерело	Кількість цитувань
Deep Learning Approach for Intelligent Intrusion Detection System [204]	R. Vinayakumar; Mamoun Alazab; K. P. Soman; Prabaharan Poornachandran; Ameer Al-Nemrat; Sitalakshmi Venkatraman	IEEE Access	804
Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization [221]	Holt T. J., Bossler A. M.	Deviant Behavior	261
BEING PURSUED ONLINE Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization [243]	Reyns B. W., Henson B., Fisher B. S.	Criminal Justice and Behavior	260
Crime data mining: A general framework and some examples [192]	H. Chen; W. Chung; J.J. Xu; G. Wang; Y. Qin; M. Chau	Computer	256
Blockchain Technology Innovations [180]	Ahram, T; Sargolzaei, A; Amaba, B	IEEE Technol. Eng. Manage. Conf. (TEMSCON)	243

Наступною за цитованістю в обох базах є робота *Holt T. J. і Bossler A. M. «Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization».* У Scopus вона отримала 484 посилання, а у Web of Science – 261. Автори адаптували теорію рутинної діяльності до контексту кіберпростору, запропонувавши новий погляд на вразливість жертв щодо наслідків цифрових злочинів. У базі Scopus третє місце посідає резонансна стаття *«User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection»* (443 цитування), присвячена проблемі конфіденційності користувацьких даних. Ця тема набула особливого розголосу після скандалу з Cambridge Analytica і стала важливою у суспільно-політичному дискурсі щодо захисту персональної інформації в цифрову епоху. Водночас у базі Web of Science на третій позиції перебуває наукова праця *«Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization»* (260 цитувань), зміст якої також ґрунтується на теорії рутинної діяльності, проте акцент здійснено на проблемі онлайн-переслідування, що є загрозою для особистої безпеки в мережі Інтернеті. У Web of Science 4 місце посідає стаття *«Crime Data Mining: A General Framework and Some Examples»* (256 цитувань), яка має практичну цінність для побудови аналітичних систем на основі великих масивів злочинної інформації. Закриває п’ятірку найцитованіших у WoS публікація про *«Blockchain Technology Innovations»* (243 цитування), що свідчить про зростання інтересу до проблеми блокчейну як інструменту забезпечення прозорості й захищеності у кіберпросторі.

Таким чином, аналіз обох таблиць показує, що найбільший науковий вплив був завданий тими публікаціями, які поєднують штучний інтелект і безпеку, кримінологічні теорії у цифровому контексті, а також етико-правові аспекти конфіденційності. Ці роботи не лише формують наукову основу подальших досліджень, а й активно впливають на практичну сферу – від створення захисних алгоритмів до вироблення цифрової політики та регулювання.

РОЗДІЛ 2

СУЧАСНИЙ СТАН ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ЯК ПЕРЕДУМОВА ФОРМУВАННЯ СТРАТЕГІЇ ІНТЕГРАЦІЇ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕРБЕЗПЕКИ

2.1. Світові тенденції кіберзлочинності та загрози інформаційні безпеці держав

В епоху цифровізації та швидкого поширення інтернет-технологій суспільство зіштовхнулося з новими загрозами у сфері безпеки та правопорядку. Кіберзлочинність стала однією з найбільших загроз сучасного світу, вплив якої відчувають усі сфери діяльності: економіка, освіта, охорона здоров'я та критична інфраструктура . Кіберзлочинності притаманний широкий діапазон різних загроз від конкретних атак у мережі Інтернет до постійних злочинів на фінансові системи та ресурси державних структур та населення загалом. Трансформація кібератак та масовість їх здійснення стали головною темою для обговорення на міжнародному рівні та вимагають нових зусиль щодо їх попередження та усунення. Вивчення статистичних даних дозволяє не лише оцінити поточний стан кіберзлочинності, а й прогнозувати її розвиток, визначати вразливі сфери та розробляти ефективні стратегії захисту. Глобальний аналіз поширеності кіберзлочинності сприяє кращому розумінню динаміки злочинності, обміну досвідом між країнами та створенню міжнародних механізмів співпраці.

Інформаційні технології щодня змінюються зі стрімкою швидкістю, а саме: хмарні сервіси, блокчейн, Інтернет-речей – це створює додаткові вразливі місця для злочинів щодо здійснення нових кібератаки, як в професійних, так і в особистих мережах. Кіберзлочинність може приймати різні форми: шахрайство з особистими даними, викрадення даних, атаки програм-вимагачів, кібератаки на критичну інфраструктуру або ж фішингові кампанії та інші.

Експерти німецької онлайн-платформи *Statista* оцінюють глобальні втрати від кіберзлочинів в 7,1 трлн дол. США у 2022 р. порівняно з 1,2 трлн дол. США у 2019 р., при цьому, згідно з даними *Chainalysis*, у 2021 і 2022 рр. різко зросли криптообмін і зломи протоколів такими плідними групами, як афілійована з державою північнокорейська хакерська команда Lazarus [196]. Згідно з дослідженнями, проведеними експертами антивірусної компанії McAfee у співпраці з Центром стратегічних та міжнародних досліджень, глобальні збитки від хакерських атак щорічно складають у середньому 600 млрд дол. США [181].

Світові організації вважають втрату особистої інформації клієнтів або співробітників одним із найнебезпечніших результатів кібератак. Втрата конфіденційної інформації може мати серйозні наслідки для компаній, наприклад, погіршити репутацію та втрату прибутку. Криза COVID-19 призвела до того, що багато організацій зіткнулися з більшою кількістю кібератак через вразливість безпеки віддаленої роботи, а також через перехід до віртуалізованих IT-середовищ, таких як інфраструктура, дані та мережа хмарних обчислень.

Дослідження, проведені у 2022 р. компанією PwC (PricewaterhouseCoopers) міжнародною мережею професійних послуг, показали значний рівень кіберзлочинності у світі. Зокрема,

Індія має найвищий відсоток користувачів, які стали жертвами кіберзлочинів (68 %), тоді як у Сполучених Штатах цей показник становить 49 %. Це свідчить про те, що кіберзлочинність залишається глобальною загрозою, яка впливає на користувачів незалежно від їхньої географічної локації. З огляду на це, важливо підвищувати рівень обізнаності та захищеності користувачів в інтернеті, вдосконалювати кібербезпекові заходи та політики для запобігання цифровим атакам (рис. 2.1).

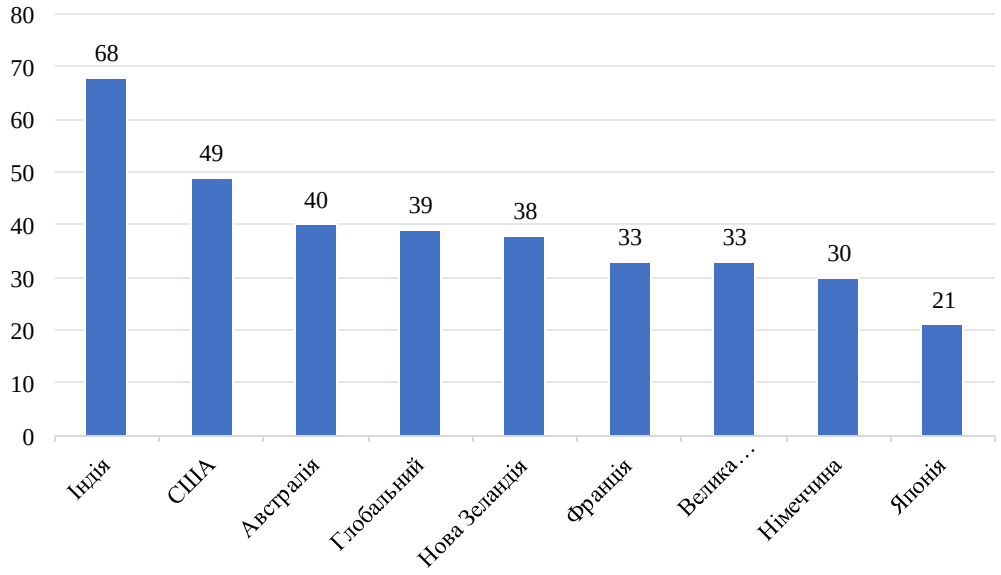

Рис. 2.1. Частка користувачів мережі Інтернету в окремих країнах, які коли-небудь стикалися з будь-якими кіберзлочинами у 2022 р., %

Джерело: побудовано на основі [22].

Слід зазначити, що фішингові атаки, які у 2022 р. склали понад половину всіх кіберзлочинів (53,2 %) і є одним із найпоширеніших методів обману в цифровому середовищі. Їхня популярність пояснюється простою реалізацією та високою ефективністю введеної жертви в оману для отримання

конфіденційної інформації, такої як паролі, даних кредитних карток або іншої чутливої інформації. Фішинг, зокрема, може бути реалізований через електронні листи, підроблені веб-сайти чи повідомлення в соціальних мережах, що сприяє підвищенню уваги з боку користувачів і впровадження профілактичних заходів, таких як двофакторна автентифікація.

Водночас, хоча інвестиційне шахрайство займає найменшу кількість учасників (5,4 %), його наслідки можуть бути особливо руйнівними. Обман інвесторів, пов'язаних із неправдивою інформацією щодо надання акцій, зобов'язань чи інших фінансових інструментів, завдає шкоди не лише окремим особам ринку, а й фінансової стабільності в цілому. Крім матеріальних втрат, такі злочини підривають довіру до фінансових установ і ринкових механізмів. Це вимагає посилення регуляторного контролю, вдосконалення системи виявлення шахрайства та підвищення фінансової грамотності серед громадян, що є ключовими кроками у боротьбі з подібними злочинами.

Слід відзначити, що у 2017 р. лідером серед кіберзлочинів була несплата або ж не доставка товарів, проте за останні роки ситуація дещо змінилася, та у 2022 р. серед найпопулярнішими з кібератак лідерами стали фішингові атаки (рис. 2.2), так їх кількість становила понад 53,2 % від загальної частки всіх кіберзлочинів. Найменшу частку при цьому займає інвестиційне шахрайство яке становить 5,4 % від загальної частки кіберзлочинів, що являє собою обман, який призводить інвесторів приймати рішення про купівлю або ж продає цінних паперів на основі неправдивої інформації, наслідком таких дій є порушення чинного законодавства та матеріальних втрат.

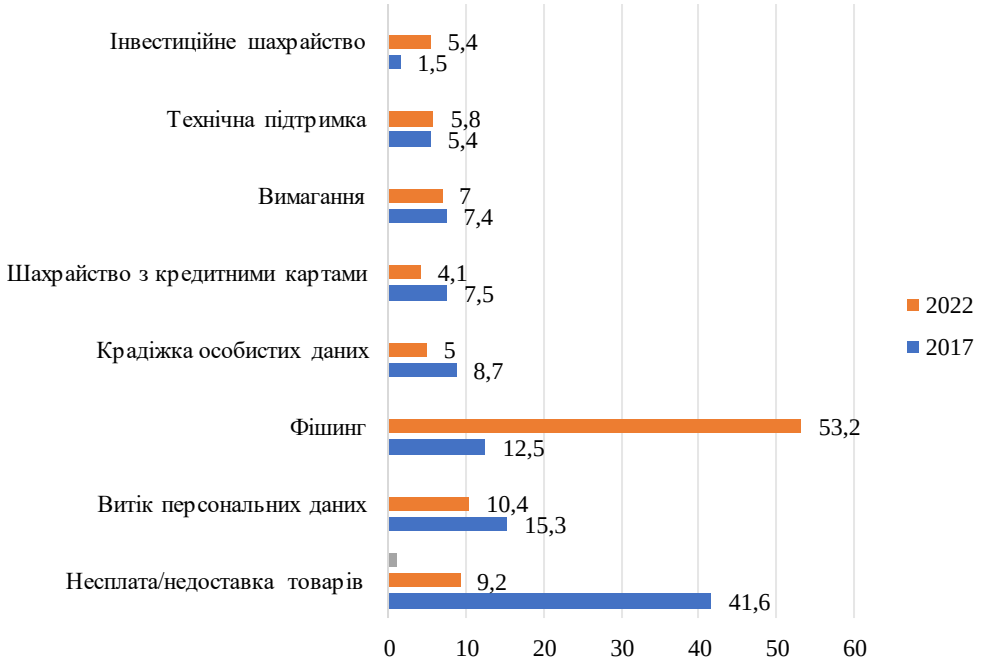

Рис. 2.2. Найпопулярніші кіберзлочини в мережі Інтернет в світі, 2017-2022 рр., %

Джерело: побудовано на основі [199; 200; 202].

Кіберзлочини з кожним роком набувають нових видів та форм, вони відображають швидку адаптацію до технологічних змін. На рис. 2.3 наведено показники кібератак протягом 2016-2023 рр. у розрізі їх видів.

Протягом досліджуваного періоду фішингові атаки мають найбільшу тенденцію розповсюдження у глобальному просторі, так у 2023 р. було зафіксовано більше ніж 9 млн випадків атак у світі, а вже у першому кварталі 2024 р. кількість унікальних фішингових сайтів становила понад 1 млн. Друге місце посідає такий вид кіберзлочинності, як порушення персональних даних, так їх кількість у 2022 р. становила понад 1,66 млн кіберінцидентів, на третьому місці знаходиться не оплата або несплата товарів та

дорівнює близько 1,5 млн випадків. За допомогою підробного листування, яке надходить на електронну скриньку чи соціальні мережі, жертв фішингу спрямовують на перехід до спеціально створених фішингових сайтів, які збирають персональні дані користувачів та потім використовуються їх для онлайн-шахрайства або викрадення особистої інформації. Крім того, посилання в таких підроблених повідомленнях нерідко служать точкою доступу для проникнення зловмисного програмного забезпечення в систему.

Дослідження, проведені у 2022 р. компанією PwC серед опитаних у вибраних країнах, які коли-небудь ставали жертвами крадіжки особистих даних, свідчить що Індія стала лідером поміж досліджуваних країн (рис. 2.4), більше ніж у 27,2 млн дорослих зловмисниками були вилучені дані. Наступною країною за величиною потерпілих від втрати даних представлені Сполучені Штати Америки та їх кількість дорівнює близько 13,5 млн осіб, на третьому місці знаходиться Японія, де показник жертв крадіжки особистих даних становить понад 3 млн. випадків [22].

У 2023 р. показники шахрайства, пов’язані з платежами, залишалися ключовими загрозами у кіберпросторі. Значна частина таких злочинів була спрямована на крадіжку платіжних даних через електронні гаманці, банківські рахунки або використання скімінгових пристроїв. Одним із розширених методів є соціальна інженерія, коли зловмисники шляхом обману змушують жертву розкрити банківські реквізити або підтвердити транзакції. У 2023 р. значне зростання таких злочинів було зафіксовано в електронній комерції.

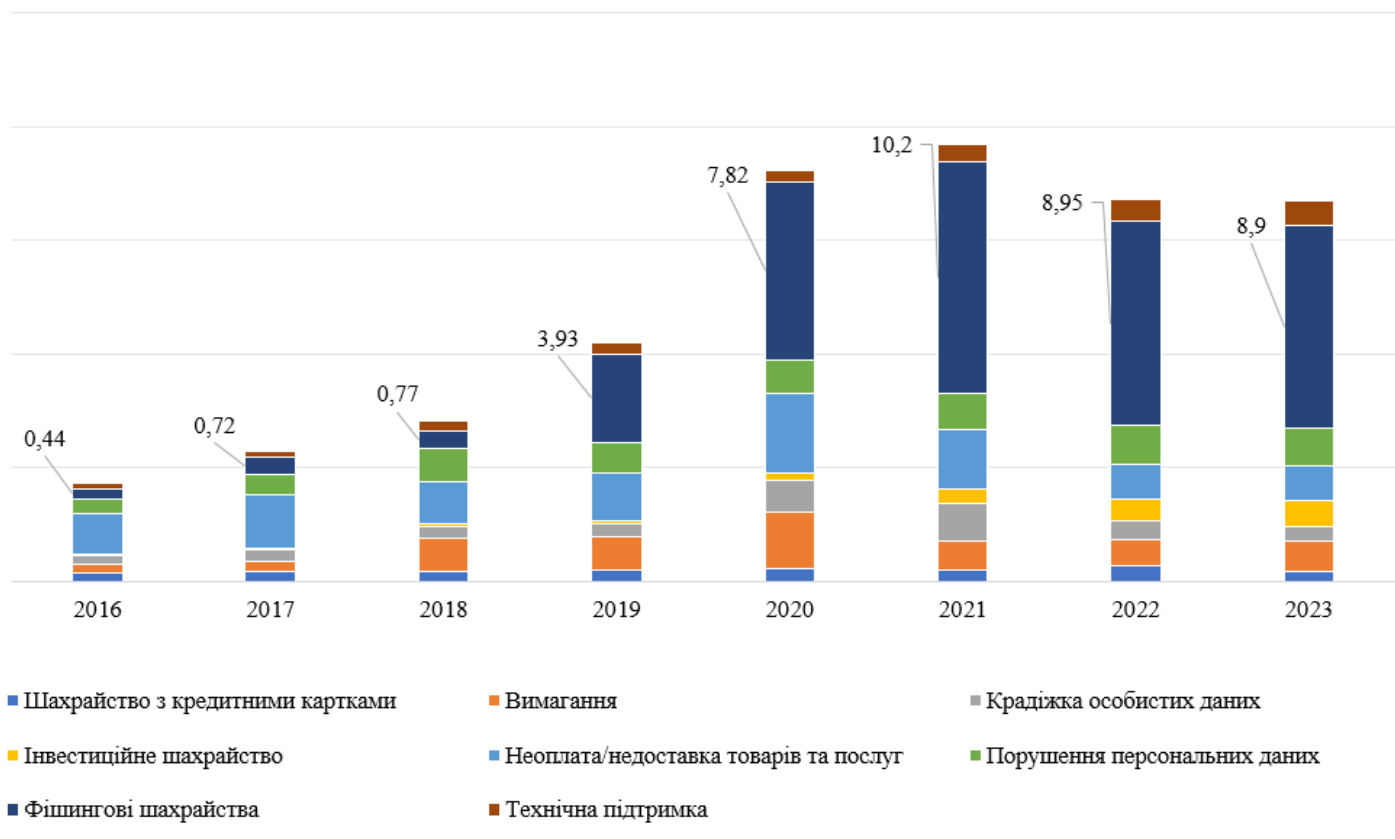

Рис. 2.3. Динаміка кібератак в світі у розрізі видів, 2016-2023 рр., млн. шт.

Джерело: побудовано на основі [203].

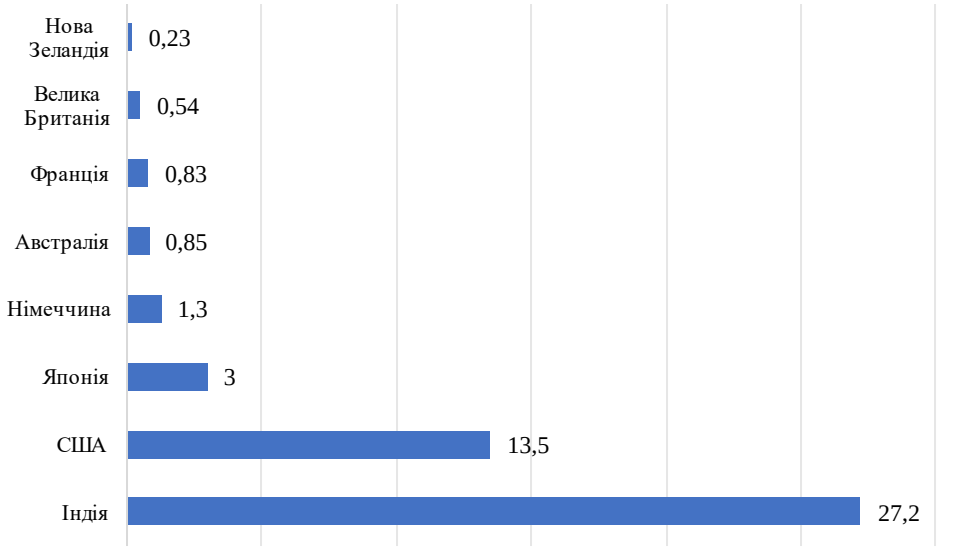

Рис. 2.4. Кількість дорослих, які ставали жертвами крадіжки персональних даних у 2022 р., млн осіб

Джерело: побудовано на основі [22].

Крім того, активізувалися атаки, спрямовані на компанії, які обробляють великий обсяг платіжних операцій. Зловмисники використовують методи зламування систем, які забезпечують електронні платежі, для вилучення коштів або компрометації даних клієнтів. Така діяльність створює значні ризики не тільки для компаній, але й для споживачів, які стикаються з фінансовими втратами та порушують конфіденційність. Враховуючи ці тенденції, боротьба з платіжним шахрайством у 2023 р. вимагала підвищення рівня кібербезпеки на всіх рівнях, включаючи впровадження технологій штучного інтелекту для виявлення аномалій у транзакціях, покращення шифрування даних і посилення закону. На рис. 2.5 представлено показники шахрайства, пов’язані з платежами у 2023 р.

Ключовими чинниками збільшення кількості платіжного шахрайства є поширення методів соціальної інженерії, фішингових атак та використання вразливостей у цифрових платіжних системах. Зростання обсягів онлайн-транзакцій під час пандемії COVID-19 також сприяло активізації шахраїв. У 2023 р. було найбільше зафіксовано повідомлень про шахрайство з кредитними картками близько 114 348 тис. звернень, наступним було звернення щодо дебетових карток та на третьому місці було зафіксовано шахрайство пов'язане з платіжними додатками.

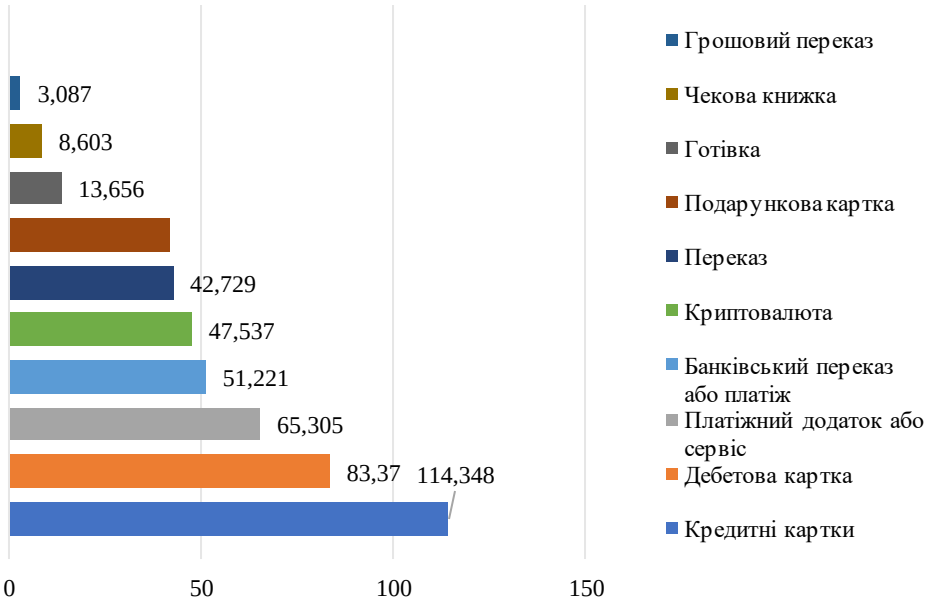

Рис. 2.5. Динаміка кількості випадків шахрайства, пов'язана з платежами у 2023 р., тис. одиниць

Джерело: побудовано на основі [223].

На рис. 2.6 представлено показники атаки зловмисного забезпечення у світі протягом 2015-2023 рр.

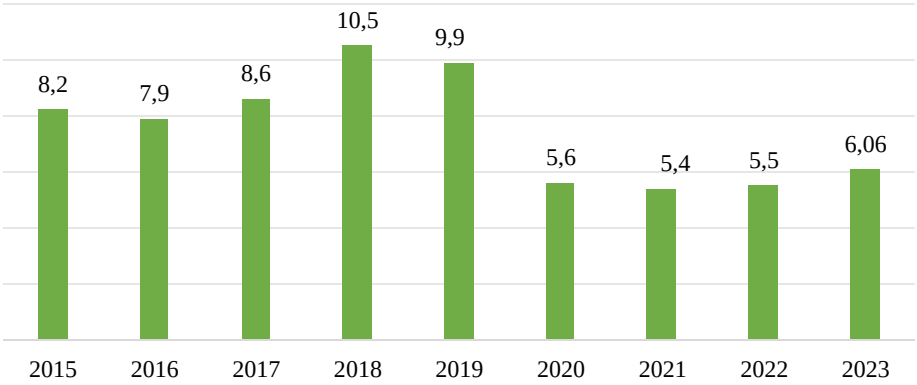

Рис. 2.6. Динаміка атак зловмисного програмного забезпечення у світі, 2015-2023 рр., тис. одиниць

Джерело: побудовано на основі [229].

У 2023 р. кількість атак із використанням зловмисного програмного забезпечення у світі зросла на 10 % порівняно з попереднім роком, досягнувши 6,06 млрд випадків. Найбільший сплеск атак було зафіксовано в 2018 р., коли їхня кількість сягнула 10,5 млрд по всьому світу. Освітній сектор у 2023 р. був найбільш ураженим зловмисним програмним забезпеченням, зокрема щотижня зазначивши в середньому 2046 атак у порівнянні з 2314 атак у попередньому році. На другому місці опинились урядові та військові організації, а за ними – медичні установи. Загалом у 2022 р. освітня галузь зазнала понад п’ять мільйонів атак зловмисного програмного забезпечення [199; 200; 202; 203].

Згідно з дослідженням SonicWall Capture Labs [229] у першій половині 2024 р. кількість зловмисного програмного забезпечення Інтернету речей (IoT) зросла на 107 %, а серед пристроїв, які зазнали кібератак, ці пристрої проводили під атакою в середньому 52,8 години. На наступному рис. 2.7 представлено сектори промисловості у світі, на які найбільше нападають зловмисні програмні забезпечення з листопада 2022 р. по жовтень 2023 р.

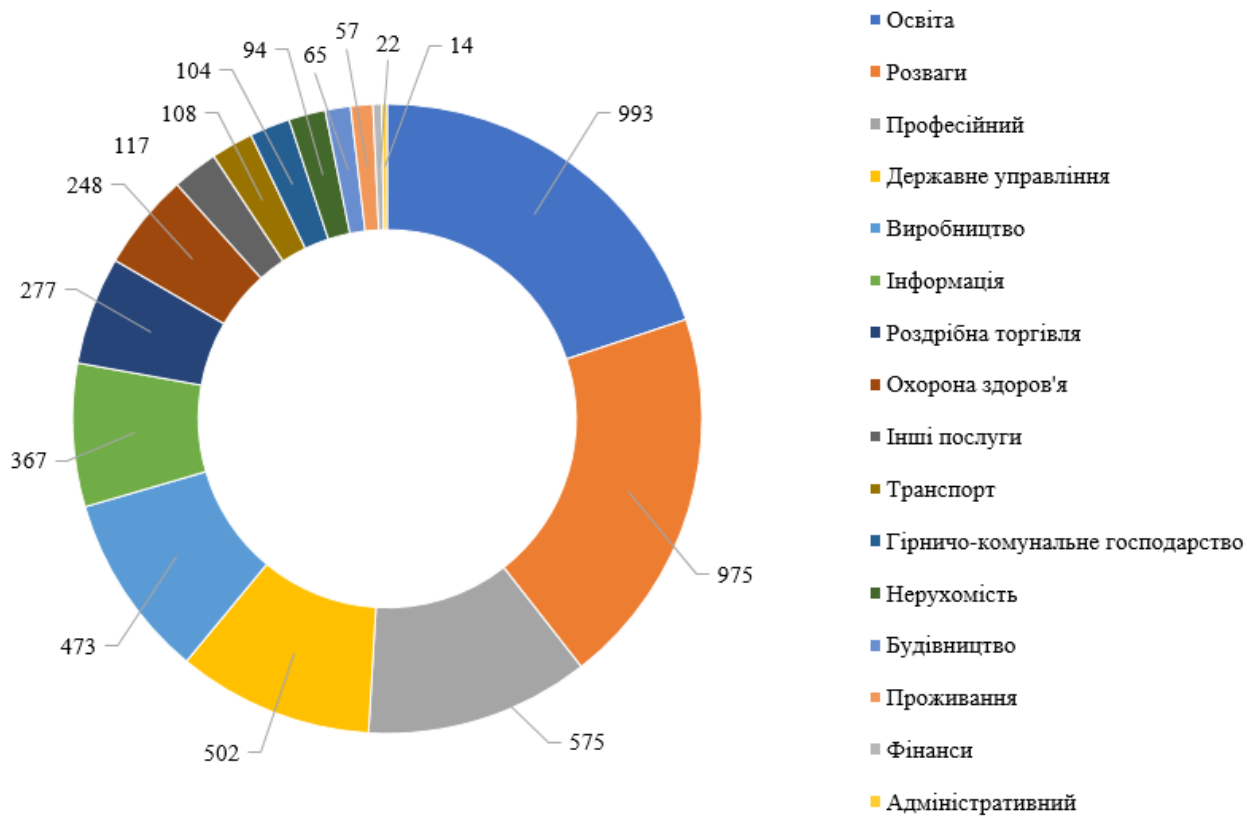

Рис. 2.7. Сектори промисловості у світі, на які найбільше нападають зловмисні програмні забезпечення, листопад 2022 р. – жовтень 2023 р., тис. одиниць

Джерело: побудовано на основі [223].

У період з листопада 2022 р. по жовтень 2023 р. освітній сектор посів перше місце серед глобальних галузей, які найбільше піддаються атакам зловмисного програмного забезпечення. Протягом досліджуваного періоду в галузі сталося більше ніж 993 інциденти зловмисного програмного забезпечення. Друге місце посів сектор розваг та становив понад 975 інцидентів, тоді як професійний сектор посідає друге місце з 575 виявленими атаками зловмисного програмного забезпечення.

У 2023 р. організації з усього світу зафіксували понад 317,59 млн спроб атак програм-вимагачів (рис. 2.8), що на 175,74 млн спроб менше, ніж у попередньому році. Атаки програм-вимагачів зазвичай спрямовані на організації, які збирають великі обсяги даних і є критично важливими. У разі атаки ці організації вважають за краще заплатити викуп за відновлення вкрадених даних, ніж негайно повідомити про атаку. Випадки втрати даних також завдають шкоди репутації компаній, що є однією з причин, чому не повідомляється про атаки програм-вимагачів.

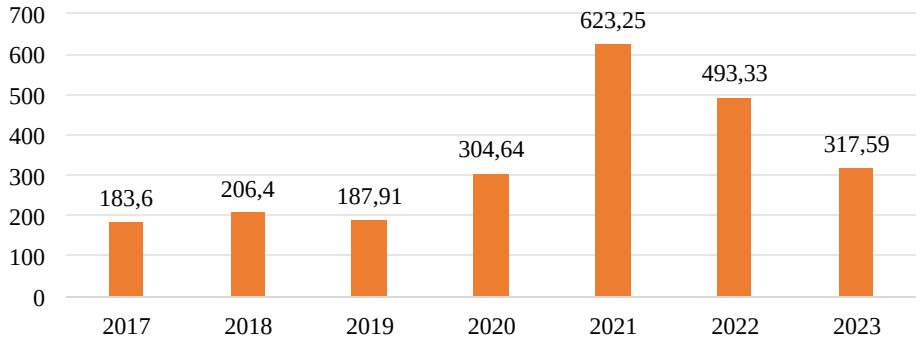

Рис. 2.8. Динаміка спроб атаки програм-вимагачів у світі, 2017-2023 рр., тис. одиниць

Джерело: побудовано автором на основі [250].

На рис. 2.9 зображено частку організацій, які постраждали від атак програм-вимагачів у всьому світі протягом 2018-2023 рр.

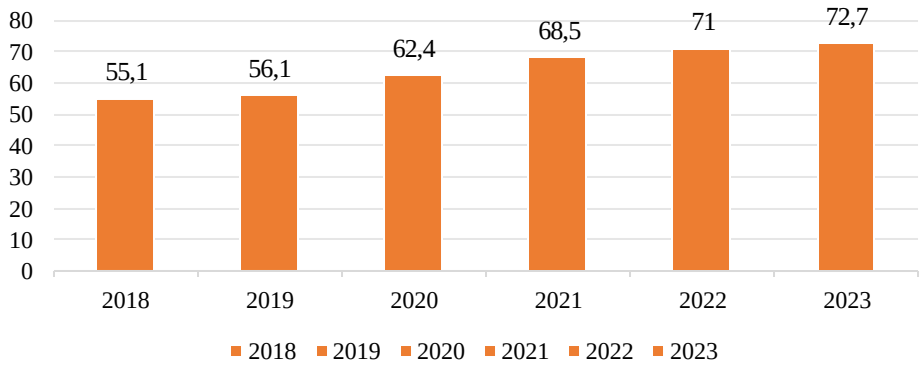

Рис. 2.9. Часта організацій, які постраждали від атак програм-вимагачів у всьому світі, 2018-2023 рр., %

Джерело: побудовано на основі [250].

Станом на 2023 р. понад 72,7 % компаній у всьому світі постраждали від атак програм-вимагачів. Даний показник являє собою збільшення порівняно з попередніми п'ятьма досліджуваними роками і є, безумовно, найвищою зазначеною цифрою. Загалом, починаючи з 2018 р., більше половини респондентів щороку заявляли, що їхні організації стали жертвами програм-вимагачів.

На рис. 2.10 представлено показники розподілу кібератак серед світових галузей у 2023 р.

Найбільша частка зафіксованих кібератак серед світових галузей у 2023 р. було спрямовано на сферу виробництва. Протягом досліджуваного року компанії-виробники зіткнулися з майже чвертю загальної кількості кібератак. На другому місці зосереджені фінансові та страхові організації, що становлять близько 18 %. Професійні, ділові та споживчі послуги посідають третє місце з 15,4 % зареєстрованих кібератак.

На рис. 2.11 зображено показник частки організацій серед країн світу, яким загрожує кібератака у розрізі країн, станом на червень 2023 р.

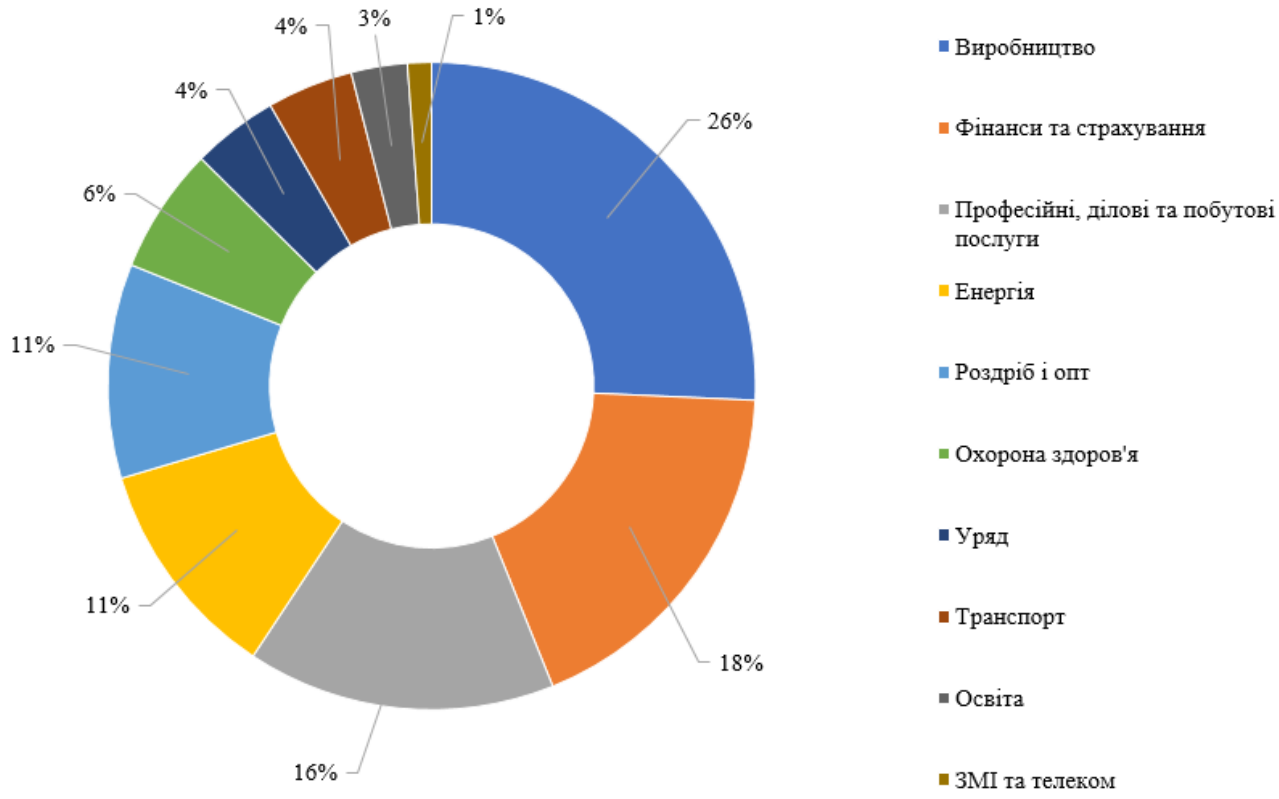

Рис. 2.10. Розподіл кібератак у світових галузях у 2023 р., %

Джерело: побудовано на основі [254-256].

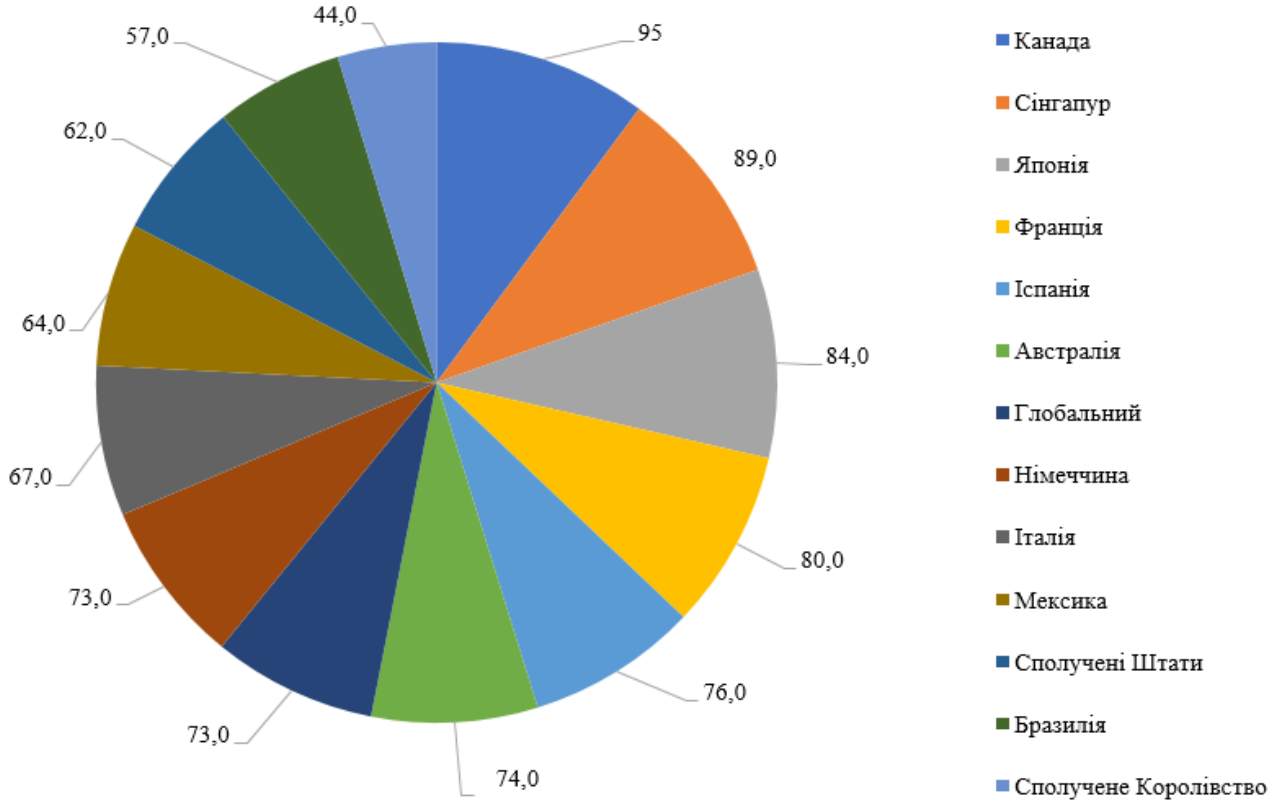

Рис. 2.11. Частка організацій серед країн світу, яким загрожує кібератака у розрізі країн, станом на червень 2023 р., %

Джерело: побудовано на основі [25б].

Серед досліджених країн світу, яким загрожують кібератаки різного виду найбільш вразливою є Канада, понад 95 % організацій були під серйозною загрозою кібератак. У Сінгапурі більшість опитаних членів правління саме понад 89% вважали, що їхні компанії зіткнуться з таким ризиком протягом наступного року. Японські компанії опинилися на третьому місці за рівнем занепокоєння щодо можливості загрози нових кіберзлочинів – близько 84% респондентів.

На наступному рис. 2.12 зображено середню вартість збитків від витоку даних у світі.

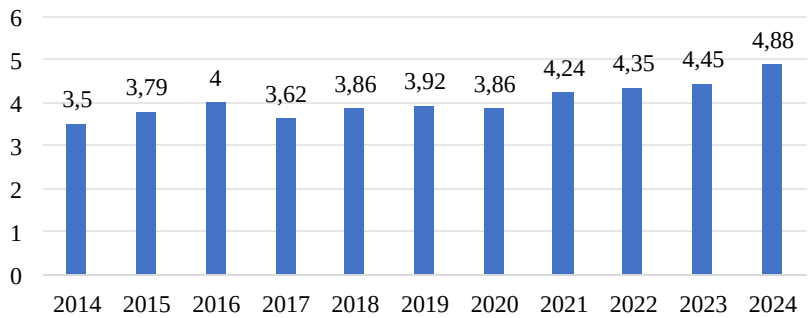

Рис. 2.12. Середня вартість витоку даних у світі, з 2018 р. по лютий 2024 рр., млрд дол. США

Джерело: побудовано автором на основі [256].

Щорічно показник середньої вартості витоку даних збільшується, так у 2023 р. розмір завданих збитків становив близько 4,45 млрд дол. США, в же на кінець лютого 2024 р. розмір витоку даних оцінювався в 4,88 млрд дол. США. Витік даних має жахливі фінансові наслідки, адже вони впливають як на окремих осіб, так і на організації, компанії чи державні установи в цілому.

На рис. 2.13 відображено наслідки втрати конфіденційної інформації для організацій у світі у 2023 р.

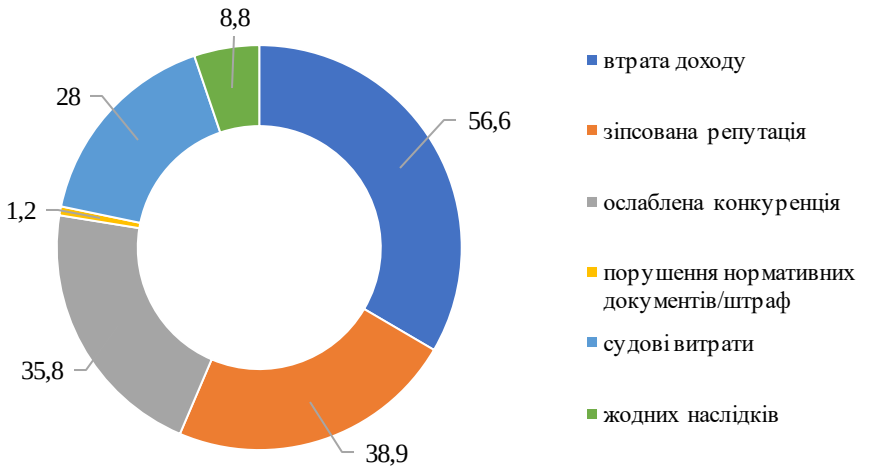

Рис. 2.13. Наслідки втрати конфіденційної інформації для організацій у світі, 2023 р., %

Джерело: побудовано на основі [256].

Серед поширених наслідків для організацій у всьому світі у 2023 р. найбільшу частку займала втрата доходу, що становила понад 56,6 % від загальної структури, на другому місці опинилися зіпсована репутація компанії та послаблення конкуренції, що дорівнюють 38,9 % та 35,8 % відповідно.

Сполучені Штати Америки станом на жовтень 2023 р. стали лідерами за кількість джерел фінансування кібератак (рис. 2.14), забезпечуючи понад 33,7 % від загальної частки атак у світі. Причиною цього явища є розміщення великої кількості серверів на інтернет-користувачів у США, на другому місці знаходиться росія та її частка становить 7,94 % серед представлених країн, на третьому місці зосереджені Франція – 7,26 % та Нідерланди – 7,15 %.

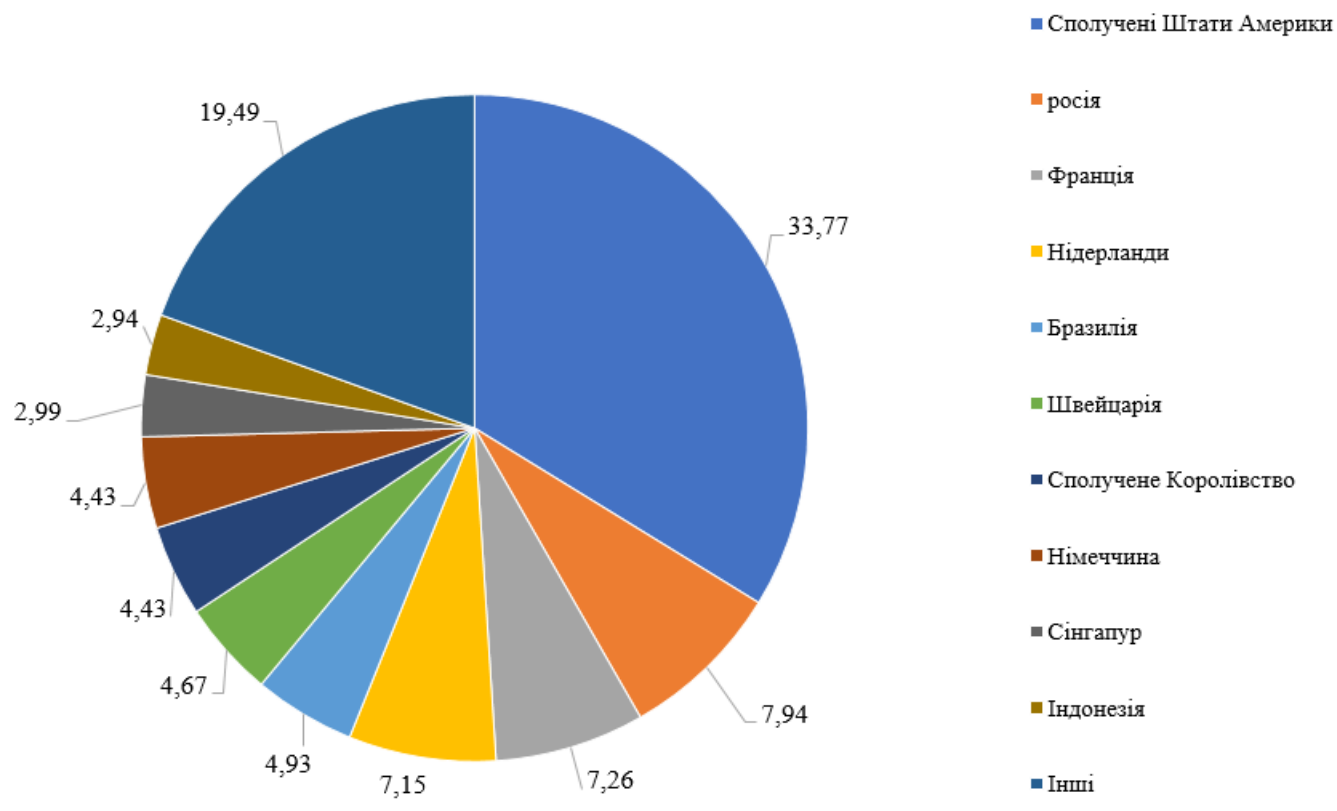

Рис. 2.14. Розподіл джерел кібератак у всьому світі з листопада 2022 р. по жовтень 2023 р. за країнами

Джерело: побудовано на основі [256].

Отже, на основі проведеного аналізу глобального стану кіберзлочинності можна зробити наступні висновки, кількість здійсненних кібератак щорічно зростає, а їх характер стає складнішим, фішингові атаки є лідерами серед кіберзлочинів у світі, із тенденцією до подальшого збільшення. У 2023 р. кількість атак із використанням зловмисного програмного забезпечення досягла 6,06 млрд дол. США, це відображає масштабність проблеми. Глобальні фінансові втрати від кіберзлочинності у 2023 р. склали понад 7,1 трлн дол. США та до 2029 р. ці втрати можуть досягти 15,63 трлн дол. США. Основні наслідки для організацій від втрати конфіденційної інформації є втрата доходу (56,6 %), погіршення репутації (38,9 %) та послаблення конкурентних позицій (35,8 %). Найбільш вразливими залишаються освітній сектор, урядові структури, сектор розваг та фінансові установи. У цих галузях є значна кількість інцидентів із використанням зловмисного програмного забезпечення. США, росія, Франція та Нідерланди є провідними країнами джерел походження кібератак, при цьому Канада та Сінгапур демонструють найвищий рівень непокоєння щодо можливих атак.

Доведено, що боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Зокрема, діяльність таких міжнародних інституцій, як Інтерпол та Європол, є одним з ефективних засобів протидії кіберзлочинності на міжнародному рівні. Встановлено, що захист від кіберзагроз залежить від усвідомлення всіх учасників цифрового простору того, що забезпечення безпеки є спільною відповідальністю. Відсутність обміну інформацією про кібератаки між державними організаціями, приватними підприємствами, бізнесом та фізичними особами, а також глибоких досліджень, ефективних інструментів протидії та організованих консультацій значно підвищує ризик

виникнення кіберзагрози. Для протистояння хакерським діям необхідна тісна співпраця між компаніями, організаціями та урядовими структурами, зокрема у сфері обміну інформацією про загрози та новітні методи захисту. Крім того, впровадження освітніх програм з кібербезпеки для широкої аудиторії сприятиме підвищенню рівня відомості користувачів і зниженню ризиків, пов'язаних із людським фактором.

2.2. Аналітичний вимір кібербезпеки та кіберзлочинності у світовому просторі

За останні роки глобальна кіберзлочинність стала однією з найбільших загроз сучасної економіки, створюючи значні виклики для державних і приватних інституцій. Ці загрози проявляються в різних формах, включаючи окремі випадки або скоординовані дії, атаки на основі програмного забезпечення, фізичне втручання, а також зовнішні або внутрішні порушення, спрямовані на національні цифрові мережеві системи. Експерти *Cybersecurity Ventures* оцінюють втрати від кіберзлочинності у 2024 р. у понад 9,5 трлн дол. США. Якщо даний розмір збитків виміряти як країну, то кіберзлочинність може бути третьою за величиною економікою світу після Китаю та Сполучених Штагів Америки. За прогнозами даної світової організації збитки від кіберзлочинності зростуть на 15 % протягом двох наступних років та дорівнюватимуть 10,5 трлн дол. США у 2025 р. Варто зазначити, що у 2016 р. сума збитків від кібератак становила 3 трлн дол. США [199].

Згідно даних звіту, *Norton Cyber Safety Insights Report* [236] у 2023 р. понад 595 млн дорослих людей стикалися з кіберзлочинністю, а 463 млн осіб заявили, що у 2022 р. стали

особисто жертвами кібератак. При цьому понад 54 % споживачів у всьому світі повідомили, що стикалися з кіберзлочинністю, а майже 2 з 5 респондентів стали жертвами у 2022 р. Середній показник втрат від кіберзлочинності становив близько 242 дол. США на особу. Крім того, кіберзлочинність завдала не лише фінансової шкоди, але й для усунення даних негативних наслідків жертви в середньому витратили 6,6 годин свого часу. Лідерами серед кіберзагроз стали шкідливе програмне забезпечення – 21 %, виток даних – 15 % та несанкціонований доступ до електронної пошти – 13 %.

Ключовим елементом аналізу економічних наслідків кіберзлочинності є вивчення ролі індексів кібербезпеки, які характеризують оцінку готовності держави до протидії загрозам. Ці індекси враховують такі аспекти, як законодавча база, технічні засоби захисту, організаційні стратегії та міжнародне співробітництво. Дані свідчать, що країни з високими показниками кібербезпеки зазнають менших економічних витрат з тими, де рівень захисту залишається низьким. Необхідними інструментами для оцінки готовності країни до захисту даних в кіберпросторі в світі застосовуються наступні показники:

– Індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index, IDI);

– Глобальний індекс кібербезпеки (GCI);

– Національний індекс кібербезпеки (NCSI);

– Національний індекс кіберпотужності (National Cyber Power Index, NCPI);

Індекс розвитку ІКТ (IDI) – це всесвітньо визнаний показник, розроблений Міжнародним союзом електрозв’язку (ITU) для оцінки та порівняння розвитку інформаційно-комунікаційних технологій (ІКТ) у різних країнах. Він оцінює готовність до ІКТ, їх

використання та навички, щоб отримати уявлення про цифровий розрив і технологічний прогрес у всьому світі [203].

На рис. 2.15 представлено показники Індексу розвитку інформаційно- комп'ютерних технологій у 2023 р. Лідерами рейтингу ІКТ у 2023 р. став Кувейт, Фінляндія та Естонія з показником 100, 98,1 та 97,9 відповідно. Найнижчий показник Індексу розвитку ІКТ зосереджено у ЧАД та становить 21,3.

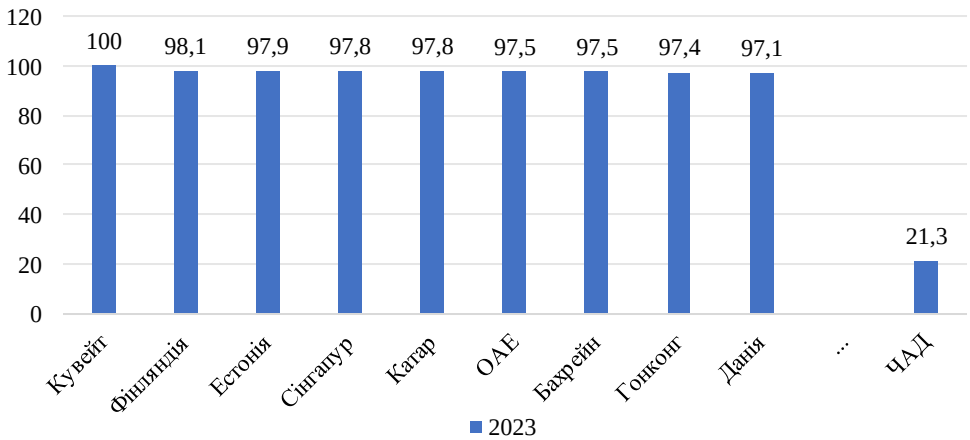

Рис. 2.15. Індекс розвитку інформаційно-комунікаційних технологій (IDI), 2023 р.

Джерело: побудовано на основі [235].

Дані свідчать про значний розрив у рівнях розвитку інформаційно-комп'ютерних технологій між різними країнами світу. Високі показники, продемонстровані Кувейтом, Фінляндією та Естонією, пояснюються значними інвестиціями в цифрову інфраструктуру, впровадженням інноваційних технологій та високим рівнем цифрової грамотності населення. З іншого боку, найнижчий показник, зафіксований у Чаді, демонструє серйозні обмеження в доступі до сучасних технологій, недостатнє фінансування сфери ІКТ і низький рівень освіти в галузі цифрових

навичок. Такий дисбаланс підкреслює необхідність глобальних зусиль для зменшення цифрового розриву, зокрема через міжнародні програми підтримки, трансфер технологій та стимулювання розвитку цифрової грамотності.

На рис. 2.16 представлено показник Глобального індексу у 2023 р.

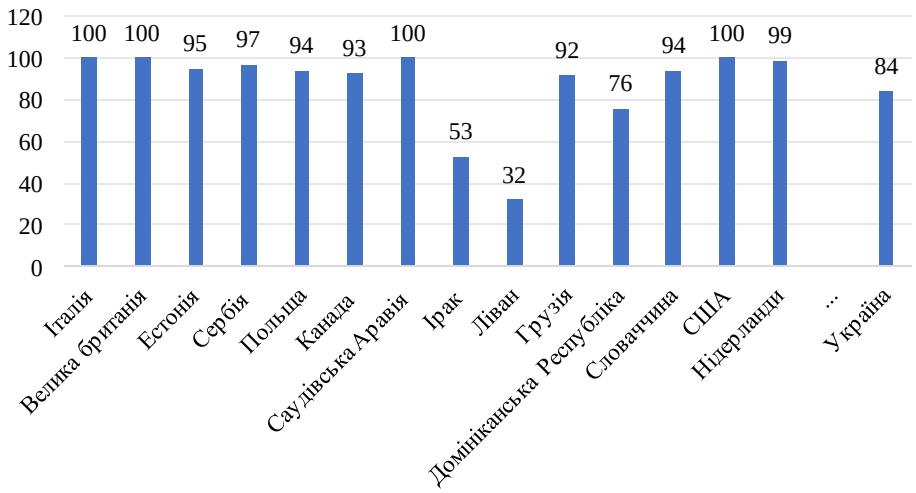

Рис. 2.16. Глобальний індекс кібербезпеки у світі (GCI), 2023 р.

Джерело: побудовано на основі [235].

Дослідивши Глобальний індекс кібербезпеки можна зробити висновок, що у 2023 р. рейтинг очолили США, Італія, Велика Британія, Єгипет, Саудівська Аравія та Португалія, Корея з оцінкою 100 балів, відповідно зайнявши лідируючу першу позицію. Друге місце розділено між такими країнами, як: Нідерланди та Йорданія ,Сінгапур, Франція, Індія та третє місце посіла Естонія. До першої десятки належать: Сербія, Іспанія, Малайзія, Литва, Канада, Австралія, Бельгія, Гана, Польща та Словаччина. Україна посіла 78 місце з показником 83,93%.

Глобальний індекс кібербезпеки (GCsI) – це комплексний показник, який вимірює рівень кібербезпеки країни, розроблений за ініціативою ITU Global Cy GCsI розраховується з 2017 р. для 194 країн світу. Глобальний індекс кібербезпеки (GCI) [240] дозволяє здійснити комплексну оцінку кібербезпеки всіх країн світу за п'ятьма складовими чинниками:

– юридичні (legal measures) – вимірювання законів і нормативних актів щодо кіберзлочинності та кібербезпеки;

– технічні (technical measures) – технічні можливості у сфері кібербезпеки;

– організаційної підготовленості (organizational measures) – вимірювання національних стратегій та організацій, які впроваджують кібербезпеку;

– розвитку освітнього та дослідницького потенціалу країни (capacity development) – наявність науково-дослідних, освітніх та підготовчих програм, а також сертифікованих фахівців та держустанов, що сприяють нарощуванню потенціалу у сфері інформаційної безпеки;

– готовності до співпраці (cooperative measures) – вимірювання партнерства між агентствами, фірмами та країнами.

На рис. 2.17 представимо у графічному вигляді оцінку рівня кібербезпеки з урахуванням п'яти критеріїв для України та порівняємо зі складовими індексу кібербезпеки сусідніх країн, зокрема: Польща, Румунія, Словаччина та Молдова.

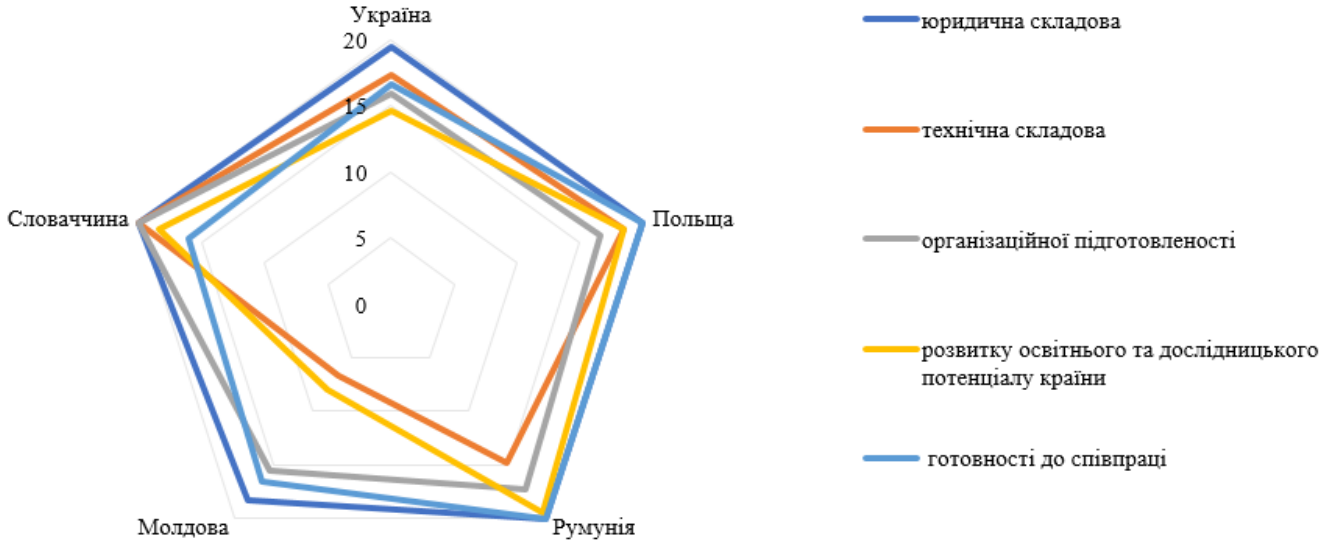

Рис. 2.17. Оцінка рівня кібербезпеки за основними критеріями Глобального індексу (GCI) у 2024 р.

Джерело: побудовано автором на основі [240].

Аналіз за кількісними показниками з використанням складових критеріїв глобального індексу кібербезпеки дозволяє зазначити, що за критерієм організаційної підготовленості показник України (13,6) перевищує аналогічний показник Молдови (15,51). Позитивну ситуацію можна спостерігати й за показником розвитку освітнього та дослідницького потенціалу країни – показник України (14,61) перевищує аналогічний показник Молдови (8,04). За всіма іншими показниками спостерігається відставання від аналогічних показників сусідніх країн.

Національний індекс кібербезпеки (NCSI), який запропоновано проєктною групою Академії електронного урядування м. Таллінн, Естонія [240]. Динаміку NCSI України та її позиціонування відносно інших країн світу наведено на рис. 2.18.

Індекс базується на чотирьох ключових категоріях, які охоплюють різноманітні аспекти кіберзахисту, таких як: законодавча база – нормативно-правові акти, положення, накази тощо; організаційна інфраструктура, яка забезпечує кібербезпеку – існуючі організації, відділи тощо; формати співпраці – комітети, робочі групи тощо; результати – політика, вправи, технології, вебсайти, програми тощо. Оцінка NCSI показує, який відсоток країна отримала від максимального значення показників. Оцінка індексу демонструє, наскільки країна наблизилася до максимально можливого рівня ефективності у впровадженні заходів кібербезпеки. Кінцева оцінка виражається у відсотках, де максимальний бал становить 100 (або 100 %).

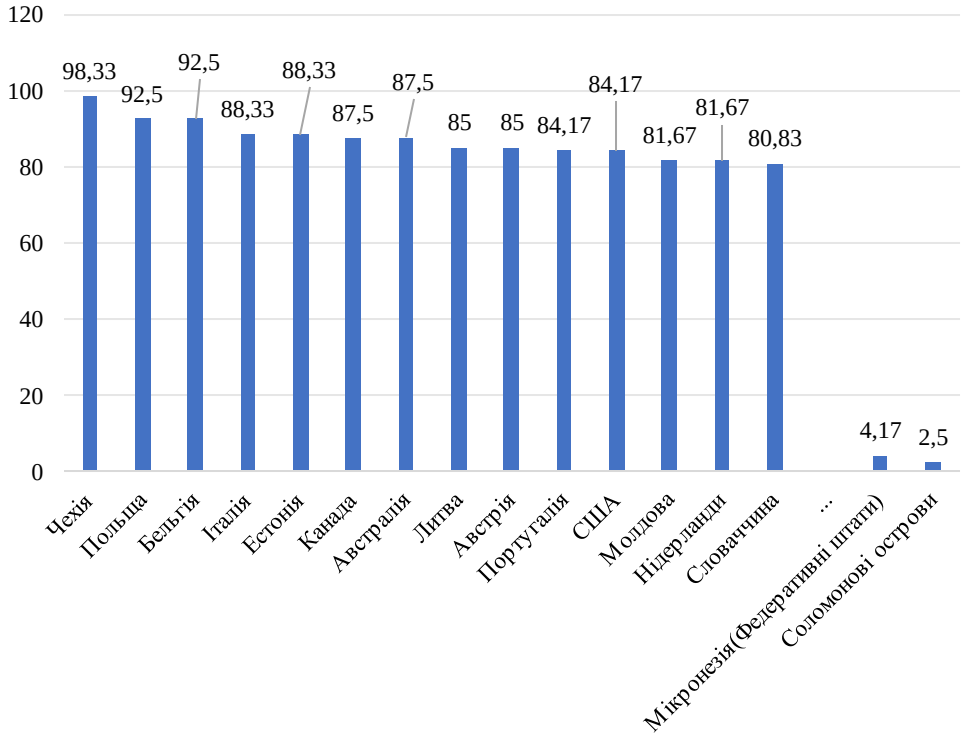

Рис. 2.18. Динаміка країн за Національним індексом кібербезпеки(NCSI) у 2023 р.

Джерело: побудовано на основі [240].

Чехія посіла перше місце серед представлених країн в рейтингу показника Національного індексу кібербезпеки у 2023 році, показник дорівнює близько 98,33% зі 100 можливих, на другому місці зосереджена Польща та Бельгія з показником 92,5 %. На третьому місці знаходиться Італія та її показник становить 88,33 % Лідерство Чехії зумовлено сильними нормативними ініціативами та надійною кіберінфраструктурою. Цифровий розвиток також демонструє стабільний прогрес, хоч і менший, ніж кібербезпека. Найменші показники серед досліджених країн зосереджено у Мікронезії та Соломонові острови. Дані свідчать про

слабкість рівня кібербезпеки, обмежені урядові ініціативи та недосконалі стратегії захисту критичної інфраструктури.

Важливим показником разом з Національним індексом кібербезпеки є рівень цифрового розвитку (рис. 2.19), адже позитивна різниця між цими показниками свідчить про розвиток кібербезпеки країни знаходиться на досить високому рівні. Негативний результат показує, що цифрове суспільство країни є більш розвиненим, ніж національна сфера кібербезпеки. Даний показник розраховується відповідно до Індексу розвитку електронного уряду (EGDI) та Індексу готовності до мереж (NRI). DDL – це середній відсоток, який країна отримала від максимального значення обох індексів [240].

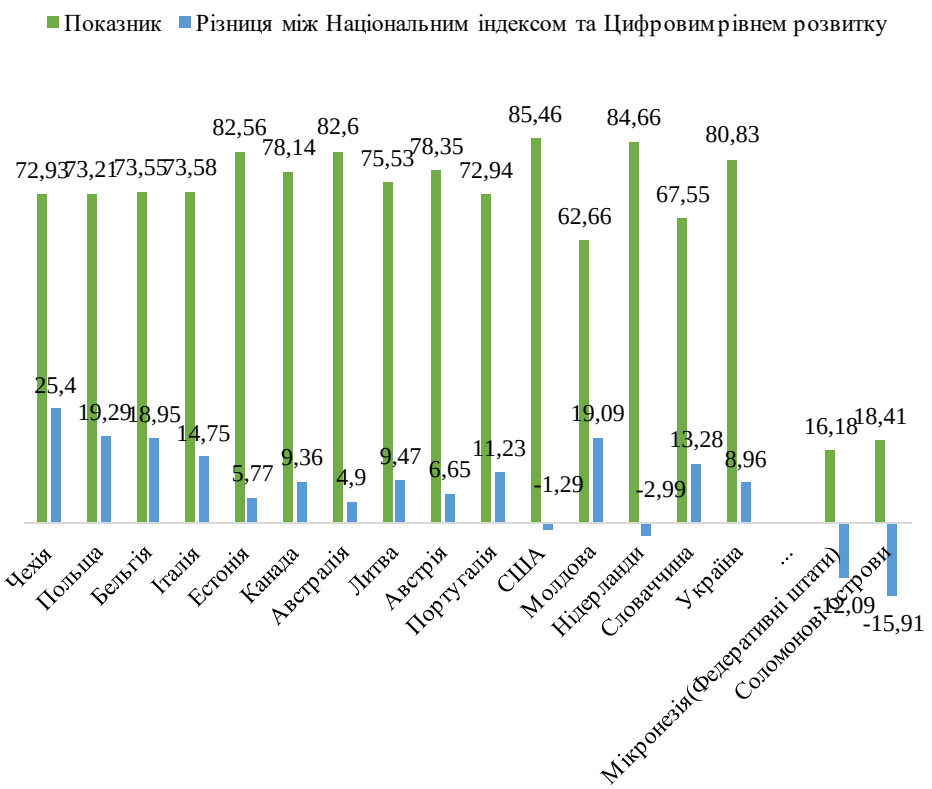

Рис. 2.19. Динаміка країн за цифровим рівнем розвитку у 2023 р.

Джерело: побудовано на основі [240].

США має незначний від'ємний баланс (-1,29) між показником та рівнем цифрового розвитку, це вказує що цифровий розвиток випереджає інвестиції у кібербезпеку. Китай теж має різницю – 17,94, цей розрив демонструє значну потребу в корисних заходах кібербезпеки. Країни з меншими розривами (наприклад, Чехія) демонструють більшу ефективність у використанні цифрових технологій без компромісів у безпеці.

На наступному рис. 2.20 зображено виконання індексу NCSI Україною у 2023 р.

Рис. 2.20. Частка виконання індексу NCSI Україною у 2023 р. у розрізі індикаторів, %

Джерело: побудовано на основі [240].

Виконання індексу NCSI Україною передбачено наступними складовими:

– військовий кіберзахист – виконано на 100%. Даний показник надає інформацію чи мають збройні сили країни (або інші фінансовані урядом та організовані військовими організаціями, яким доручено територіальну оборону) визначені організації, які

пов'язані або з кібероперaціями, або з кібербезпекою військових операцій, з відповідними завданнями та мандатів;

– боротьба з кіберзлочинністю – виконано на 100 %. Індикатор відстежує, чи криміналізовані національним законодавством наступні кіберзлочини: навмисний доступ без права до комп'ютерної системи (шляхом порушення заходів безпеки) (незаконний доступ); умисне перехоплення з використанням технічних засобів непублічної передачі комп'ютерних даних без права (незаконне перехоплення); навмисне пошкодження, видалення, погіршення, зміна або приховування комп'ютерних даних без права (втручання в дані); навмисне серйозне перешкоджання без права функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, видалення, погіршення, зміни чи приховування комп'ютерних даних (системне втручання); та навмисне вчинення конкретних дій підготовчого характеру з використанням певних пристроїв або доступу до даних, які будуть використані для вчинення кіберзлочинів, згаданих вище (неправомірне використання пристроїв);

– кіберкризове управління виконано на 56 % зі 100 %. Індикатор вимірює наявність національного кризового плану для боротьби з широкомасштабними кібератаками, інцидентами або значними загрозами;

– реагування на кіберінциденти – виконано на 64 % зі 100 %. Індикатор відстежує наявність національного CSIRT/CERT/CIRT у країні. Згідно з визначенням Університету Карнегі-Меллона, NCSI визнає національними CSIRT ті CERT, які визначені країною чи економікою як відповідальні за кіберзахист країни чи економіки. Такі національні CSIRT можуть бути розташовані в уряді чи за його межами, але мають бути спеціально визнані урядом як такі, що мають загальнонаціональні повноваження та відповідальність;

– захист персональних даних – виконано на 100%. Показник відстежує наявність національного законодавства, яке встановлює принципи обробки даних, права особи (суб'єкта даних) щодо їхніх даних, а також зобов'язання та відповідальність контролерів і обробників даних;

– аналіз кіберзагроз та підвищення обізнаності – виконано на 75 %. Даний показник оцінює спроможність і практику проведення оцінок кіберзагроз і тенденцій на національному рівні. Оцінки можуть, наприклад, складатися встановленою державною установою чи підрозділом (наприклад, департаментом чи агентством) або міжвідомчою спільною робочою групою;

– кібербезпека цифрових трансформацій – виконано на 83 %. Даний показник є національно визнане рішення, яке дозволяє безпечно та надійно ідентифікувати осіб під час онлайн-транзакцій. Таке рішення повинно, як мінімум, бути доступним для взаємодії з організаціями державного сектору з можливістю застосування в приватному секторі;

– кібербезпека критичної інформаційної інфраструктури – виконано на 75 %. Показник вимірює наявність законодавчо встановленої основи або механізму для ідентифікації компонента інформаційної інфраструктури КІ або основних послуг;

– дослідження та розробка кібербезпеки – виконано на 100 %. Показник вимірює участь уряду в дослідженнях і розробках у сфері кібербезпеки, що підтверджується офіційним визнанням та/або державним фінансуванням і підтримкою відповідної дослідницької програми;

– освіта та професійний розвиток – виконано на 60 %. До сфери застосування цього показника входять компетенції з кібербезпеки в системі державної освіти, тобто найдоступнішій формі початкової освіти, доступній в країні;

– внесок у світову кібербезпеку – виконано на 67 %. Цей показник оцінює готовність країни фінансувати, організовувати або іншим чином сприяти проекту(ам) з розбудови потенціалу, спрямованому на конкретні країни або групу країн;

– політика кібербезпеки – виконано на 100 %. Цей показник визначає, чи було офіційно покладено відповідальність за кібербезпеку на найвищий урядовий чи політичний рівень.

Невиконання деяких складових свідчить про необхідність вдосконалення національних кризових навчань щодо кібербезпеки та відсутність повної інтеграції до міжнародних кіберкризових навчань. Брак участі з міжнародними партнерами у спільних навчаннях з міжнародними партнерами знижує ефективність у протидії масштабними кіберзагрозами. Відсутність кадрів у сфері кібербезпеки збільшує ризики для загрози критичної інфраструктури та національної безпеки. Регулярні перевірки щодо кіберризиків відсутні або ж є неефективними на державному рівні що призводить до погіршення кіберкризового управління в цілому.

Для оцінки кіберпотужності держави використовується аналітичний інструмент – Національний індекс кіберпотужності (рис. 2.21) розроблений дослідницькою групою з Belfer Center for Science and International Affairs (Гарвардський університет), цей індекс дозволяє аналізувати як можливості, так і амбіції країни у сфері кіберпростору. Він складається з 98 показників, які оцінюють наступні стратегічні напрями: кібероборона, кібернапад, регулювання, технологічна розбудова, економічна кіберпотужність тощо.

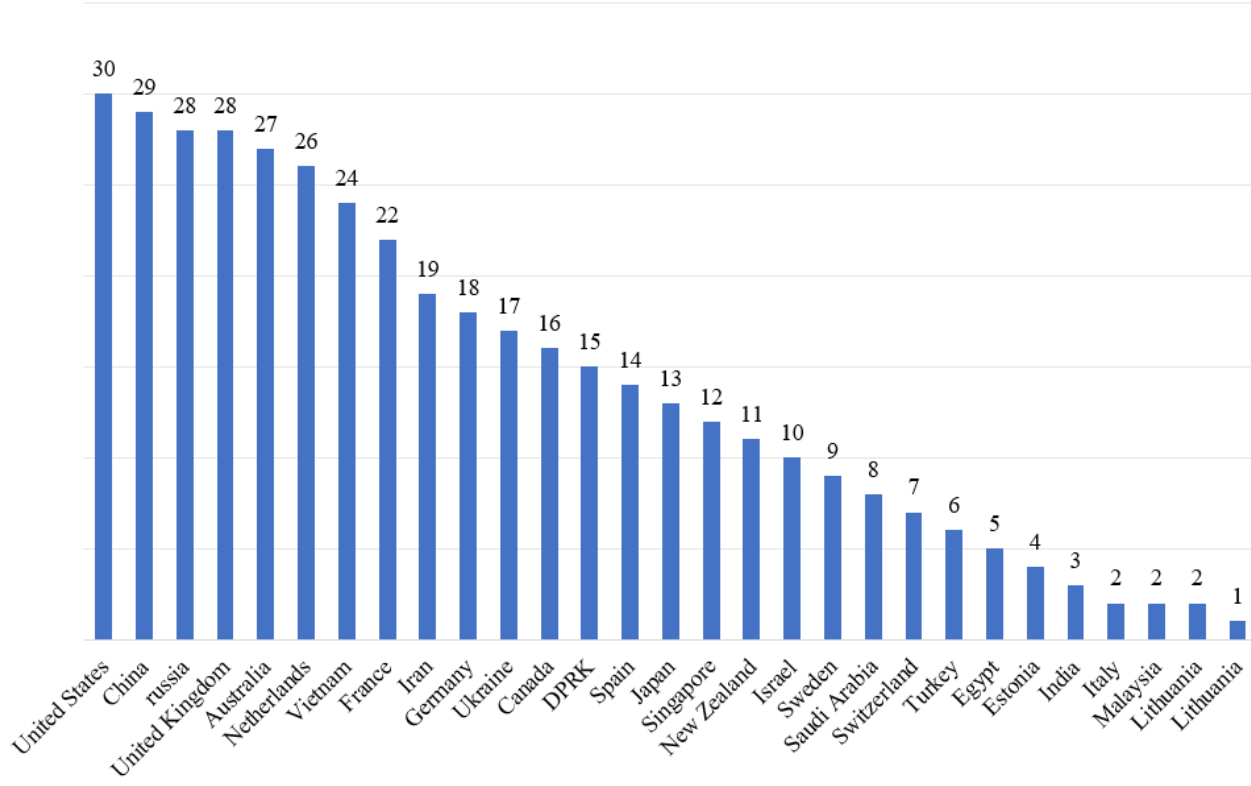

Рис. 2.21. Національний індекс кіберпотужності у 2022 р.

Джерело: побудовано на основі [261].

Лідером серед досліджених країн щодо Національного індексу кіберпотужності є Сполучені Штати Америки, Китай знаходиться на другому місці, на третьому місці знаходиться росія. Свою першість серед інших країн США забезпечує завдяки великому бюджету, високотехнологічним розробкам та глобальній координації. Також до десятки лідерів ввійшли наступні країни: Велика Британія, Австралія, Нідерланди, В'єтнам, Франція, Іран та Корея. Україна зайняла 12 місце, хоча не потрапила до ТОП-10, проте здійснила різке переміщення свого показника з 29 місця до 12 за допомогою збільшення рівня кіберзахисту розвідки та руйнівної діяльності. Україна знаходиться на позиціях разом з Канадою та Німеччиною.

Отже, проаналізувавши основні показники кіберзлочинності, можна зробити висновок, що зберігається тенденція щодо збільшення негативних фінансових наслідків від кіберзагроз. Необхідними заходами є впровадження комплексних і скоординованих заходів щодо загрози кіберзлочинності на національному та міжнародному рівнях. Це забезпечить активну участь органів влади, бізнесу та суспільства для запобігання кіберінцидентам. На основі аналізу позицій України в міжнародних рейтингах кібербезпеки та вивчення індикаторів, що лежать на основі глобальних індексів NCSI, GCI та NCPI, визначено сильні та слабкі сторони кіберспроможності країни. До перспективних напрямків віднесено вдосконалення систем захисту інформації об'єктів критичної інфраструктури, спираючись на найкращі світові практики, а також координацію дій з міжнародними організаціями у протидії загрозам, що працюють в умовах розвитку цифрової економіки та інформатики.

2.3. Оцінка наслідків кіберзагроз та кібервійни росії проти України

В сучасних умовах розвитку кіберпростір надає багато нових можливостей, але й одночасно є ареною для створення глобальних загроз, яким не властиві кордони. Кібератаки стали невід' ємною частиною сучасних гібридних війн. Вони застосовуються для підриву державних інститутів, створення економічного тиску, дестабілізації суспільства та інформаційного маніпулювання. Нині завдати шкоди державним установам або критичній інфраструктурі можна не лише фізично, але й дистанційно за допомогою хакерських дій спрямованих на руйнування цілісності, конфіденційності та доступності інформаційних ресурсів.

Починаючи з 2014 р., росія активно здійснює масові кібератаки проти України, спрямовані на підрив економічної стабільності, руйнування критичної інфраструктури та дестабілізацію суспільства. З початком повномасштабного вторгнення росії в Україну у 2022 р. масштаби та інтенсивність кібероперацій значно зросли. Атаки на державні установи, енергетичний сектор, медіа та банківську систему стали регулярною практикою, доповнюючи фізичні військові дії. Щоденно російськими хакерами здійснюється більше ніж десять кібератак на Україну. Для економіки України спричинені кібератаки стали надзвичайно руйнівними, а особливо негативно вплинули на об'єкти критичної інфраструктури.

Лише у 2023 р. в Україні було зафіксовано понад 2500 тис. кіберінцидентів, що на 15,9% більше ніж у 2022 р. За даними урядової організації реагування на комп'ютерні надзвичайні події CERT-UA, яка займається запобіганням, виявленням і реагуванням на кібератаки та кіберінциденти було зареєстровано понад 347 атак

на урядові організації та уряд, близько 276 атак на органи місцевої влади, 175 – на організації у секторі безпеки та оборони і 127 атак на приватні організації [35].

Кібератаки стали фактично віртуальною зброєю, яка синхронізується з фізичними бойовими діями на території України. Росія застосовує атаки на інформаційні системи, просуває у медіапросторі дезінформаційну кампанію, шпигунські програми не лише паралізують роботу інфраструктури, а й формують негативне інформаційне поле серед населення. Незважаючи на виклики, які зараз стоять перед Україною, держава демонструє високий рівень стійкості, зокрема розвиваючи системи кіберзахисту, отримуючи підтримку від міжнародних партнерів та запроваджує на законодавчому рівні нові стратегічні документи протидії існуючим кібератакам.

Так, у Стратегії кібербезпеки України вказується, що "Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури"[139].

Сучасні кібератаки стають дедалі складнішими та небезпечнішими, створюючи серйозні загрози для критично важливої інфраструктури. Хакери зосереджуються на виявленні вразливостей у системах управління і застосовують інноваційні засоби, включаючи багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети для розподілених атак (DDoS), а також втручання у хмарні сервіси й виробничі

системи через ланцюги постачання. З огляду на розвиток штучного інтелекту, масштаби й наслідки таких загроз у найближчі 5-10 років можуть значно зрости, створюючи нові виклики для глобальної кібербезпеки.

Дослідження тематики кібервійни у контексті російсько-української війни обумовлена необхідністю аналізу ролі кіберзагроз у сучасних війнах, вивчення їх впливу на економіку, обороноздатність та суспільство. Важливо також визначити стратегічні підходи до протидії кібератакам, що можуть бути використані іншими країнами для захисту в умовах зростаючої цифровізації. Необхідним завданням є здійснення аналізу масштабів та наслідків кібервійни як частини повномасштабної агресії росії проти України, розглядаючи ключові напрямки кібератак, механізми захисту та перспективи розвитку національної кібербезпеки.

Важливо відмітити, що у світовій спільноті кібератаки здійснюються, як поодинокими хакерами, так і професійними хакерськими організаціями, які підпорядковуються безпосередньо діючому уряду. Агресивна війна росії проти України висвітлює ключові тенденції у сфері кіберзагроз, а також нові вектори атаки та вразливості, що відображаються в сучасному цифровому середовищі. Кібератаки та операції спрямовувалися на знищення даних і функціональних систем, порушення роботи критично важливої інфраструктури й основних послуг, контроль над інформаційним простором, викрадання великих обсягів даних, здійснення розвідки та шпигунства. Крім того, були реалізовані операції впливу, включаючи дезінформаційні кампанії, які підтримували довіру до публічної інформації та інституцій, створювали хаос і дискредитували воюючі сторони.

Основними видами кібератак, які застосовуються зловмисниками проти інших держав є: деструктивні атаки, підривні атаки, озброєння даними, дезінформація. Визначення даним видам атак є наступними:

– деструктивні атаки – це кібератаки, спрямовані на безповоротне видалення даних або пошкодження систем таким чином, що їхнє відновлення стає неможливим. Такі атаки можуть мати тривалі наслідки для організацій, особливо якщо вони не мають доступу до резервних копій або можливості відновлення систем. Прикладом є використання шкідливого програмного забезпечення для знищення даних, спрямованого на українські урядові установи та інші важливі сектори [233];

– підривні атаки – це кібератаки, спрямовані на дестабілізацію роботи служб і порушення операцій. Вони мали місце під час конфлікту, зокрема, проти українських організацій на початкових етапах вторгнення, а також проти державних установ у деяких країнах НАТО у зв'язку з оголошеннями про загрози громадській безпеці чи економіці. Найпоширенішим типом таких атак стали розподілені атаки на відмову в обслуговуванні (DDoS), які особливо часто вражали державний і фінансовий сектори [233];

– озброєння даними – кібератаки, що призводять до крадіжки або витоку даних або отримання даних з метою шпигунства, спостереження або розвідки. Хоча останні є очікуваною діяльністю в кіберпросторі в контексті війни та геополітики, перші – це атаки, які активно здійснюються колективами суб'єктів в ім'я активізму. Дані, що стосуються приватних і громадських організацій, викрадаються і публікуються в Інтернеті з небаченою раніше швидкістю. Дані стали зброєю в операціях зі зламу та витоку [233];

– дезінформація – інформаційні операції, засновані на дезінформації та пропаганді, не є новими методами ведення війни,

але кіберпростір дозволив розгортати їх з безпрецедентною швидкістю і масштабами. Атаки, спрямовані на поширення неправдивої інформації та пропаганди, стали характерною рисою цього збройного конфлікту. Від SMS-спаму, що поширює неправдиву інформацію про технічні несправності банкоматів, до кібератак на телеканали, під час яких неправдива інформація відображається у стрічці новин або в глибині ефіру, а також фейкові відеоролики, а також зловмисники зламують електронні поштові скриньки, щоб отримати доступ до акаунтів у соціальних мережах високопоставлених українців для розміщення дезінформації [232].

В цілому у світі протягом 2021 р. щотижня було здійснено понад 200 тис. атак, при цьому частка України серед країн, на яких було здійснено атаки становить близько 19 % (рис. 2.22). На першому місці знаходиться США з часткою більше ніж 46% від питомої ваги всіх інцидентів.

Серед найпопулярніших країн, які є ініціаторами здійснення кібератак, що є політично вмотивованими є Китай та росія, так протягом 2000-2023 рр. було завдано понад 295 та 288 атак по відношенню до інших країн. На другому місці знаходиться Іран з показником більше, ніж 131 вмотивована атака. У період з липня 2023 р. по червень 2024 р. приблизно 33 % зафіксованих мережевих вторгнень, здійснених російськими державними або афілійованими кіберзагрозовими суб'єктами, були спрямовані на урядові структури. Ще 15 % атак націлювалися на аналітичні центри та неурядові організації. Крім того, 9 % кібератак російські державні суб'єкти спрямували на навчальні заклади інших країн, згідно з проведеним дослідженням (рис. 2.23).

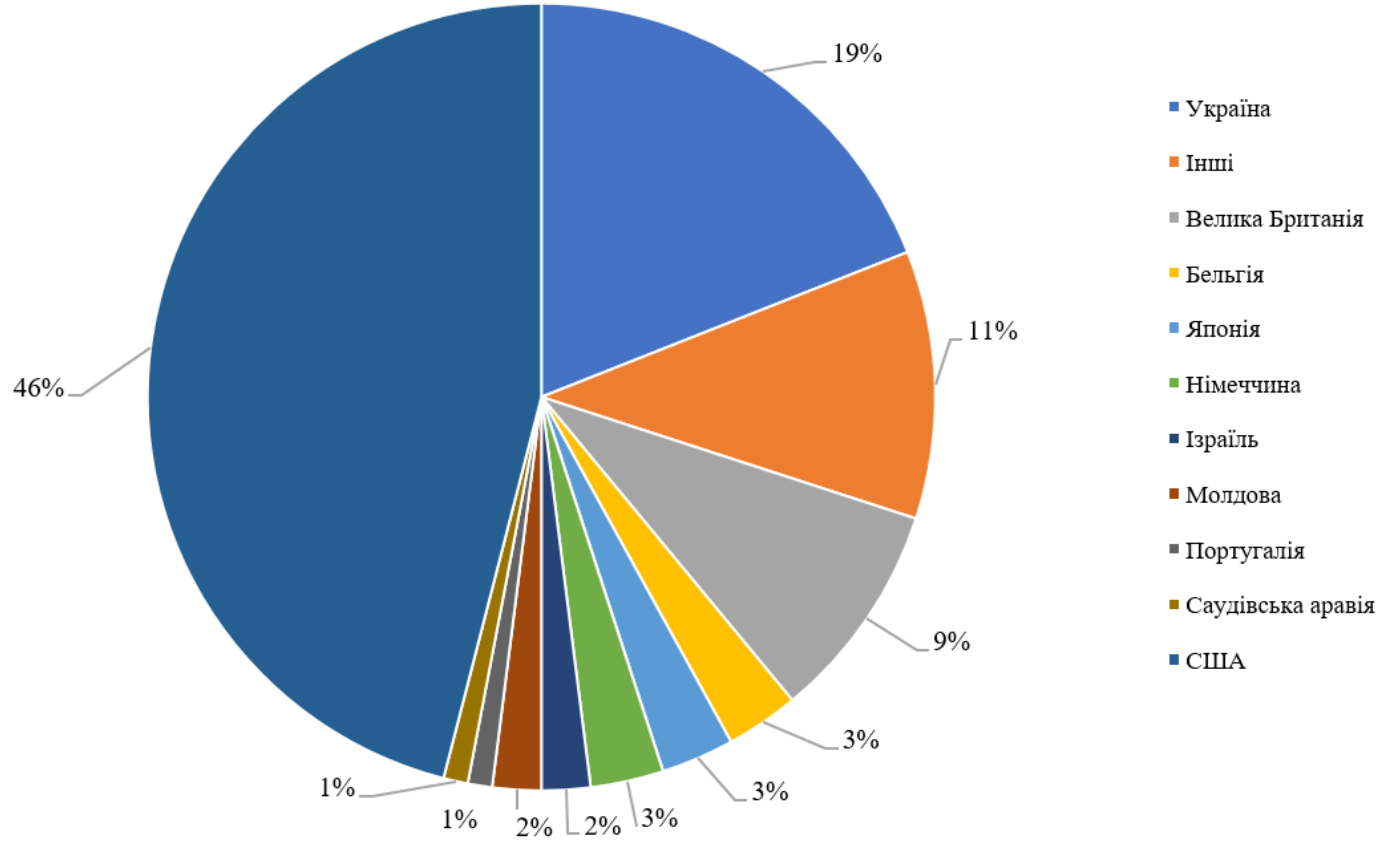

Рис. 2.22. Географічний розподіл завданих кібератак у світі, 2020-2021 рр.

Джерело: побудовано на основі [232].

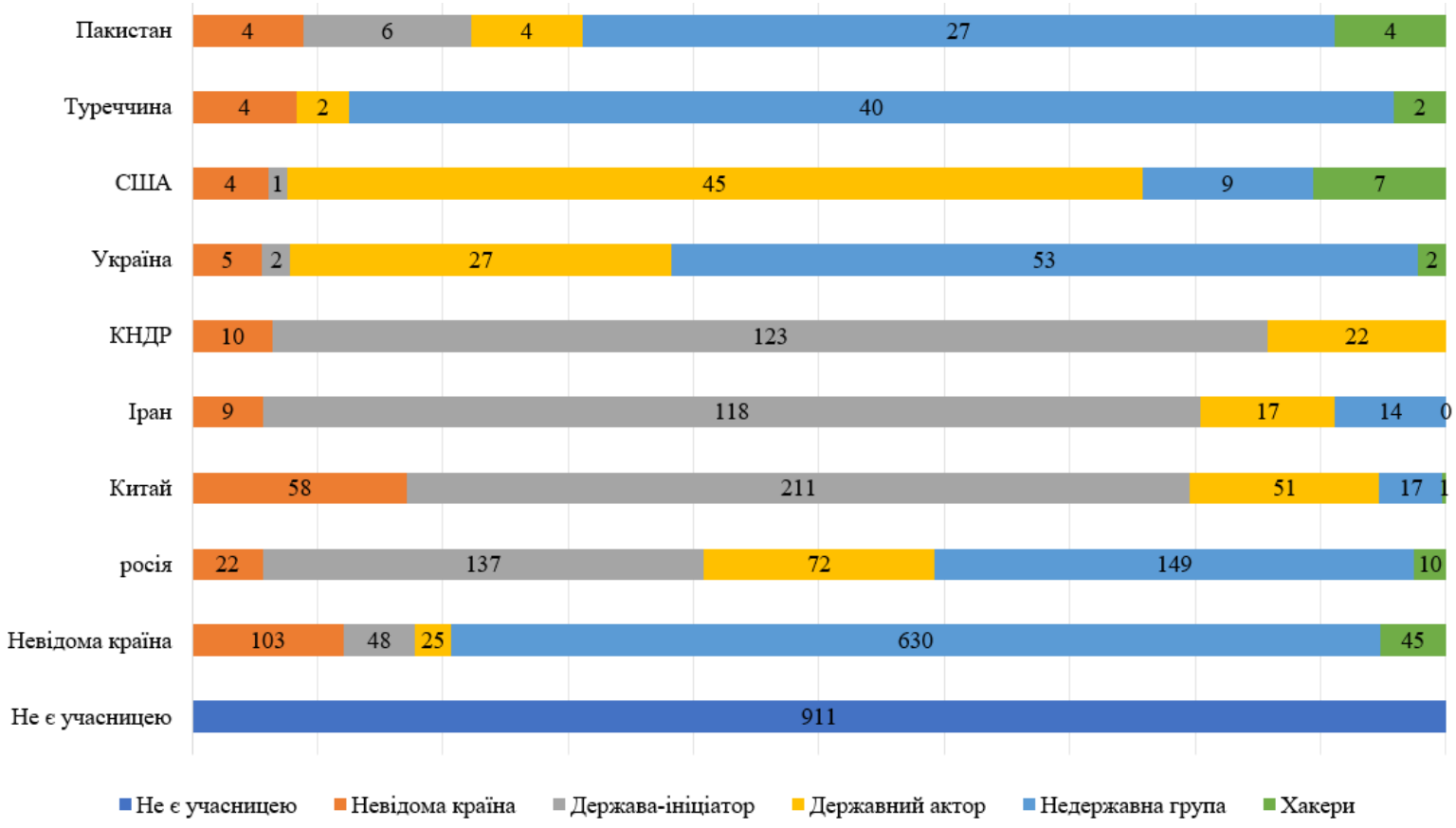

Рис. 2.23. Країни-ініціатори, якими здійснено політично вмотивовані кібератаки, 2000-2023 рр.
Джерело: побудовано на основі [232].

Слід відмітити, що кіберзлочинці застосовують широкий спектр методів для отримання початкового доступу до своїх цілей. Серед основних підходів – фішингові кампанії, використання невиправлених вразливостей у локальних серверах Exchange та компрометація ІТ-постачальників. Це стає ключовою ланкою для подальших операцій, таких як знищення даних, їх викрадення, а також тривалого доступу чи спостереження. Щоб уникнути виявлення, зловмисники постійно модифікують своє шкідливе програмне забезпечення, адаптуючи його під шкірну нову атаку. У звіті Microsoft особливу увагу приділено атакам із використанням шкідливого програмного забезпечення типу «wiper». Назва wiper (стирач) відображає його основну функцію – повне стирання даних із жорсткого диска машини-жертви, що призвело до незворотної втрати інформації. Це робить такі атаки надзвичайно небезпечними для організацій, які залишають їх мішенями [233].

За даними Microsoft, пов'язані з росією злочинні угруповання вже використовувалися для атак в Україні ще в березні 2021 р. Вони здійснювали періодичні напади на Україну, завдаючи шкоди як організаціям всередині країни, так і її союзникам. Згідно даних організації, були відстежені наступні російські кіберугрупування ще задовго до вторгнення, а саме Actinium, Nobelium, Bromine, Seaborgium і dev-0257, які намагалися отримати постійний доступ до своїх конкретних інтересів, що включали: українську оборону, оборонно-промислову базу, зовнішню політику, національну та місцеву адміністрацію, правоохоронні органи та гуманітарні організації [233]. Хоча Microsoft наразі утримується від остаточних висновків щодо рівня координації між цими угрупованнями, їхня спільна діяльність спрямована на забезпечення постійного доступу до систем з метою збору стратегічної та бойової розвідувальної

інформації. Крім того, їхні дії потенційно готують ґрунт для майбутніх руйнівних атак на Україну в умовах війни [233].

За день до військового вторгнення, яке відбулося 24 лютого 2022 р., оператори пов'язані з ГРУ (російською військовою розвідкою) здійснили деструктивні атаки на сотні систем українського уряду, ІТ сектору, енергетичних та фінансових організацій. Діяльність, яку спостерігала компанія Microsoft, включала в себе спроби зловмисників знищити, порушити або потрапити в мережі державних установ, та об'єкти критичної інфраструктури. На деякі з них російські збройні сили одночасно здійснили наземні атаки та ракетні удари. Ці мережеві операції повинні були не лише погіршити функції установ, на які вони були спрямовані, а й перешкодити доступу громадян до надійної інформації та життєво важливих послуг, похитнути довіру до керівництва країни [233].

Слід підкреслити, що протягом 2022 р. масово піддавалися кібератакам такі сфери, як: державне управління – 132 атаки, фінансовий сектор – 63 атаки, медіа сфера – 61 атака, ІКТ (інформаційно-комп'ютерні технології) – 59 випадків та об'єкти енергетики – 31 інцидент (рис. 2.24).

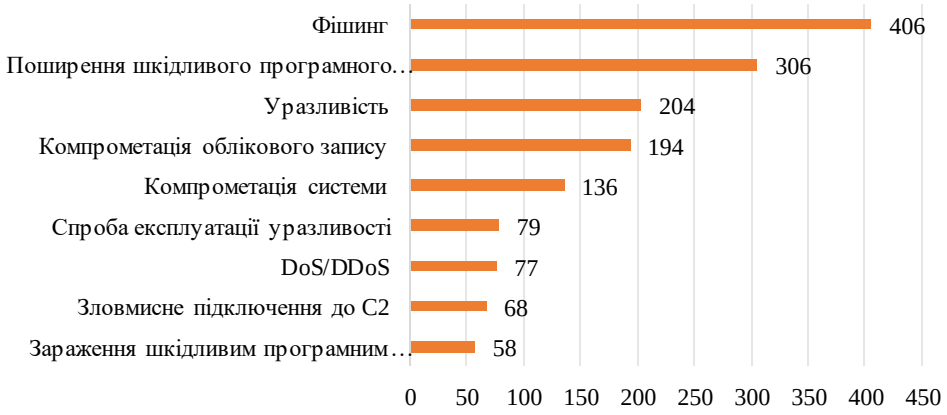

Рис. 2.24. Кількість російських кібератак, здійснених проти України у розрізі їх видів, 2023 р.

Джерело: побудовано на основі [232].

За даними Укренерго, у 2022 р. кількість атак на енергетичний сектор України зросла на 20-25 %. Найпоширенішими атаками були DDoS, фішинг і спроби виконання зловмисного коду. Найінтенсивніший період кібератак був зафіксований у березні 2022 р., коли Україна підключалася до енергосистеми ЄС [222]. У першому півріччі 2023 р. найпомітнішою тактикою, яку зловмисники використовували для завдання кіберінцидентів був фішинг, так кількість зафіксованих атак склала понад 406 випадків. Це суттєва відмінність, адже в першому та другому півріччі 2022 р. домінувало розповсюдження шкідливих програм забезпечення. Особливо шкідливою тенденцією є націленість на українські неприбуткові організації, які є вразливою мішенню через їхню загальну низьку готовність та відсутність заходів стійкості (рис. 2.25).

У 2023 р. до здійснення різного роду кібератак були залучені працівники ГУР та ФСБ російської федерації. Так, наприклад, у першому півріччі 2023 р., команди військової розвідки – ідентифіковані як UAC-0056 (Ember Bear), UAC-0028, (APT28) і UAC-0082 (Sandworm) завдали понад 50 небезпечних атак, представниками ГУР було здійснено близько 11 інцидентів критичного або високого рівня тяжкості. Основними цілями для російської федерації з липня 2023 р. по червень 2024 р. серед інших країн світу, включно з Україною залишаються атаки на уряд, що становить понад 33 %, ІТ-сфера та аналітичні центри та неурядові організації є другою мішенню та дорівнює понад 15 %, на сферу освіти припадає понад 9 % кіберзлочинів, що скоюються російськими угрупуваннями (рис. 2.26).

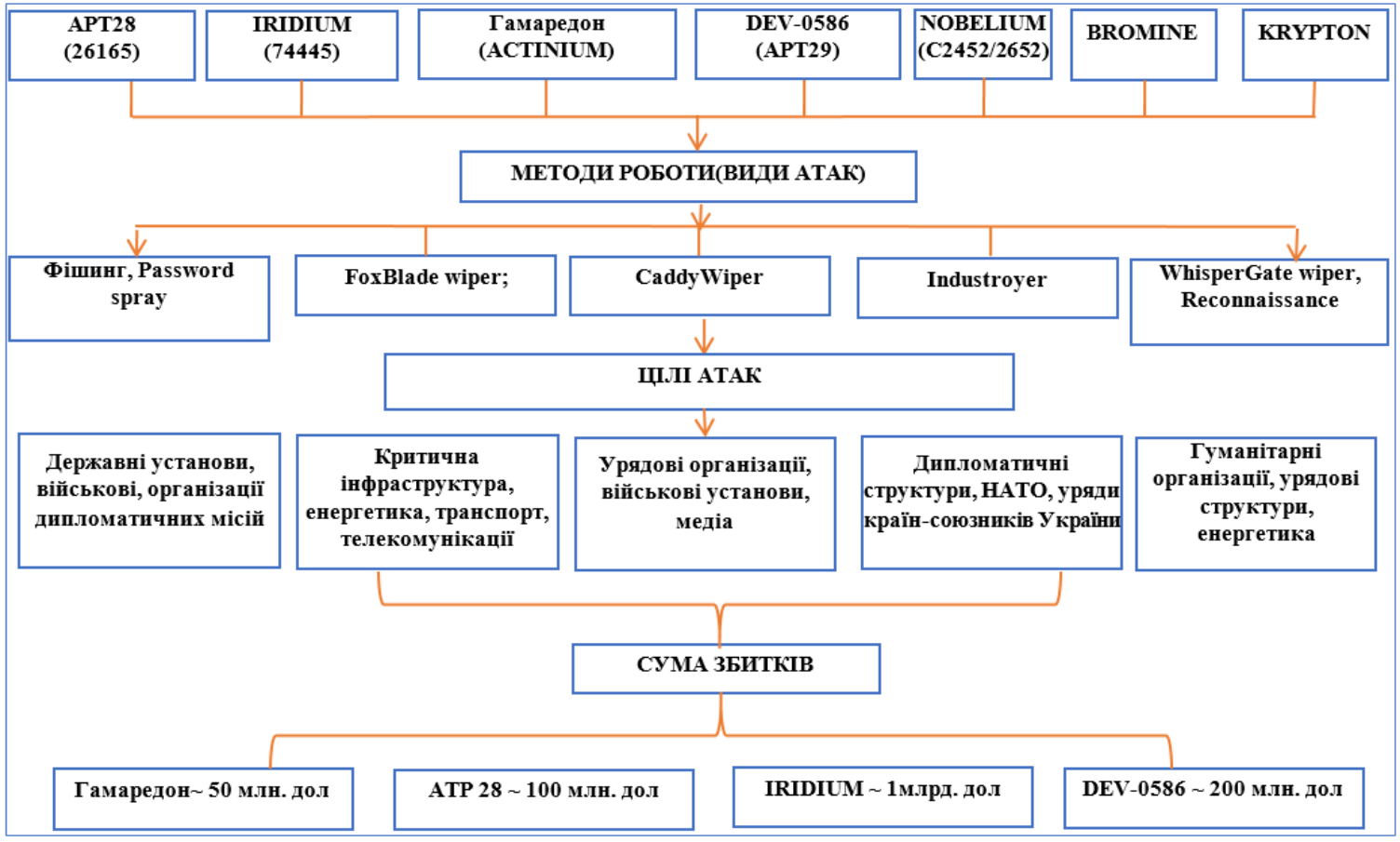

Рис. 2.25. Основні російські кіберугрупування: методи, цілі та орієнтовні збитки у 2021-2022 рр.

Джерело: побудовано на основі [222].

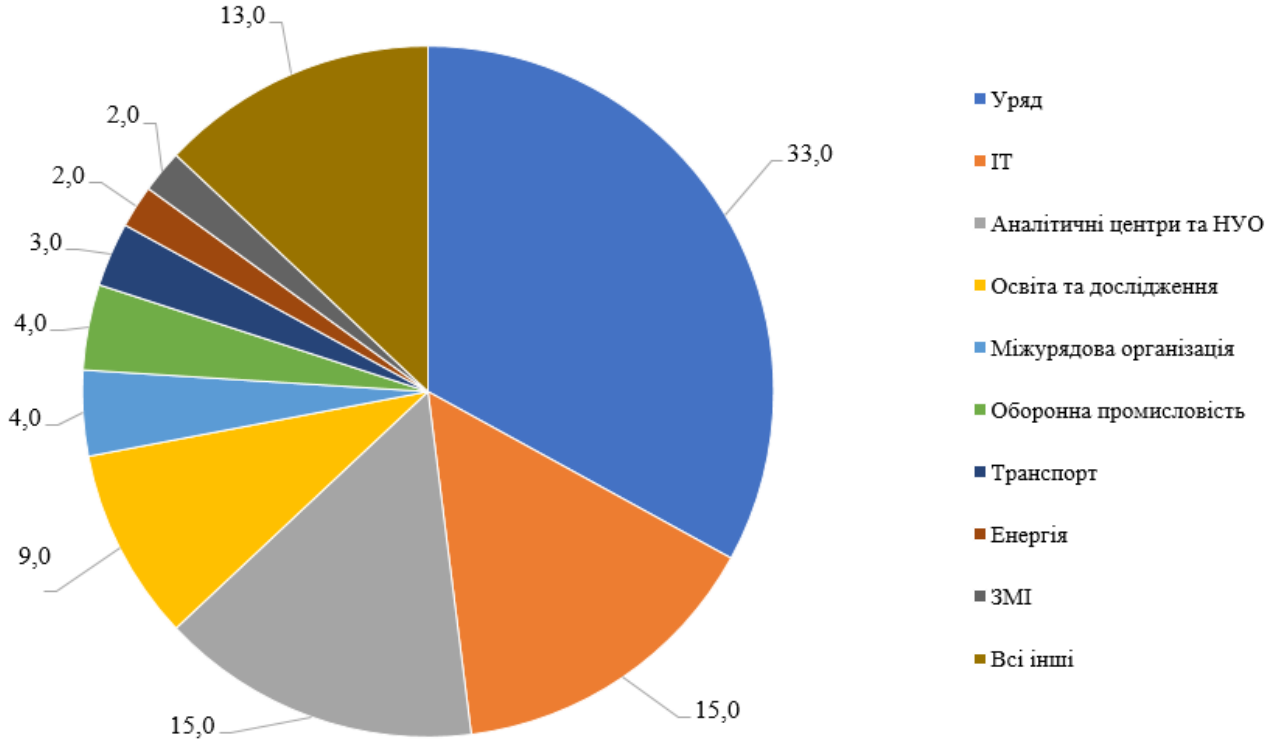

Рис. 2.26. Цілі російських кібератак проти інших країн світу, в тому числі України, з липня 2023 р. по червень 2024 р.

Джерело: побудовано на основі [196].

Серед українських сфер у 2023 році засоби масової інформації стали однією з ключових і актуальних цілей для військових хакерів, підконтрольних Головному розвідувальному управлінню Міністерства оборони російської федерації. Хоча засоби масової інформації є суто цивільними об'єктами, вони мають стратегічне значення для російського командування, яке розглядає їх як важливу складову воєнних та інформаційних операцій. Відтак, ЗМІ залишаються під постійним прицілом російських хакерів, які використовують їх для реалізації операцій впливу. Використання хакерських атак доповнюється іншими формами агресії, такими як пропаганда, ракетні удари та атаки безпілотниками по критичній енергетичній інфраструктурі та по шляхах експорту сільськогосподарської продукції. Військові хакери, відповідно до цього підходу, спрямовують значну частину своїх атак на важливі цивільні служби, зокрема ЗМІ, комунікаційні мережі та громадський сектор. Це підкреслює системний характер російської стратегії, спрямованої на підрив стабільності та дестабілізацію ключових секторів суспільства (рис. 2.27).

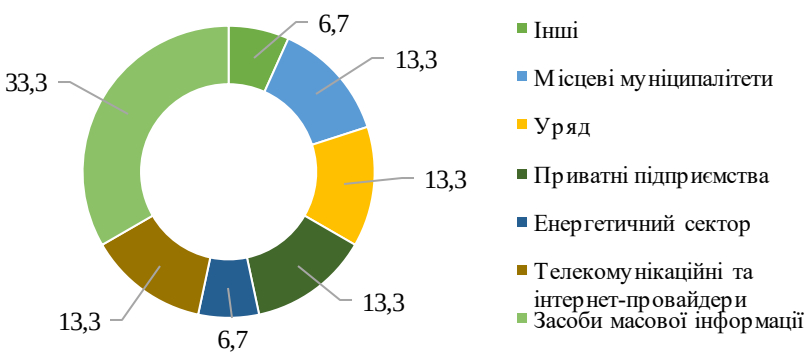

Рис. 2.27. Розподіл кібератак здійснених рф проти України за секторами, 2023 р.

Джерело: побудовано на основі [196].

Вкрай важливим сектор забезпечення функціонування об'єктів критичної та цивільної інфраструктури на території України є енергетичний сектор. Щоразу хакери вдаються до спроби здійснити атаки на енергетичні об'єкти за допомогою тактики багатоетапного впливу: знеструмлення, знищення контролю підстанції, знищення проміжної телекомунікаційної підстанції (модему), руйнування робочої станції працівника і затирання серверного обладнання. Складність атак на енергетичний сектор істотно підвищилася, оскільки хакерам відомо, що ці мережі та компанії (з 2014 р.) мають схожу будову і спільні слабкі місця чи передові практики захисту. Це дало їм змогу краще готувати операції. На жаль, IT команди на об'єктах не завжди мають компетенцію та засоби для виявлення та протидії.

Під час виявлення кібератак виникає низка проблем, які перешкоджають протидії та ефективному усуненні їх наслідків. Серед них наступні:

– *недостатній рівень обізнаності та підготовки персоналу*. Працівники, які не мають достатніх знань у сфері кібербезпеки, можуть не розпізнати ознаки кібератаку, наприклад, рибальські листи чи враження від системи поведінки. Відсутність регулярного навчання та тренінгів фактично до того, що навіть прості атаки, як-от соціальна інженерія, залишаються непоміченими. Погана підготовка спеціалістів з кібербезпеки може ускладнити процес реагування на інциденти;

– *високий рівень складності атак*. Зловмисники вибирають передові методи, як такі APT, що включають тривалий час підготовки, складні інструменти та маскування під легітимну активність;

– *великий обсяг даних для аналізу*. Сучасні інформаційні системи генерують величезну кількість логів і подій, що роблять

аналіз трудомістким і тривалим. Автоматичні системи часто створюють помилкові спрацьовування (false positives), що ускладнює виявлення реальних загроз. Недостатня кількість ресурсів для обробки такого обсягу інформації знижує ефективність роботи аналітиків;

– *відсутність ефективних інструментів моніторингу.* Застаріле програмне забезпечення може бути неефективним проти сучасних кіберзагроз. Відсутність інтеграції між системами (наприклад, SIEM, антивірусами, IDS/IPS) ускладнює повний аналіз інциденту. Нестача сучасних рішень на основі штучного інтелекту для автоматизації виявлення аномалій;

– *складність внутрішніх загроз*. Інсайдери можуть використовувати своє право доступу для здійснення шкідливих дій, які важко відрізнити від легітимної діяльності;

– *відсутність постійного моніторингу дій користувачів у системі*. Інсайдерські прогнози часто залишаються непоміченими через низький рівень довіри до співробітників;

– *швидкість змін у загрозах*. Нові методи атак з'являються постійно, що вимагає постійного оновлення системи безпеки та підпису бази даних. Постійна еволюція інструментів атаки ускладнює їх виявлення стандартними засобами;

– *обмеження в ресурсах*. Нестача фінансових ресурсів ускладнює придбання сучасного обладнання та програмного забезпечення для кібербезпеки. Відсутність достатньої кількості цих спеціалістів через низький рівень оплати праці або інших обмежень;

– *недосконаліть нормативно-правового регулювання*. Відсутність чітких інструкцій щодо реагування на кібератаки може привести до хаосу в процесі управління інцидентами;

– *складність у визначені джерела загрози*. Зловмисники часто використовують VPN, анонімні мережі (Tor) або базові сервери для збереження своєї активності. Мультиетапні атаки, які включають різні проміжні етапи, ускладнюють аналіз. Відсутність необхідного обладнання або програмного забезпечення для трасування джерела атак;

– *проблеми з комунікацією між підрозділами*. ІТ-відділи та служби безпеки часто працюють ізольовано, що уповільнює обмін інформацією. Відсутність єдиних протоколів і стандартизованих процесів для реагування на інциденти. Погана координація між державними структурами та приватним сектором під час спільного реагування на загрози.

Ці проблеми підкреслюють необхідність комплексного підходу до кібербезпеки, що включає технологічні рішення, навчання персоналу та вдосконалення нормативно-правової бази.

Зокрема у Стратегії кібербезпеки України [138; 141], затвердженій Указом Президента України від 26.08.21 р. № 447/2021 були встановлені нові виклики і кіберзагрози, а також підкреслена роль забезпечення кібербезпеки, як одного із пріоритетів у системі національної безпеки України.

Україна активно розвиває та удосконалює законодавчу базу для протидії кіберзагрозам, особливо в контексті гібридної війни та зростання масштабів кібератак. Основними документами, що формують нормативно-правове забезпечення у сфері кібербезпеки, є Конституція України, яка забезпечує основи захисту інформації та прав громадян у цифровому просторі. Закон України «Про основні засади забезпечення кібербезпеки України» [135] від 05.10.2017 р. № 2163-VIII визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів

України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки України, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності із забезпечення кібербезпеки України.

Кримінальний кодекс України від 05.04.2001 № 2341-III [74] передбачає кримінальну відповідальність за злочини у сфері кібербезпеки, зокрема за:

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

– створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361- 1);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2).

Закон України «Про інформацію» від 13.01.2011 р. № 2938-VI [116] регламентує основи інформаційної безпеки, захисту даних та правовідносини у сфері обробки інформації. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах": від 05.07.1994 р. № 80/94-ВР [129] встановлює вимоги до технічного захисту інформації в інформаційних системах та обов'язує операторів критичної інфраструктури впроваджувати системи кіберзахисту.

Рішення Ради національної безпеки і оборони України від 14.05.2021 р. "Про Стратегію кібербезпеки України" від 14.05.2021 р. [139] спрямоване на зміцнення кіберстійкості

критичної інфраструктури, забезпечення захисту державних і приватних інформаційних систем. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23.02.2006 р. [118] відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації України. Закон України "Про електронні довірчі послуги" від 05.10.2017 р. [119] регулює питання використання електронних підписів і забезпечення безпеки цифрових транзакцій.

Міжнародні угоди набувають особливого значення у боротьбі з кіберзлочинністю. Зокрема:

1. Будапештська конвенція [60]. Україна ратифікувала конвенцію в 2005 р., передбачивши деякі важливі застереження до неї, в тому числі щодо того, чи передбачати в національному законодавстві кримінальну відповідальність за виробництво або використання програм або пристроїв з метою незаконного доступу чи перехоплення даних, а також втручання у дані або систему. Україна залишила за собою право не застосовувати пункт 1 ст. 6 Будапештської конвенції, яким передбачено, що "...кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: і. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів [60]; комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів[60]".

2. Указ Президента України від 01.02.2022 № 37/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»» [139].

3. План заходів у сфері реалізації положень Стратегії кібербезпеки України на 2023-2024 рр., затверджений розпорядженням Кабінету Міністрів України від 19 грудня 2023 року, передбачає «створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору» [120].

4. Постанова Кабінету Міністрів України від 04.04.2023 р. № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» [36] та ін.

Оскільки закони, що регулюють кібербезпеку, приймалися в різний час, їхня термінологія часто є непослідовною, а розмежування повноважень між кібербезпековими агенціями залишається нечітким. У зв'язку з цим правова база кібербезпеки України потребує комплексного перегляду. Окрім цього, законодавство містить низку прогалин і неоднозначностей, серед яких особливо важливими є такі аспекти:

– невідповідність національного законодавства міжнародним зобов'язанням;

– непослідовність у термінології;

– брак регулювання критичної інфраструктури;

– відсутність положення щодо проведення аудитів інформаційної безпеки КІ;

– дублювання підзвітності;

– відсутність чіткої вимоги до розпорядників об'єктів КІ та надавачів цифрових послуг повідомляти про кіберінциденти;

– відсутність стратегічного плану кібербезпеки; та жорсткі бюджетні рамки, які локалізують здатність уряду платити конкурентоспроможні зарплати для залучення та утримання потрібних фахівців з питань кібербезпеки.

Суттєвим недоліком законодавчої бази протидії кіберзлочинності є те, що в Кримінальному кодексі України відсутня чітка регламентація щодо електронних доказів, які повинні подаватися виключно у формі електронних документів. Очевидно, що файли або інші цифрові сліди зазвичай не підписуються електронними підписами, адже важко уявити, щоб хакер навмисно виконував такі дії. Запровадження можливості використання електронних доказів у кримінальних справах сприятиме ефективнішій взаємодії між сторонами, які підписали відповідні міжнародні угоди, у розслідуванні злочинів і провадженнях, пов'язаних із використанням комп'ютерних систем і даних. Також для ефективної реалізації необхідних положень Будапештської конвенції українському уряду необхідно вжити заходів щодо більш розширених та докладних визначень кібербезпеки, зокрема таких як: "користувач послуг", "інформація про користувача послуг".

Україна, визнаючи, що вона вже багато років є об'єктом кібератак, у своїй підготовці залучила державно-приватне партнерство. З початком війни приватні гравці, такі як Microsoft, Google, Amazon і ESET, публічно визнали свою роль у відстеженні і прогнозуванні кіберзагроз, розміщенні урядових даних у публічній хмарі за межами України та в інших формах співпраці з урядом України з метою запобігання кіберзагрозам [218]. Не менш важливо підкреслити, що Україна зміцнює стійкість своєї національної інфраструктури інформаційно-комунікаційних технологій (ІКТ) та реагування на кіберінциденти до і під час війни

у співпраці з урядами країн-союзників та приватними компаніями [252]. Приватний сектор України також зробив значний внесок у цей процес. Це включало заходи з посилення кіберстійкості України до і після військових вторгнень 2014 і 2022 рр., а також співпрацю з Центром передового досвіду НАТО з питань спільного кіберзахисту (CCDCOE) [249].

Країни-партнери України активно аналізують досвід та вивчають уроки російсько-української кібервійни. У своїх звітах вони підкреслюють, що західна допомога відіграла ключову роль у посиленні кіберстійкості України, значно підвищивши її здатність протидіяти кібератакам. Водночас Україна продемонструвала ефективну стратегію забезпечення стійкості критично важливих функцій. Ця стратегія базується на усвідомленні, що навіть найсучасніші засоби захисту можуть бути обійдені, і, відповідно, необхідно забезпечувати основні послуги альтернативними шляхами.

Окремі дослідники зазначають, що Україна наразі більш пристосована до кіберпротистояння та реагування на нові виклики у кіберпросторі, ніж навіть США та їхній приватний сектор, зокрема промислові підприємства. Пріоритетним напрямом залишається подальший розвиток систем захисту інформації критично важливих об’єктів, що базуються на найкращих міжнародних практиках, а саме необхідне прийняття спеціального закону захисту критично важливої інфраструктури, в якому буде заначено комплексне регулювання основних напрямків, механізмів і правового регулювання захисту критичної інфраструктури. Кібератаки, які стали невід’ємною частиною сучасних конфліктів, використовуються для руйнування критичної інфраструктури, дестабілізації економіки, маніпулювання інформаційним простором і підриву довіри до державних інститутів. Зростання

кількості атак і їхньої складності, як у випадку України, підкреслює важливість адаптації до нових викликів у кіберпросторі.

Доведено, що для підвищення кіберстійкості України необхідна реалізація таких першочергових завдань як: впровадження новітніх систем моніторингу кіберзагроз (наприклад, на базі ШІ), створення кібервійськ, що можуть протистояти загрозам на державному рівні, запровадження програм постійного навчання для спеціалістів з кібербезпеки, підвищення рівня обізнаності працівників державних та приватних організацій щодо базових кіберзагроз, таких як фішинг і соціальна інженерія, використання сучасних засобів шифрування для захисту даних, розгортання інтегрованих систем кібербезпеки для моніторингу мереж і оперативного реагування на загрози, підвищення готовності до атак через ланцюги постачання, підвищення безпеки критичних об'єктів інфраструктури через регулярні аудити та тестування на проникнення.

Встановлено, що важливим є зміцнення координації з міжнародними організаціями для ефективної протидії кіберзагрозам, які супроводжують розвиток цифрової економіки та інформаційного суспільства. Формування комплексної системи кібербезпеки, орієнтованої на попередження та стримування кіберзагроз, стане вагомим кроком до підвищення кіберстійкості. Це дозволить Україні не лише адаптуватися до динамічних змін у кіберпросторі, але й випереджати їх, забезпечуючи швидке реагування на нові виклики.

РОЗДІЛ 3

ЗАРУБІЖНИЙ ДОСВІД ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

3.1. Досвід формування правового поля державної політики протидії кіберзлочинності в країнах пострадянського простору

Найбільш важливою складовою державної політики протидії кіберзлочинності є формування правового забезпечення її реалізації. Зокрема система правового регулювання щодо протидії кіберзлочинності має визначати кримінальну відповідальність за такі протиправні діяння. Кіберзлочинність є відносно новим об'єктом системи кримінального права та, відповідно до державної політики не лише для України, а й світу в цілому, «із запровадженням новітніх інформаційних технологій розвиток науково-технічного прогресу спричинив появу нових видів злочинів, і в тому числі щодо протиправного втручання в роботу електронно-обчислювальних машин, комп'ютерних мереж та систем, крадіжок, привласнення, маніпуляції комп'ютерної інформації, а тому це підсумовується як небезпечне антисоціальне явище під назвою «кіберзлочинність»» [162]. Щодо вище зазначених видів кримінальних правопорушень існує багато колізій: і в міжнародному кримінальному праві, і в контексті кримінального права країн світу. При формуванні правового механізму державної політики протидії кіберзлочинності є потреба у вивченні зарубіжного досвіду, що можливо здійснити шляхом вивчення кримінального законодавства країн світу.

Дослідження кримінального права зарубіжних країн в цілому та в частині протидії кіберзлочинності розкрито у дисертаційних дослідженнях вітчизняних вчених, зокрема в галузях таких наук, як-от: державне управління (Д. О. Грицишен, В. В. Євдокимов, К. В. Малишев, В. В. Нонік, І. В. Супрунова,), юридичних наук (Т. В. Барановська, С. О. Перхун, М. М. Забарний, О. І. Миргородський, Е. В. Малютін, М. О. Думчиков, Б. Б. Теплицький, М. Ю. Яцишин, О. М. Бодунова, В. В. Сисолятін, Т. А. Білобров), економічних (А. П. Дикий, О. С. Кушнерьов).

«За останні десятиріччя світ зазнав кардинальних змін. Сучасне суспільство не може уявити свого життя без інтернету, комп'ютерів, смартфонів та інших технологічних «плюшок». Паралельно із реальним світом розвивається метавсесвіт, який у майбутньому може змінити багато сфер нашого звичного життя. Все це є наслідком цифрової революції, яка відбувається завдяки розвитку інформаційно-телекомунікаційних технологій. Прогрес нікого не залишає байдужим, що й зумовило появу такого явища як кіберзлочинність. У всьому світі злочини у кіберпросторі щороку завдають збитків на десятки мільярдів доларів США не лише державам, а й приватним компаніям <…> Таким чином, кіберзлочинність охоплює різноманітні сфери життя людей, будь-хто може стати її жертвою. Світове суспільство вже оголосило боротьбу із кіберзлочинністю як одним із пріоритетних напрямків діяльності державних та правоохоронних органів, адже рівень небезпеки від протиправних дій у кіберпросторі є дуже високим» [68].

«До основних ознак високотехнологічної злочинності належить її транснаціональний характер, що означає взаємозв'язок із більш ніж одним правопорядком. А тому, ефективна протидія кіберзлочинності неможлива, якщо розслідування злочинів, викриття правопорушників, їхні обвинувачення у суді ускладнені або взагалі неможливі через значні відмінності у національних кримінальних законах, а також відповідних регіональних угодах. Фактично, така

неузгодженість дозволяє злочинцям уникнути відповідальності, залишаючи їхні дії безкарними. Отже, чинні законодавчі акти, засновані на принципі nulla poena sine lege, повинні містити вичерпний перелік протиправних діянь з використанням ІКТ, а тому створення відповідних універсальних стандартів є об'єктивною необхідністю» [177]. Одним із напрямів вирішення зазначеної проблеми є дослідження кримінального законодавства у сфері протидії кіберзлочинності на рівні різних країнах світу: «Оскільки жодна країна не може діяти лише на національному рівні, щоб захистити себе, комплексна боротьба з кіберзлочинністю вимагає:

– гармонізувати кримінальне законодавство щодо кіберзлочинності на міжнародному рівні;

– розроблення на міжнародному рівні та імплементування в національне законодавство процесуальних стандартів, з метою ефективного розслідування злочинів у глобальній інформаційній мережі, отримання, розслідування та надання електронних доказів із урахуванням транскордонного характеру цього питання;

– налагодження співпраці на оперативному рівні правоохоронних органів при розслідуванні кіберзлочинів;

– наявність механізмів вирішення питань юрисдикції у кіберпросторі» [162].

Зазначене має стати основою формування та реалізації державної політики з питань протидії кіберзлочинності в Україні як складової забезпечення інформаційної безпеки держави: «Питання кіберзлочинності є надзвичайно важливим на державному рівні. Найчастіше під ударами кібератак опиняються об'єкти критичної інфраструктури: енергетичні об'єкти, транспорт та банківський сектор. Вартість захисту зазвичай у 10 разів дорожча за саму атаку. Тому пріоритетним напрямком у політиці багатьох держав є кібербезпека» [26]. «У зв'язку з тим, що більшість кіберзлочинів вчиняється з корисливих мотивів, завдання держави – створити такі умови для спеціалістів, аби

останні працювали на громадянське суспільство, а не проти нього. Поряд з цим необхідно розуміти, що на кожного комп'ютерного «генія», знайдеться більш розумний, а тому викрити кіберзлочинця можливо, для цього лише потрібний більш кваліфікований фахівець. Україні потрібен подальший розвиток кібербезпеки, адже лише завдяки її належному рівню, стане можливим нормальне функціонування систем та мереж, які з кожним днем все більше інтегруються в життя нашого суспільства» [68]. Відповідно, для цього пропонуємо визначити ключові особливості національних систем кримінального права країн світу, що можуть визначити як позитивний так і негативний досвід.

Варто зазначити, що в умовах євроінтеграційних процесів та необхідності подолання наслідків російсько-української війни й, відповідно, протидії інформаційній війні, Україна має визначити власну модель правової протидії кіберзлочинам. Вивчення зарубіжного досвіду дозволить встановити пріоритетні напрями трансформації та сприятиме удосконаленню змісту Кримінального Кодексу України і щодо розширення кримінальної відповідальності за певні види діянь, і в контексті розширення змісту тих обставин, які ускладнюють зміст покарання, внаслідок скоєного кіберзлочином.

«Вважається, що джерелом права є зовнішня форма об'єктивізації правової норми. Причому лише об'єктивізована (у певній формі) норма стає загальнообов'язковою правовою нормою, реалізація якої забезпечується відповідними засобами державного впливу. Це стосується і норм кримінального права. Основними джерелами кримінального права більшості зарубіжних країн є кримінальні кодекси (інколи вони мають назву кримінальних законів, інколи це певні розділи у зводі законів). Джерелом кримінального права в більшості розвинених зарубіжних країн є не лише кримінальні кодекси. Таким джерелом можуть бути також конституції, інші закони та підзаконні нормативні акти, судові прецеденти (останнє характерне для загального права), міжнародні договори, думки

авторитетів, що характерно для англійського права; це може бути й рішення Європейського суду з прав людини» [176].

Для оцінки особливостей національних систем кримінального права країн світу, у рамках встановлення відповідальності за кримінальні правопорушення в сфері кібербезпеки, розглянемо Кримінальні Кодекси сукупності країн:

– країн, які були у складі Радянського Союзу та мають спільне політичне минуле з Україною й, відповідно, їхні правові системи є подібними та мають багато спільних рис. Так, у цьому контексті буде досліджено Кримінальні Кодекси Республіки Узбекистан, Республіки Таджикистан, Грузії. Варто зазначити, що серед зазначених країн свої наміри щодо вступу до європейської спільноти має Грузія;

– які є членами Європейського Союзу, що стане основою визначення пріоритетних напрямів формування дорожньої карти європейської інтеграції національної системи кримінального права. Зокрема будуть досліджені законодавчі акти країн Центральної та східної Європи, що були у складі країн соціалістичного табору та Радянського Союзу й успішно пройшли процес європейської інтеграції, відтак уже досить довгий час є членами Європейського Союзу. Зокрема буде вивчено нормативно-правове регулювання щодо протидії кіберзлочинності (Кримінальні Кодекси) таких країн, як-от: Республіка Болгарія, Чеська Республіка, Литовська Республіка, Республіка Польща. Питання кримінального законодавства зазначених країн буде розглянуто в наступних підрозділах.

Розглянемо Кримінальні Кодекси зазначених країн у наступному форматі: по-перше, загальна характеристика основного документу, що визначає кримінальне законодавство в цілому та в частині протидії кіберзлочинності; по-друге, ідентифікація та характеристика кримінальних правопорушень, що є кіберзлочинами, за які передбачається кримінальна відповідальність в досліджуваній країні; по-третє, визначення мір покарання та обставин, які ускладнюють зміст покарання за скоєні кіберзлочини.

Розглянемо змістовні та формальні характеристики кримінального законодавства зарубіжних країн, зокрема країн, які були у складі Радянського Союзу, щодо протидії кіберзлочинності.

Республіка Узбекистан. У Республіці Узбекистан основним документом, що регулює державну кримінально-правову політику є Кримінальний Кодекс Республіки Узбекистан [73], [265], що був прийнятий Верховною Радою Республіки Узбекистан у 1994 р. Звісно, за це час було внесено багато змін та доповнень, зокрема у 2019 р. були внесені основні зміни, що стосуються протидії кіберзлочинності.

Так, відповідно до кримінального Кодексу Республіки Узбекистан, питання встановлення відповідальності за кіберзлочини регулює Глава XX.1. – «Злочини в сфері інформаційних технологій». На сьогодні зазначеною главою визначені наступні види кіберзлочинності:

– *порушення правил інформатизації:* тобто створення, впровадження та експлуатація інформаційних систем і баз даних, систем обробки та передачі інформації, санкціонований доступ до інформаційних систем без прийняття встановлених механізмів захисту, що завдало великої шкоди чи доволі значної, непоправної шкоди правам чи збереженим законним інтересам громадян або державним чи громадським інтересам (Стаття 278.1);

– *незаконний (несанкціонований) доступ до комп'ютерної інформації:* йдеться про незаконний доступ до інформації в інформаційно-обчислювальних системах, мережах та їхніх складових частинах, якщо ця дія призвела до знищення, блокування, модифікації, копіювання або перехоплення інформації, порушення роботи електронно-обчислювальних машин, системи електронно-обчислювальних машин або їх мережі (Стаття 278.2);

– виготовлення з метою збуту або збут і розповсюдження спеціальних засобів для отримання незаконного (несанкціонованого) доступу до комп'ютерної системи (Стаття 278.3);

– *модифікація комп'ютерної інформації* – незаконна зміна, пошкодження, стирання інформації, що зберігається в комп'ютерній системі, а також внесення до неї завідомо неправдивої інформації, яка завдала великої шкоди чи значної шкоди правам чи законним інтересам громадян (безпека яких охороняється законом), або державним чи громадським інтересам (Стаття 278.4);

– *комп'ютерний саботаж* – умисне виведення з ладу чужого або службового комп'ютерного обладнання, а також саморуйнування комп'ютерної системи (комп'ютерний саботаж) (Стаття 278.5);

– *створення, використання або поширення шкідливих програм* – створення комп'ютерних програм або внесення змін до існуючих програм, з метою несанкціонованого знищення, блокування, модифікації, копіювання або перехоплення інформації, що зберігається або передається комп'ютерною системою, а також саморозробка спеціальних вірусних програм, їхнє умисне використання або поширення (Стаття 278.6);

– *незаконний (несанкціонований) доступ до мережі телекомунікацій* – незаконний доступ до мережі телекомунікацій, з метою її використання та пропуску міжнародного трафіку в обхід встановлених систем захисту, а також зберігання та створення умов для функціонування призначених для цього спеціальних програмних або апаратних засобів (Стаття 278.7);

– *порушення законодавства у сфері обігу крипто-активів* – незаконне придбання, збут або обмін крипто-активів, провадження діяльності провайдерських послуг у сфері обігу крипто-активів без отримання ліцензії в установленому порядку або здійснення операцій з анонімними крипто-активами, провайдерами послуг у сфері обігу крипто-активів, здійснених після застосування адміністративного стягнення за такі ж дії (Стаття 278.8);

– *незаконне провадження діяльності з майнінгу* – заняття майнінгом анонімних крипто-активів або здійснення майнінгу з порушенням встановленого порядку, вчиненого після застосування адміністративного стягнення за такі ж дії (Стаття 278.9).

Варто зауважити, що статті 278.8 та 278.9, які визначають відповідальність за порушення законодавства у сфері обігу крипто-активів та незаконне провадження діяльності з майнінгу були прийняті у 2024 р., що є логічним в умовах все більшої актуальності та фінансової спроможності криптовалюти. Варто зазначити, що досліджуваним нормативним документом встановлюється відповідальність за визначені кіберзлочини, що представлено в табл. 3.1.

Аналізуючи підходи узбецького кримінального законодавства щодо встановлення міри покарання за кіберзлочини, варто наголосити, що найбільша міра покарання, яка визначена Кримінальним Кодексом Республіки Узбекистан, є обмеження волі від трьох до п'яти років за наступними злочинами:

– порушення законодавства у сфері обігу крипто-активів, якщо незаконне придбання, збут або обмін крипто-активів здійснюється із використанням службового становища або ж організованою групою чи в її інтересах. З цією ж статтею, якщо не виявлено обставин, які обтяжують покарання на момент скоєння злочину, передбачено штраф до ста базових розрахункових величин, або ж покарання надається у форматі виправних робіт терміном від двох до трьох років, чи обмеженням волі до одного року або позбавленням волі до одного року. Розмір штрафу може бути збільшений від трьохсот до чотирьохсот базових розрахункових величин або ж передбачено обмеження волі терміном до трьох років, якщо є такі обставини, що обтяжують покарання, як-от: злочин, вчинений за попередньою змовою групою осіб, вчинений повторно або скоєний небезпечним рецидивістом або ж особливо у великих розмірах;

Таблиця 3.1

Кримінальна відповідальність за кіберзлочини в Республіці Узбекистан

Кіберзлочин	Покарання	Обставини, які обтяжують зміст покарання за скоєння кіберзлочину (та сама дія, вчинена)				
		А[3]	Б[4]	В[5]	Г[6]	Д[7]
1	*2*	*3*	*4*	*5*	*6*	*7*
Порушення правил інформатизації	Штраф до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами до одного року	-	-	-	-	+
		Штраф до п'ятдесяти неоподатковуваних мінімумів				
Незаконний (несанкціонований) доступ до комп'ютерної інформації	Штраф до ста неоподатковуваних мінімумів доходів громадян або позбавленням певного права до трьох років, або виправними роботами до одного року	+	+	+	+	-
		Штраф від ста до трьохсот неоподатковуваних мінімумів доходів громадян або виправними роботами від одного року до двох років, або обмеженням волі від одного року до трьох років, або позбавленням волі до трьох років.				
Виготовлення, з метою збуту або збут і розповсюдження спеціальних засобів для отримання незаконного (несанкціонованого) доступу до комп'ютерної системи	Штраф до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами до одного року	+	+	+	+	-
		Штраф від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян або виправними роботами від одного року до трьох років				
Модифікація комп'ютерної інформації	Штраф до ста неоподатковуваних мінімумів доходів громадян або виправними роботами до одного року, або обмеженням волі до двох років, або позбавленням волі до двох років	+	+	-	-	+
		Виправні роботи від одного року до двох років або обмеженням волі від двох до трьох років, або позбавленням волі від двох до трьох років				

[3] А – Та сама дія, вчинена за попередньою змовою групою осіб
[4] Б – Та сама дія, вчинена повторно або небезпечним рецидивістом
[5] В – Та сама дія, вчинена з використанням службового становища
[6] Г – Та сама дія, вчинена організованою групою або в її інтересах
[7] Д – Та сама дія, вчинена із заподіянням особливо великого збитку

Продовження табл. 3.1

1	*2*	*3*	*4*	*5*	*6*	*7*
Комп'ютерний саботаж	Штраф від трьохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян із позбавленням певного права до трьох років або обмеженням волі на строк до двох років, або позбавленням волі до двох років	+	+	-	-	-
		Виправні роботи від двох до трьох років або обмеженням волі від двох до трьох років, або позбавленням волі від двох до трьох років				
Створення, використання або поширення шкідливих програм	Штраф від ста до трьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до двох років, або позбавленням волі до двох років	+	+	-	+	+
		Обмеження волі від двох до трьох років або позбавленням волі від двох до трьох років				
Незаконний (несанкціонований) доступ до мережі телекомунікацій	Штраф від ста до трьохсот базових розрахункових величин або обмеженням волі від одного до трьох років або позбавленням волі до трьох років	+	+	+	+	-
		Штраф від трьохсот до шестисот базових розрахункових величин або обмеженням волі від трьох до п'яти років або позбавленням волі від трьох до п'яти років				
Порушення законодавства у сфері обігу крипто-активів	Штраф до ста базових розрахункових величин або виправними роботами від двох до трьох років або обмеженням волі до одного року або позбавленням волі до одного року	+	+	-	-	+
		Штраф від трьохсот до чотирьохсот базових розрахункових величин або обмеженням волі до трьох років або позбавленням волі до трьох років				
		-	-	+	+	-
		Позбавлення волі від трьох до п'яти років				
Незаконне провадження діяльності з майнінгу	Штраф до ста базових розрахункових величин або виправними роботами від двох до трьох років або обмеженням волі до одного року або позбавленням волі до одного року	+	+	-	-	+
		Штраф від трьохсот до чотирьохсот розмірів основного обчислення або обмеженням волі на строк до трьох років, або позбавленням волі на строк до трьох років				
		-	-	+	+	-
		Позбавлення волі від трьох до п'яти років				

– незаконне провадження діяльності з майнінгу, яке стосується анонімних крипто-активів або реалізації майнінгу із порушенням встановленого порядку, вчиненого після застосування адміністративного стягнення за такі ж дії і водночас зумовлені такими обставинами, що обтяжують покарання. Додатково це незаконне діяння реалізовується шляхом маніпулювання службовим становищем у рамках організованої групи чи її інтересів. За цією ж статтею, без обставин, які обтяжують покарання, передбачено штраф до ста базових розрахункових величин або ж виправні роботи терміном від двох до трьох років, чи обмеження волі до одного року, або позбавлення волі до одного року. Якщо до обставин, які обтяжують покарання, належить попередня змова, організована групою осіб, повторне скоєння злочину або вчинений небезпечним рецидивістом злочин в особливо великих розмірах, то міра покарання буде наступною: штраф від трьохсот до чотирьохсот базових розрахункових величин або обмеження волі терміном до трьох років або позбавленням волі до трьох років.

Республіка Таджикистан. Кримінальний Кодекс Республіки Таджикистан [72] був прийнятий у 1998 р., відповідно, за понад 25 років було внесено багато змін. Кримінальний кодекс складається із загальної та особливої частини. Особлива частина передбачає кримінальну відповідальність за наступні злочини:

– злочини проти особистості (проти життя та здоров'я, проти особистої свободи, честі та гідності, проти статевої свободи або статевої недоторканості, проти конституційних прав і свобод людини і громадянина, проти сім'ї та неповнолітніх);

– злочини проти громадської безпеки та здоров'я населення (проти громадської безпеки, проти здоров'я населення, проти безпеки руху та експлуатації транспорту);

– злочини проти екологічної безпеки та природнього середовища;

– злочини проти громадського порядку та моральності;

– злочини у сфері економіки (злочини проти власності, злочини у сфері економічної діяльності);

– злочини проти інформаційної безпеки;

– злочини проти державної влади (проти основ конституційного устрою і безпеки держави, проти державної влади, інтересів державної служби, проти порядку управління, проти правосуддя);

– злочини проти військової служби;

– злочини проти миру і безпеки людства.

Питанням щодо протидії кіберзлочинності, через встановлення кримінальної відповідальності та міри покарання, присвячено Главу 28 – «Злочини проти інформаційної безпеки», відповідно до якого передбачено наступні кримінальні правопорушення:

– неправомірний доступ до комп'ютерної інформації: йдеться про інформацію, що зберігається у комп'ютерній системі, мережі або на електронних носіях і паралельно цей процес супроводжується порушенням системи захисту (Стаття 298);

– модифікація комп'ютерної інформації – зміна інформації, що зберігається у комп'ютерній системі, мережі або на електронних носіях, а також внесення до них завідомо неправдивої інформації, що завдало значної шкоди або створило загрозу внаслідок її заподіяння (Стаття 299);

– комп'ютерний саботаж – знищення, блокування або приведення у непридатний стан комп'ютерної інформації; сприяння збою у певній програмі; виведення із ладу комп'ютерного

обладнання, а також комп'ютерної системи, мережі або електронного носія (Стаття 300);

– незаконне заволодіння комп'ютерною інформацією: а) незаконне копіювання або інше неправомірне заволодіння інформацією, що зберігається у комп'ютерній системі, мережі або на машинних носіях, а також перехоплення інформації, що передається із використанням комп'ютерного зв'язку; б) примус щодо передачі інформації, яка зберігається у комп'ютерній системі, мережі або на електронних носіях; висунення погрози щодо розголошення ганебних відомостей про особу або її близьких, оприлюднення відомостей про такі обставини, які потерпілий бажає зберегти в таємниці; здійснення залякування щодо застосування насильства над особою або її близькими; висунення погроз щодо знищення чи пошкодження майна особи, її близьких чи інших осіб, у веденні або під охороною яких знаходиться ця інформація (Стаття 301);

– виготовлення та збут спеціальних засобів для отримання неправомірного доступу до комп'ютерної системи або мережі: йдеться про виготовлення з метою збуту, а також збуту спеціальних програмних або апаратних засобів задля отримання неправомірного доступу до захищеної комп'ютерної системи або мережі (Стаття 302);

– розробка, використання і поширення шкідливих програм – розробка комп'ютерних програм або внесення змін в уже існуючі програми, з метою несанкціонованого знищення, блокування, модифікації або копіювання інформації, що зберігається у комп'ютерній системі, мережі або на електронних носіях, а також розробка спеціальних вірусних програм, цілеспрямоване й усвідомлене їх використання, або поширення носіїв із такими програмами (Стаття 303);

– порушення правил експлуатації комп'ютерної системи або мережі: йдеться про такі порушення правил експлуатації особою, яка має доступ до певної системи або мережі, внаслідок чого це спричинило необережне знищення, блокування, модифікацію комп'ютерної інформації, призвело до порушення роботи комп'ютерного обладнання або заподіяло іншої значної шкоди (Стаття 304).

У цьому розділі визначено міру покарання та встановлено зміст обставин, які обтяжують злочин, що систематизовано представлено у табл. 3.2

Такими обставинами, які обтяжують скоєні злочини, у Кримінальному Кодексі Республіки Таджикистан визнано наступні:

– якщо вони з необережності спричинили зміну, знищення або блокування інформації, а також виведення із ладу комп'ютерного обладнання, або завдали значної шкоди. Це стосується, насамперед, такого виду злочину як «неправомірний доступ до комп'ютерної інформації»;

– злочини, які з необережності спричинили тяжкі наслідки, як-от: неправомірний доступ до комп'ютерної інформації; модифікація комп'ютерної інформації; комп'ютерний саботаж; розробка, використання і поширення шкідливих програм; порушення правил експлуатації комп'ютерної системи або мережі;

– злочин, поєднаний із неправомірним доступом до комп'ютерної системи або мережі. Такий фактор обтяження скоєного злочину віднесено до наступних видів кіберзлочинів, як: модифікація комп'ютерної інформації і комп'ютерний саботаж;

– протиправні дії, пов'язані із застосуванням насильства над особою або його близькими у контексті здійснення відповідного злочину – незаконне заволодіння комп'ютерною інформацією;

Таблиця 3.2

Кримінальна відповідальність за кіберзлочини в Республіці Таджикистан

Стаття	Покарання	Обставини, які обтяжують покарання на момент скоєння кіберзлочину (та сама дія, вчинена)									
		А[8]	Б[9]	В[10]	Г[11]	Д[12]	Е[13]	Є[14]	Ж[15]	З[16]	К[17]
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
Неправомірний доступ до комп'ютерної інформації	Штраф у розмірі від двохсот до чотирьохсот показників для розрахунків або позбавленням волі на строк до двох років	+	-	-	-	-	-	-	-	-	-
		Штраф у розмірі від трьохсот до п'ятисот показників для розрахунків або виправними роботами на строк до двох років або позбавленням волі на строк до трьох років									
		-	+	-	-	-	-	-	-	-	-
		Штраф у розмірі від чотирьохсот до семисот показників для розрахунків або позбавленням волі на строк до чотирьох років									

[8] А – якщо вони спричинили з необережності зміну, знищення або блокування інформації, а також виведення з ладу комп'ютерного обладнання, або завдали значної шкоди
[9] Б – спричинили з необережності тяжкі наслідки
[10] В – поєднане з неправомірним доступом до комп'ютерної системи або мережі
[11] Г – пов'язані із застосуванням насильства над особою або його близькими
[12] Д – вчинені групою осіб за попередньою змовою
[13] Е – що заподіяли значної шкоди потерпілому
[14] Є – вчинені, з метою отримання особливо цінної інформації
[15] Ж – вчинені повторно
[16] З – вчинені організованою групою
[17] К – що призвело з необережності до смерті людини або інших тяжких наслідків

Продовження табл. 3.2

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
Модифікація комп'ютерної інформації	Штраф у розмірі від трьохсот до п'ятисот показників для розрахунків, або виправними роботами на строк до двох років або позбавленням волі на той самий строк	-	+	+	-	-	-	-	-	-	-
		Штраф у розмірі від п'ятисот до однієї тисячі показників для розрахунків або позбавленням волі до трьох років									
Комп'ютерний саботаж	Штраф у розмірі від двохсот до п'ятисот показників для розрахунків або обмеженням волі на строк до двох років або арештом на строк до чотирьох місяців	-	+	+	-	-	-	-	-	-	-
		Штраф у розмірі від п'ятисот до однієї тисячі показників для розрахунків або позбавленням волі до трьох років									
Незаконне заволодіння комп'ютерною інформацією	а) Штраф у розмірі від двохсот до п'ятисот показників для розрахунків або позбавленням волі до двох років б) Обмеження волі на строк до п'яти років або позбавленням волі на строк від двох до чотирьох років	-	-	-	+	+	+	+	-	-	-
		Позбавлення волі на строк від п'яти до семи років									
		-	-	-	-	-	-	-	+	+	+
		Позбавлення волі на строк від семи до десяти років									
Виготовлення та збут спеціальних засобів для отримання неправомірного доступу до комп'ютерної системи або мережі	Штраф у розмірі від двохсот до п'ятисот показників для розрахунків або обмеженням волі на строк до двох років, або арештом на строк від двох до шести місяців	Обставини, які обтяжують покарання на момент скоєння злочину, не визначено									

Продовження табл. 3.2

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
Розробка, використання і поширення шкідливих програм	Штраф у розмірі від трьохсот до п'ятисот показників для розрахунків або обмеженням волі на строк до двох років	-	+	-	-	-	-	-	-	-	-
		Штраф у розмірі від п'ятисот до однієї тисячі показників для розрахунків або позбавленням волі до трьох років									
Порушення правил експлуатації комп'ютерної системи або мережі	Штраф у розмірі до трьохсот показників для розрахунків, або обмеженням волі на строк до двох років	-	-	-	-	-	-	+	-	-	-
		Штраф у розмірі від трьохсот до п'ятисот показників для розрахунків або виправними роботами на строк до двох років або позбавленням волі на той самий строк									
		-	+	-	-	-	-	-	-	-	-
		Штраф у розмірі від п'ятисот до однієї тисячі показників для розрахунків або позбавленням волі до трьох років									

– злочини, які вчинені групою осіб за попередньою змовою і стосується незаконного заволодіння комп'ютерною інформацією;

– завдали значної шкоди потерпілому, що також визначається у межах статті «Незаконне заволодіння комп'ютерною інформацією»;

– вчинені з метою отримання особливо цінної інформації; до змісту таких злочинів належить: незаконне заволодіння комп'ютерною інформацією; порушення правил експлуатації комп'ютерної системи або мережі;

– вчинені повторно – це стосуються лише незаконного заволодіння комп'ютерною інформацією;

– вчинені організованою групою – це стосуються лише незаконного заволодіння комп'ютерною інформацією;

– призвело з необережності до смерті людини або інших тяжких наслідків. Така обставина передбачає зміст обтяження за злочином у поєднанні із незаконним заволодінням комп'ютерною інформацією.

Особливістю зазначеного нормативного документу є те, що означені кіберзлочини можуть призвести до смерті людини. Відповідно за таких обставин, які носять відповідний зміст обтяження, передбачається покарання у вигляді позбавлення волі на строк від семи до десяти років.

Грузія. У Грузії Кримінальний кодекс [266] прийнято у 1999 р., відповідно, за такий довгий період він також зазнав низки змін. Особлива частина Кримінального Кодексу Грузії передбачає відповідальність за наступні види злочинів:

– злочини проти людини (проти життя, проти здоров'я; проти статевої свободи та недоторканості, проти прав та свобод людини, проти сім'ї та неповнолітніх; сприяння виникненню загрози життю та здоров'ю людини);

– економічні злочини (проти власності, проти підприємницької або іншої економічної діяльності, реалізованої у сферах грошової, кредитної, фінансової систем; спрямованої проти інтересів служби у підприємницьких або інших організаціях);

– злочини проти правил охорони довкілля і користування природними ресурсами (проти охорони довкілля);

– злочини проти людства (проти миру, безпеки людства та міжнародного гуманітарного права);

– злочини проти громадської безпеки і громадського порядку (порушення правил безпеки при проведенні робіт; протиправні дії, спрямовані проти стану здоров'я населення і його суспільної моралі, а також проти культурної спадщини, злочини міжнародного, міжкультурного характеру; злочини пов'язані із наркотиками, транспортні злочини, кіберзлочини);

– злочини проти держави (проти основ конституційного ладу і безпеки Грузії, порушення правового режиму на окупованих територіях, тероризм, службові злочини, дії проти порядку управління);

– злочини проти судової влади (проти діяльності судових органів, проти процесуального порядку добування доказів, проти своєчасного запобігання і розкриття злочинів, проти виконання судових актів);

– злочини проти військової служби (проти порядку підпорядкування та дотримання військової честі, проти порядку зберігання або експлуатації військового майна).

Питання кіберзлочинності представлено у Главі XXXVV, що була введена в дію у 2010 р. Зазначений розділ передбачає кримінальну відповідальність за наступні види злочинів:

– самовільне проникнення до комп'ютерної системи (Стаття 284);

– незаконне використання комп'ютерних даних або (1) комп'ютерних систем – самовільне виготовлення, зберігання, продаж, поширення комп'ютерної програми або (та) іншого пристрою, а також паролю, коду допуску, необхідного для проникнення до комп'ютерної системи, або інших подібних даних або інше забезпечення доступу до них, з метою скоєння злочину (Стаття 285);

– посягання на комп'ютерні дані або (і) комп'ютерну систему – самовільне пошкодження, знищення, підміна або приховування комп'ютерних даних (Стаття 286).

– зазіхання на комп'ютерні дані або комп'ютерну систему, з метою отримання фінансової вигоди – самовільне проникнення у комп'ютерну систему, самовільне внесення, знищення, підміна або приховування комп'ютерних даних, з метою отримання майнового права або отримання будь-якої фінансової вигоди для себе чи іншої особи, або будь-яке самовільне втручання у функціонування комп'ютерної системи, що спричинило заподіяння фінансової шкоди іншій особі (Стаття 286.1);

– створення підроблених офіційних комп'ютерних даних – отримання підроблених офіційних комп'ютерних даних шляхом самовільного внесення, знищення, підміни або приховування комп'ютерних даних, з метою їх збуту або (і) використання як справжніх/дійсних даних, (Стаття 286.2).

Кримінальна відповідальність та зміст обставин, які обтяжують покарання за скоєний злочин, відповідно до Кримінального Кодексу Грузії представлено в табл. 3.3. Так, за значеним кодексом передбачено сукупність таких обставин, які обтяжують покарання:

– здійснення злочину групою осіб за попередньою змовою;

Таблиця 3.3

Кримінальна відповідальність за кіберзлочини в Грузії

Стаття	Покарання	Обставини, які обтяжують покарання на момент скоєння кіберзлочину (та сама дія, вчинена)							
		А[18]	Б[19]	В[20]	Г[21]	Д[22]	Е[23]	Є[24]	Ж[25]
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Самовільне проникнення до комп'ютерної системи	Штраф або виправними роботами на строк до двох років, або позбавленням волі на той самий строк	+	+	+	+	-	-	-	-
		Штраф або покарання виправними роботами на строк до двох років, або позбавленням волі на строк від двох до п'яти років							
		-	-	-	-	+	-	-	-
		Позбавлення волі на строк від трьох до шести років							
Незаконне використання комп'ютерних даних або (і) комп'ютерних систем	Штраф або виправними роботами на строк до двох років або (і) позбавленням волі на строк до трьох років	+	+	+	+	-	-	-	-
		Штраф або покарання виправними роботами на строк до двох років або (і) позбавленням волі на строк від трьох до шести років							
		-	-	-	-	+	-	-	-
		Позбавлення волі на строк від чотирьох до семи років							
Посягання на комп'ютерні дані або (і) комп'ютерну систему, з метою отримання фінансової вигоди	Суспільно-корисна праця на строк від ста сімдесяти до двохсот годин, або покарання виправними роботами на строк до двох років, або домашнім арештом на строк від одного до двох років, або позбавленням волі на строк від двох до чотирьох років	+	-	-	-	-	+	-	-
		Позбавлення волі на строк від п'яти до семи років							
		-	-	+	+	-	-	+	+
		Позбавлення волі на строк від шести до десяти років							
		-	-	-	-	+	-	+	-
		Позбавлення волі на строк від семи до одинадцяти років							

[18] А – здійснене групою осіб за попередньою змовою
[19] Б – здійснене за умови зловживання службовим становищем
[20] В – здійснено неодноразово
[21] Г – спричинило значну шкоду
[22] Д – здійснено щодо суб'єкта критичної інфраструктури
[23] Е – спричинило значні фінансові збитки
[24] Є – особою, двічі чи більше разів судимою за протиправне присвоєння або вимагання чужої речі/чужого майнового права або за скоєння злочину
[25] Ж – здійснено організованою групою

Продовження табл. 3.3

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Створення підроблених офіційних комп'ютерних даних	Штраф чи позбавленням волі на строк до трьох років	-	+	+	+	-	-	-	-
		Позбавлення волі на строк від трьох до шести років							
Посягання на комп'ютерні дані або (і) комп'ютерну систему	Штраф або виправними роботами на строк до двох років або (і) позбавленням волі на той самий строк	+	+	+	+	-	-	-	-
		Штраф або покарання виправними роботами на строк до двох років або позбавленням волі на строк від трьох до п'яти років							

– здійснення злочину шляхом зловживання службовим становищем;

– кількаразове скоєння злочину;

– здійснення злочину, який спричинив значну шкоду;

– здійснення злочину щодо суб'єкта критичної інфраструктури;

– спричинення значних фінансових збитків;

– скоєння його особою, яка була двічі чи більше разів судимою за протиправне присвоєння або вимагання чужої речі/чужого майнового права або за скоєння злочину;

– здійснення злочину організованою групою.

Зазначенні обставини, які обтяжують покарання через скоєний злочин, майже в усіх кіберзлочинах визначають таку міру покарання, як позбавлення волі. Найбільший строк позбавлення волі – від семи до одинадцяти років. Таке покарання передбачено за посягання на комп'ютерні дані або (і) комп'ютерну систему, з метою отримання фінансової вигоди за умови, що такий злочин скоєний щодо суб'єкта критичної інфраструктури; здійснений особою, яка була двічі чи більше разів судимою за протиправне присвоєння або вимагання чужої речі/чужого майнового права або за скоєння злочину.

Вивчення досвіду зазначених країн щодо встановлення кримінальної відповідальності за кіберзлочини дає можливість визначити напрями трансформації кримінального законодавства України. Зважаючи на повномасштабну війну, сучасні фінансові інструменти, геополітичні трансформації, при удосконаленні кримінального законодавства варто врахувати наступний досвід:

– по-перше, передбачити кримінальну відповідність у сфері незаконного поводження з криптоактивами. Так, вітчизняним кримінальним законодавством не передбачено відповідальності за

кримінальні правопорушення, що стосуються криптоактивів. Відповідно, в Україні необхідно врегулювання це питання не лише з позиції господарського, фінансового, грошово-кредитного, податкового законодавства, а й з позиції кримінальної відповідальності за їх порушення в частині криптоактивів;

– по-друге, передбачити кримінальну відповідальність або ж визначити як обставину, яка покликана обтяжити зміст покарання за скоєні кіберзлочини, пов'язану, насамперед, із критичною інфраструктурою. Це дозволить забезпечити ефективні інструменти протидії кібератакам на критичну інфраструктуру та визначити напрями забезпечення кібербезпеки держави;

– по-третє, розширення змісту обставин, які обтяжують покарання через скоєння кіберзлочину, зокрема йдеться про такі, що завдають значних фінансових збитків для держави або суб'єктів господарювання чи фізичних осіб; також сюди входить скоєння кіберзлочину посадовою особою або за її посередництва.

Таким чином, вивчення досвіду Республіки Узбекистан, Республіки Таджикистан та Грузії, дозволило встановити напрями трансформації кримінального законодавства України в частині розширення видів кіберзлочинів та кримінальної відповідальності за їх скоєння.

3.2. Удосконалення державної політики протидії кіберзлочинності на основі досвіду країн Європейського Союзу (Польща, Болгарія, Чехія)

Забезпечення ефективних процесів європейської інтеграції неможливе без вивчення досвіду її країн-членів, зокрема у питаннях формування та реалізації різних видів політик, особливо

тих, які визначають рівень безпеки держави. «Масштаби кібератак є проблемою для національної безпеки держав та їхньої внутрішньої стабільності. За даними Pew Research Center, у 2018 р. кібератаки на міжнародному рівні посіли третє місце серед глобальних загроз. Масштаби проблеми засвідчує динаміка заражень шкідливим програмним забезпеченням, що є найбільш поширеним видом кіберзлочинів» [33]. Україна не може бути поза межами міжнародної системи інформаційної безпеки, а в контексті обрання євроінтеграційного шляху має відповідати певним нормам Європейського Союзу. Зазначимо, що кожна країна обирає власні інструменти відповідності вимогам Європейського союзу, а тому врахування його досвіду при формуванні вітчизняної політики з питань протидії кіберзлочинності є вкрай важливим.

Питання трансформації державної політики у сфері протидії різним видам злочинів, проблеми правоохоронної діяльності та інформаційної безпеки піднімалися у працях вітчизняних вчених, серед яких: Т. В. Барановська, Т. А. Білобров, О. М. Бодунова, Д. О. Грицишен, А. П. Дикий, М. О. Думчиков, В. В. Євдокимов, М. М. Забарний, О. С. Кушнерьов, К. В. Малишев, Е. В. Малютін, О. І. Миргородський, В. В. Нонік, С. О. Перхун, В. В. Сисолятін, І. В. Супрунова, Б. Б. Теплицький, М. Ю. Яцишин. Незважаючи на значні досягнення вітчизняних дослідників у цьому ключі, залишилося багато невирішених проблемних питань, які стосуються, в першу чергу, обрання власної моделі інтеграції у європейський правовий простір. Незважаючи на спільне законодавство Європейського Союзу, кожна країна обирає власну правову модель.

У цьому дослідженні приділимо увагу тим країнам, які вже є членами Європейського Союзу відносно недавно, а також мають з Україною спільне минуле, зокрема перебували в складі країн

соціалістичного табору. Отже, проведемо аналіз Кримінальних Кодексів Республіки Польщі, Республіки Болгарії, Чеської Республіки.

Республіка Польща. «Перший сучасний Кримінальний Кодекс Польщі (ККП) діяв із 1932 р. Він був першим європейським Кримінальним Кодексом міжвоєнної доби і вважався найпрогресивнішим у Європі. Саме цей нормативно-правовий акт заклав прогресивні європейські тенденції кримінального законотворення і став важливим кроком для створення сучасної Польщі – правової європейської держави. Наступним був ККП 1969 р., що також взяв за основу положення класичної і соціологічної шкіл кримінального права, серед яких: принцип рівності всіх перед законом, гуманізму, індивідуалізації кримінальної відповідальності та багато інших. Цей Кримінальний Кодекс набув чинності 1970 року. У 1971 році були прийняті Кодекс про проступки і Кодекс про провадження у справах про проступки. Із 1982 року діяв Закон про провадження у справах неповнолітніх. Це був загальний огляд кримінального законодавства Польщі до 1997 року. Із 1987 року у Польщі відбувалася кодифікація права, яка закінчилася через 10 років. Вона усунула багато недоліків і вплинула на розв'язання питань, які раніше не були регламентовані» [178]. Це, в свою чергу, вплинуло на сучасний Кримінальний Кодекс Республіки Польща.

«Визначально на історію становлення держави Республіки Польща вплинула зміна устрою держави, а, відповідно, і зміна кримінального права та карної політики. Кримінальне право Республіки Польща зазнало нових реформ, що обумовило прийняття 6 червня 1997 р. нового Кримінального кодексу. Того ж дня було прийнято також Кримінально-процесуальний та

Кримінально-виконавчий кодекси, які остаточно набули чинності 1 вересня 1998 року» [17].

Особливістю Кримінального Кодексу Республіки Польща [260], [71] є три розділи, а саме: загальна частина, особлива частина та військова частина. У контексті об'єктно-предметного поля цього дослідження особлива частина передбачає кримінальну відповідальність за наступні види злочинів: злочини проти миру, людства та військові злочини; злочини проти Республіки Польщі; злочини проти оборони; злочини проти життя і здоров'я; злочини проти суспільної безпеки; злочини проти безпеки дорожнього руху; злочини проти навколишнього середовища; злочини проти свободи; злочини проти свободи совісті та віросповідання; злочини проти статевої свободи і моральності; злочини проти сім'ї та опіки; злочини проти гідності та тілесної недоторканості; злочини проти прав людей, які виконують оплачувану працю; злочини проти діяльності державних установ і органів місцевого самоврядування; злочини проти здійснення правосуддя; злочини проти виборів та референдуму; злочини проти публічного порядку; злочини проти охорони інформації; злочини проти достовірності документів; злочини проти власності; злочини проти господарського обороту; злочини проти обігу грошових коштів та цінних паперів. Особливістю зазначеного нормативного документу є особливі побудова та зміст, а саме наявність механізму встановлення особи, яка вчинила чи не вчинила певні дії.

Питання встановлення кримінальної відповідальності передбачено Розділом XXXIII «Злочини проти охорони інформації» [260], [71], який вміщує наступні види злочинів:

– розголошення або використання, всупереч закону, закритої інформації, що належить до «таємної» або «абсолютно таємної» (Стаття 265, § 1);

– неумисне розповсюдження інформації, що належить до «таємної» або «абсолютно таємної», яка стала відомою у зв'язку з виконанням публічних функцій чи, відповідно до отриманих уповноважень (Стаття 265, § 1);

– розкриття чи використання інформації, всупереч приписам закону або прийнятим на себе зобов'язанням, які особа дізналася у зв'язку з функціями, чи роботою, які виконувалися; а також публічною, соціальною, господарською чи науковою діяльністю (Стаття 266, § 1);

– розкриття посадовою особою неповноважній особі інформації, що не підлягає розголошенню, або яка визначена, як: «обмежена» або «конфіденційна»» чи інформації, яку було отримано у зв'язку з виконанням службових обов'язків, та розкриття якої може завдати шкоди інтересам, які охороняються законом (Стаття 266, § 2);

– отримання доступу до інформації без повноважень, що для особи не призначена, відкриття закритих листів, підключення до телекомунікаційної мережі, або зламування чи нівелювання електронного, магнітного, інформаційного або іншого спеціального її захисту (Стаття 267, § 1);

– отримання доступу до частини або до всієї інформаційної системи без повноважень, що для особи не призначена (Стаття 267, § 2);

– підкладання або використання підслуховуючого, візуального пристрою або іншого пристрою чи програмування, з метою отримання інформації, для отримання якої немає повноважень (Стаття 267, § 3);

– знищення, пошкодження, відміна чи зміна запису важливої інформації або розладнання в інший спосіб чи ускладнення доступу до неї для особи, яка має повноваження на ознайомлення з

такою інформацією, особою, що немає на це повноваження (Стаття 268, § 1);

– знищення, пошкодження, відміна чи зміна запису важливої інформації на інформаційному носії даних або в інший спосіб розладнання чи ускладнення доступу до неї для особи, яка має повноваження на ознайомлення з такою інформацією, особою, що немає на це повноваження (Стаття 268, § 2);

– знищення, пошкодження, підміна, зміна або ускладнення доступу до інформаційних даних або, істотним чином, порушення чи унеможливлення автоматичної обробки, накопичення чи передачі таких даних особою без повноважень на такі дії (Стаття 268 а);

– знищення, пошкодження, підміна або зміна інформаційних даних, що мають спеціальне призначення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, або унеможливлює автоматичну обробку, накопичення чи передачу таких даних (Стаття 269, § 1);

– знищення або заміна інформаційного носія даних, або знищення чи пошкодження пристрою, що служить для автоматичної обробки, накопичення чи передачі інформаційних даних (Стаття 269, § 1);

– порушення роботи комп'ютерної системи або телекомунікаційної мережі особою, що немає таких повноважень, шляхом передачі, знищення, підміни, пошкодження, ускладнення доступу або зміни інформаційних даних значним чином (Стаття 269 а);

– виробництво, придбання, збут чи забезпечення інших осіб пристроями або комп'ютерними програмами, адаптованими для

вчинення злочину комп'ютерними паролями, кодами доступу чи іншими відомостями що уможливлюють доступ до інформації, яка зберігається в комп'ютерній системі чи телекомунікаційній мережі (Стаття 269 b).

На відміну від Кримінального Кодексу Грузії, Республіки Узбекистан та Республіки Таджикистан, Кримінальним Кодексом Республіки Польщі, передбачена кримінальна відповідальність саме за злочини, пов'язані зі створенням, обігом, використанням та зберіганням інформації без прив'язки лише до комп'ютерного середовища. Звісно, в умовах інформаційного суспільства більшість інформації зберігається в цифровому вигляді.

Розглянемо більш детально питання щодо покарання за визначені злочини, що представлено в таблиці 3.4.

Основними видами покарання за скоєння кіберзлочинів у Республіці Польща є обмеження або позбавлення волі, штраф, а в окремих випадках конфіскація майна. Найбільший строк позбавлення волі від 6-ти місяців до 8-ми років передбачено за такі види кіберзлочинів:

1) знищення, пошкодження, підміна або зміна інформаційних даних, що мають спеціальне значення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, або унеможливлюють автоматичну обробку, накопичення чи передачу таких даних (Стаття 269);

2) розголошення або використання, всупереч закону, закритої інформації, що має статус «таємної» або «абсолютно таємної» за умови, що розголошена особі, що діє від імені або в інтересах іноземної юридичної особи (стаття 265 3).

Таблиця 3.4

Кримінальна відповідальність за кіберзлочини в Республіка Польща

Злочин	Покарання	Обставини, які обтяжують/пом'якшують зміст покарання	
		Обставина	Покарання
1	*2*	*3*	*4*
Стаття 265			
Розголошення або всупереч закону використання закритої інформації, що відноситься до «таємної» або «абсолютно таємної»	Позбавлення волі на строк від 3 місяців до 5 років	Розголошена особі, що діє від імені або в інтересах іноземної юридичної особи	Позбавлення волі на строк від 6 місяців до 8 років
		Неумисне розповсюдження інформації	Штраф, обмеження волі або позбавлення волі на строк до 1 року
Стаття 266			
Розкриття чи використання інформації, всупереч приписам закону або прийнятим на себе зобов'язанням, які особа дізналася у зв'язку із покладеними на неї функціями, дорученою роботою, публічною, соціальною, господарською чи науковою діяльністю	Штраф, обмеження волі чи позбавлення волі на строк до 2 років	Розкриття посадовою особою неповноважній особі інформацію, що не підлягає розголошенню як «обмежена» або «конфіденційна», чи інформацію, яка отримала у зв'язку з виконанням службових обов'язків, та розкриття якої може завдати шкоди інтересам, які охороняються законом	Позбавлення волі на строк до 3 років

Продовження табл. 3.4

1	*2*	*3*	*4*
Стаття 267			
Отримання доступу до інформації без повноважень, що для особи не призначена, відкриття закритих листів, підключення до телекомунікаційної мережі або зламування чи нівелювання електричного, магнітного, інформаційного або іншого спеціального захисту	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Отримання доступу до частини або до всієї інформаційної системи без повноважень, що для особи не призначена	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Підкладання або використання підслуховуючого, візуального пристрою або іншого пристрою чи програмування, з метою отримання інформації, для отримання якої не має повноважень	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Не передбачено	
Стаття 268			
Знищення, пошкодження, підміна чи зміна запису важливої інформації; ускладнення доступ до інформації для особи, яка має повноваження на ознайомлення з такою інформацією, особою, що немає на це повноваження	Штраф, обмеження волі або позбавлення волі на строк до 2 років	Запис даних здійснений на інформаційний носій	Позбавлення волі на строк до 3 років
		Завдано значної матеріальної шкоди	Позбавлення волі на строк від 3 місяців до 5 років

Продовження табл. 3.4

1	*2*	*3*	*4*
Стаття 268а.			
Знищення, пошкодження, підміна, зміна або ускладнення доступу до інформаційних даних або істотним чином порушення чи унеможливлення автоматичної обробки, накопичення чи передачі таких даних особою без повноважень на такі дії	Позбавлення волі на строк до 3 років	Завдано значної матеріальної шкоди	Позбавлення волі на строк від 3 місяців до 5 років
Стаття 269			
Знищення, пошкодження, підміна або зміна інформаційних даних, що мають спеціальне значення для оборони держави, безпеки комунікації, функціонування урядової адміністрації, іншого державного органу або державної інституції, або територіального органу місцевого самоврядування чи закладу, що унеможливлює автоматичну обробку, накопичення чи передачу таких даних	Позбавлення волі від 6-ти місяців до 8-ми років	Не передбачено	Не передбачено
Стаття 269а.			
Порушення роботи комп'ютерної системи або телекомунікаційної мережі істотним чином без уповноваження на це через передачу, знищення, підміну, пошкодження, ускладнення доступу або зміну інформаційних даних	Позбавлення волі на строк від 3 місяців до 5 років	Не передбачено	Не передбачено

Продовження табл. 3.4

1	*2*	*3*	*4*
Стаття 269b.			
Виробництво, придбання, збут чи забезпечення інших осіб пристроями або комп'ютерними програмами, пристосованими для вчинення злочину, комп'ютерними паролями, кодами доступу чи іншими даними, що уможливлюють доступ до інформації, яка зберігається в комп'ютерній системі чи телекомунікаційній мережі	Позбавлення волі на строк до 3 років	Не передбачено	Не передбачено

Джерело: сформовано на основі [260], [71]

Досліджуваним нормативно-правовим документом передбачено ряд обставин, які обтяжують покарання за скоєний злочин, відтак:

– за статтею 265 щодо розголошення інформації – інформація розголошена особі, що діє від імені або в інтересах іноземної юридичної особи;

– за статтею 266 щодо розкриття чи використання інформації: йдеться про розкриття посадовою особою не уповноваженій особі інформації, що не підлягає розголошенню як «обмежена» або «конфіденційна», чи інформації, яка була отримана, у зв'язку із виконанням службових обов'язків, та розкриття якої може завдати шкоди інтересам, які охороняються законом;

– завдання значної матеріальної шкоди за статтями 268 та 268 а;

– запис даних, здійснений на інформаційний носій за статтею 268.

Представлена інформація вказує на функціонування двох ключових напрямів щодо здійснення кіберзлочинів:

– по-перше, розголошення інформації, використання якої є обмеженим;

– по-друге, порушення роботи систем збору, обробки, передачі та зберігання інформації;

– по-третє, виробництво та збут пристроїв, що дозволяють скоїти кіберзлочин.

Чеська Республіка. Чеська Республіка має давню історію формування системи кримінального права. Це зумовлено, в першу чергу, становленням держави та її політичною еволюцією. Зважаючи на політичну історію Чеської республіки та історичні епохи розвитку суспільства, можна виділити наступні етапи: 1) Середньовіччя, що характеризуються значним впливом правових

традицій Священної Римської імперії; 2) Новий час (або Модерна доба), що пов'язана із втратою незалежності та входженням до складу Австрії; 3) Австро-угорський період, який характерний утворенням Австро-Угорщини та використанням системи Права Австрії; 4) Чехословаччина (1918–1993) – система кримінального права якої можна розділити на дорадянський та радянський періоди; 5) сучасний період, який характеризується розпадом на Чеську республіку та Словаччину.

Середньовічна система права в цілому та кримінального права зокрема характеризувалася значним впливом на неї правової системи Священної Римської імперії. Відповідно, основними джерелами права були звичаєві норми, а в окремих випадках – укази Короля. Вважається, що важливим фактором у кодифікації та систематизації права стало заснування у 1348 році Празького університету. Засновником університету вважається Карл IV, король Богемії та імператор Священної Римської імперії. Саме тоді почалося викладатися римське право, що мало неабиякий вплив на усю правову систему країни.

Формування правової системи в Новий час є досить дискусійним з позиції розвитку країни та державотворення. У першу чергу, це пов'язано із тим, що Фердинант II увів у дію дві провінційні конституцій Богемії (від 10 травня 1627 року) та Моравії (від 10 травня 1628 року) без згоди сейму. Як вказують чеські дослідники, «оновлена провінційна конституція зовсім не була, як ми часто читаємо, конституцією. Це сучасний термін, який не підходить для давньої історії, до того ж провінційні конституції взагалі містили, крім державного права, процесуальне, кримінальне або спадкове право, тому ми могли б скоріше назвати їх провінційними кодексами з певним ступенем спрощення» [237]. З позиції цього дослідження, вказана конституція є цікавою щодо

наявності першої спроби кодифікації, зокрема у визначенні таки галузей права, як: державне, приватне та кримінальне.

У подальшому втрата незалежності Чехії та її входження до складу Австрії зумовили реформування кримінального права, що значним чином пов'язано із виданням Терезіанського кримінального кодексу (1768 р., за часів правління Марії-Терезії) та Йозифінського кримінального кодексу (1787 р., за часі правління Йосифа II). Терезіанський кодекс був досить дискусійним, що й зумовило реформування та прийняття через два десятиліття Йозифінського кримінального кодексу. Зазначений кодекс складався із частин процесуального та матеріального права, а усі злочини поділялися на: дуже тяжкі, тяжкі та легкі. Перші два виглядали як смертна кара та тілесні покарання, а до легких належали штрафи та конфіскація майна.

Австро-угорський період розвитку кримінального права на території сучасної Чехії пов'язаний з Австрійським Кримінальним кодексом 1852 р., який ще називають Кримінальним Кодексом Франца-Йосифа. Цей кодекс передбачав регулювання процесуального та матеріального кримінального права: «Австрійський Кримінальний кодекс 1852 р. був основним джерелом кримінального права, одним із засобів протидії злочинності, важливим регулятором кримінально-правових відносин у Галичині і Буковині як складової Австрійської імперії, а з 1867 р. – Австро-Угорської монархії, а також у Першій Австрійській республіці (1918–1938 рр.) на території Австрії, яка була у складі Третього Рейху, і на території незалежної Австрійської республіки, утвореної у 1955 р. Цей Кодекс врегульовував лише питання матеріального кримінального права. Незважаючи на значну кількість актів, якими у нього вносились зміни та доповнення, він діяв аж до 1975 р. Цей факт пояснюється

не досконалістю норм цього Кодексу, а лише відсутністю волі правлячої верхівки до прийняття нового Кодексу» [174]. Проте, зазначений нормативно-правовий документ свідчить про еволюцію системи кримінального права.

Чехословаччина є країною, яка утворилася у 1918 р. в результаті відділення від Австро-Угорщини, яка отримала поразку в Першій світовій війні. Варто зазначити, що ця країна має три періоди свого розвитку, а саме: I) 1918-1939 рр. як Чехословацька республіка; II) 1939-1945 рр. Чехословацька республіка у складі нацистської Німеччини; III) Чехословацька соціалістична республіка, яка перебувала під впливом Радянського Союзу. У період до Другої світової війни кримінальне право базувалося на австрійській правовій традиції, з відповідними реформами. У 1950 р. до влади в країні прийшли комуністи із соціалістичною ідеологією. Зміна політичного режиму та необхідність становлення нової соціалістичної ідеології зумовили прийняття нового кримінального кодексу у 1950 року, який визначив покарання як загрозу соціалістичному політичному режиму. Цей кодекс діяв до реформи 1961 року, коли було прийнято новий Кримінальний Кодекс. Варто зазначити, що менше ніж за рік до цього, був прийнятий Кримінальний Кодекс Української РСР та інших країн-членів СРСР.

Після розпаду у 1993 року Чехія та Словаччина стали на шлях формування власних правових систем, які, у свою чергу, відповідали їхньому прагненню вступу до Європейського Союзу. Так, у 2009 році був прийнятий новий Кримінальний Кодекс (закон № 40/2009 Sb.). Структура Кримінального Кодексу Чеської Республіки визначає дві частини: загальна та особлива. Загальна визначає систему регулювання кримінальної відповідальності; обставини, що виключають протиправність дій; звільнення від

кримінальної відповідальності; кримінальні стягнення; зняття судимості; особливі положення щодо окремих видів суб'єктів кримінальних правопорушень.

Варто зазначити, що сьогодні питання кібербезпеки та протидії кіберзлочинам є особливо важливими для Чехії. Проведене «Zlatá koruna» опитування, під назвою «KYBERNETICKÁ, вказує на наступні особливості:

– у частині банківського захисту: «Результати опитування показують, що чехи вірять, що банки захистять свої фінанси. Загалом банкам довіряють 89 % респондентів, з них дуже довіряють 38 %, а скоріше – 51 %. Цікаво, що найбільшою довірою до банків користуються молоді люди віком 25-34 роки (95 %), а також жителі великих міст – із населенням понад 100 тис. (94 %), а також жителі Праги (97 %)»;

– щодо кібератак: «Третина респондентів (31 %) стикалися з тією чи іншою формою кібератаки. Найпоширенішими були: фішинг (47 %), зловмисне програмне забезпечення (26 %) і крадіжка особистих даних (31 %). Викликає тривогу те, що більше п'ятої частини (21 %) цих жертв втратили свої кошти під час нападу»;

– у напрямку джерела кіберризиків: «Інформацію про кіберризики люди найчастіше отримують із ЗМІ (42 %), соціальних мереж (27 %) та банків (27 %). Незважаючи на те, що 82 % респондентів вважають, що банки достатньо інформують про ці ризики, все ще є можливості для покращення»;

– щодо самооцінки та запобіжних заходів: «Більше половини респондентів (57 %) оцінюють себе як помірно обізнаних у питаннях кіберризиків, натомість лише 5 % вважають себе експертами. Із тих, хто вважає себе експертами, 78 % застосовують

двофакторну автентифікацію, а 72 % використовують надійні паролі, що вище, ніж серед населення (62 % і 58 %, відповідно)»;

– встановлення відповідальності за кібератаки: «Опитування також вивчало погляди на те, хто повинен нести відповідальність за шкоду, заподіяну кібератакою. Більшість респондентів (41 %) вважає, що метою атаки має бути фінансова установа. Ще 29 % звинувачують особу в недотриманні вказівок із безпеки, а 26 % звинувачують уряд і регуляторів»;

– щодо електронних атак: «Згідно з опитуванням, 36 % респондентів коли-небудь відкривали підозрілий електронний лист, а 44 % із них не усвідомлювали, що це був підозрілий електронний лист. Навпаки, 64 % респондентів не відкривали підозрілий електронний лист, з яких 51 % видаляли лист, не відкриваючи його, а 32 % перемістили його до спаму»;

– у частині про роль уряду: «Що стосується урядових заходів щодо боротьби з кіберзагрозами у фінансовому секторі, то респонденти віддають перевагу освіті та підвищенню обізнаності щодо кібербезпеки (33 %). Далі йдуть створення та застосування законів (22 %), співпраця із банками та іншими фінансовими установами (22 %) і підтримка досліджень та розробок (20 %)».

Ключовими складовими у формуванні та реалізації державної кримінально-правової політики щодо протидії кіберзлочинності в Чеській республіці є два нормативно-правові акти, а саме: Кримінальний Кодекс Чеської Республіки [264] та Закон Чеської Республіки «Про кібербезпеку» [264]. Зміст зазначених нормативно-правових актів розглянемо більш детально.

Кримінальний Кодекс Чеської республіки, прийнятий у 2009 р., піддавався деяким змінам протягом останніх 15-ти років та складається із загальної та особливої частин. Питання

встановлення кримінальної відповідальності за різні види злочинів, в тому числі і кіберзлочинів, визначено в особливій частині.

Особлива частина Кримінального Кодексу Чеської республіки [75] визначає сукупність злочинів та кримінальну відповідальність за їхнє скоєння, зокрема передбачає наступні кримінальні правопорушення:

– злочини проти життя та здоров'я (Глава I), що визначають наступні види кримінальних правопорушень: проти життя, проти здоров'я, проти вагітних жінок; порушення, що створюють загрозу життю або здоров'ю, пов'язані із незаконним обігом тканин та органів людини, людського ембріона та геному людини;

– кримінальні правопорушення проти свободи, особистих прав, недоторканності приватного життя і таємниці кореспонденції (Глава II). Вони включають кримінальні правопорушення проти свободи та прав на захист особистості, приватного життя та таємниці кореспонденції;

– кримінальні правопорушення проти людської гідності у сексуальній сфері (Глава III);

– злочини проти сім'ї та дітей (Глава IV);

– злочини проти власності (Глава V);

– економічні кримінальні правопорушення (Глава VI), що включають кримінальні правопорушення щодо: валютних цінностей та засобів платежу; податків, зборів та іноземної валюти; обов'язкових правил ринкової економіки та обігу товарів при співробітництві з іноземними державами; промислових прав та авторського права;

– загально-небезпечні кримінальні правопорушення (Глава VII), зміст яких полягає у створенні небезпеки для суспільства та небезпеки для повітряного судна, цивільних кораблів та нерухомої платформи;

– кримінальні правопорушення проти навколишнього середовища (Глава VIII);

– кримінальні правопорушення проти Чеської Республіки, іноземних держав та міжнародних організацій (Глава VIII), які включають кримінальні правопорушення проти: основ Чеської Республіки, іноземних держав та міжнародних організацій; безпеки Чеської Республіки, іноземної держави та міжнародних організацій;

– кримінальні правопорушення проти порядку у публічних питаннях (Глава X), де передбачено кримінальну відповідальність за наступні правопорушення, які спрямовані: проти здійснення повноважень органами державної влади та службовими особами; скоєні службовими особами; корупція; інше втручання у діяльність органів державної влади; порушують спільне проживання людей; інші порушення публічного порядку характеру, скоєні організованою злочинною групою; інші форми злочинного співробітництва;

– кримінальні правопорушення проти військової служби (Глава XI);

– військові кримінальні правопорушення (Глава XII). Так, Кримінальним Кодексом Чеської Республіки передбачено такі види військових злочинів: проти військової субординації та військової честі; проти обов'язку проходження військової служби; проти порядку здійснення охорони, нагляду або виконання інших обов'язків, які створюють загрозу для боєздатності або збройних сил; проти обов'язків членів сил оборони;

– кримінальні правопорушення проти людства, миру та військові злочини (Глава XIII), що включають протиправні дії, воєнні злочини, спрямовані проти людства та миру в цілому.

Питання протидії кіберзлочинам частково регулюються Розділом 2: «Кримінальні правопорушення проти прав на захист особистості, приватного життя та таємниці кореспонденції», II-ї глави «Кримінальні правопорушення проти свободи, особистих прав, недоторканності приватного життя і таємниці кореспонденції».

Зазначеним розділом передбачено кримінальну відповідальність за:

– незаконне розповсюдження особистих даних (стаття 180);

– посягання на права іншої особи (стаття 181);

– порушення таємниці кореспонденції (стаття 182);

Проте основною складовою встановлення кримінальної відповідальності за кіберзлочини є Розділ V «Злочини проти власності» [264]. Зокрема в цій частині кримінального кодексу встановлена кримінальна відповідальність за наступні види кіберзлочинів:

– несанкціонований доступ до комп'ютерної системи та несанкціоноване втручання в комп'ютерну систему чи носій інформації (стаття 230). Цей вид злочину характеризується Кримінальним Чеської Республіки з двох позицій: 1) подолання заходів безпеки і, таким чином, отримання несанкціонованого доступу до комп'ютерної системи або її частини; 2) втручання в комп'ютерну систему або носій інформації шляхом:

a) несанкціонованого використання даних, що зберігаються у комп'ютерній системі або на носії інформації;

b) незаконне видалення або знищення, пошкодження, зміна, приховування, зниження їхньої якості або здійснення їх непридатними для використання даних, що зберігаються у комп'ютерній системі або на носії інформації;

c) фальсифікація або зміна даних, що зберігаються в комп'ютерній системі або на носії інформації, таким чином, що вони вважаються справжніми або діють так, ніби це справжні дані, незалежно від того, чи є дані безпосередньо розбірливими та зрозумілими;

г) несанкціоноване введення або передача даних у комп'ютерну систему чи на носій інформації або здійснення іншого втручання у програмне чи технічне обладнання комп'ютерної системи чи інше технічне обладнання для обробки даних. Надання та зберігання пристрою доступу до комп'ютерної системи, пароля та інших схожих даних (стаття 231).

Такий злочин характеризується, як: виробництво, введення в обіг, імпорт, експорт, транспорт, пропозиція, посередництво, продаж або іншим чином надання, збір або зберігання для себе чи іншої особи:

a) пристрій або його компонент, процедура, інструмент або будь-який інший засіб, включаючи комп'ютерну програму, створений або адаптований для несанкціонованого доступу до електронної комунікаційної мережі, до комп'ютерної системи або її частини або для несанкціонованого втручання в комп'ютерну систему або інформацію носій;

b) комп'ютерний пароль, код доступу, дані, процедуру або будь-які інші аналогічні засоби, за допомогою яких можна отримати доступ до комп'ютерної системи або її частини.

Несанкціоноване втручання у комп'ютерну систему або носій інформації через необережність (стаття 232). Передбачається кримінальна відповідальність за грубу недбалість, через порушення обов'язків, що випливають із роботи, професії, посади чи функції, або накладених законом або прийнятих за контрактом:

a) знищення, пошкодження, зміна або дія, що робить непридатними для використання дані, що зберігаються у комп'ютерній системі або на носії інформації;

b) втручання в технічне або програмне обладнання комп'ютерної системи або інше технічне обладнання для обробки даних.

Міра покарання за зазначеними кіберзлочинами представлена в табл. 3.5.

Відповідно до представлених результатів аналізу Кримінального Кодексу Чеської Республіки, можна визначити, що найбільшим покаранням за кіберзлочини є позбавлення волі до 8-ми років. Досліджуваним нормативно-правовим документом визначено наступні види обставин, які обтяжують покарання:

– намір завдати шкоду чи заподіяти іншу шкоду іншій особі або отримати несанкціоновану вигоду для себе чи іншої особи (застосовуються до статті 230);

– намір незаконно обмежити функціональність комп'ютерної системи чи іншого технічного пристрою для обробки даних (застосовуються до статті 230);

– дії, вчинені членом організованої групи (застосовуються до статей: 230, 231);

– діяння, яке завдає значної шкоди (застосовуються до статті 230);

– діяння, яке могло б мати серйозний вплив на функціонування держави, здоров'я людей; на питання безпеки, економіки або забезпечення основних життєвих потреб населення (застосовуються до статті 230);

Таблиця 3.5

Кримінальна відповідальність за кіберзлочини в Чеській Республіці

Злочин	Покарання	Обставини, які обтяжують/пом'якшують зміст покарання	
		Обставина	Покарання
1	*2*	*3*	*4*
Стаття 230			
Несанкціонований доступ до комп'ютерної системи та несанкціоноване втручання в комп'ютерну систему чи носій інформації	(1) Позбавлення волі на строк до 2-х років, заборона діяльності або конфіскація майна	Намір заподіяти шкоду чи іншу шкоду іншій особі або отримати несанкціоновану вигоду для себе чи іншої особи	Позбавлення волі на строк від 6-ти місяців до 4-х років із забороною діяльності або конфіскацією майна
	(2) Позбавлення волі на строк до 3-х років, із забороною діяльності або конфіскацією майна	Намір незаконно обмежити функціональність комп'ютерної системи чи іншого технічного пристрою для обробки даних	
		Дії, вчинені членом організованої групи	Позбавлення волі на строк від 1-го до 5-ти років або штраф
		Діяння завдає значної шкоди	
		Діяння могло б мати серйозний вплив на функціонування держави, здоров'я людей, безпеку, економіку або забезпечення основних життєвих потреб населення	

Продовження табл. 3.5

1	*2*	*3*	*4*
		Отримує значну вигоду для себе чи іншої особи	
		Діяння спричинило серйозні порушення в діяльності юридичної особи або фізичної особи-підприємця	
		Завдає шкоди великого масштабу	Позбавлення волі на строк від 3-х до 8-ми років або штраф
		Отримує велику вигоду для себе або для іншої особи	
Стаття 231			
Надання та зберігання пристрою доступу до комп'ютерної системи, пароля та інших подібних даних	Позбавлення волі на строк до 2-х з конфіскацією майна або забороною займатися діяльністю	Дії, вчинені членом організованої групи	Позбавлення волі на строк від 3-х років із забороною займатися діяльністю або конфіскація майна
		Отримує значну вигоду для себе чи іншої особи	
		Отримує велику вигоду для себе або для іншої особи	Позбавлення волі на строк від 6-ти місяців до 5-ти років
Стаття 232			
Несанкціоноване втручання у комп'ютерну систему або носій інформації через необережність	Позбавлення волі на строк до 6-ти місяців із забороною займатися діяльністю або конфіскація майна	Завдає шкоди великого масштабу	Позбавлення волі на строк до 2-х з конфіскацією майна або заборона займатися діяльністю

– отримання значної вигоди для себе чи іншої особи (застосовуються до статей: 230, 231);

– діяння, яке спричинило серйозні порушення в діяльності юридичної особи або фізичної особи-підприємця (застосовуються до статті 230);

– дії, які завдають шкоди великого масштабу (застосовуються до статей: 230, 232);

– отримання значної вигоди для себе або для іншої особи (застосовуються до статей: 230, 231).

Окремо увагу варто приділити відповідальності за шахрайство. Цей вид злочину визначено у статті 209 «Шахрайство Кримінального Кодексу Чеської Республіки». Хоча, нормативним документом не визначено власне питання комп'ютерного шахрайства, проте юридична практика в Чехії вказує на значні досягнення у цьому напрямку. У частині щодо порушень громадського порядку у практиці кримінального процесу та притягнення до відповідальності в Чехії, є приклади засудження за кіберзлочини, зокрема в частині статті 357 «Поширення тривоги» (йдеться про свідомі дії, які викликають паніку серед населення). Зміст цієї статті передбачає покарання за: навмисне спричинення небезпеки, провокування серйозного занепокоєння, принаймні серед частини населення, поширення повідомлень про загрозу чи небезпеку, що не є правдивим.

Закон Чеської Республіки «Про кібербезпеку» [264] був затверджений у 2014 р., а поточна редакція набула чинності від 6 серпня від 2022 р. Цей закон переважно регулює кіберпростір та діяльність у кіберпросторі, з метою забезпечення кібербезпеки держави, не встановлюючи при цьому відповідальності за його порушення. Зокрема сферою дії зазначеного закону є регулювання прав та обов'язків осіб та повноваження і компетенції органів

державної влади у сфері кібербезпеки, а також встановлення вимог щодо безпеки електронних комунікаційних мереж. Прийняття цього закону зумовлене необхідністю щодо відповідності національній системі кіберзахисту, згідно з чинними нормами Європейського Союзу, зокрема директивою NIS: «Головною метою закону є: встановити базовий рівень заходів безпеки; покращити виявлення інцидентів кібербезпеки; запровадити звітність про інциденти кібербезпеки; запровадити систему заходів реагування на інциденти кібербезпеки; коригувати діяльність наглядових робочих місць» [264].

Таким чином, Закон «Про кібербезпеки» визначає правове поле функціонування кіберпростору, а Кримінальний Кодекс встановлює відповідальність за його порушення. Варто зазначити, що система державного управління кібербезпекою є інституціолізованою, адже у 2017 р. було утворено спеціалізований орган – Національне управління з кібербезпеки та інформаційної безпеки (NÚKIB).

Республіка Болгарія. Болгарія – одна із небагатьох країн постсоціалістичного табору, яка використовує Кримінальний Кодекс другої половини минулого століття. Це можна пов'язати із багатьма політичними, соціально-економічними та правовими аспектами. Хоча й кримінальне право в Республіці Болгарія має давню історію, проте розвивалося революційно, що унеможливлює прослідкувати певні національні особливості у сучасному кримінальному законодавстві.

Розвиток і трансформація системи кримінального права Болгарії відбувався за наступними етапами: 1) Болгарське Царство (VII – XIV ст.); 2) Османський період (1396 – 1878 рр.); 3) Національне відродження та визволення (XVIII – XIX ст.); 4) Князівство та Царство

Болгарії (1878 –1944 рр.); 5) Соціалістичний період (1944 –1989 рр.); 6) Сучасний період (після 1989 р.).

Особливостями Першого Болгарського Царства, яке припадає на 681 – 1018 рр. та другого Болгарського Царства, яке датується 1185–1396 рр., є те, що основою кримінального права були звичаєві норми та церковні канони, які відігравали найбільшу роль. Так, поєднання візантійського права та слов'янських традицій спостерігається у нормативному акті, прийнятому в період правління князя Бориса I – «Закон судний людям» («Законъ соудный людємъ») [20], який вважається одним із перших нормативних актів серед слов'янських народів, що регулював багато аспектів процесуального характеру. «Закон судний людям» став помітним рубежем у розвитку болгарського феодального права. У його основу покладено кілька джерел, зокрема болгарське звичаєве право. Другим джерелом для укладача слугувала Еклога.

При укладанні «Закону судного людям» активно перероблялися візантійські формули, з метою привести їх у відповідність із болгарською дійсністю. Термінологія пам'ятки – суто слов'янська. Норми «Закону судного людям» дозволяють судити про суспільний лад Болгарії 9 ст. Основна маса болгарського народу складалася з вільних землевладців, які жили громадами. Однак, відносини серед громад були досить крихкими через розвиток приватної власності. Селяни, періоду функціонування «Закону судного людям», вільно розпоряджалися своїми «маєтками». Болгарське суспільство було вже розшарованим. Особи, які належали до землевласної аристократії, як це видно із «Закону судного людям», користувалися у суді привілеями перед простими людьми. Через апелювання до «Закону судного людям» відбувся процес збіднiння і розорення значної частини вільних селян. У тексті закону постійно згадуються

злидарі; йдеться про покарання за крадіжки або напад, з метою грабежу. Все це свідчить про наявність людей, які втратили зв'язки з громадою, були позбавлені землі та засобів виробництва і перетворилися на бідняків. Злидарі та безземельні «свободники» потрапляли у боргову кабалу. «Закон судний людям» згадує не тільки особу боржника, а й «мзденника», який повинен був відпрацьовувати борг. У Болгарії, у 8 – 9 ст., продовжувало існувати патріархальне рабство: у пам'ятці є багато згадок про рабів, яких протиставлено «свободникам». Раб не міг свідчити в суді проти свого пана. Раба, який скоїв крадіжку, передавали тому, у кого він украв, якщо його пан не погоджувався відшкодувати вкрадене. Рабами ставали військовополонені, діти рабині; вільні люди ставали рабами за борги або злочини» [20].

Варто зазначити, що в більшості цей документ регулював питання відповідальності за злочини у сфері економіки та господарських відносин, які мали б відповідати християнським цінностям. Відповідно, покарання найчастіше мали релігійний характер та реалізовувалися у вигляді страти, тілесних покарань чи вигнання. Варто зазначити, що «Закон судний людям», на думку багатьох вчених, був використаний при укладанні «Уставу Ярослава Мудрого» та збірки стародавнього руського права «Руської правди».

Релігійний характер кримінального права в Болгарії не змінився і після завоювання її Османською Імперією. Османське правління припадає на 1396 – 1878 рр., що характеризуються відповідністю кримінального права нормам Шаріату та указам Султана. Лише в окремих місцевих громадах збереглося звичаєве болгарське право в обмеженому вигляді. Зазначимо, що основними формами покарання залишилися: смертна кара, тілесні покарання та конфіскація майна.

Сучасна правова система почала формуватися після визволення Болгарії від Османської Імперії, що відбулося у 1878 році. У цей період формуються та розвиваються революційні налаштування, що в історії характеризується як національне відродження. Саме революціонери заклали основи щодо уявлення про право, а Болгарський революційний центральний комітет почав обговорювати принципи справедливості та покарань.

Перший кримінальний кодекс Болгарії був прийнятий у період Князівства та Царства Болгарії, що припадали на 1878 – 1944 рр. Так, у 1896 р. був прийнятий кримінальний кодекс, основні положення якого базувалися на Кримінальному кодексі російської імперії 1845 р., та регулював протидію злочинам проти особи, власності, громадського порядку та держави. Така ситуація пов'язана з російською підтримкою при визволенні Болгарії. Європейський вплив на Болгарію цього періоду став причиною реформування кримінального законодавства.

Прихід комуністів до влади в Болгарії у 1944 р. визначив вектор політичного та правового розвитку, відповідно до соціалістичних положень. Особливим був Кримінальний кодекс, який було прийнято у 1951 р. Ключовими нововведеннями зазначеного Кримінального кодексу стала кримінальна відповідальність за контрреволюційну діяльність та діяльність, спрямовану проти соціалістичної держави.

Основними формами покарань було визначено: довготривале ув'язнення, смертна кара, ув'язнення у трудових таборах та заслання.

Новий кодекс за часів соціалістичної Болгарії був прийнятий у 1968 р., який, до речі, в реформованому вигляді діє й досі. Цей кодекс був значно реформований після європейського вектору розвитку Болгарії з 1989 р., коли відбулося падіння комуністичного політичного режиму. Приєднання Болгарії у 2007 р. до

Європейського Союзу визначало необхідність реформування Кримінального кодексу, особливо в частині протидії корупції, торгівлі людьми, транснаціональній злочинності та організованій злочинності.

Структура сучасного кримінального кодексу Болгарії [70] передбачає загальну та спеціальну частину. Загальна частина визначає: завдання та механізм дії кримінального кодексу; характеристику злочинів; підготовку та досвід щодо їх здійснення; поняття співучасті та множинності злочинів; визначення кримінально-відповідальної особи; особливості встановлення покарання; особливості відповідальності неповнолітніх; порядок звільнення від покарання; порядок помилування; особливості звільнення від кримінальної відповідальності; особливості реабілітації та примусових медичних заходів.

Особлива частина визначає кримінальну відповідальність за наступні види злочинів:

– злочини проти республіки: державний переворот; зрада та шпигунство; саботаж та диверсія; інші злочини;

– злочини проти особистості: вбивство, тілесні ушкодження, зловживання; викрадення людини та незаконне позбавлення волі; примус, розголошення чужої таємниці; образа і наклеп; розпуста; торгівля людьми;

– злочини проти прав громадян: злочини проти рівноправності громадян; злочини проти свободи віросповідання; злочини проти політичних прав громадян; порушення недоторканності житла, приміщення або транспортного засобу; порушення таємниці листування; злочини проти трудових прав громадян; злочини проти інтелектуальної власності; злочини проти свободи зборів, мітингів і демонстрацій; злочини проти права робітників і службовців об'єднуватися у профспілки;

– злочини проти шлюбу, сім'ї та молоді: злочини проти укладання шлюбу та створення сім'ї; злочини проти молоді;

– злочини проти власності: крадіжка; грабіж; привласнення; шахрайство; вимагання; приховування чужого майна; знищення та пошкодження; зловживання довірою;

– злочини проти підприємництва (бізнесу): загальногосподарські злочини; злочини проти кредиторів; злочини в окремих галузях економіки; злочини проти митного режиму; злочини проти грошово-кредитної системи;

– злочини проти фінансової, податкової та страхової систем;

– злочини проти діяльності державних органів, громадських організацій та осіб, що виконують державні функції: злочини проти державного управління; службові злочини; злочини проти правосуддя; хабарництво;

– злочини проти спорту;

– злочини щодо документів;

– комп'ютерні злочини;

– злочини проти громадського порядку та спорту;

– загально-небезпечні злочини: злочини, вчинені загально-небезпечним способом або загально-небезпечними засобами; злочини у сфері транспорту та зв'язку; злочини проти здоров'я населення та проти довкілля; інші загально-небезпечні злочини; злочини при використанні атомної енергії в мирних цілях;

– злочини проти обороноздатності республіки, проти відомостей, що складають державну таємницю, проти іноземної секретної інформації: злочини проти відомостей, що становлять державну таємницю, та проти іноземної секретної інформації; злочини проти військової служби; злочини проти проходження альтернативної служби в мирний час; інші злочини;

– військові злочини: злочини проти порядку підпорядкування та військової честі; ухилення від військової служби; службові злочини; злочини проти вартової, постової, патрульної, внутрішньої та прикордонної служби; інші військові злочини; військові злочини, вчинені у воєнний час або у рамках бойової обстановки, або під час участі у місії чи операції за межами країни; злочини, пов'язані із військовими діями;

– злочини проти миру та людства: злочини проти миру; порушення законів та звичаїв війни; знищення груп населення (геноцид) і апартеїд.

У контексті об'єктного поля зазначеного дослідження кримінальна відповідальність за кіберзлочини встановлюється Главою 9 а – «Комп'ютерні злочини». Ця глава була введена в дію у 2002 р. та передбачає кримінальну відповідальність за наступні діяння:

– отримання доступу до інформаційної системи або її частин, у малозначних випадках;

– неправомірне додавання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних у малозначних випадках;

– неправомірне додавання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону в електронному вигляді або на електронному чи іншому носії;

– внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу;

– створення, закупівля для себе чи іншої особи, імпорт, експорт, передача, транспортування, надання чи поширення іншим чином комп'ютерної програми, паролів, кодів чи інших подібних даних для доступу до інформаційної системи або її частини, з метою вчинення злочину;

– порушення закону про електронний документообіг під час надання інформаційних послуг та послуг електронної автентифікації.

Покарання за вказані злочини та особливі умови їхнього скоєння визначено в таблиці 3.6.

Відповідно до представлених даних, за кожен вид скоєних комп'ютерних злочинів передбачено позбавлення волі на певний строк, а за окремими видами – ще й штраф. Якщо не аналізувати ті обставини, які обтяжують зміст покарання, то найжорсткіше покарання – це позбавлення волі на строк до семи років. Відповідно, передбачено покарання за такі злочини, як:

а) неправомірне додавання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону, в електронному вигляді або на електронному чи іншому носії;

Таблиця 3.6

Кримінальна відповідальність за кіберзлочини в Болгарії

Злочин	Покарання	Обставини, які обтяжують/пом'якшують зміст покарання	
		Обставина	Покарання
1	*2*	*3*	*4*
Отримання доступу до інформаційної системи або її частин, у малозначних випадках	Позбавленням волі на строк до шести років, а також штраф до трьох тисяч левів	Діяння, вчинене двома або більше особами, які заздалегідь домовилися вчинити таке діяння	Позбавлення волі на строк до шести років і штраф до п'яти тисяч левів
		Діяння, вчинене повторно або стосується даних для створення електронного підпису	Позбавлення волі на строк до семи років і штраф до двадцяти тисяч левів
		Діяння, вчинені щодо інформації, яка становить державну чи іншу охоронювану законом таємницю	Позбавлення волі на строк від чотирьох до восьми років, якщо не передбачено більш суворого покарання
		Діяння, яке було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	
		Таке діяння призвело до тяжких наслідків	Позбавлення полі від п'яти до дванадцяти років

Продовження табл. 3.6

1	*2*	*3*	*4*
Неправомірне додавання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютерних даних в інформаційній системі або припинення доступу до таких даних у малозначних випадках	Позбавлення волі на строк до шести років і штраф до десяти тисяч левів	Були завдані значні збитки або це спричинило інші тяжкі наслідки	Позбавлення волі на строк до семи років і штраф до двадцяти тисяч левів
		Діяння, вчинене з метою отримання майнової вигоди	Позбавлення волі на строк від п'яти до семи років і штраф до десяти тисяч левів
		Діяння, яке було здійснено за допомогою комп'ютерної програми, пароля, коду доступу чи інших даних доступу до інформаційної системи або до її частини, призначених для впливу на більше ніж одну інформаційну систему; було завдано значних збитків або спричинено ряд інших тяжких наслідків	Позбавлення волі від п'яти до восьми років і штраф до двадцяти тисяч левів
		Діяння, вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи	Позбавлення волі від дев'яти до дванадцяти років і штраф до тридцяти тисяч левів
		Діяння було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	

Продовження табл. 3.6

1	*2*	*3*	*4*
Неправомірне додавання, копіювання, використання, зміна, передача, видалення, пошкодження, псування, приховування, знищення комп'ютер-них даних в інформаційній системі або припинення доступу до таких даних, які можуть бути передані на підставі закону, в електронному вигляді або на електронному чи іншому носії	Позбавлення волі на строк до семи років і штраф до п'яти тисяч левів	Діяння має на меті перешкодити виконанню зобов'язання	Позбавлення волі від п'яти до семи років і штраф до семи тисяч левів
Внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу	Позбавлення волі на строк до семи років і штраф до п'яти тисяч левів	Діяння завдало значної шкоди	Позбавлення волі до дев'яти років і штраф до двадцяти тисяч левів
		Діяння було вчинено повторно	
		Діяння вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури	Позбавлення волі на строк від п'яти до дванадцяти років і штраф до двадцяти тисяч левів

Продовження табл. 3.6

1	*2*	*3*	*4*
Створення, закупівля для себе чи іншої особи, імпорт, експорт, передача, транспортування, надання чи поширення іншим чином комп'ютерної програми, паролів, кодів чи інших подібних даних для доступу до інформаційної системи або її частини з метою вчинення злочину	Позбавлення волі на строк до шести років	Відбулося розголошення персональних даних, секретної інформації чи іншої таємниці, що охороняється законом, якщо вчи-нене не становить більш тяжкого злочину	Позбавлення волі на строк від чотирьох до семи років
		Діяння вчинено з метою отримання майнової вигоди	Позбавленням волі на строк до дев'яти років
		Діяння, вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи	
		Діяння завдало значної шкоди	
		Внаслідок діяння було завдано важких наслідків	
Порушення закону про електронний документообіг під час надання інформаційних послуг та послуг електронної автентифікації	Позбавлення волі на строк до шести років і штраф у розмірі до п'яти тисяч левів, якщо не підлягає суворішому покаранню	Не передбачено	Не передбачено

б) внесення комп'ютерного вірусу в інформаційну систему або комп'ютерну мережу. Варто зазначити, що за такими видами злочинів передбачено не лише загальноприйняті обставини, які обтяжують покарання за скоєння злочину, а й наведено певні спеціальні обставини. Серед двох груп обставин виділяємо наступні:

– такі, що завдали значних збитків або спродукували низку тяжких наслідків;

– протизаконні дії, які призвели до тяжких наслідків;

– відбулося розголошення персональних даних, секретної інформації чи іншої таємниці, що охороняється законом, якщо вчинене не становить більш тяжкого злочину;

– діяння було вчинено повторно;

– діяння було вчинено проти інформаційної системи або комп'ютерної мережі, яка є частиною критичної інфраструктури;

– діяння було скоєно за допомогою комп'ютерної програми, пароля, коду доступу чи інших даних доступу до інформаційної системи або до її частини, призначених для впливу на більше ніж одну інформаційну систему, і були завдані значні збитки або це призвело до інших тяжких наслідків;

– діяння вчинено двома або більше особами, які заздалегідь домовилися вчинити таке діяння;

– діяння вчинене особою, яка діяла на замовлення або на виконання рішення організованої злочинної групи;

– діяння вчинено повторно або щодо даних для створення електронного підпису;

– діяння вчинені щодо інформації, що становить державну чи іншу охоронювану законом таємницю;

– діяння вчинено з метою отримання майнової вигоди (корисливих цілей);

– діяння завдало значної шкоди;

– діяння має на меті перешкодити виконанню зобов'язань.

Зазначена увага до досвіду Болгарії, у встановленні кримінальної відповідальності за кіберзлочини, має бути приділена саме у розширенні спектру специфічних загальних обставин, які обтяжують покарання. Це є вкрай важливим при необхідності протидії гібридним війнам та становить цінність для інформаційного захисту критичної інфраструктури.

Таким чином, в результаті дослідження було ідентифіковано особливості еволюції кримінального права країн Європейського Союзу (Болгарії, Чехії, Польщі), які перебували у складі соціалістичного табору. Здійснено структурний та змістовний аналіз основних нормативних документів, що встановлюють кримінальну відповідальність за злочини. Визначено, що кіберзлочинам, у кримінальних кодексах досліджуваних країн, приділено окремі розділи, зокрема в Польщі – Розділ XXXIII «Злочини проти охорони інформації»; у Чехії – Розділ V «Злочини проти власності»; у Болгарії – Главу 9 а «Комп'ютерні злочини». Варто зазначити, що в Польщі досліджувані злочини визначають як злочини проти охорони інформації, а в Чехії як злочини проти власності. Натомість, у Кримінальних кодексах Болгарії ці злочини є відокремленими. Встановлено, що в досліджуваних країнах, незважаючи на їх членство в Європейському Союзі, відсутні єдині підходи щодо механізму покарання та поняття «кіберзлочину», що можна пояснити національними правовими традиціями та особливою увагою політиків до інформаційної безпеки держави.

При реформуванні кримінального права в Україні в умовах євроінтеграційних процесів є потреба у врахуванні лише часткового досвіду зазначених країн, адже вже майже десятиліття точиться дискусія щодо необхідності прийняття нового кримінального кодексу, який має врахувати сучасні методи скоєння

злочинів, їхню класифікацію та систему групування. Оскільки кіберзлочини можуть бути скоєні в різних сферах суспільного життя, то матимуть різноманітні наслідки соціального, економічного, політичного, правового характеру, що, врешті, визначатиме їхню домінантну складову.

3.3. Досвід політики протидії кіберзлочинності Литовської республіки як країни ЄС з радянським минулим

Правова історія Литовської Республіки визначається сукупністю соціально-економічних, політичних та міжнародних факторів. За всю історію свого існування Литовська республіка пережила епохи незалежності при різних політичних режимах й епохи анексії частини територій та окупації. Натомість, історію кримінально-правової системи Литви умовно можна розділити на наступні етапи:

1) Велике князівство Литовське, що припадає на середньовічні часи (XIII – XVI ст.). Особливістю зазначеного періоду розвитку правової системи на території сучасної Литви є орієнтація на звичаєві норми та зміст руського права. Проте, на перетині XIII – XIV століть система права починає кодифікуватися, що пов'язано із прийняттям Литовських статутів у 1529, 1566 та 1588 роках. Зазначені статути визначали особливості державного, цивільного, сімейного, кримінального та процесуального права. Положення статутів базувалися на положеннях римського, польського, руського та німецького права. Зокрема в першому, або як його прийнято називати Старий литовський статут, що був прийнятий 29 вересня 1529 р., правові положення регулювали кримінальне, цивільне та господарське право, а також визначали

судово-процесуальні особливості. Варто зазначити, що особливі права, навіть в частині кримінальної відповідальності, надавалися шляхті. Особливістю Другого Литовського Статуту (1566 р.) (у деяких джерелах його називають Волинським, через особливу роль волинської шляхти) є те, що він мав релігійну основу, адже до його утворення було залучено 5 католиків та 5 православних. Цей статут переважно був спрямований на реалізацію адміністративної реформи в країні. Третій, або Великий Литовський статут, був введений в дію у 1588 р. та мав 14 розділів, які включали 488 артикулів. Цим статутом в частині кримінального права були закріпленні положення щодо навмисних злочинів та злочинів, скоєних із необережності. У частині процесуальних дій було визначено, що суд мав враховувати вік злочинця, зокрема вводилося поняття покарання неповнолітніх осіб. Значна увага приділялася співучасті у скоєнні злочинів, яка поділялася на просту та складну. Вводиться поняття рецидиву. У той же час злочин, вчинений шляхтичами, карався значено меншою мірою покарання.

2) Розвиток у складі Речі Посполитої, що припадає на період з другої половину XVI по кінець XVIII. Люблінська унія 1569 року передбачала входження Литви до складу Речі Посполитої, що значно вплинула на правову систему та сучасній території Литви в цілому та системи кримінального права зокрема, незважаючи на те, що Великий Литовський статут залишався чинним. Великий вплив мало польське право, що передбачало значні міри покарання за злочини проти релігії, держави та власності.

3) окупаційний період в складі російської імперії (з кінця XVIII століття по початок XX століття). Зазначений період пов’язаний із поділами речі посполитої (1772 р., 1793 р. та 1795 р.) між Австрією, Пруссією та росією. Відповідно до зазначеного, сучасні литовські території відійшли російській імперії. Варто

стверджувати, що Великий Литовський статут 1588 р., із відповідними змінами в результаті впливу польського законодавства, діяв до 1840 р. Відповідно, з 1840 р. усі закони були замінені на закони російської імперії, Кримінальний Кодекс якої вміщував найбільші покарання, які тільки могли передбачалися за злочини проти імперії;

4) міжвоєнний період або період незалежності Литви, що припадає на роки між Першою та Другою світовою війнами. Зазначений період характеризується значними політичними змінами. У частині права варто наголосити на прийнятті Конституції 1922 р.;

5) період радянської окупації, що припадає на період з початку Другої світової війни до 1990 р. У липні 1940 р. була утворена Литовська радянська соціалістична республіка. Питання долі Литовської республіки вирішувалося в серпні 1939 р. підписанням пакту Молотова-Ріббентропа, згідно з яким території Литви мали знаходитися під впливом Німеччини. Проте, розв'язання Другої світової війни Німеччиною та напад на Польщу, сприяли обміну Литви на частину Польщі. Після нападу Німеччини на Радянський Союз, сучасна територія Литви була окупована, проте у 1944 р. Литва опинилася знову під впливом Радянського Союзу, а вже 1946 р. відбулися перші вибори – і Литовська радянська соціалістична республіка висунула своїх представників до верховної ради СРСР.

У цей період система кримінального права відповідала радянським положенням, а тому, як і в більшості країн членів СРСР, у 1961 р. був прийнятий новий кримінальний кодекс, значна увага якого були сконцентрована на захисті ідеологічних положень соціалістичної держави та захисті державної власності.

6) Сучасний період розпочався із проголошення незалежності та виходу зі складу Радянського Союзу. Отримання незалежності Литви у 1990 р. стало початком політичних змін, а саме демократизації усіх суспільних процесів у державі. У 2000 р. в Литві був прийнятий новий кримінальний кодекс. Стаття 1 Кримінального кодексу Литовської республіки визначає наступне: «Кримінальний кодекс Литовської Республіки є єдиним кримінальним законом, метою якого є захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних діянь засобами кримінального права. Цей кодекс: 1) визначає, які діяння є злочинами та проступками, і забороняє їх; 2) визначає покарання, заходи стягнення та систему заходів виховного характеру за діяння, передбачені цим Кодексом, а також примусові заходи медичного характеру; 3) визначає підстави та умови кримінальної відповідальності, а також підстави та умови, за яких особи, які вчинили злочинні діяння, можуть бути звільнені від кримінальної відповідальності чи покарання. Положення цього Кодексу співзвучне із положеннями законодавства Європейського Союзу» [230]. Аналізуючи структуру Кодексу, визначимо наступні характеристики загальної та особливої частини.

Загальна частина містить положення, що регулюють: сферу дії кодексу та загальні положення кримінальної відповідальності; тривалість кримінальної відповідальності; чинність положень кримінального кодексу щодо осіб, які вчинили злочинні діяння на території Литовської Держави або на морських чи повітряних суднах під прапором чи знаками розрізнення Литовської Держави; кримінальна відповідальність за злочини, що вчинені резидентами за кордоном; кримінальна відповідальність іноземців за злочинні дії, вчинені за кордоном проти громадян Литовської Республіки та інших осіб, які постійно проживають у Литві; кримінальна

відповідальність іноземців за злочини проти Литовської держави, вчинені за кордоном; кримінальна відповідальність за злочини, передбачені міжнародними договорами; кримінальна відповідальність за злочинні діяння, вчинені за кордоном; екстрадиція; передача особи за європейським ордером на арешт; характеристика злочинності та кримінальних правопорушень; стадій та форми злочинних дій; обставини виключення кримінальної відповідальності; звільнення від кримінальної відповідальності; призначення та види покарання; міри, які мають злочинно-правові наслідки; зупинення відбування покарання та звільнення від покарання; строки давності кримінальної відповідальності; примусові заходи медичного характеру.

Особлива частина Кримінального кодексу Литовської республіки [230] визначає особливості кримінальної відповідальності за різні види злочинів, зокрема:

– злочини проти людяності та воєнні злочини;

– злочини проти незалежності, територіальної цілісності та конституційного ладу Литви;

– злочини проти життя людини;

– злочини проти здоров'я людини;

– злочини, небезпечні для здоров'я та життя людини;

– злочини та кримінальні порушення проти свободи людини;

– злочини та кримінальні правопорушення проти статевої свободи;

– злочини проти честі та гідності особи;

– злочини та кримінальні правопорушення проти дитини та сім'ї;

– злочини проти особистого приватного життя;

– злочини та кримінальні правопорушення проти рівності та свободи совісті;

– проти виборчих прав осіб та процедури виборів або референдумів Президента, Сейму, Європейського Парламенту, Муніципальних рад та мерів, процедури фінансування політичних організацій, аналітичних центрів і політичні кампанії;

– злочини та кримінальні порушення проти особистих соціальних прав;

– злочини і проступки проти власності, майнових прав і майнових інтересів;

– злочини проти інтелектуальної власності;

– злочини проти безпеки електронних даних та інформаційних систем;

– злочини та кримінальні правопорушення проти економіки та бізнесу;

– злочини та кримінальні правопорушення щодо фінансової системи;

– злочини та кримінальні правопорушення у контексті публічних служб та суспільних інтересів;

– злочини та проступки для правосуддя;

– злочини проти громадської безпеки;

– злочини та кримінальні правопорушення, пов'язані зі зберіганням зброї, боєприпасів, вибухових речовин, вибухових пристроїв або радіоактивних матеріалів чи військової техніки;

– злочини та кримінальні правопорушення, пов'язані зі зберіганням наркотичних та психотропних, токсичних або сильнодіючих речовин;

– злочини та кримінальні правопорушення проти навколишнього середовища та здоров'я людини;

– злочини та кримінальні правопорушення щодо безпеки руху;

– злочини та кримінальні порушення проти громадського порядку;

– злочинна діяльність проти державного службовця або особи, що виконує функції державного управління;

– злочини та кримінальні правопорушення щодо підробки документів або іншої інформації;

– злочини та кримінальні порушення проти моралі;

– злочини та кримінальні правопорушення щодо пам'яті померлих;

– злочини та кримінальні правопорушення проти служби нацгвардії та мобілізації.

Кримінальна відповідальність щодо кіберзлочинів встановлена розділом XXX «Злочини проти безпеки електронних даних та інформаційних систем»; у цьому розділі визначено наступні види злочинів та кримінальних правопорушень:

– незаконний доступ до електронних даних (стаття 196), якою передбачено кримінальну відповідальність особи, до речі, і фізичної, і юридичної, яка незаконно знищила, пошкодила, вилучила або змінила електронні дані або обмежила використання таких даних за допомогою апаратних, програмних чи інших засобів, що завдають шкоди;

– протиправний вплив на інформаційну систему (стаття 197). Цією статтею визначено кримінальну відповідальність фізичної та юридичної особи, яка незаконно порушила або перервала роботу інформаційної системи шляхом заподіяння шкоди;

– незаконне перехоплення та використання електронних даних (стаття 198), що характеризуються як: незаконне відстеження, записування, перехоплення, отримування, зберігання, привласнення, поширення або іншим чином використання

непублічних електронних даних фізичною та / або юридичною особою;

– незаконний доступ до інформаційної системи (стаття 198.1), що передбачає відповідальність особи, яка незаконно підключилася до інформаційної системи або її частини з порушенням заходів захисту інформаційної системи;

– незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних (стаття 198.2), зміст якої полягає в наступному: сюди входить будь-хто, хто зі злочинною метою або іншим чином незаконно виготовляв, транспортував, імпортував, продавав, надавав доступ або іншим чином поширював, придбав або зберігав пристрої чи програмне забезпечення, безпосередньо призначені або адаптовані для вчинення злочинних дій, а також паролі, коди чи інші подібні дані для реєстрації в інформаційну систему або її частину.

У таблиці 3.7 визначено особливі наслідки скоєння таких злочинів та види покарань, що передбачені Кримінальним Кодексом.

Відповідно представлені за кіберзлочини покарання можуть бути у формі:

– громадських робіт;

– накладання штрафу;

– обмеження волі;

– арешту;

– позбавлення волі.

Таблиця 3.7

Кримінальна відповідальність за кіберзлочини в Литовській Республіці

Злочин	Покарання	Обставини, які обтяжують/пом'якшують зміст покарання	
		Обставина	Покарання
1	*2*	*3*	*4*
Стаття 196 . Незаконний доступ до електронних даних			
Незаконне знищення, пошкодження, вилучення або зміна електронних даних або обмеження використання таких даних за допомогою апаратних, програмних чи інших засобів, що завдають шкоди	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до двох років	Діяння, вчинене щодо електронних даних багатьох інформаційних систем або електронних даних інформаційної системи, що має стратегічне значення для національної безпеки або має важливе значення для державного управління, економіки чи фінансів системи, або використання чужих персональних даних, або заподіяння великої шкоди	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до шести років
Стаття 197 . Протиправний вплив на інформаційну систему			
Незаконне порушення або припинення роботи інформаційної системи шляхом заподіяння шкоди	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до двох років	Діяння, вчинене щодо ряду інформаційних систем або інформаційної системи, що має стратегічне значення для національної безпеки, або щодо інформаційної системи, яка має велике значення для державного управління, економіки чи фінансової системи, або використання чужих персональних даних, чи заподіяння великої шкоди	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до шести років
Стаття 198 . Незаконне перехоплення та використання електронних даних			
Незаконне відстеження, записування, перехоплювання, отримування, зберігання, привласнення, по-ширення або іншим чином використання непублічних електронних даних	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до чотирьох років	Діяння, скоєне щодо закритих електронних даних, що мають стратегічне значення для національної безпеки або мають важливе значення для державного управління, економіки чи фінансової системи	Штраф або обмеження волі, або арешт, або позбавленням волі на строк до шести років

Продовження табл. 3.7

1	*2*	*3*	*4*
Стаття 198.1. Незаконний доступ до інформаційної системи			
Незаконне підключення до інформаційної системи або її частини з порушенням заходів захисту інформаційної системи	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до двох років	Діяння, скоєне щодо інформаційної системи, що має стратегічне значення для національної безпеки або важливе для державного управління, економіки чи фінансової системи	Громадські роботи або штраф, або обмеження волі, або арешт, або позбавлення волі на строк до трьох років
Стаття 198.1. Незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних			
Зі злочинною метою або іншим чином, незаконне виготовлення, транспортування, імпортування, продаж, надання доступу або іншим чином поширення, придбання або зберігання пристроїв чи програмного забезпечення, безпосередньо призначених або адаптованих для вчинення злочинних дій, а також паролі, коди чи інші подібні дані для реєстрації в інформаційну систему або її частину	Штраф або обмеження волі, або арешт, або позбавлення волі на строк до чотирьох років	Не передбачено	Не передбачено

Щодо позбавлення волі, то найбільший строк передбачено (якщо не зважати та обставини, які обтяжують покарання) за такі статті, як-от: незаконне перехоплення та використання електронних даних (стаття 198) та незаконна утилізація пристроїв, програмного забезпечення, паролів, кодів та інших даних (стаття 198.1). Основними складовими, що визначають обставини, які обтяжують покарання за скоєння кіберзлочину, в Литовські Республіці є наступні:

– злочин скоєно щодо інформаційної системи, що має стратегічне значення для національної безпеки;

– злочин скоєно щодо інформаційної системи, що має важливе значення для державного управління;

– злочин скоєно щодо інформаційної системи, що має важливе значення для економіки чи фінансової системи;

– у результаті були використані або оприлюдненні чужі персональні дані;

– у результаті злочину було завдано великої шкоди.

Досвід Литовської Республіки вказує на різноманітність покарання за кіберзлочини. Особливістю досліджуваного Кримінального Кодексу Литовської Республіки є встановлення кримінальної відповідальності юридичних осіб. Цей фактор відрізняє Кримінальний Кодекс Литовської Республіки від Кримінальних Кодексів інших досліджуваних країн.

РОЗДІЛ 4

МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

4.1. Модернізація діяльності суб'єктів формування та реалізації державної кримінально-правової політики протидії кіберзлочинності

Визначальним у формуванні державно-кримінальної політики щодо протидії кіберзлочинності є формування трансформації суб'єктної структури державного управління. На сьогодні відсутнє інституційне забезпечення з питань протидії кіберзлочинності, адже в цьому напрямку працює лише департамент кіберполіції при Національній поліції України, що має обмежені функції. Відповідно, доречною видасться актуалізація наукового пошуку щодо встановлення адміністровано-правового статусу суб'єктів державного управління, які реалізують державну кримінально-правову політику з питань протидії кіберзлочинності, а також сприяють розширенню суб'єктної структури.

Зазначені питання частково викладено в наукових працях вітчизняних та зарубіжних вчених, зокрема: Т. В. Барановської, М. О. Будакового, О. М. Будонової, В. М. Бутузова, М. М. Галамбо, Д. О. Грицишена, А. П. Дикого, М. О. Думчикова, В. В. Євдокимова, Н. А. Загребельної, І. Д. Казанчук, Р. А. Калюжного, Н. В. Камінської, І. В. Каріх, К. О. Кислої, В. В. Коваленко, Я. Ю. Кондратьєва, Б. А. Кормичема, А. В. Котелевець, О. В. Кравчука, В. О. Кучменка,

Ю. Є. Максименка, К. В. Малишева, А. І. Марущака, Г. В. Новицького, Т. М Пушкарьової, С. О. Савчука, Т. С. Ярового, Т. П. Яцик та інших.

У попередніх дослідженнях нами визначено, що суб'єктна структура державної політики з питань протидії кіберзлочинності визначається як механізм, у якому центральні органи виконавчої влади реалізують державну кримінально-правову політику з протидії кіберзлочинності (Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Міністерство оборони України, Міністерство юстиції України, Міністерство фінансів України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, Національне агентство з питань запобігання корупції, Державна служба фінансового моніторингу України); суб'єкти правоохоронної діяльності, на які покладаються функції з протидії кіберзлочинності, що прямо пов'язані із протидією кіберзлочинності (Служба безпеки України, Національна поліція України, Державне бюро розслідувань, Служба зовнішньої розвідки України); суб'єкти правоохоронної діяльності, на які покладаються функції із протидії кіберзлочинності, що опосередковано пов'язані із протидією кіберзлочинності (Національне антикорупційне бюро України, Бюро економічної безпеки України, Державна прикордонна служба України, Національна гвардія України, Державна митна служба України, Управління державної охорони України). Для визначення їхньої ролі в реалізації досліджуваної політики доречно буде здійснити правовий аналіз нормативних документів щодо їхнього адміністративно-правового статусу та повноважень.

Міністерство цифрової трансформації України, відповідно до [108] виконує наступні завдання:

– забезпечення формування та реалізації державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектру, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронної ідентифікації та електронних довірчих послуг та інвестицій в IT-індустрію; у сфері розвитку IT-індустрії;

– бере участь у формуванні державної політики у сферах криптографічного і технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

– бере участь у забезпеченні розвитку віртуальних активів, блокчейну та токенізації, штучного інтелекту;

– бере участь у розробленні норм, стандартів у сферах електронної ідентифікації та електронних довірчих послуг, у тому числі для забезпечення інтероперабельності та

технологічної нейтральності технічних рішень, а також недопущення їх дискримінації;

– бере участь у розробленні критеріїв і порядку проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-комунікаційних системах; організації та проведенні оцінки стану захищеності державних інформаційних ресурсів, наданні відповідних рекомендацій;

– бере участь в розробленні та погодженні проєкту порядку користування радіочастотним спектром в Україні в особливий період та в умовах надзвичайного або воєнного стану, порядку користування радіочастотним спектром в Україні для потреб дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні та військових формувань іноземних держав, які тимчасово перебувають на території України;

Вище вказане засвідчує, що Міністерство цифрової трансформації України є суб'єктом державного управління, шо унормовує та керує віртуальним простором України, а також визначає особливості впровадження та застосування сучасних інформаційних технологій.

Міністерство внутрішніх справ України здійснює свою діяльність на основі [123], яким передбачено наступні складові, що визначають напрями державної кримінально-правової політики з питань протидії кіберзлочинності:

– розробляє проєкти законів та інших нормативно-правових актів з питань, що належать до його компетенції;

– погоджує проєкти законів, інших актів законодавства, які надходять на погодження від інших міністерств та центральних органів виконавчої влади; готує в межах повноважень, передбачених законом, висновки і пропозиції до проєктів законів, інших актів законодавства,

які подаються на розгляд Кабінету Міністрів України, та проектів законів, внесених на розгляд Верховної Ради України іншими суб'єктами права законодавчої ініціативи, нормативно-правових актів Верховної Ради Автономної Республіки Крим;

– розробляє проєкти державних програм із питань забезпечення публічної безпеки і порядку, протидії злочинності, безпеки дорожнього руху, охорони державного кордону, захисту об'єктів і територій на випадок виникнення надзвичайних ситуацій, а також із питань міграції;

– забезпечує міжнародне співробітництво, бере участь у розробленні проєктів та укладенні міжнародних договорів України з питань, що належать до його компетенції; забезпечує у межах повноважень, передбачених законом, виконання укладених міжнародних договорів України;

– забезпечує функціонування криміналістичного обліку та обліку знарядь кримінальних правопорушень, інших об'єктів;

– забезпечує належне функціонування єдиної інформаційної системи МВС, формує та підтримує в актуальному стані інформаційні ресурси, що входять до єдиної інформаційної системи МВС, здійснює обробку персональних даних у межах повноважень, передбачених законом, забезпечує режим доступу до інформації, надає інформаційні та кваліфіковані електронні довірчі послуги, забезпечує здійснення повноважень з питань цифрового розвитку;

– здійснює інформаційну взаємодію з іншими державними органами, правоохоронними органами іноземних держав та міжнародними організаціями;

– організовує та забезпечує експлуатацію, розвиток, координацію та функціонування системи зв'язку МВС, управління і моніторинг єдиної цифрової відомчої електронної комунікаційної мережі МВС та закріпленого радіочастотного спектра;

– забезпечує виконання функцій радіочастотного органу спеціального користувача радіочастотного спектру;

– забезпечує у межах повноважень, передбачених законом, захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Відповідно, на Міністерство внутрішніх справ покладається сукупність завдань, які полягають у формуванні правового, інформаційного, технічного, технологічного, криміналістичного та кримінологічного забезпечення функціонував правоохоронної системи в цілому та інформаційної безпеки держави зокрема. Крім того, важливим завданням є реалізація міжнародно-правового механізму щодо протидії злочинності загалом.

Міністерство закордонних справ України [124] має наступні повноваження, які визначають його роль та значення щодо реалізації державної політики, відтак воно:

– забезпечує підтримання дипломатичних і консульських зносин з іноземними державами, представництво України у міжнародних організаціях та спеціальних місіях;

– забезпечує національні інтереси і міжнародну безпеку України шляхом підтримання мирного та взаємовигідного співробітництва з іноземними державами і міжнародними організаціями за загальновизнаними принципами та нормами міжнародного права;

– вносить пропозиції щодо визнання Україною іноземних держав, встановлення з ними дипломатичних зносин;

– забезпечує інформування Президента України, Верховної Ради України, Кабінету Міністрів України та інших державних органів про найбільш важливі та резонансні події у світі, вносить пропозиції щодо реагування на події, що безпосередньо стосуються національних інтересів, надає їм інформацію, необхідну для реалізації ефективної зовнішньої та внутрішньої політики;

– вносить пропозиції щодо ініціатив міжнародного характеру, здійснення заходів, спрямованих на підвищення ефективності співпраці України з іноземними державами і міжнародними організаціями;

– поширює за кордоном інформацію про Україну, її місце і роль у світі для зміцнення позитивного міжнародного іміджу держави, забезпечує закордонні дипломатичні установи України відповідною інформаційною продукцією;

– забезпечує реалізацію в межах повноважень, передбачених законом, державної політики у сфері європейської інтеграції та євроатлантичного співробітництва;

– забезпечує діяльність Комісії з питань партнерства України з Організацією Північноатлантичного договору та здійснює координацію роботи з розроблення проекту Річної національної програми співробітництва Україна – НАТО;

– здійснює захист прав та інтересів України під час вирішення міжнародних спорів за участю України та інших суб'єктів міжнародного права;

– забезпечує охорону державної таємниці в системі органів дипломатичної служби під час здійснення зовнішніх зносин.

Відповідно до зазначеного, на Міністерство закордонних справ покладається завдання, які полягають у забезпеченні інформаційної безпеки представництвами за кордоном, а також передбачено ряд завдань щодо реалізації міжнародно-правового механізму, особливо в частині європейської та північно-атлантичної інтеграції та ратифікації сукупності міжнародних нормативно-правових актів.

Міністерство оборони України, відповідно до [125] наділено сукупністю повноважень, які можна віднести до реалізації державної кримінально-правової політики з питань протидії кіберзлочинності. Воно, насамперед:

– провадить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави;

– координує створення та розвиток ефективної системи стратегічних комунікацій у Міноборони та Збройних Силах як складової загальнодержавної системи стратегічних комунікацій, забезпечення її стійкості та адаптивності до реагування на виклики та загрози;

– бере участь у виконанні завдань державної інформаційної політики у сфері оборони, інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та протидію інформаційним операціям агресора (противника), а під час дії правового режиму воєнного стану координує складові сил оборони з питань забезпечення формування та реалізації державної інформаційної політики у сфері оборони;

– проводить постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози у сфері оборони, здійснює відповідні заходи;

– забезпечує впровадження та розвиток новітніх інформаційних технологій у сфері оборони;

– відповідно до компетенції, забезпечує електронну інформаційну взаємодію з органами державної влади під час обміну інформацією для здійснення повноважень, визначених законодавством;

– в установленому порядку розробляє та затверджує цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником яких є Збройні Сили.

Міністерство оборони України є основним суб'єктом державного управління, що забезпечує національну безпеку та оборону держави, у тому числі інформаційну, а також кіберзахист суб'єктів оборони держави.

Міністерство юстиції України, згідно з відповідним положенням [127], здійснює свою діяльність, яка пов'язана із протидією кіберзлочинності, зокрема:

– розробляє проєкти законів та інших нормативно-правових актів;

– розробляє пропозиції щодо вдосконалення законодавства та подає їх в установленому порядку на розгляд Кабінету Міністрів України;

– здійснює науково-методичне та організаційно-управлінське забезпечення діяльності судових експертів, які не є працівниками державних спеціалізованих установ; визначає порядок здійснення контролю за дотриманням законодавства з питань судово-експертної діяльності судовими експертами, які не є працівниками державних спеціалізованих установ, та здійснює такий контроль;

– організовує науково-методичне забезпечення судово-експертної діяльності та здійснює організаційно-управлінські функції щодо діяльності науково-дослідних установ судових експертиз Мін'юсту; визначає порядок здійснення контролю за дотриманням законодавства з питань судово-експертної діяльності науково-дослідними установами судових експертиз Мін'юсту та здійснює такий контроль;

– готує пропозиції щодо укладення міжнародних договорів України з питань міжнародно-правових відносин та правового співробітництва у цивільних і кримінальних справах, у галузі міжнародного приватного права, захисту прав людини;

– здійснює міжнародне співробітництво у сфері примусового виконання рішень, налагоджує і підтримує зв'язки з міжнародними організаціями;

– перевіряє стан виконання органами державної влади зобов'язань, узятих за міжнародними договорами України з питань

міжнародно-правових відносин і правового співробітництва у цивільних і кримінальних справах, надає рекомендації щодо поліпшення відповідної роботи, вносить пропозиції щодо усунення виявлених порушень і недоліків та притягнення до відповідальності посадових осіб, винних у допущених порушеннях;

– бере в установленому порядку участь у роботі двосторонніх і багатосторонніх комісій, а також інших міжнародних органів та інституцій, погоджує кандидатури членів та іншого персоналу від України в міжнародних судових органах і радників із правових питань закордонних дипломатичних установ України;

– у межах повноважень, передбачених законом, бере участь у діяльності міжнародних організацій, членом яких є Україна, та вживає заходів для виконання зобов'язань, що випливають із членства України в цих організаціях.

Конкретних завдань щодо забезпечення протидії кіберзлочинності в досліджуваному положенні не вміщено, проте представлені вище положення характеризують діяльність Міністерства з позиції формування та експертної оцінки правового поля щодо функціонування віртуального простору та використання інформаційно-комп'ютерних технологій. Крім того, Міністерство визначає особливості реалізації кримінально-правового механізму щодо протидії кіберзлочинності, зокрема в частині правового, кримінологічного та криміналістичного забезпечення. Вагоме значення діяльність Міністерства має при реалізації міжнародно-правового механізму – через участь у міжнародних організаціях, ратифікацію міжнародних договорів.

Міністерство фінансів України провадить свою діяльність відповідно до положення [126]. Згідно із вказаним положенням, можна визначити наступні складові діяльності, які пов'язані із реалізацією економічного механізму державної кримінально-правової політики з

питань протидії кіберзлочинності та тих моментів, які стосуються інформаційного захисту. Йдеться про:

– забезпечення умов для здійснення повноважень головного розпорядника бюджетних коштів в установах і організаціях, які належать до сфери управління Мінфіну, в центральних органах виконавчої влади, діяльність яких координується та спрямовується Кабінетом Міністрів України через Міністра фінансів;

– проведення оцінки відповідності бюджетному законодавству бюджетних запитів, паспортів бюджетних програм, проєктів зведених кошторисів для складення розпису державного бюджету;

– проведення аналізу бюджетного запиту, поданого головним розпорядником бюджетних коштів, на предмет його відповідності Бюджетній декларації, а також ефективності використання бюджетних коштів;

– забезпечення обробки та захисту персональних даних під час здійснення верифікації та моніторингу державних виплат, а також під час проведення перевірки достовірності інформації та документів, внесених до електронної системи охорони здоров'я (крім інформації про стан здоров'я людини), на підставі яких формуються звіти, що є підставою для оплати наданих медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій, або які містять персональні дані пацієнтів, медичних працівників, яким (якими) надано відповідні медичні послуги, лікарські засоби та медичні вироби.

Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів. Метою діяльності є виявлення та розшук активів, зокрема тих, що отримані у результаті скоєння кіберзлочинів, а також виявлення активів у віртуальному середовищі. Відповідно до положення [128] передбачено наступні завдання:

– виявлення та розшуку активів, на які може бути накладено арешт у кримінальному провадженні чи у справі про визнання необґрунтованими активів та їх стягнення в дохід держави;

– управління активами, на які накладено арешт у кримінальному провадженні чи у справі про визнання необґрунтованими активів та їх стягнення в дохід держави або які конфісковано у кримінальному провадженні чи стягнено за рішенням суду в дохід держави, внаслідок визнання їх необґрунтованими;

– управління активами, на які накладено арешт або які підлягають стягненню в дохід держави в позовному провадженні у справах про визнання необґрунтованими активів та їх стягнення в дохід держави;

– здійснення міжнародного співробітництва у сфері виявлення, розшуку та управління активами;

– участь у забезпеченні представництва прав та інтересів України у закордонних юрисдикційних органах у справах, пов'язаних із поверненням в Україну активів, одержаних від корупційних та інших кримінальних правопорушень.

Діяльність Агентства є досить важливою із позиції протидії кіберзлочинам, зокрема це стосується фінансових наслідків.

Національне агентство з питань запобігання корупції здійснює свою діяльність за наступними напрямками:

«– аналізує ситуацію з корупцією в Україні та розробляє відповідну Антикорупційну стратегію та державну програму з її реалізації, а також координує виконання цих документів;

– виявляє корупційні норми у законодавстві та проєктах актів;

– контролює дотриманням правил етичної поведінки, законодавства щодо запобігання конфлікту інтересів у діяльності публічних службовців;

– координує та надає методичну допомогу державним органам та органам місцевого самоврядування у виявленні та усуненні

корупціогенних ризиків у їх діяльності, погоджує та контролює виконання антикорупційних програм у цих органах;

– контролює та перевіряє декларації публічних службовців, проводить моніторинг способу їх життя;

– стежить за дотриманням обмежень щодо фінансування політичних партій, законним та цільовим використанням партіями виділених з державного бюджету коштів, своєчасністю подання партіями відповідних звітів та достовірністю включених до них відомостей, розподіляє виділені з державного бюджету кошти на фінансування статутної діяльності політичних партій» [131].

Питання запобігання корупції є вкрай важливим в умовах нових методів здійснення корупційних правопорушень через запровадження інформаційно-комп'ютерних технологій та систем, а також все більшої діяльності людини у віртуальному просторі. Відповідно, агентство постає своєрідним суб'єктом виявлення кіберзлочинів.

Державна служба фінансового моніторингу України «є центральним органом виконавчої влади, діяльність якого спрямовується та координується Кабінетом Міністрів України через Міністра фінансів, який реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [122]. Діяльність служби особливо важлива у контексті здійснення фінансових операції у віртуальному середовищі, а також при використанні інформаційно-комп'ютерних технологій.

Адміністрація Державної служби спеціального зв'язку та захисту інформації України «є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України і який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту

інформації, кіберзахисту, активної протидії агресії у кіберпросторі» [121]. Цю службу включаємо до суб'єктів правоохоронної діяльності, на які покладаються функції із протидії кіберзлочинності. На вказаний орган покладаються такі завдання:

– в частині нормативно-правового забезпечення:

а) забезпечення нормативно-правового регулювання у сферах криптографічного і технічного захисту інформації, організації спеціального зв'язку, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації. Вимога висувається щодо захисту, встановленого законом, у: кіберпросторі, в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, з метою протидії технічним розвідкам, задля організації кіберзахисту об'єктів критичної інформаційної інфраструктури;

б) контроль виконання вимог законодавства у сфері захисту інформації в приміщеннях абонентів урядового зв'язку;

в) встановлення порядку організації та проведення державної експертизи у сфері криптографічного і технічного захисту інформації, проведення державної експертизу та експертних досліджень у сфері криптографічного захисту інформації, визначення криптографічних алгоритмів як рекомендованих, допуск до експлуатації засобів криптографічного захисту інформації, засобів, комплексів та систем спеціального зв'язку. Крім того, вище зазначений орган надає та/або реєструє експертні висновки за результатами державної експертизи у сфері криптографічного та технічного захисту інформації, свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, засобів, комплексів та систем спеціального зв'язку, декларації та атестати відповідності комплексних систем захисту інформації;

– у частині міжнародної діяльності:

а) бере участь у підготовці міжнародних договорів України з питань, що належать до повноважень Держспецзв'язку, готує пропозиції щодо укладення, денонсації таких договорів і забезпечення їх виконання;

б) здійснює міжнародне співробітництво, розробляє пропозиції щодо укладення відповідних міжнародних договорів України, взаємодіє відповідно до міжнародних договорів України з міжнародними організаціями з питань, що належать до повноважень Держспецзв'язку;

– у частині технічного та технологічного забезпечення:

а) здійснює технічне регулювання у сферах криптографічного і технічного захисту інформації, кіберзахисту об'єктів критичної інфраструктури, протидії технічним розвідкам, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, організацію, координацію та проведення робіт із підтвердження відповідності, розроблення в установленому порядку технічних регламентів;

б) організовує забезпечення урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного стану і в особливий період;

в) установлює порядок створення та допуску до експлуатації, допускає до експлуатації засоби криптографічного захисту службової інформації та інформації, що становить державну таємницю, засоби, комплекси та системи спеціального зв'язку, визначає криптографічні алгоритми для застосування у засобах криптографічного захисту інформації;

г) організовує впровадження комплексних систем захисту інформації на об'єктах інформаційної діяльності та в інформаційно-комунікаційних системах;

ґ) установлює порядок та висуває вимоги технічного захисту інформації на об'єктах інформаційної діяльності, створення та атестації комплексів технічного захисту інформації, реєструє акти атестації комплексів технічного захисту інформації;

– у частині організаційно-методичного забезпечення:

а) здійснює методичне керівництво та координацію діяльності державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій, незалежно від форми власності у сферах криптографічного і технічного захисту інформації, протидії технічним розвідкам, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-комунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах;

б) установлює порядок здійснення державного контролю і здійснює державний контроль.

Державна служба спеціального зв'язку та захисту інформації України є особливим суб'єктом забезпечення інформаційної безпеки та кіберзахисту. Фактично формує безпекові засоби функціонування віртуального простору та використання інформаційно-комп'ютерних технологій та систем діяльності органів державної влади. Конкретних завдань щодо протидії кіберзлочинності не передбачено, проте цей суб'єкт має спеціальний статус та може проводити контрольні заходи для забезпечення протидії кібератакам та кіберзлочинам.

Служба безпеки України. «На Службу безпеки України покладається, у межах визначеної законодавством компетенції, захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України» [140]. Ключовим завданням на сьогодні є забезпечення інформаційної безпеки та кіберзахисту, а також протидія гібридним загрозам, кібертероризму, кіберзлочинам та іншим загрозам у віртуального просторі, які шкодять державній безпеці через застосування інформаційно-комп'ютерних технологій.

Національна поліція України є ключовим правоохоронним органом, що здійснює діяльність у сфері протидії кіберзлочинності. Зокрема законодавством передбачено наступні повноваження. Національна поліція України: «здійснює у визначеному законом порядку протидію злочинним посяганням на об'єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об'єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об'єктів критичної інфраструктури» [134].

Державне бюро розслідувань, відповідно до законодавства [117] виконує наступні завдання, серед яких викриття:

– злочинів, вчинених службовими особами, які займають особливо відповідальне становище, відповідно до частини першої статті 9 Закону України «Про державну службу»; злочинів, скоєних особами, посади яких віднесено до першої-третьої категорій посад державної служби, суддями та працівниками правоохоронних органів, крім випадків, коли ці злочини віднесено до підслідності детективів Національного антикорупційного бюро України;

– злочинів, вчинених службовими особами Національного антикорупційного бюро України, заступником Генерального прокурора – керівником Спеціалізованої антикорупційної прокуратури або іншими прокурорами Спеціалізованої антикорупційної прокуратури, крім випадків, коли досудове розслідування цих злочинів віднесено до підслідності детективів підрозділу внутрішнього контролю Національного антикорупційного бюро України;

– злочинів проти встановленого порядку несення військової служби (військових злочинів), крім злочинів, передбачених статтею 422 ККУ.

Такі злочини можуть бути скоєні у віртуальному просторі або ж з використанням інформаційно-комп'ютерних технологій, що визначає їх як кіберзлочинність.

До суб'єктів правоохоронної діяльності, що опосередковано пов'язані із протидією кіберзлочинності, належать:

– Національне антикорупційне бюро України, яке «є центральним органом виконавчої влади зі спеціальним статусом, на який покладається попередження, виявлення, припинення, розслідування та розкриття корупційних та інших кримінальних правопорушень, віднесених до його підслідності, а також запобігання вчиненню нових. Завданням Національного бюро є протидія корупційним та іншим кримінальним правопорушенням, які вчинені вищими посадовими особами, уповноваженими на виконання функцій держави або

місцевого самоврядування, та становлять загрозу національній безпеці, а також вжиття інших передбачених законом заходів щодо протидії корупції» [132]. Варто зазначити, що в умовах розвитку інформаційного суспільства протидія корупції має бути «відбудована» й у віртуальному просторі, зважаючи на використання корупціонерами інформаційно-комп'ютерних технологій.

Бюро економічної безпеки України – «це центральний орган виконавчої влади, на який покладаються завдання щодо протидії правопорушенням, що посягають на функціонування економіки держави. Відповідно до покладених завдань, Бюро економічної безпеки України виконує правоохоронну, аналітичну, економічну, інформаційну та інші функції» [115]. Особлива увага сьогодні має бути приділена питанням криптоактивів та криптовалюти.

Таким чином, у процесі вивчення правового регулювання діяльності суб'єктів реалізації державної кримінально-правової політики та їх адміністративно-правового статусу, варто наголосити на відсутності злагодженої роботи щодо протидії кіберзлочинності, презентованої у різних сферах державного управління, що потребує трансформації суб'єктного складу. Наше бачення зазначеного представлено в табл. 4.1.

Таким чином, для ефективної реалізації державної кримінально-правової політики з питань протидії кіберзлочинності є необхідність змістовної та структурної модернізації суб'єктів державного управління. Встановлено напрями розширення завдань та повноважень суб'єктів, що реалізують державну політику у сферах: забезпечення економічної безпеки, фінансового моніторингу, міжнародної співпраці у сфері інформаційної безпеки; захисту критичної інфраструктури; правоохоронної діяльності.

Таблиця 4.1

Трансформація діяльності суб'єктів реалізації державної кримінально-правової політики протидії кіберзлочинності

ЦЕНТРАЛЬНІ ОРГАНИ ВИКОНАВЧОЇ ВЛАДИ, ЩО РЕАЛІЗУЮТЬ ДЕРЖАНУ КРИМІНАЛЬНО-ПРАВОВУ ПОЛІТИКУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ			
питання розвитку економічної безпеки			
Міністерство цифрової трансформації України	**Міністерство юстиції України**	**Міністерство фінансів України**	**Національне агентство з питань запобігання корупції**
покласти завдання та розширити повноваження			
– унормувати питання виготовлення, обміну, обігу та купівлі-продажу криптоактивів та криптовалюти	– унормувати методи бухгалтерського обліку виготовлення, обміну, обігу та купівлі-продажу криптоактивів та криптовалюти	– унормувати питання декларування криптоактивів та криптовалюти суб'єктами, що зобов'язані подавати декларацію про доходи	
– унормувати процедуру сертифікації та впровадження інформаційних технологій та систем у економічному просторі	– передбачити державні програми підвищення грамотності населення в віртуальному просторі і використанні інформаційних технологій	– налагодити взаємодію між суб'єктами реалізації економічної політики щодо використання інформаційних технологій	
– узгодити питання захисту інформаційних систем щодо криптоактивів та криптовалюти	– узгодити питання формування резервів у криптовалюті	– узгодити питання страхування в сфері криптоактивів та криптовалюти	
питання розшуку активів фінансового моніторингу			
АРМА[26]	**Міністерство фінансів України**	**Міністерство юстиції України**	
Державна служба фінансового моніторингу України	**Національне агентство з питань запобігання корупції**	**Міністерство цифрової трансформації України**	
покласти завдання та розширити повноваження			
– унормувати методики дослідження походження криптоактивів та криптовалюти	– узгодити питання взаємодії щодо розшуку грошових, матеріальних та нематеріальних активів у віртуальному просторі		
– унормувати питання фінансового моніторингу за криптоактивами та криптовалютою	– унормувати питання аналізу підозрілих операцій у віртуальному просторів щодо фінансуванню терористичних операцій		

[26] Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів

Продовження табл. 4.1

– узгодити питання створення резервів грошових, матеріальних та нематеріальних активів у віртуальному просторі для оперативно-розшукової діяльності		– узгодити питання створення резервів криптоактивів та криптовалюти для оперативно-розшукової діяльності	
питання міжнародної співпраці в сфері інформаційної безпеки			
Міністерство закордонних справ	**Міністерство юстиції України**	**Міністерство внутрішніх справ України**	**Державна служба спец. зв'язку та захисту інформації**
Служба безпеки України	**Національна поліція України**	**Державне бюро розслідувань**	**Національне антикорупційне бюро України**
– унормувати питання європейської та північноатлантичної інтеграції віртуального простору України		– унормувати питання використання інформаційно-комп'ютерних технологій та систем у відповідності до вимог ЄС та НАТО	
– унормувати інтеграційні процеси в загальноєвропейські кібероперативні та аналітичні механізми: EU-CyCLONe, CERT-EU		– унормувати питання моніторингу за виконання міжнародних нормативних актів, що ратифіковані в Україні	
– унормувати питання імплементації принципів пропорційності у всіх заходах із моніторингу та збору даних у кіберпросторі		– унормувати питання імплементації стандартів та протоколів ЄС щодо виявлення, розслідування та попередження кіберзлочинів	
– організація аналізу та постійного моніторингу відповідності законодавства України до норм ЄС (NIS/NIS2, рекомендації Європолу, ENISA)		– розробити та моторити досягнення ключових показників забезпечення інформаційної безпеки та протидії кіберзлочинам	
питання захисту критичної інфраструктури			
Міністерство оборони України	**Служба безпеки України**	**Міністерство внутрішніх справ України**	**Інші суб'єкти[27]**
– унормувати питання упровадження систем моніторингу та раннього попередження (SOC)		– унормувати питання оперативного моніторингу критичної інфраструктури та ключових питань віртуального	
питання правоохоронного характеру			
діюча структура			
Міністерство внутрішніх справ України	**Бюро економічної безпеки України**	**Національне антикорупційне бюро України**	
Служба безпеки України	**Національна поліція України**	**Державне бюро розслідувань**	
АРМА[28]	**Державна служба фінансового моніторингу України**	**Державна служба спец. зв'язку та захисту інформації**	
– розширення співпраці з Інтерпол та Європол щодо протидії кіберзлочинності		– сформувати єдину державну інформаційну систему щодо розслідування кіберзлочинів	

[27] Суб'єкти державного управління, що реалізують державну політику в сфері критичної інфраструктури

[28] Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів

Продовження табл. 4.1

<table>
<tr><td colspan="2">– налагодити співпрацю з суб'єктами реалізації державної політики щодо попередження кіберзлочинів</td><td colspan="2">– забезпечити імплементацію стандартів та протоколів ЄС щодо виявлення, розслідування та попередження кіберзлочинів</td></tr>
<tr><td colspan="4">розширення суб'єктної структури правоохоронної системи щодо протидії кіберзлочинності</td></tr>
<tr><td>Міністерство внутрішніх справ України</td><td colspan="2">Бюро економічної безпеки України</td><td>Національне антикорупційне бюро України</td></tr>
<tr><td>Державна служба фінан. моніторингу України</td><td colspan="2">Національна поліція України</td><td>Держане бюро розслідувань</td></tr>
<tr><td>Служба безпеки України</td><td colspan="2">взаємодія з</td><td>АРМА</td></tr>
<tr><td>підпорядкування</td><td colspan="2" rowspan="2">НАЦІОНАЛЬНЕ БЮРО РОЗСЛІДУВАНЬ КІБЕРЗЛОЧИНІВ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ</td><td>підзвітність</td></tr>
<tr><td>Кабінету міністрів України</td><td>Верховній Раді України</td></tr>
<tr><td colspan="4">Національне бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки є державним правоохоронним органом, на який покладаються завдання щодо попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень скоєних у віртуальному (кібернетичному) простору та інших сферах із застосуванням інформаційно-комп'ютерних технологій та забезпечення кібернетичної безпеки України</td></tr>
<tr><td colspan="4">Основні завдання:</td></tr>
<tr><td colspan="2">– попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, що полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливий програмних продуктів (як на матеріальних так і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробка інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивою інформації, розповсюдження незаконно здобутої інформації, та інших дій, що заборонено кримінальним законодавством України</td><td colspan="2">– попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, що скоєне з використанням інформаційно-комп'ютерних технологій проти особи, підприємства, органу державної влади, держави, міжнародних організацій, органів державного управління інших держав, що призводить до сукупності негативних наслідків економічного, соціального, політичного, інфраструктурного та іншого характеру та становить загрозу інформаційній, економічній, соціальній, продовольчій, енергетичній, воєнній, екологічній та політичній безпеці</td></tr>
<tr><td colspan="2">– формування заходів із забезпечення кібернетичної безпеки суб'єктів законодавчої, виконавчої та судової влади</td><td colspan="2">– формування заходів з протидії гібридним загрозам внутрішньополітичної та зовнішньополітичної безпеки держави</td></tr>
<tr><td colspan="4">Повноваження:</td></tr>
<tr><td colspan="2">– здійснює гласні та негласні оперативно-розшукові, оперативно-розшукову діяльність, слідчі (розшукові) та негласні слідчі (розшукові) дії, з метою попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень скоєних у віртуальному (кібернетичному) простору та інших сферах із застосуванням інформаційно-комп'ютерних технологій</td><td colspan="2">– безоплатно одержують в порядку, передбаченому законодавством, доступ до державних інформаційних систем та ресурсів за умови обґрунтованості їх використання при здійсненні гласних та негласних оперативно-розшукових, оперативно-розшукової діяльності, слідчих (розшукових) та негласних слідчих (розшукові) дій щодо при розслідуванні викритих проваджень щодо кримінальних правопорушень, скоєних у віртуальному (кібернетичному) простору та інших сферах із застосуванням інформаційно-комп'ютерних технологій</td></tr>
</table>

Продовження табл. 4.1

– вживають заходів для припинення фізичними та юридичними особами протиправних діянь, що перешкоджають здійсненню повноважень Національне бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки	– у цілях оперативно-розшукової та слідчої діяльності створюють інформаційні системи та ведуть оперативний облік в обсязі і порядку, передбачених законодавством
– здійснюють співпрацю з фізичними особами, у тому числі на договірних засадах, дотримуючись умов добровільності і конфіденційності цих відносин, матеріально та морально заохочують осіб, які надають допомогу в запобіганні, виявленні, припиненні і розслідуванні кримінальних правопорушень, віднесених до підслідності Національного бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки	– вживають заходів щодо розшуку та арешту коштів та іншого майна, що можуть бути предметом конфіскації або спеціальної конфіскації у кримінальних правопорушеннях, віднесених до підслідності Національного бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки, або мають ознаки необґрунтованості та можуть бути стягнуті в дохід держави – в межах компетенції, провадять діяльність із зберігання коштів та іншого майна, на яке накладено арешт;
– вживають заходів щодо розшуку та арешту інформаційно-комп'ютерних технологій та систем, що використовувалися при вчиненні кримінального правопорушення, віднесеного до компетенції Національного бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки	– залучають у межах компетенції на добровільній основі, у тому числі на договірних засадах, кваліфікованих спеціалістів та експертів, у тому числі іноземців, з будь-яких установ, з метою оцінки інформаційно-комп'ютерних технологій та систем,
– здійснює облік кримінальних кіберзлочинів	– формує та оприлюднює статистичні дані про кіберзлочинність

Запропоновано напрями розширення суб'єктної структури правоохоронної системи щодо протидії кіберзлочинності. Зокрема, запропоновано створення Національного бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки (державний правоохоронний орган, на який покладаються завдання щодо попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень скоєних у віртуальному (кібернетичному) простору та інших сферах із застосуванням інформаційно-комп'ютерних технологій та забезпечення кібернетичної безпеки України). Визначено ключові завдання та повноваження зазначеної структури та сформовано напрями взаємодії із іншими суб'єктами, що реалізують правоохоронну функцію. Запропоновано підпорядкувати Національне бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки Кабінетові Міністрів України та визначити необхідність звітування перед Верховною Радою України.

4.2. Трансформація правового регулювання реалізації державної кримінально-правової політики протидії кіберзлочинності

Питання протидії кіберзлочинам в Україні є вкрай важливим і з позиції забезпечення інформаційної безпеки держави, і в контексті інформаційного захисту бізнесу. Кіберзлочини можуть здійснюватися у різноманітних сферах суспільного життя й, відповідно, мати різноманітні наслідки не лише для держави в цілому, а й для суб'єктів господарської діяльності та громадян зокрема. «В умовах гібридної війни, тотального використання засобів масової інформації та її комунікаційних складових частин особливої актуальності набуває

попередження основних загроз кіберзлочинності. Як свідчать результати наукових досліджень, проблематика кіберзлочинності непокоїть не тільки державу в цілому, а й хвилює окремих суб'єктів господарювання.

Кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів, який несе основну загрозу соціогуманітарній та іншим сферам. Значна кількість випадків кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і нові можливості «вдосконалення» інструментів їх скоєння створюють економічні загрози для глобальних інформаційних мереж» [172].

Щодо захисту бізнесу варто зазначити, що «серед ТОП-3 країн за кількістю кіберзлочинів – США, Китай та Німеччина. І проблема полягає не в слабкому захисті з боку уряду. А саме в зацікавленості злочинців. Адже названі країни мають велику кількість зареєстрованих компаній, що є дуже цінними для зловмисників. Незважаючи на усі законодавчі ініціативи та створені агентства (як-от Federal Bureau of Investigation, National Cyber Investigative Task Force, National Security Agency у США, Cyberspace Administration у Китаї, European Cybercrime Centre в ЄС), про захист компанії, в першу чергу, мають пам'ятати все ж її власники. Адже кібератаки спричиняють колосальні репутаційні та фінансові втрати. Причому від цього не застрахований ані малий, ані великий бізнес» [49]. Це вказує на незахищеність бізнесу й, відповідно, економічної системи держави. Значні ризики проявляються через скоєння кіберзлочинів, спрямованих на порушення інформаційної безпеки держави зокрема та національної безпеки в цілому, адже кібератаки на критично важливу інфраструктуру загрожують воєнній, економічній, продовольчій та іншим сферам. «Існування кіберзлочинності становить досить серйозну проблему в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх: не лише на окремих фізичних та

юридичних осіб, а й на об'єкти критичної інфраструктури й державні органи. Окрім відповідної прямої шкоди, кіберзлочинність є величезною перешкодою щодо цифрової довіри, внаслідок чого значною мірою підриваються переваги кіберпростору» [142]. Відповідно, для України, в умовах війни, як ніколи виникає потреба в посиленні кримінальної відповідальності за скоєні кіберзлочини. Це вимагає дослідження еволюції суспільно-державних підходів щодо питання кримінальної відповідальності за скоєні кіберзлочини, а також визначення ключових пріоритетів та векторів розвитку державної політики.

Питання кримінальної відповідальності за кіберзлочини в Україні стали об'єктом наукового дослідження багатьох вітчизняних вчених у сфері юридичних, економічний, політичних наук та наук державного управління. Зокрема, варто наголосити на працях таких вчених, як: Т. В. Барановської, М. О. Будакового, О. М. Будонової, В. М. Бутузова, М. М. Галамбо, Д. О. Грицишена, А. П. Дикого, М. О. Думчикова, В. В. Євдокимова, Н. А. Загребельної, І. Д. Казанчук, Р. А. Калюжного, Н. В. Камінської, І. В. Каріх, К. О. Кислої, В. В. Коваленко, Я. Ю. Кондратьєва, Б. А. Кормичема, А. В. Котелевець, О. В. Кравчука, В. О. Кучменка, Ю. Є. Максименка, А. І. Марущака, К. В. Малишева, Г. В. Новицького, Т. М Пушкарьової, С. О. Савчука, Т. С. Ярового, Т. П. Яцик та інших.

«Інтернет зруйнував бар'єри між країнами, спільнотами та громадянами, дав можливість взаємодіяти та обмінюватися інформацією та ідеями по всьому світу. Щоб кіберпростір залишався відкритим, вільним та безпечним, в Інтернеті повинні застосовуватися ті ж норми, принципи та цінності, що існують в офлайн-режимі. У сучасному світі розвиток інформаційних технологій відкриває нові можливості для комунікації, бізнесу та науки. Однак, поряд з позитивними аспектами цифровізації, зростає і рівень

кіберзлочинності, яка стає однією із найсерйозніших загроз для безпеки держав, організацій та окремих осіб. Кіберзлочинність охоплює широкий спектр кримінальних правопорушень – від крадіжки особистих даних і фінансових шахрайств до атак на об'єкти критичної інфраструктури. Незважаючи на зусилля урядів та міжнародних організацій щодо створення ефективних заходів протидії кіберзлочинності, кількість та складність таких кримінальних правопорушень продовжує зростати. Це вимагає постійного вдосконалення правових, технологічних та організаційних механізмів захисту» [2].

«Наразі кіберзлочинність є, напевно, однією із найбільших глобальних загроз, як для України так і для усього світу. За даними всесвітнього огляду економічних злочинів Pricewaterhouse Coopers (PwC) за 2021 рік, кримінальні правопорушення у кіберпросторі показали найвищий рівень за весь період публікаційних оглядів. Так, рівень злочинності збільшився з 24 % у 2014 році, до 39 % у 2021 році, таким чином посівши 2 місце серед економічних кримінальних правопорушень у світі, залишивши позаду кримінальні правопорушення, пов'язані з легалізацією грошових коштів, отриманих незаконним шляхом, через скоєння різних корупційних кримінальних правопорушень. Однак, зазначені дані відповідають дійсності не в повній мірі, адже кримінальні правопорушення, вчинені в кіберпросторі, є дуже латентним за своєю ознакою, тому реальна картина та реальна статистика набагато більша. Це зумовлено, перш за все, відсутністю чітких методів збирання даних про вчинення кримінальних правопорушень у кіберпросторі та певними характерними особливостями зазначеного виду кримінальних правопорушень» [48].

Особливості становлення та розвитку державної кримінально-правової політики з питань протидії кіберзлочинам та становлення

кримінальної відповідальності за ці злочини вивчено у попередніх дослідженнях. У цьому параграфі приділимо увагу сучасному стану кримінальної відповідальності за вказаний вид злочинів.

«Одним із напрямків боротьби з цим негативним явищем є прийняття на законодавчому рівні нормативно-правових актів, які регулюють відносини у цій сфері. Зокрема, нормативно-правову базу у цій сфері складають: Конституція України, Кримінальний кодекс України, закони України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про основи національної безпеки», Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Також, з метою недопущення зростання рівня кіберзлочинності, Верховною Радою України прийнято Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах воєнного стану», який набув чинності 24 березня 2022 року. Метою цього закону є забезпечення надійності та безпеки використання цифрових послуг, впровадження дієвих кримінально-правових механізмів з протидії кіберзлочинності, оптимізація національної системи кібербезпеки щодо протидії кіберзагрозам. Відповідне посилення санкцій та додаткова криміналізація окремих діянь, на нашу думку, здатні частково стримати потенційних злочинців від вчинення нових кримінальних правопорушень» [142].

Наголосимо на тому, що повномасштабне вторгнення призвело до потреби у підвищенні рівня кримінальної відповідальності за кіберзлочини. Це зумовило активність законодавців в цьому напрямку, зокрема в першій половині 2022 р. У цьому контексті рішенням Ради національної безпеки та оборони України, введеним у дію наказом Президента було посилено заходи щодо інформаційної безпеки

України. Це, в свою чергу, стало підставою для оптимізації змісту Кримінального Кодексу України, відповідно до законодавства, щодо забезпечення кібербезпеки. «Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану», 03.04.2022 р. набув чинності, (Опублікований у газеті «Голос України» від 02.03.2022 р.) за яким: 1) ст.ст. 361 та 361-1 КК України узгоджені із законодавством у сфері кібербезпеки; 2) у ст. 361 КК України розмежована суворість покарання за кібератаку, залежно від наслідків, та сказано про посилення покарання – від штрафу – до 15 років в'язниці; 3) пошук та виявлення вразливостей – не кібератака (ч. 6 ст. 361 КК України); 4) посилено покарання за ст. 361-1 КК України – від штрафу до 5 років в'язниці» [114].

Вітчизняна дослідниця з проблем транснаціональної злочинності І. М. Леган, вважає, що окрім цих факторів «в Україні створено розгалужене нормативно-правове підґрунтя для боротьби з кіберзлочинністю, а саме:

1) Конституція України;

2) Кримінальний Кодекс України;

3) Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 року;

4) Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 року;

5) Закон України «Про інформацію» від 2 жовтня 1992 року;

6) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року;

7) Закон України «Про внесення змін до Закону України «Про платіжні системи та переказ грошей в Україні» від 6 жовтня 2004 року;

8) Закон України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» (щодо відповідальності за комп'ютерні злочини)» від 23 грудня 2004 року;

9) Закон України «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах» від 31 травня 2005 року;

10) Доктрина інформаційної безпеки від 25 лютого 2017 року;

11) Закон України «Про національну безпеку України» від 21 червня 2018 року;

12) Закон України «Про основні засади забезпечення кібербезпеки України» від 24 жовтня 2020 року;

13) інші міжнародні договори» [78].

Питання розвитку правового механізму державної кримінально-правової політики у сфері протидії кіберзлочинності є вкрай важливим, адже має узгодити та забезпечити задоволення інтересів усіх стейкхолдерів. Попередні дослідження визначили ключові напрямки удосконалення кримінального законодавства на основі зарубіжного досвіду та сучасного стану кіберзлочинності у контексті розширення суб'єктної структури. Відповідно, зазначене має бути врегульовано на законодавчому рівні, що вимагає удосконалення правового забезпечення реалізації державної кримінально-правової політики з питань протидії кіберзлочинності, що пропонуємо здійснити наступним чином:

– по-перше, йдеться про удосконалення кримінально-правового регулювання системи протидії кіберзлочинності;

– по-друге, мається на увазі врегулювання модернізації суб'єктної структури реалізації державної кримінально-правової політики.

Розвиток кримінального законодавства щодо протидії кіберзлочинності. Розглянемо більш детальніше положення

кримінального кодексу України, в частині встановлення кримінальної відповідальності за кіберзлочини. Кримінальний Кодекс України був введений у дію у 2001 р., проте за понад 20 років неодноразово піддавався критиці, а станом на 1 січня 2025 року до нього було внесено понад 800 змін та доповнень. Цим нормативним актом встановлено кримінальну відповідальність за досліджувані злочини. Зокрема, цьому присвячено Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який передбачає покарання за наступні види кримінальних правопорушень:

– несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361);

– створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361.1);

– несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (стаття 361.2);

– несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах

або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію (стаття 363);

– умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 363.1).

Види покарань за зазначеними статтями кримінального кодексу та обставини, які обтяжують покарання за скоєння злочину, представлено в таблиці 4.2.

Відповідно до наведених в таблиці даних, можемо констатувати на наступних видах покарання за скоєння кіберзлочинів:

– штраф. За кожною із вище представлений статей Кримінального кодексу передбачено різну суму штрафу. В цілому, зазначена сума може варіюватися від однієї тисячі до чотирьох тисяч неоподатковуваних мінімумів доходів громадян. Якщо мова йде про обставини, які обтяжують зміст покарання, передбаченні досліджуваним розділом Кримінального Кодексу, то сума штрафу буду варіюватися від трьох тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян і лише за статтею 361 – «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»;

Таблиця 4.2

Кримінальна відповідальність за кіберзлочини в Україні

Злочин	Покарання	Обставини, які обтяжують/пом'якшують зміст покарання	
		Обставина	Покарання
1	*2*	*3*	*4*
Стаття 361			
Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	Штраф від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційний нагляд на строк до трьох років, або обмеження волі на той самий строк	Дії, вчинені повторно або за попередньою змовою групою осіб	Штраф від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк від двох до п'яти років, або позбавлення волі на той самий строк
		Дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації	Штраф від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
		Дії заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків	Позбавлення волі на строк від восьми до дванадцяти років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
		Дії вчинено під час дії воєнного стану	Позбавлення волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років

Продовження табл. 4.2

1	*2*	*3*	*4*
Стаття 361.1			
Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або позбавлення волі на строк до трьох років	Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Позбавлення волі на строк до п'яти років
Стаття 361.2			
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк до двох років	Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Позбавлення волі на строк від двох до п'яти років
Стаття 362			
Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років	Дії призвели до витоку інформації	Позбавлення волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк
		Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років

Продовження табл. 4.2

1	*2*	*3*	*4*
Стаття 363			
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційний нагляд на строк до трьох років, або обмеження волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк	Не передбачено	Не передбачено
Стаття 363-1			
Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років	Дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду	Обмеження волі на строк до п'яти років або позбавлення волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років

– обмеження волі, один з видів покарань за кримінальні правопорушення, що визначається статтею 61 Кримінального кодексу України. Зокрема, зазначеною статтею визначено наступне: «Покарання у виді обмеження волі полягає у триманні особи в кримінально-виконавчих установах відкритого типу без ізоляції від суспільства в умовах здійснення за нею нагляду з обов'язковим залученням засудженого до праці» [74]. Максимальний трок обмеження волі до п'яти років, за кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку і лише за статтею 361;

– виправні роботи. Відповідно до статті 57 Кримінального Кодексу України передбачено, що «покарання у виді виправних робіт встановлюється на строк від шести місяців до двох років і відбувається за місцем роботи засудженого. Із суми заробітку засудженого до виправних робіт провадиться відрахування в дохід держави у розмірі, встановленому вироком суду, в межах від десяти до двадцяти відсотків» [74]. За статями 361.1 та 362 передбачено можливість покарання у вигляді виправних робіт до двох років;

– пробаційний нагляд регулюється статтею 59.1, згідно з якою: «покарання у вигляді пробаційного нагляду полягає в обмеженні прав і свобод засудженого, визначених законом і встановлених вироком суду, із застосуванням наглядових та соціально-виховних заходів без ізоляції від суспільства» [74]. Цією статей передбачено різносторонні види нагляду;

– позбавлення волі, як найбільш суворий вид покарання за кіберзлочини. Якщо не враховувати обставини, які обтяжують зміст покарання, то, за досліджуваними статтями кримінального кодексу, найбільший строк сягає до трьох років, що передбачено статтею 361.1: «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх

розповсюдження або збут. У той же час, якщо дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, передбачено позбавлення волі на строк до п'яти років»;

- позбавлення права обіймати певні посади або займатися певною діяльністю: «Позбавлення права обіймати певні посади або займатися певною діяльністю може бути призначене як основне покарання на строк від двох до п'яти років або як додаткове покарання на строк від одного до трьох років» [74]. Цей вид покарання на строк до трьох років передбачено за статтею 361 за наступних тих умов, якщо: а) дії призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації; б) дії завдали значної шкоди чи створили небезпеку у вигляді тяжких технологічних аварій або екологічних катастроф, призвели до загибелі або масового захворювання населення чи інших тяжких наслідків; в) дії були вчинені під час воєнного стану. Таке ж покарання передбачено за статтями 362 та 363, за умови, якщо протиправні дії вчинено повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Щодо реформування кримінального законодавства, варто наголосити, що уже протягом декількох років йде робота над розробкою нового Кримінального Кодексу України. «Відповідно до Указу Президента України №584/2019 від 07.08.2019, було утворено Комісію із питань правової реформи, основним завданням якої є сприяння подальшого розвитку правової системи України на основі конституційних принципів верховенства права, пріоритетності прав і свобод людини і громадянина, з урахуванням міжнародних зобов'язань України. Частиною цієї Комісії стала робоча група з питань розвитку кримінального права, до складу якої увійшли одні з кращих представників провідних юридичних шкіл України та на яку покладено низку завдань, одним з яких є підготовка пропозицій стосовно змін до

законодавства України про кримінальну відповідальність. Діяльність цієї групи підтримується Консультативною Місією Європейського Союзу в Україні» [105].

Відповідно, на сьогодні Робочою групою з питань розвитку кримінального права розроблено декілька проєктів нового Кримінального Кодексу України. Так, на сайті Робочої групи розміщено черговий Проєкт від 01.08.2024 р. [62].

Проаналізувавши зміст зазначеного Кодексу, необхідно наголосити на розумінні кіберзлочинів як кримінальних правопорушень проти суспільства (книга сьома «Кримінальні правопорушення проти суспільства»). Так, кіберзлочини розглядаються як злочини, скеровані проти безпеки інформаційних систем. Варто зазначити, що Проєкт значно відрізняється від діючого Кримінального кодексу, зокрема в частині встановлення покарання за злочини. Так, Проєктом передбачено ступені тяжкості злочину, відповідно до яких визначається рівень покарання, видами якого є наступні: 1) громадські роботи; 2) штраф; 3) обмеження волі; 4) строкове ув'язнення; 5) довічне ув'язнення.

Відповідно до розділу 7.7 «Кримінальні правопорушення проти безпеки інформаційних систем», передбачено наступні види кримінальних правопорушень:

– незаконний доступ до інформаційної системи;

– незаконне перехоплення комп'ютерних даних (1) при їх виході з інформаційної системи, 2) при їх надходженні до інформаційної системи або 3) при операції з ними всередині інформаційної системи);

– незаконне поводження з комп'ютерними даними (1) знищення комп'ютерних даних, 2) пошкодження комп'ютерних даних, 3) блокування комп'ютерних даних, 4) порушення цілісності комп'ютерних даних, 5) порушення порядку маршрутизації комп'ютерних даних або 6) спотворення процесу обробки комп'ютерних даних);

– незаконні діяння зі шкідливим програмним чи технічним засобом або шкідливими даними (даними доступу) (1) виготовлення, 2) набуття, 3) переміщення, 4) збут або 5) поширення).

Ознаки, що підвищують тяжкість кіберзлочину, передбачені наступні:

– у складі простої групи;

– із використанням службових повноважень чи професійних обов'язків або пов'язаних із ними можливостей;

– із використанням шкідливого програмного чи технічного засобу або шкідливих даних (даних доступу);

– в особливий період чи в умовах надзвичайного стану;

– особою, яка має правомірний доступ до інформаційних систем або інформації з обмеженим доступом;

– з метою здійснення переказу грошей, майнових цінностей або віртуальної валюти.

Зважаючи на представлені попередні дослідження, пропонуємо наступні напрями удосконалення Кримінального Кодексу України в частині встановлення кримінальної відповідальності за кібернетичні злочини:

1. У частині основних понять визначити наступні:

а) *кримінальні правопорушення в сфері кібернетичного простору* – протизаконне діяння, зміст якого полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливих програмних продуктів (на матеріальних і на нематеріальних носіях), елементів комп'ютерних систем задля зміни та підробки інформації, перехоплення інформації, втручання в базу даних, отримання незаконного доступу до інформації, продукування неправдивої інформації, розповсюдження незаконно здобутої інформації та інші дії, заборонені кримінальним законодавством України;

б) *кримінальні правопорушення з використанням інформаційно-комп'ютерних технологій та систем протисуспільних відносин* – суспільно-небезпечне протиправне діяння, скоєне з використанням інформаційно-комп'ютерних технологій проти особи, підприємства, органу державної влади, держави, міжнародних організацій, органів державного управління інших держав, яке призводить до сукупності негативних наслідків економічного, соціального, політичного, інфраструктурного та іншого характеру та становить загрозу інформаційній, економічній, соціальній, продовольчій, енергетичній, воєнній, екологічній та політичній безпеці

2. Передбачити окремий розділ у Кримінальному Кодексі України, під назвою «*Кримінальні правопорушення в сфері кібернетичного простору*». У цьому розділі пропонуємо передбачити наступні статті, що характеризують види кримінальних правопорушень:

– особа, що сприяла виготовленню, використанню, реалізації, обміну та розповсюдженню шкідливих програмних продуктів, карається законом;

– особа, яка здійснювала виготовлення, використання, реалізацію, обмін, фінансування та розповсюдження елементів комп'ютерних систем, для цілей, що заборонені законом, зокрема для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивої інформації, розповсюдження незаконно здобутої інформації, карається законом;

– особа, що організувала та фінансувала діяльність щодо виготовлення, використання, реалізації, обміну та розповсюдження шкідливих програмних продуктів, карається законом;

– особа, що організувала та фінансувала діяльність щодо виготовлення, використання, реалізації, обміну, фінансування та розповсюдження елементів комп'ютерних систем для цілей, що

заборонені законом, зокрема для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, продукування неправдивої інформації, розповсюдження незаконно здобутої інформації, карається законом;

3. Передбачити ознаки тих обставин, які обтяжують зміст покарання за скоєння кримінального правопорушення у сфері кібернетичного простору, зокрема:

– кримінальне правопорушення, скоєне у складі простої групи;

– кримінальне правопорушення, скоєне у складі організованого злочинного угрупування;

– кримінальне правопорушення, скоєне в умовах особливих правових режимів;

– кримінальне правопорушення, скоєне з використанням службових повноважень чи професійних обов'язків, або пов'язаних із ними можливостей;

– кримінальне правопорушення, яке призвело до смерті особи чи осіб;

– кримінальне правопорушення, скоєне щодо критичної інфраструктури;

– кримінальне правопорушення, яке призвело до значних матеріальних та фінансових збитків;

4. У частині розділу «Кримінальні правопорушення проти економіки» передбачити кримінальну відповідальність за наступні дії:

– особа, що здійснювала виготовлення, зберігання, обмін, купівлю-продаж, організацію біржової торгівлі криптоактивами та криптовалютою, що заборонено законом, карається законом;

– особа, що здійснювала посередництво та поширення інформації про виготовлення, зберігання, обмін, купівлю-продаж, організацію біржової торгівлі криптоактивами та криптовалютою, що заборонено законом, карається законом;

5. У розділах Кримінального Кодексу України щодо кримінальних правопорушень проти безпеки руху та експлуатації транспорту; громадського порядку та моральності; охорони державної таємниці; статевої свободи та статевої недоторканності; виборчих, трудових та інших особистих права та свобод людини і громадянина; органів державної влади, місцевого самоврядування, об'єднань громадян; миру, безпеки людства та міжнародного правопорядку; громадської безпеки; безпеки виробництва; життя та здоров'я особи; господарської діяльності; національної безпеки; державних кордонів; волі, честі та гідності; службової діяльності; правосуддя; військової служби; довкілля; власності, передбачити статті регулюють встановлення кримінальної відповідальності за зазначені злочини, що скоєнні з використанням інформаційно-комп'ютерних технологій та систем.

Модернізація суб'єктної структури реалізації державної кримінально-правової політики. Модернізацію суб'єктної структури державного управління в сфері протидії кіберзлочинності пропонуємо здійснити наступним чином:

– у частині забезпечення економічної безпеки держави розширити повноваження Міністерства цифрової трансформації України, Міністерства юстиції України, Міністерство фінансів України, Національного агентства з питань запобігання корупції, щодо виконання наступних завдань: 1) унормувати питання виготовлення, обміну, обігу та купівлі-продажу криптоактивів та криптовалюти; 2) унормувати методи бухгалтерського обліку з виготовлення, обміну, обігу та купівлі-продажу криптоактивів та криптовалюти; 3) унормувати питання декларування криптоактивів та крипто валюти суб'єктами, що зобов'язанні подавати декларацію про доходи; 4) унормувати процедуру сертифікації та впровадження інформаційних технологій та систем у економічному просторі; 5) передбачити державні програми з підвищення грамотності населення у віртуальному просторі щодо використання інформаційних

технологій; 6) налагодити взаємодію між суб'єктами реалізації економічної політики щодо використання інформаційних технологій; 7) узгодити питання захисту інформаційних систем щодо криптоактивів та криптовалюти; 8) узгодити питання формування резервів в криптовалюті; 9) узгодити питання страхування у сфері криптоактивів та криптовалюти;

– у частині розшуку активів фінансового моніторингу є потреба розширення повноважень Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів; Міністерства фінансів України, Міністерства юстиції України, Державної служби фінансового моніторингу України, Національного агентства з питань запобігання корупції; Міністерства цифрової трансформації України, що стосуються виконання завдань: 1) унормувати методики з дослідження походження криптоактивів та криптовалюти; 2) узгодити питання взаємодії щодо розшуку грошових, матеріальних та нематеріальних активів у віртуальному просторі; 3) унормувати питання фінансового моніторингу за криптоактивами та криптовалютою; 4) унормувати питання аналізу підозрілих операцій у віртуальному просторів щодо фінансування терористичних операцій; 5) узгодити питання створення резервів грошових, матеріальних та нематеріальних активів у віртуальному просторі для оперативно-розшукової діяльності; 6) узгодити питання створення резервів криптоактивів та криптовалюти для оперативно-розшукової діяльності;

– в частині міжнародної співпраці в сфері інформаційної безпеки розширити повноваження Міністерства закордонних справ; Міністерства юстиції України; Міністерства внутрішніх справ України; Державної служби спеціального зв'язку та захисту інформації; Служба безпеки України; Національної поліції України; Держаного бюро розслідувань; Національного антикорупційного бюро України щодо виконання наступних завдань: унормувати питання

європейської та північноатлантичної інтеграції віртуального простору України; унормувати питання використання інформаційно-комп'ютерних технологій та систем, відповідно до вимог ЄС та НАТО; унормувати інтеграційні процеси в загальноєвропейські кібероперативні та аналітичні механізми: EU-CyCLONe, CERT-EU; унормувати питання моніторингу за виконання міжнародних нормативних актів, що ратифіковані в Україні; унормувати питання імплементації принципів пропорційності у всіх заходах із моніторингу та збору даних у кіберпросторі; унормувати питання імплементації стандартів та протоколів ЄС щодо виявлення, розслідування та попередження кіберзлочинів; організація аналізу та постійного моніторингу відповідності законодавства України до норм ЄС (NIS/NIS2, рекомендації Європолу, ENISA); розробити та моторити досягнення ключових показників забезпечення інформаційної безпеки та протидії кіберзлочинам;

– щодо питання захисту критичної інфраструктури, пропонуємо розширення повноважень Міністерства оборони України, Служби безпеки України, Міністерства внутрішніх справ України для виконання наступних завдань: унормувати питання упровадження систем моніторингу та раннього попередження (SOC); унормувати питання оперативного моніторингу критичної інфраструктури та ключових питань віртуального середовища.

– щодо правоохоронної діяльності пропонуємо розширити повноваження Міністерства внутрішніх справ України; Бюро економічної безпеки України; Національного антикорупційного бюро України; Служби безпеки України; Національної поліції України; Державного бюро розслідувань; Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів; Державної служби фінансового моніторингу України; Державної служби спеціального зв'язку та захисту інформації.

Важливе значення в реалізації державної політики з питань протидії кіберзлочинності має розширення суб'єктної структури правоохоронної системи щодо протидії кіберзлочинності. Зокрема, пропонуємо створити Національне бюро з розслідувань кіберзлочинів та забезпечення кібернетичної безпеки і визначити його зміст. Відтак, Національне бюро є державним правоохоронним органом, на який покладаються завдання щодо попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, скоєних у віртуальному (кібернетичному) просторі та інших сферах, із застосуванням інформаційно-комп'ютерних технологій, з метою забезпечення кібернетичної безпеки України. На агентство покладатимуться наступні завдання:

– запобігання, виявлення, припинення, розкриття та розслідування кримінальних правопорушень щодо виготовлення шкідливих програмних продуктів (на матеріальних і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивої інформації, розповсюдження незаконно здобутої інформації та інших дій;

– запобігання, виявлення, припинення, розкриття та розслідування кримінальних правопорушень щодо фінансування виготовлення шкідливих програмних продуктів (на матеріальних і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивою інформації, розповсюдження незаконно здобутої інформації, та інших дій;

– запобігання, виявлення, припинення, розкриття та розслідування кримінальних правопорушень щодо використанні шкідливий програмних продуктів (як на матеріальних так і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та

підробка інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, утворення неправдивої інформації, розповсюдження незаконно здобутої інформації та інших дій.

Для забезпечення реалізації зазначених завдань пропонуємо визначити наступні повноваження:

– здійснює гласні та негласні, оперативно-розшукові дії; оперативно-пошукову діяльність, слідчі (розшукові) та негласні слідчі (розшукові) дії, з метою попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, скоєних у віртуальному (кібернетичному) просторі та інших сферах із застосуванням інформаційно-комп'ютерних технологій;

– в порядку, передбаченому законодавством, безоплатно одержують доступ до державних інформаційних систем та ресурсів, за умови обґрунтованості їх використання при здійсненні гласних та негласних оперативно-пошукових дій, оперативно-пошукової діяльності, слідчих (розшукових) та негласних слідчих (розшукові) дій, з метою розслідування викритих проваджень щодо кримінальних правопорушень, скоєних у віртуальному (кібернетичному) просторі та інших сферах із застосуванням інформаційно-комп'ютерних технологій;

– вживання заходів для припинення фізичними та юридичними особами протиправних діянь, що перешкоджають здійсненню повноважень – Національне бюро із розслідувань кіберзлочинів та забезпечення кібернетичної безпеки;

– здійснюють співпрацю з фізичними особами, у тому числі на договірних засадах, дотримуючись умов добровільності і конфіденційності цих відносин; матеріально та морально заохочують осіб, які надають допомогу при запобіганні, виявленні, припиненні і розслідуванні кримінальних правопорушень, віднесених до

підслідності Національного бюро розслідувань кіберзлочинів та заходів із забезпечення кібернетичної безпеки;

– вживають заходів щодо розшуку та арешту інформаційно-комп'ютерних технологій та систем, що використовувалися при вчиненні кримінального правопорушення, віднесеного до компетенції Національного бюро розслідувань кіберзлочинів, з метою забезпечення кібернетичної безпеки;

– у цілях оперативно-розшукової та слідчої діяльності створюють інформаційні системи та ведуть оперативний облік в обсязі і порядку, передбачених законодавством;

– вживають заходів щодо розшуку та арешту коштів та іншого майна, що можуть бути предметом конфіскації або спеціальної конфіскації у кримінальних правопорушеннях, віднесених до підслідності Національного бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки, або мають ознаки необґрунтованості та можуть бути стягнуті в дохід держави – в межах компетенції провадять діяльність із зберігання коштів та іншого майна, на яке накладено арешт;

– залучають у межах компетенції на добровільній основі, у тому числі на договірних засадах, кваліфікованих спеціалістів та експертів, у тому числі іноземців, з будь-яких установ, з метою оцінки інформаційно-комп'ютерних технологій та систем.

Таким чином, в результаті проведеного дослідження визначено специфічні риси кримінальної відповідальності за кіберзлочини, відповідно до діючого кримінального законодавства (Кримінальний Кодекс України 2001 р.). Вивчення Проєкту кримінального Кодексу України від 01.08.2024 р., що розроблений Робочою групою з питань розвитку кримінального права, передбачає встановлення ряду: і в частині визначення міри покарання, і в розділі щодо формулювання правового положення. Зокрема, такі поняття, як: автоматизовані системи та мережі електрозв'язку не згадуються, натомість є поняття

кіберзлочинів, пов'язаних із діями щодо інформаційних систем, комп'ютерних даних та програмних продуктів. Крім того, важливого значення в умовах війни мають кібератаки на критичну інфраструктуру, про що також не згадується в Проєкті нового кримінального Кодексу. Відповідно, зазначене дослідження є підґрунтям для розробки векторів розвитку кримінального законодавства в частині протидії кіберзлочинам. Зокрема запропоновано внести зміни до Кримінального кодексу України, які стосуються того, щоб: а) розширити перелік основних понять (кримінальні правопорушення у сфері кібернетичного простору та кримінальні правопорушення з використанням інформаційно-комп'ютерних технологій та систем протисуспільних відносин); б) передбачити окремий розділ в Кримінальному кодексі України під назвою «Кримінальні правопорушення у сфері кібернетичного простору»; в) передбачити ознаки обставин, які обтяжують зміст покарання за скоєння кримінального правопорушення у сфері кібернетичного простору; г) у частині розділу «Кримінальні правопорушення проти економіки» передбачити кримінальну відповідальність за діяльність в сфері криптовалюти та криптоактивів; д) передбачити статті, що регулюють кримінальні правопорушення із використанням інформаційно-комп'ютерних технологій та систем протисуспільних відносин різних видів. Визначено напрями правового регулювання щодо модернізації суб'єктної структури у контексті реалізації державної кримінально-правової політики.

РОЗДІЛ 5

МЕХАНІЗМИ ІНТЕГРАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕРБЕЗПЕКИ

5.1. Нормативно-правові важелі Європейського Союзу у сфері протидії кіберзлочинності та забезпечення кібербезпеки

В Європейському Союзі створено багаторівневу систему нормативно-правового регулювання заходів з кібербезпеки. Наявна система законодавства направлена на протидію сучасним загрозам, які створюються в цифровому середовищі. Національні системи захисту самостійно не здатні ефективно протидіяти кіберзагрозам, більше того ізольовані системи є більш вразливими до кібератак. Таким чином, викликом для ЄС є те, що в результаті порушення безпеки в одній державі-члені ЄС відбувається ланцюговий негативний вплив на систему Союзу в цілому, та кожної з країн зокрема. Такий транснаціональний вимір зобов'язує до скоординованого підходу в галузі кібербезпеки. В першу чергу координація має відбуватись в частині управління ризиками та звітності про випадки порушень безпеки цифрового середовища.

Запровадження уніфікованих стандартів кібербезпеки, ЄС мінімізує ризики створення фрагментованих нормативних актів, де за інших умов існує можливість нормативних прогалин та нерівних безпекових умов. Єдиний цифровий ринок ЄС залежить від надійних заходів кібербезпеки для зміцнення довіри споживачів, заохочення чесної конкуренції та стимулювання розвитку інновацій.

Налагодження ефективних інструментів та методів регулювання створює основу для всієї екосистеми, яка, в свою чергу, чинить трансформаційний вплив на формування безпечного кіберсередовища.

Огляд основоположних законодавчих актів і директив Європейського Союзу, які регулюють сферу кібербезпеки, дозволить визначити напрями адаптації вітчизняного законодавства до норм ЄС. У табл. 5.1 наведено сфери впливу та ключові особливості кожного нормативно-правового документа, а також описано їх значення для формування кібербезпекового середовища в різних секторах. Представлені нормативні акти охоплюють питання безпеки мереж та інформаційних систем, захисту персональних даних, встановлення вимог до рівня безпеки у фінансовому секторі та забезпечення загальних стандартів кібербезпеки для країн Європейського Союзу.

Таблиця 5.1

Основні нормативно-правові документи в галузі кібербезпеки ЄС

Назва нормативного документу	Сфера впливу	Особливості
NIS Directive (2016) [207]	Безпека мереж та інформаційних систем	Управління ризиками, звітування про інциденти, OES і DSP
NIS2 Directive (2022) [208]	Розширений обсяг рамок кібербезпеки	Більш широкі сектори, зосередженість на ланцюзі поставок, суворіше управління
Cybersecurity Act (2019) [241]	Мандат і структура сертифікації ENISA	Загальноєвропейські сертифікати, робочі можливості ENISA
GDPR (2016) [53]	Захист даних і повідомлення про порушення	Організаційні заходи, значні штрафи за порушення
Digital Operational Resilience Act (DORA) [206]	Стійкість фінансового сектора до цифрових технологій	Комплексні стандарти для фінансових установ
Digital Services Act (DSA) [206]	Безпека та підзвітність платформи	Безпека даних для платформ, підзвітність модерації контенту
Digital Markets Act (DMA) [206]	Ринкова конкуренція та кібербезпека	Безпечні ринкові процеси, чесна конкуренція
Cyber Resilience Act [197]	Стандарти кібербезпеки на рівні продукту	Безпечний дизайн, безпека життєвого циклу для IoT і програмного забезпечення

Джерело: побудовано авторами.

Головним нормативним документом, який сформував рекомендації щодо регулювання галузі кібербезпеки та визначив правила для учасників цієї галузі є Директива NIS (прийнята в 2016 р.). Визначальною метою Директиви було визначення вимог для досягнення високого рівня безпеки мережевих та інформаційних систем. Тобто, Директива безпосередньо стосується операторів послуг критичних секторів (OES): енергетика, транспорт, банки та страхові установи, а також постачальників цифрових послуг. Редакція 2016 р. Директиви фокусувалась на регламентації безпекових вимог до таких цифрових послуг як хмарні сервіси та онлайн-ринки. Також в документі було сформовано рекомендації з управління ризиками, вимоги до звітності про кіберзагрози та механізми взаємодії між національними групами реагування комп'ютерної безпеки (CSIRT).

Безпека цифрового середовища характеризується високою частотою змін, тому регуляторні органи та органи державного управління змушені постійно вдосконалювати систему протидії кібеззагрозам. Таким чином, відповідаючи на новостворені небезпеки та з метою забезпечення стабільності безпеки цифрового середовища ЄС, в 2022 р. прийнято Директиву NIS2. Нові регламентні норми націлені на розширення сфери регулювання операторів послуг критичних секторів. Так, під дію NIS2 потрапляють сектори управління стічними водами, все державне управління та космічна інфраструктура. Директива NIS2 розширює вимоги Директиви NIS щодо безпеки ланцюгів постачання, запроваджує суворіші заходи державного управління та передбачає санкціонування суб'єктів різних рівнів за невиконання передбачених вимог.

Наступним основоположним документом, який регулює галузь кібербезпеки ЄС є Закон про кібербезпеку (Cybersecurity Act). Прийняття Закону передбачає створення Агентства ЄС з кібербезпеки – ENISA [211] та регламентує його роботу. Додатково в Законі регламентовано вимоги загальноєвропейської системи сертифікації кібербезпеки для товарів, процесів і послуг інформаційно-

комп'ютерних технологій. Незважаючи на те, що вимоги системи у багатьох випадках є рекомендаційними, для програм із високим ризиком передбачені обов'язкові процедури.

В 2016 р. Парламент ЄС прийняв Регламент захисту персональної інформації – GDPR [53]. Регламент пов'язаний з заходами кібербезпеки через обов'язкові вимоги щодо сповіщень про порушення даних, а також впровадження технічних і організаційних заходів для захисту персональних даних. Правила GDPR стосуються всіх суб'єктів, які є учасниками цифрового середовища ЄС, а недотримання вимог загрожує значними штрафами.

Закон про цифрову операційну стійкість (Digital Operational Resilience Act – DORA) направлений на визначення правил та норм для заходів кібербезпеки фінансового сектору ЄС. Закон встановлює стандарти цифрової стійкості для таких суб'єктів ринку, як банки та постачальники платіжних послуг [206]. Натомість Закон про цифрові послуги (DSA) і Закон про цифрові ринки (DMA) регулюють онлайн-платформи, а точніше контент який там розміщений. Завданням DSA та DMA є забезпечення безпечної обробки даних користувачів та підзвітність платформ про використання даних, що відповідно впливає на загальний рівень кібербезпеки ЄС. На перспективні напрямки розвитку кібербезпеки ЄС вказує остання законодавча ініціатива з метою підвищення рівня кібербезпеки країн-учасниць – Cyber Resilience Act [193]. Ініційований закон спрямований на те, щоб цифрові продукти були безпечними за своєю конструкцією та підтримували безпеку протягом усього життєвого циклу. В Законі попередньо передбачені вимоги до безпеки для пристроїв Інтернету речей, тому таке рішення є досить революційним в частині правової регламентації галузі кібербезпеки.

Проаналізовані нормативно-правові документи в галузі кібербезпеки, які прийняті в ЄС вказують на те, що основні їх зусилля направлені на захист критичних секторів економіки, даних та персональної інформації користувачів. Оскільки критична інфраструктура забезпечує соціальну та економічну стабільність, то кіберзагрози в цих секторах потенційно несуть серйозні наслідки для

безпеки всього регіону, а не лише окремої країни. Таким чином суттєвість кіберзагроз вимагає чіткого, дієвого та ефективного регуляторного контролю.

Регламентація вимог до кібербезпеки сервісів хмарних обчислень, онлайн-платформ та пошукових систем перебувають під постійними змінами та уточненнями. Також варто відмітити постійне розширення зобов'язань, на що вказує прийняття Директиви NIS2, яка не лише оновила вимоги до кібербезпеки в межах ЄС, але і визначила широке коло вимог до розширеного переліку критичних галузей, які функціонують присутні в цифровому середовищі ЄС. Усвідомлюючи ризики, пов'язані з кібератаками на державні установи, Директива NIS2 передбачає взаємодію між національними, регіональними та місцевими органами влади. Окрім цього, запропонований Закон про стійкість до кіберзагроз вказує на потребі визначення обов'язкового рівня захисту цифрових продуктів та послуг. Таким чином, європейський ринок спільно переходить до стандартизації «безпеки продуктів» з метою мінімізації кіберзагроз.

Такі нормативні акти, як GDPR [53] і Закон про кібербезпеку [241], безпосередньо застосовуються в країнах-членах, тоді як такі директиви, як NIS2, вимагають імплементації визначених норм в національному законодавстві. Попри розвинуту нормативно-правову базу ЄС, недоліком залишаються відмінності у застосуванні та тлумаченні регламентних норм серед країн-учасниць. Таким чином, законодавство ЄС має враховувати регіональні особливості для забезпечення ефективної його гармонізації. Швидкі цифрові трансформації вимагають швидкої реакції з боку регуляторів, однак це суттєво ускладнює розробку уніфікованих підходів до регламентації правил кібербезпеки. Законодавство ЄС в галузі кібербезпеки характеризується екстра територіальністю, що гарно видно з результатів застосування GDPR до суб'єктів, які мають доступ та користуються даними резидентів ЄС. Подібні принципи поширюються на правила кібербезпеки, що стосуються компаній за межами ЄС, але які працюють на цьому ринку.

Регламентні норми ЄС в галузі кібербезпеки зобов'язують суб'єктів застосовувати надійні методи управління ризиками та звітувати про виникнення будь-яких інцидентів. Такі дії сприяють упередженню та мінімізації негативних кіберзагроз. Таким чином, для посилення безпеки цифрового середовища всього регіону, ЄС запроваджує мінімальні базові вимоги безпеки для критичної інфраструктури та цифрових послуг. Ефективним прикладом таких ініціатив є схеми сертифікації, які визначені в Законі про кібербезпеку. Сам Закон визначає свою мету як підвищення рівня довіри споживачів і бізнесу до цифрових технологій, через стимулювання інновацій та розвиток. З метою забезпечення ефективної дії закону, прийнято децентралізовану систему взаємодії між країнами ЄС. Така система лише курується Агентством з кібербезпеки ЄС, яке сприяє співпраці через налагодження мережі національних центрів – CSIRT [194]. CSIRT є галузевими центрами обміну інформацією та аналізу (ISAC) і Організаційної мережі зв'язку з кіберзагроз (CyCLONe) [212]. Така структура взаємодії прискорює обмін розвідувальною інформацією про загрози, а головне координує дії при виникненні загрозам безпеки в кіберпросторі Союзу.

Заходи кібербезпеки відповідають зобов'язанням ЄС щодо конфіденційності та захисту даних, зокрема через захист прав громадян у цифровому середовищі. Поява нових технологій, таких як штучний інтелект, квантові обчислення та 5G, вимагає постійної адаптації нормативно-правової бази для упередження та мінімізації нових загроз. На тлі таких викликів, не можна ігнорувати наявні відмінності в соціально-економічному розвитку, ресурсному забезпеченні та правових традиціях країн ЄС. Існування цих відмінностей призводить до зменшення ефективності спільних заходів ЄС у кібербезпеці та ускладнює можливості застосування спільних стандартів кібербезпеки. В свою чергу міжнародний характер кіберзагроз вимагає узгодження з глобальними стандартами та співпраці з партнерами не просто європейського регіону, але і за межами ЄС. Таким чином, виклик усунення нормативної асиметрії інформації є суттєвим. В цих умовах завданням органів державного

управління як регулятора є встановлення балансу між суворими вимогами безпеки цифрового середовища, захист даних та сприяння інноваційному розвитку.

Нормативна база ЄС щодо кібербезпеки спрямована на створення стійкої та надійної цифрової екосистеми. Звертаючи увагу на нові загрози та розширюючи сферу дії основного законодавства, ЄС прагне узгодити свої принципи конфіденційності, захист прав громадян і гармонізацію ринку з вимогами цифрової трансформації. Умовою безпечного і надійного кіберпростору в межах ЄС є посилення співпраці між державами-членами, зацікавленими сторонами приватного сектору та інституціями ЄС. Вдосконалення взаємодії є гарантією розвитку в динамічних трансформаційних умовах.

За останнє десятиліття законодавча база Європейського Союзу в галузі кібербезпеки розширилася та ускладнилася. Ці процеси пояснюються як мінливістю загроз, так і потребою в захисті цілісності єдиного цифрового ринку. Діюча структура ЄС передбачає існування декількох правових інструментів. Їх синергетична дія спрямована на підвищення безпеки мережевих та інформаційних систем, встановлення загальних стандартів, роз'яснення ролей і обов'язків на національному рівні кожної країни-учасниці та в цілому ЄС. Кожен з інструментів нормативно-правової системи здійснює свій вплив на національне законодавство, що в свою чергу трансформує усталені регулятивні підходи, механізми забезпечення дотримання законодавчих норм та розподіл ресурсів для заходів кібербезпеки.

Результати дослідження свідчать, що визначальним елементом системи є Директива NIS (прийнята 2016 р.) [207]. Будучи першим загальноєвропейським нормативним документом в галузі кібербезпеки, Директива заклала основу для безпеки критичних соціальних послуг (енергетика, транспорт і охорона здоров'я) та для учасників цифрового ринку. Директива передбачала низку обов'язкових змін на рівні національного законодавства кожної країни ЄС. Очікувано, що нові вимоги призвели до різного ступеня реалізації. Ключовими факторами, які вплинули на успішність прийняття вимог Директиви були існуюча правова інфраструктура, адміністративні

можливості і стратегічні пріоритети кожної країни. Директива вимагала створення груп реагування на інциденти комп'ютерної безпеки (CSIRT) і компетентних органів у кожній державі. Головною метою було підвищення рівня транснаціональної співпраці та створення механізму звітування про вчинені та виявлені кіберзагрози. Саме визначення «основних послуг» і мінімальні умови для повідомлення про безпекові інциденти здійснили найбільш негативний вплив на успішність впровадження вимог Директиви NIS. У результаті, попри досягнення Директиви, країни зіткнулися з нерівномірним навантаженням щодо дотримання нормативних вимог та різними підходами у стандартизації забезпечення виконання передбачених правил.

Враховуючи досвід та нові виклики в галузі кібербезпеки, у 2022 р. в ЄС було запроваджено вдосконалені підходи протидії кіберзагрозам шляхом прийняття Директиви NIS2. NIS2 розширює сферу дії, щоб охопити ширший спектр секторів, посилює вимоги до управління та встановлює більш суворі режими покарань для тих, хто не відповідність. З точки зору національного законодавства, розширення норм Директиви – охоплення державного управління та критичної цифрової інфраструктури на додаток до початкових основних послуг – посилило як адміністративну, так і фінансову відповідальність національних органів влади. Впровадження NIS2 зобов'язує держави-члени оновити або замінити своє існуюче законодавство, уточнити повноваження національних CSIRT та розширити канали співпраці для реагування на інциденти. Ініціативи з підвищення рівня підзвітності та формування чітких зобов'язань в управлінні ризиками ланцюга постачання цифрових послуг демонструє спробу ЄС досягти вищого рівня гармонізації законодавства. Однак, успішність цих ініціатив залежить безпосередньо від національних змін.

Прийняття в 2019 р. Закону про кібербезпеку дієво посилив законодавчу основу ЄС, доповнюючи ті ініціативи, які були передбачені Директивами NIS [241]. Закон про кібербезпеку додав ще один рівень до регуляторної архітектури ЄС. На відміну від Директив,

будучи нормативним актом, Закон набув чинності в усіх державах-членах. Таким чином прослідковується зменшення правової фрагментації, яка виникала при імплементації Директив, оскільки вони передбачають лише рекомендації до законодавчих змін. Закон про кібербезпеку посилив роль Агентства Європейського Союзу з кібербезпеки (ENISA). Згідно нового законодавства на рівні ЄС з'явився орган державного управління в галузі кібербезпеки найвищого рівня. Прямий вплив Агентства на країни ЄС полягав у тому, щоб заохотити, а в деяких випадках і примусити, національні органи з кібербезпеки співпрацювати. Головним завданням ENISA на початковому етапі було встановлення та підтримка стандартів сертифікації кібербезпеки. Незважаючи на те, що сертифікація залишається добровільною для багатьох секторів, існує ймовірність того, що вимоги до сертифікації стануть обов'язковими в сферах високого ризику. Такі зміни створюють обов'язкову відповідність як для національних регуляторів, так і для приватних організацій на цифровому ринку ЄС.

Іншим законодавчим заходом, який здійснив суттєвий вплив на загальний рівень кібербезпеки, хоча й не зосередженим виключно на цій сфері, є Загальний регламент захисту даних (GDPR). Встановлюючи жорсткі зобов'язання щодо безпеки даних, сповіщення про порушення та штрафні санкції за невідповідність, GDPR здійснив суттєвий вплив на те, як організації та регулятори реагують на ризики кібербезпеки. Кожна з країн ЄС через свої національні органи із захисту даних повинна забезпечувати виконання вимог GDPR. При цьому Регламент діє продовжуючи національне законодавство, що в свою чергу має відповідати NIS, NIS2 та Закону про кібербезпеку. Створення системи подвійного нагляду потенційно може ускладнювати дотримання всіх норм, оскільки суб'єктам ринку може знадобитися час щоб орієнтуватися у зобов'язаннях. Також учасники цифрового ринку повинні гарантувати як заходи безпеки захисту даних, так і безпеки мережі, що підвищує фінансові витрати. Незважаючи на це, розроблений та прийнятий графік сповіщення про

порушення GDPR сприяв проактивному підходу в галузі кібербезпеки. Спостерігається і підвищення якості практик безпеки даних, а також послідовне звітування про кіберзагрози національним органам влади та органам ЄС.

Останнім доповненням до нормативно-правової системи ЄС щодо кібербезпеки є Закон про цифрову операційну стійкість (DORA) [206]. Фокус передбачених вимог направлений на фінансовий сектор ЄС, враховуючи його важливість для всієї системи безпеки Союзу. Галузь фінансових послуг стала центром уваги для ЄС, враховуючи її системну важливість і вразливість до цілеспрямованих кібератак. DORA передбачає комплекс заходів для забезпечення безперервності фінансової діяльності у разі кіберзагроз. Основними заходами Закон визначає оцінку ризиків, стрес-тестування та суворий нагляд за сторонніми постачальниками. Фінансові регулятори держав-членів, як наслідок, отримують розширені повноваження щодо нагляду як за місцевими, так і закордонними фінансовими установами. Негативним наслідком для суб'єктів є підвищення витрат, які виникають у зв'язку з законодавчими ініціативами. Така динаміка змін демонструє рух ЄС у бік більш детального та секторального регулювання, визнаючи, що загрози кібербезпеці для критично важливих економічних секторів потребують спеціалізованих регламентів, інструкцій та регулятивних механізмів.

Попри те, що Закон про цифрові послуги (DSA) і Закон про цифрові ринки (DMA) не зосереджуються безпосередньо на кібербезпеці, вони містять положення, які опосередковано формують практику кібербезпеки серед великих онлайн-платформ і гейткіперів. Вимоги DSA націлені на основні цифрові платформи щодо проведення оцінки ризиків і зменшення шкоди від незаконного вмісту або неправильного використання їхніх послуг. Такі вимоги безпосередньо пов'язані з кіберзагрозами через зловживання цифровою інфраструктурою, що часто включає зловмисні дії: фішинг, дезінформація, незаконна пропаганда та інші форми кіберзагроз.

Вимоги законів зобов'язують національні органи влади узгоджувати нагляд і забезпечення виконання положень DSA з існуючими правилами кібербезпеки. Таким чином, утворюється багатогранне нормативне середовище, в якому постачальники онлайн-послуг несуть відповідальність за широкий спектр цифрових ризиків.

Запропонований Закон про захист від кіберактивності [197] демонструє вектор законодавчих ініціатив ЄС у сфері кібербезпеки. Закон передбачає орієнтування на весь життєвий цикл продуктів і послуг із цифровими елементами. Головним завданням Закону є те, що розробники та дистриб'ютори програмного забезпечення, апаратного забезпечення та пристроїв Інтернету речей повинні будуть вбудовувати функції безпеки «за проектом», підтримувати їх за допомогою своєчасних виправлень і забезпечувати прозоре звітування про інциденти кіберзагроз. Закон про захист від кіберактивності, як і Закон про кібербезпеку, матиме форму нормативно-правового акту, що встановлюватиме однакові вимоги для всіх держав-членів. По суті, запропоновані зміни сигналізують про трансформацію цифрового середовища, де кінцеві користувачі несуть основну відповідальність за безпеку своїх пристроїв, натомість покладаючи на виробників більший обов'язок гарантії базового рівня захисту.

Діючі правила ЄС щодо кібербезпеки сприяли створенню уніфікованого підходу до управління ризиками, звітності про інциденти кіберзагроз та транскордонної співпраці, але їх загальна ефективність щодо пом'якшення загроз кібербезпеці залишається дискусійним питанням. Одним з аспектів, який часто обговорюють політики та експерти галузі, є ефект від гармонізації директив, таких як початкова Директива мережевої та інформаційної безпеки (NIS) та NIS2. Саме ці Директиви встановили базові вимоги безпеки для критичних і важливих секторів, спонукали до створення національних груп реагування на інциденти комп'ютерної безпеки та сприяли більш структурованому обміну інформацією про загрози. Порівняно з періодом до NIS в ЄС впроваджено повноцінну скоординовану систему для виявлення, звітування та управління кібербезпековими заходами, що в свою чергу підвищує рівень безпечності в усьому Союзі.

Незважаючи на реальні результати роботи, зберігаються відмінності в тому, яким чином різні держави-члени впроваджують і забезпечують дотримання регламентів та політик в галузі кібербезпеки. Різниця в національних стратегіях кібербезпеки, бюджетах і технічному досвіді потенційно може призвести до фрагментованих результатів. Директива NIS, зокрема, залежала від національної транспозиції, що дозволяло державам-членам певну свободу дій у визначенні порогових значень і операційних деталей. Наявні розбіжності час від часу загрожували практичному впровадженню Директиви щодо створення єдиної бази безпеки. Навіть з розширенням вимог через прийняття NIS2, яка передбачала охоплення додаткових секторів кібербезпековими заходами, адміністративний тягар відповідності, вартість технологічних оновлень і проблема забезпечення безпеки складних ланцюгів постачання створюють постійні перешкоди для ефективного пом'якшення кіберзагроз.

Деякі аналітики стверджують, що перехід до прямого регулювання, прикладом якого є Закон про кібербезпеку та Закон про захист від кіберактивності, може ще більше посилити оборонну позицію Європейського Союзу [193]. Норми застосовуються однаково в усьому Європейському Союзі без необхідності транспонування, тим самим зменшуючи законодавчі колізії та невідповідності. Закон про кібербезпеку також передбачає створення централізованих механізмів у вигляді загальноєвропейської рамки сертифікації, що підвищує безпеку продуктів і послуг в цифровому середовищі. Проте, варто зазначити, що добровільний характер багатьох схем сертифікації та швидкий розвиток таких технологій, як штучний інтелект і квантові обчислення, означають, що навіть єдині стандарти можуть відставати від нових загроз. Незважаючи на те, що Закон про кібербезпеку посилив повноваження Агентства Європейського Союзу з кібербезпеки (ENISA) і покращив координацію загальноєвропейських навчань з кібербезпеки, доступність і розподіл технічних ресурсів залишаються нерівномірними, і, зокрема, меншим державам-членам може бути важко відповідати рівню більших або більш забезпечених держав.

Підходи щодо інтеграції політики в галузі кібербезпеки, зокрема через Закон про цифрову операційну стійкість для фінансових послуг і Закон про цифрові послуги для онлайн-платформ, висвітлюють тенденцію до більш детального регулювання практики кібербезпеки. Вказані заходи можуть краще реагувати на унікальні профілі загроз, з якими стикаються різні галузі. Вони також відображають розуміння того, що фінансові ринки, системи охорони здоров'я та цифрові платформи мають особливу вразливість для потенційних загроз в цифровому середовищі. Незважаючи на те, що різні кола стейкхолдерів у галузі позитивно ставляться до таких законодавчих ініціатив, швидке поширення нових нормативно-правових актів – деяких у формі директив, а інших – у вигляді нормативних актів, викликає занепокоєння щодо дублювання або конфлікту вимог до звітності, особливо в ситуацій, коли кілька органів влади беруть участь у моніторингу відповідності.

Науковці, які розглядали емпіричний вплив правил на результати ефективності заходів кібербезпеки, загалом визнають, що головний показник результативності проявляється у встановленні основних вимог безпеки, якими інакше могли б знехтувати приватні та державні організації [227]. Щорічні звіти ENISA про потенційні загрози вказують, що обізнаність про ризики кібербезпеки зросла як у приватному, так і в державному секторах, а також збільшився обсяг зареєстрованих інцидентів [239; 241], що можна інтерпретувати як ознаку підвищеної прозорості та покращеного регуляторного нагляду. Проте є обмежені емпіричні дані, які підтверджують пряме зменшення загальної тяжкості або частоти кібератак у ЄС. Багато експертів зазначають, що висококваліфіковані супротивники, включно зі спонсорованими державою суб'єктами, продовжують використовувати вразливості, що вказує на те, що лише регулювання не є рішенням від системних викликів кібербезпеці.

Регламент Європейського парламенту щодо спільної протидії кіберзагрозам [256] встановлює заходи для зміцнення солідарності та потенціалу в ЄС для виявлення, підготовки та реагування на кіберзагрози та інциденти та вносить зміни до Регламенту (ЄС)

2021/694 [242], імплементує надійну структуру, розроблену для підвищення стійкості Європейського Союзу проти кіберзагроз. Законодавча ініціатива, прийнята 20 листопада 2024 р., відображає прихильність Європейського Союзу зміцненню колективних механізмів кібербезпеки та зміцненню солідарності між державами-членами. По суті, положення наголошує на створенні розширених можливостей виявлення та ситуаційної обізнаності. Ключовою особливістю є створення Європейського кіберщита, мережі національних і транскордонних центрів безпеки (SOC) [193]. SOC призначені для полегшення виявлення кіберзагроз у режимі реального часу та сприяння безперебійному обміну важливою інформацією між державами-членами, таким чином забезпечуючи узгоджений та скоординований підхід до управління інцидентами кібербезпеки.

В Регламенті розроблено механізм дії для випадків надзвичайних ситуацій у кібернетичному просторі для підвищення готовності та можливостей реагування ЄС. Ключове місце в механізмі займає Резерв кібербезпеки ЄС [261], який складається з попередньо укладених послуг, що надаються довіреними організаціями. Сервіс Резерву призначений для швидкого розгортання у разі суттєвих або масштабних інцидентів кібербезпеки. Крім того, механізм підкреслює важливість взаємної допомоги між державами-членами, забезпечуючи єдину та ефективну відповідь на кіберкризи.

Важливим аспектом Закону про кіберсолідарність є його зосередженість на солідарності та взаємній підтримці між державами-членами. Регламент визначає заходи щодо надання технічної та фінансової допомоги країнам, які постраждали від кіберінцидентів. Такий колективний підхід спрямований на мінімізацію впливу кіберзагроз, захисту критичної інфраструктури та забезпечення безперервності основних послуг у всьому Союзі. На додаток до цих заходів, регламент вносить зміни до Регламенту програми «Цифрова Європа» (EU 2021/694) [242], щоб виділити фінансові ресурси для реалізації цих ініціатив. Фінансування спеціально спрямоване на

розробку та функціонування Європейського кіберщита, Механізму кібернадзвичайних ситуацій та інших ініціатив, які зміцнюють інфраструктуру кібербезпеки ЄС.

Наслідки регулювання є частиною довгострокової політики ЄС в галузі кібербезпеки. Регламент заохочує держави-члени посилити співпрацю та спільне використання ресурсів, а також розвивати національні можливості, сумісні з загальноєвропейськими системами. Заходи спрямовані на сприяння згуртованому та єдиному захисту від загроз кібербезпеці. Регламент також підкреслює роль приватного сектору шляхом включення надійних постачальників до Резерву кібербезпеки ЄС, таким чином сприяючи державно-приватному партнерству та заохочуючи розвиток надійної галузі кібербезпеки в ЄС. Для громадян і компаній закон спрямований на захист критично важливої інфраструктури та цифрових послуг, тим самим зберігаючи довіру до цифрової економіки та захищаючи суспільний та економічний добробут.

Чинні нормативні акти Європейського Союзу сприяли розвитку екосистеми, у якій кібербезпека визнається спільною відповідальністю урядів держав, приватних підприємств та установ Європейського Союзу. В створеній системі встановлено офіційні процеси для звітування про інциденти, співпрацю та розробку спільних стандартів безпеки. Однак ефективність цих заходів залежить від ресурсів і можливостей, доступних окремим державам-членам, ступеня впровадження рекомендованих практик приватним сектором і глобального характеру кіберзагроз. Хоча законодавство Європейського Союзу, безсумнівно, підвищило базові заходи безпеки, залишаються значні прогалини в тому, наскільки ефективно ці заходи перетворюються на довгострокове зниження ризику, що підкреслює необхідність постійного вдосконалення як механізмів політики, так і оперативних можливостей.

Україна, прагнучи інтегруватися до європейського правового та політичного простору, стикається з низкою викликів у сфері кібербезпеки. Відповідно до вимог Європейського Союзу та практик його держав-членів, українське законодавство потребує наближення як

у технічних аспектах (встановлення чітких стандартів безпеки, процедури інцидент-репортингу), так і в організаційній структурі (удосконалення координаційних органів, розподілу повноважень та відповідальності). Серед першочергових змін, які необхідні для гармонізації з європейською системою, можна виокремити кілька напрямів. Для цього пропонуємо наступну інформаційну модель процесу формування та реалізації Стратегії гармонізації державної політики протидії кіберзлочинності в систему кібербезпеки Європейського Союзу (табл. 5.2).

Перш за все, вкрай важливо ухвалити чи оновити законодавчу базу, яка встановлює вимоги до операторів критичної інфраструктури, а також до компаній, що надають цифрові послуги. Директива Європейського Союзу щодо безпеки мереж і інформаційних систем (NIS/NIS2) передбачає обов'язкове визначення «операторів основних послуг» і «важливих суб'єктів». Для України це означає потребу внести зміни до вже існуючих законодавчих актів або підготувати нові, що чітко формалізують критерії, за якими обираються критичні об'єкти, та встановити для них вимоги з управління ризиками й реагування на інциденти. Без формалізації цих вимог у національному праві важко досягти єдиного підходу в масштабах усієї держави.

Крім того, необхідно запровадити системи обов'язкового звітування про кіберінциденти. У країнах Європейського Союзу оператори essential services і digital service providers мають визначені строки та процедури інформування національних компетентних органів про інциденти, що можуть негативно впливати на безпеку надаваних послуг або на нормальну роботу критичної інфраструктури. Для України актуально розробити чіткий механізм, де буде вказано, хто й протягом якого часу зобов'язаний повідомляти про інциденти, як відбуватиметься їхня класифікація та які санкції застосовуватимуться в разі недотримання вимог. Такий підхід дасть змогу підвищити рівень прозорості та оперативності, з якими компанії і державні структури реагують на кібератаки.

Таблиця 5.2

Стратегія гармонізації державної політики протидії кіберзлочинам в європейський кіберпростір

ВИХІДНІ ПОЛОЖЕННЯ		
Метою Стратегії гармонізації державної політики протидії кіберзлочинам в європейський кіберпростір є створення цілісної системи запобігання, виявлення та розслідування кіберзлочинів, яка повною мірою відповідає правовим, організаційним і технічним стандартам Європейського Союзу		
Завдання Стратегії		
1. Гармонізація національного законодавства з Директивами, регламентами та рекомендаціями ЄС (зокрема NIS/NIS2, стандартами ENISA, практиками Європолу) для формування єдиної правової основи протидії кіберзлочинності.	2. Модернізація організаційних механізмів координації між правоохоронними органами, державними інституціями, приватним сектором і громадськими організаціями з метою оперативного обміну інформацією, проведення спільних навчань та формування системи інцидент-репортингу	3. Імплементація єдиних стандартів та протоколів для виявлення, розслідування та попередження кіберзлочинів, включно з розробкою уніфікованої платформи або реєстру кіберінцидентів.
4. Забезпечення підготовки та перепідготовки фахівців, які володіють сучасними методами розслідування кіберзлочинів та здатні ефективно взаємодіяти з європейськими колегами	5. Сприяння інтеграції України в загальноєвропейські кібероперативні та аналітичні механізми: EU-CyCLONe, CERT-EU	6. Підвищення рівень технічної оснащеності та кадрової компетентності державних і недержавних суб'єктів у сфері кібербезпеки.
7. Забезпечення оперативного моніторингу критичної інфраструктури та ключових цифрових сервісів	8. Імплементація принципів пропорційності у всіх заходах із моніторингу та збору даних у кіберпросторі	9. Забезпечити баланс між безпековими заходами і дотриманням прав людини, конфіденційністю та свободою слова.
І. ОРГАНІЗАЦІЙНИЙ ЕТАП		
Основні складові Стратегії гармонізації державної політики		
Правова уніфікація – адаптація Кримінального кодексу та суміжного законодавства до вимог NIS/NIS2, законодавчі ініціативи щодо відповідальності за нові види кіберзлочинів (наприклад, DDoS-атаки, фішинг із використанням «deepfake» тощо		
Організаційна перебудова – чітке розмежування повноважень між Кіберполіцією, СБУ, Міністерством цифрової трансформації та іншими гравцями; формування єдиної координаційної платформи під егідою уряду	Громадська та міжнародна взаємодія – просвітницькі кампанії щодо ризиків у кіберпросторі, механізми швидкого інцидент-репортингу для бізнесу й населення, інтеграція у спільні європейські центри координації й аналізу загроз	

Продовження табл. 5.2

Технічна модернізація – упровадження систем моніторингу та раннього попередження (SOC), обов'язкове впровадження стандартів безпеки для критичної інфраструктури, розгортання захищених каналів зв'язку		Освітній та кадровий розвиток – розробка спільних академічних і тренінгових програм з європейськими університетами, запровадження сертифікації фахівців у сфері кіберрозслідувань та цифрової криміналістики	
1. Створення робочої групи з розробки Стратегії гармонізації державної політики протидії кіберзлочинам в європейський кіберпростір			
1.А. Визначення кола фахівців держорганів (Мінцифра, МВС, СБУ та МО), ІТ-асоціації, міжнародні партнери		2.Б. Загальна координаційна підгрупа – підгрупа з визначення складу учасників	
2. Порядок затвердження робочої групи та формування забезпечення її діяльності			
2.1. Офіційне затвердження структури й регламенту групи. Визначення фінансових, технічних, кадрових ресурсів, необхідних для сталої роботи		2.2. Підгрупа з правового супроводу	
Визначення потенційних ризиків організаційного етапу			
Недостатня міжвідомча координація	Політичні зміни, що можуть вплинути на мандат робочої групи	Брак фахівців або їх дублювання	Нестабільне фінансування
II. ПРОЦЕДУРНО-АНАЛІТИЧНИЙ ЕТАП			
3. Характеристика складових процесу розробки Стратегії			
3. А. Оцінка стану зовнішнього та внутрішнього середовища	**3.Б. Визначення місії, візії та цілей Стратегії**		**3.В. Формування завдань Стратегії**
Аналіз чинного законодавства України, норм ЄС (NIS/NIS2, рекомендації Європолу, ENISA) і рівня загроз (фішинг, кібершпигунство, атаки на критичну інфраструктуру). Оцінка технічних, організаційних, правових бар'єрів гармонізації.	Формулювання місії (основне призначення політики протидії кіберзлочинам), візії (бачення інтеграції України в європейський кіберпростір) та стратегічних цілей (правова реформа, технічна уніфікація, розвиток персоналу тощо).		Визначення конкретних завдань для кожної стратегічної цілі. Урахування ресурсів, строків, потенційних партнерів, а також зв'язку із суміжними державними програмами (цифрова трансформація, захист критичної інфраструктури).

Продовження табл. 5.2

3.Г. Розробка Плану дій з реалізації стратегічних цілей	3.Д. Оцінка впливу Стратегії на стейкхолдерів	3.Е. Попередня оцінка ефективності заходів
Розробляється узгоджений план заходів із дедлайнами, виконавцями й джерелами фінансування. Враховуються вимоги ЄС і національних пріоритетів, а також можливий вплив воєнного стану.	Здійснюється аналіз потенційного впливу на державні органи, бізнес, громадськість. Зважування прав людини й принципу пропорційності при розробці заходів контролю та моніторингу.	Зіставлення пропонованих дій з європейськими практиками та стандартами (ENISA, Європол). Формування ключових показників (зниження рівня кібершахрайства, швидкість реагування).

Визначення потенційних ризиків організаційного етапу				
Протиріччя між різними аналітичними джерелами	Недоступність критичних даних або небажання певних органів ділитися інформацією	Несинхронізованість між різними держорганами	Поява правових колізій, зокрема у сфері захисту персональних даних	Ризик недостатнього фінансування чи брак фахівців
Суб'єкти процедурно-аналітичного етапу				
Експерти із державних органів, приватного сектору	Правоохоронні органи	Міжнародні та донорські інституції	Аналітичні центри	Профільні підгрупи робочої групи
ІІІ. ЕТАП ВЕРИФІКАЦІЇ ЗМІСТУ СТРАТЕГІЇ				
4.А. Оприлюднення, громадське та експертне обговорення, верифікація пропозицій зацікавлених сторін, узгодження з донорами		4.Б. Публічне винесення проєкту Стратегії. Отримання коментарів від громадськості, бізнес-спільноти, міжнародних партнерів. Корегування документа з урахуванням національних планів цифрової трансформації та вимог європейських інституцій.		
Визначення потенційних ризиків організаційного етапу				
Затягування узгоджень з зовнішніми стейкхолдерами	Брак інформації	Низька зацікавленість громадськості		

Продовження табл. 5.2

СТРАТЕГІЧНИЙ АНАЛІЗ СТРАТЕГІЇ ГАРМОНІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ В ЄВРОПЕЙСЬКИЙ КІБЕРПРОСТІР			
SWOT-аналіз	**PEST-аналіз**	**SOART-аналіз**	**VMOST-аналіз**
Визначення внутрішніх сильних і слабких сторін, а також зовнішніх можливостей і загроз у сфері протидії кіберзлочинності. Оцінка політичних, економічних, соціальних і технологічних факторів, які впливають на успішність гармонізації української системи з європейською			
Аналіз середовища функціонування системи протидії кіберзлочинам			
Зовнішня. Європейський кіберпростір, що включає вимоги директив NIS/NIS2, рекомендації Європолу та ENISA, а також досвід європейських країн у боротьбі з кіберзлочинами. Також береться до уваги посилений фокус на безпеку критичної інфраструктури та транскордонний обмін даними.		***Внутрішня.*** Вітчизняні норми кримінального права, що регулюють сферу кіберзлочинів; національні структури та підрозділи, які відповідають за кібербезпеку (Кіберполіція, СБУ, профільні департаменти міністерств та відомств). Оцінюються ресурси (технічні, кадрові, фінансові) й рівень координації між державою, приватним сектором та громадськістю.	
Оцінка впливу воєнного стану та наслідків російсько-української війни. Дестабілізаційні фактори, пов'язані з війною, створюють передумови для зростання кіберзлочинної активності, включно з кібершпигунством, кібератаками на критичну інфраструктуру, інформаційно-психологічними операціями. Також бойові дії можуть негативно впливати на фізичну безпеку дата-центрів, доступ до електроенергії і зв'язку, що ускладнює роботу фахівців із кібербезпеки.		***Оцінка ресурсного, фінансового та матеріального забезпечення.*** Для ефективного запобігання та розслідування кіберзлочинів потрібна достатня кількість кваліфікованого персоналу, спеціалізоване програмне й апаратне забезпечення, доступ до спільних інформаційних баз у рамках співпраці з європейськими структурами. Воєнний фактор збільшує навантаження на бюджет, тому важливо врахувати грантові, донорські та міжнародні програми підтримки.	
Аналіз середовища функціонування системи протидії кіберзлочинам			
Посилення законодавчої бази з урахуванням директив ЄС та вимог європейських правоохоронних органів	Розбудова інфраструктури кіберзахисту з фокусом на критичні об'єкти та комунікаційні вузли, які часто є мішенню кібератак	Підвищення кадрового потенціалу шляхом створення навчальних програм і курсів з урахуванням європейських стандартів	Розвиток міжнародної взаємодії, зокрема через спільні навчання, обмін даними про загрози та проведення транскордонних розслідувань
IV. ЗАТВЕРДЖЕННЯ СТРАТЕГІЇ ТА ПОЧАТОК ЇЇ РЕАЛІЗАЦІЇ			

Джерело: побудовано авторами.

Наступним важливим моментом є створення або посилення незалежного координаційного органу, відповідального за кібербезпеку на державному рівні. У контексті європейської інтеграції України потрібно забезпечити, аби цей орган мав чітко прописані функції щодо моніторингу, контролю, методичної підтримки й міжнародної взаємодії. У низці країн Європейського Союзу такими органами виступають національні CERT або спеціалізовані агентства, що підтримують зв'язок із ENISA (Агентство Європейського Союзу з кібербезпеки), а також беруть участь у спільних вправах і кризових координаційних ініціативах (наприклад, EU-CyCLONe). Участь України в подібних тренуваннях і обмін досвідом з європейськими інституціями допомагають інтегрувати національну систему кіберзахисту в загальноєвропейський механізм реагування.

Окремо варто наголосити на важливості запровадження системи сертифікації та стандартів кібербезпеки, сумісних з EU Cybersecurity Act. На рівні Європейського Союзу поступово формується підхід до добровільної чи обов'язкової сертифікації IT-продуктів і цифрових послуг. Для України доречно передбачити механізм, який у перспективі дозволить вітчизняним виробникам та постачальникам послуг отримувати європейські сертифікати і виходити на європейський ринок без додаткових бар'єрів. Водночас це підвищить конкурентоспроможність українських компаній та стимулюватиме їх покращувати рівень безпеки власної продукції.

Не менш суттєвою є сфера захисту персональних даних. Загальний регламент Європейського Союзу із захисту даних (GDPR) хоч і не є виключно кібербезпековим, однак вимагає дотримання високих стандартів захисту інформації. Україна вже робить кроки до наближення свого законодавства про персональні дані до європейських стандартів, але задля повноцінної інтеграції потрібно вдосконалити підходи до контролю, інцидент-менеджменту та штрафних санкцій за порушення. Це дасть змогу уникнути суперечностей між різними аспектами регулювання (наприклад, інцидент-репортинг у рамках кібербезпеки та повідомлення про витік даних за нормами GDPR) і зробить систему більш цілісною.

У контексті реформування законодавства Україна також потребує підтримки в розвитку інституційної спроможності. Прийняття нових законів чи оновлених норм саме по собі не вирішить проблему, якщо на державному і приватному рівнях бракуватиме кваліфікованих кадрів або дієвих механізмів реалізації. Тому варто зосередитися на формуванні стратегії кібербезпеки, що передбачатиме підготовку спеціалістів, а також залучення необхідних фінансових та організаційних ресурсів. Окрему роль відіграє освіта для державного сектора і керівників приватних компаній, оскільки саме вони приймають стратегічні рішення щодо інформаційної безпеки та реагування на загрози.

Проведене дослідження дає підстави стверджувати, що запровадження принципів євроінтеграції в сфері кібербезпеки насамперед вимагає законодавчих змін, які врегулюють обов'язки операторів критичної інфраструктури, забезпечать прозорий та своєчасний інцидент-репортинг, створять незалежний і ефективний координаційний орган, узгодять систему сертифікації та гармонізують підходи до захисту персональних даних із європейськими стандартами. Усі ці кроки є першочерговими, тому що становлять основу для побудови комплексної, дієвої та прозорої системи кіберзахисту, що відповідає сучасним викликам і стандартам Європейського Союзу.

5.2. Механізми інтеграції України в європейський кіберпростір в контексті інституційної структури кібербезпеки ЄС

Агентство Європейського Союзу з кібербезпеки – ENISA є головним органом ЄС, який відповідає за створення послідовної та ефективної структури кібербезпеки [211]. ENISA було засновано в 2004 р. зі штабквартирою в Греції. Повноваження Агентства з часу заснування поступово розширювалося. Поворотним моментом еволюції ENISA стало прийняття в 2019 році Закону про кібербезпеку. Прийняття закону запроваджувало нові вимоги до галузі кібербезпеки та місце Агентства в ній [211]. Завданнями ENISA як спеціалізованого

органу управління кібербезпекою є: зміцнення потенціалу кібербезпеки в країнах Європейського Союзу, координація транснаціонального реагування на кіберзагрози та розробка загальних стандартів і практик протидії кіберзагрозам.

Роль ENISA в структурі безпекових органів Європейського Союзу передбачає створення мережі співпраці між національними групами реагування на кіберзагрози та розвиток цифрової безпеки загалом. Агентство відіграє важливу роль у розробці та впровадженні законодавства. Саме ENISA можна вважати головним координатором імплементації положень Директив NIS та NIS2 [207; 208], а також при налагодженні діалогу між державними та приватними заінтересованими сторонами. Координаційна функція поширюється на управління загальноєвропейськими навчаннями з кібербезпеки, які розроблені для перевірки колективної готовності на протидії кіберзагрозам та перевірці механізмів реагування на потенційні кіберзагрози. Шляхом імітації великомасштабних кібератак навчання виявляють вразливі місця та операційні прогалини, які інакше могли б залишитися непоміченими. Таким чином, ENISA демонструє для національних регуляторів їх вразливості, що спонукає країни Європейського Союзу вдосконалювати свої стратегії виявлення та звітування про кіберзагрози, а також сприяє їх взаємодії в межах цифрового простору Європейського Союзу.

Сферою впливу ENISA, якою займається Агентство є створення та розповсюдження ефективних практик кіберзахисту та поширення технічної документації. Звіти Агентства про загрози, які публікуються щорічно, відстежують нові вектори атак і зловмисників, надаючи державам-членам, установам Європейського Союзу і приватним організаціям консолідований огляд середовища кібербезпеки [211]. Оцінювання рівня безпеки базуються на даних про виявлені кіберзагрози, висновках експертів і міжнародному обміні розвідувальними даними. Звіти висвітлюють вразливі місця в критичній інфраструктурі, ланцюгах постачання і мережевих системах як національного рівня, так і приватного сектору. Розвідувальна функція дозволяє ENISA бути регулятором та координатором для

національних органів влади. Таким чином складна та бюрократична система підвищує ефективність діяльності, через зменшення дублювання та фрагментацію при зборі та аналізі інформації, а також забезпечуючи синхронізовану відповідь на нові кіберзагрози.

Запровадження загальноєвропейської системи сертифікації кібербезпеки відповідно до Закону про кібербезпеку ще більше зміцнило роль ENISA. Хоча схеми сертифікації залишаються добровільними в багатьох секторах, ENISA уповноважена розробляти та підтримувати такі схеми у співпраці з національними органами влади та представниками галузі. На практиці це передбачає скликання робочих груп і технічних груп, де експерти обговорюють базові вимоги безпеки для продуктів, процесів і послуг ІКТ. Мета загальноєвропейської системи сертифікації полягає в тому, що після прийняття такої схеми вона застосовувалася в усіх країнах Європейського Союзу, а не приймалась окремо на національному рівні. Такий механізм співпраці з ENISA в центрі розкриває ідею координованого управління. Відповідальність за кібербезпеку в Європейському Союзі розподіляється між стейкхолдерами різних рівнів – від великих транснаціональних компаній до малих і середніх підприємств, а також між різними національними регуляторами та органами управління кожної країни.

Підтримка розробки політики протидії кіберзагрозам також розкриває координаційну функцію ENISA. Політики в Європейській комісії та Європейському парламенті часто покладаються на досвід ENISA для формулювання пропозицій, пов’язаних з кібербезпекою. Наприклад, прийняття директиви чи оновлення існуючих законодавчих актів. Володіючи великим масивом інформації про стан та рівень безпеки цифрового середовища Європейського Союзу ENISA надає технічні оцінки та консультації з провідних тем в галузі кібербезпеки: безпеки штучного інтелекту, захисту інфраструктури 5G та управління ризиками в ланцюзі поставок. Дорадча роль Агентства впливає на забезпечення того, щоб політичні пропозиції відображали новітні технологічні реалії та щоб нормативні акти могли бути реально запроваджені як на рівні Європейського Союзу, так і на національному рівнях.

Попри те, що діяльність ENISA передбачає вагомий вплив на галузь як на рівні Європейського Союзу, так і на рівні кожної з країн, Агентство стикається з низкою проблемам в забезпеченні синхронної роботи в галузі кібербезпеки в країнах Європейського Союзу. Різниця в ресурсному забезпеченні та можливості фінансування заходів з кібербезпеки, суттєво відрізняються на рівні країн. Тому здатність ENISA формувати потенціал кіберзахисту частково залежить від бажання країн Європейського Союзу інвестувати у власні внутрішні системи та приймати рекомендації ENISA. Незважаючи на те, що з часом Агентство набуло більшої оперативної спрямованості, зокрема на координацію кіберінцидентів, воно все ще значною мірою покладається на співпрацю національних команд і організацій приватного сектора для виявлення, аналізу та реагування на загрози. Описана система взаємодії призводить до складної багаторівневої динаміки управління. Правові основи країн, зокрема національні стратегії кібербезпеки та адміністративні норми країн, створюють обмеження впливу ENISA на створення цілісної системи кібербезпеки Європейського Союзу.

ENISA є ключовим органом державного управління, який відповідає за гармонізацію стандартів і заходи кібербезпеки в Європейського Союзу. Таке стратегічне значення поступово скорочує розриви між національними органами влади. Як головний координатор ENISA сприяє передачі знань і послідовному застосуванню нормативних актів, які регулюють галузь кібербезпеки. Стимулюючи ініціативи з розбудови потенціалу, підтримуючи спільні оперативні дії та розвиваючи спільну культуру безпеки, Агентство допомогло розвинути спільну відповідальність за проблеми кібербезпеки, які виходять за межі національних кордонів. Завдяки цим спільним зусиллям ENISA підтримує ширшу мету підвищення колективної стійкості проти кіберзагроз, відображаючи визнання того, що фрагментований підхід до кібербезпеки зробить критичну інфраструктуру та цифрові послуги вразливими у все більш взаємозалежному Союзі.

Архітектура кібербезпеки Європейського Союзу спирається на тісно взаємопов’язану мережу інституцій, агентств і оперативних груп, які працюють у цивільних, урядових, військових і приватних сферах.

На рис. 5.1 показано, як екосистема прагне об'єднати стратегічний нагляд, оперативне співробітництво та технічну експертизу в рамках спільної структури, що відображає імператив колективної стійкості у глобально-взаємопов'язаному середовищі [240].

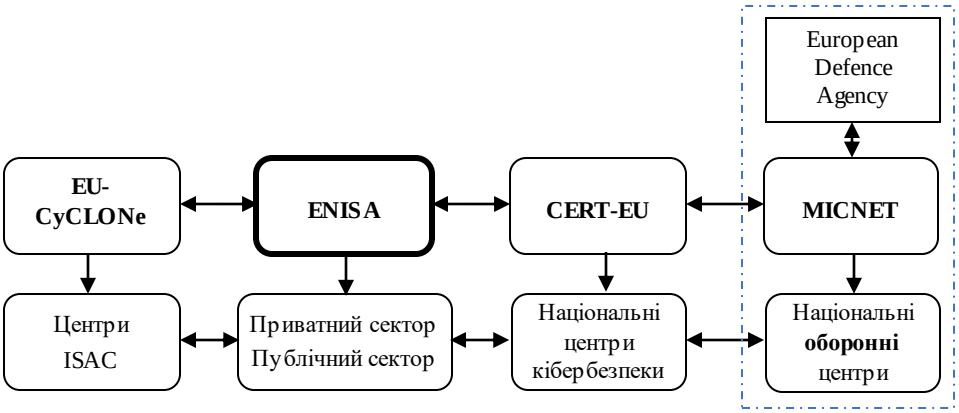

Рис. 5.1. Архітектура кібербезпеки Європейського Союзу
Джерело: створено на основі [240].

Як вже зазначалося, центральне місце в системі займає Агентство Європейського Союзу з кібербезпеки (ENISA). Відповідно до наведеної архітектури Агентство надає рекомендації, формує програми з розбудови потенціалу та надає технічну підтримку країнам Європейського Союзу та органам Європейського Союзу. Наведена архітектура демонструє, що роль ENISA виходить за рамки консультативних функцій і включає сприяння обміну інформацією та стимулювання гармонізації стандартів кібербезпеки. Через налагодження співпраці з приватними підприємствами, державними органами управління ENISA сприяє впровадженню передових форм, інструментів та методів у сфері кібербезпеки. Завдяки цій взаємодії з багатьма заінтересованими сторонами Агентство підтримує більшу частину політично-орієнтованої структури Європейського Союзу, перетворюючи Директиви NIS/NIS2 та Закон про кібербезпеку у практичні заходи, які можуть бути прийняті як на національному, так і на галузевому рівнях.

Поряд з ENISA Європейська мережа організації зв'язку з кіберкриз (EU-CyCLONe) [212] більш вузько зосереджується на оперативних аспектах кібербезпеки та врегулюванні криз, особливо під

час масштабних або транскордонних кіберзагроз. Спираючись на підтримку галузевих центрів обміну та аналізу інформації (ISAC), EU-CyCLONe допомагає координувати відповіді стейкхолдерів, гарантуючи, що приватний сектор, державні органи та спеціалізовані агентства оперативно обмінюються розвідувальною інформацією про загрози та узгоджують свої зусилля зі стримування та пом'якшення. Розподілені ISAC за секторами створюють точки взаємодії для критично важливих галузей: енергетика, фінанси, транспорт. Така система взаємодії дозволяє установам та організаціям в галузі кібербезпеки обмінюватися спеціальними галузевими даними та досвідом фактично в режимі реального часу. EU-CyCLONe працює під егідою ENISA, при цьому має власні незалежні права, що дозволяють працювати в напрямку подолання розриву між національними рамками в галузі кібербезпеки. Налагодження комунікації між національними органами країн Європейського Союзу, дозволяє EU-CyCLONe ефективно протидіяти кіберзагрозам, які можуть містити ризик поширення між декількома країнами, або навіть вийти за ці межі.

Важливим елементом в архітектурі кібербезпеки Європейського Союзу є CERT-EU. Цей орган служить спеціальною групою реагування на надзвичайні ситуації для установ, органів і агенцій Європейського Союзу в галузі кібербезпеки [191]. CERT-EU здійснює координацію між національними центрами кібербезпеки країн Європейського Союзу шляхом оперативної підтримки, аналізу виявлених кіберзагроз та надаючи рекомендації щодо захисту цифрової інфраструктури Європейського Союзу. Взаємодія між CERT-EU та національними центрами дозволяє швидше реагувати на критичні кіберзагрози. Таким чином, досягається однорідність в забезпеченні стабільності роботи цифрового середовища.

В ході роботи CERT-EU налагоджує співпрацю зі спеціалізованими державними та недержавними організаціями. Прикладом такої ефективної взаємодії є Спільний центр передового досвіду кіберзахисту НАТО (CCDCOE). Таким чином створюються спільні інструменти та методи між ЄС і НАТО в протидії кіберзагрозам. Особливо результативною така робота є при аналізі загроз і в технічних

дослідженнях [190]. Хоча CCDCOE формально є афілійованим центром НАТО, результати його досліджень з кіберзахисту інформують національні органи та органи рівня Європейського Союзу про кіберзагрози, що дозволяє зміцнювати транснаціональні зв'язки у створенні безпечного цифрового середовища.

Європейське оборонне агентство (EDA), яке в основному зосереджено на військовій співпраці між державами-членами, співпрацює з ENISA щодо ініціатив, які мають як цивільне, так і оборонне застосування. Оперативна мережа військової комп'ютерної команди реагування на надзвичайні ситуації (MICNET) [210], що працює під егідою EDA, об'єднує національні військові CERT (milCERT) з кількох країн [234]. Встановивши цю паралельну, але пов'язану оперативну структуру для інцидентів, пов'язаних з обороною, Європейського Союзу може протидіяти специфічним військовим загрозами або передовим постійним загрозами (APT), які можуть бути спрямовані на оборонну інфраструктуру, водночас координуючи роботу з цивільною владою, у ситуації, де кібератаки охоплюють кілька доменів.

Вказана взаємодія між цивільною та військовою сферами – MICNET, CERT-EU та ENISA, підкреслює зростаюче визнання в Європейського Союзу того, що кіберінциденти не завжди обмежуються інституційними кордонами. Військові системи, державні установи, оператори критичної інфраструктури та приватні компанії можуть скоординовано стати ціллю зловмисників. Таким чином, система Європейського Союзу передбачає сумісність: ресурси та досвід ENISA керують встановленням стандартів, EU-CyCLONe та CERT-EU координують управління кризовими ситуаціями для широкого цивільного сектора, тоді як EDA та MICNET займаються специфікою оборонних операцій. Водночас національні центри кібербезпеки залишаються базовими органами системи для місцевого правозастосування, реагування на кіберінциденти та впровадження політики, при цьому центри кожної держави-члена зберігають остаточну відповідальність за національну інфраструктуру та процедури транскордонного співробітництва.

Результатом є багаторівнева та взаємопов'язана екосистема, розроблена для функціонування як горизонтально, коли агенції та національні центри співпрацюють, так і вертикально, коли приватний сектор і академічні установи передають інформацію вгору, отримуючи вказівки та підтримку від органів на рівні Європейського Союзу. На практиці ефективність системи залежить від бажання та спроможності держав-членів використовувати ці канали, обмінюватися своєчасною інформацією та інвестувати в розширення можливостей національних CSIRT і milCERT. Крім того, система спирається на певний ступінь довіри та взаємну співпрацю з транснаціональними та міжнародними партнерами, враховуючи глобальний характер кіберзагроз. Тим не менш, окресливши конкретні ролі для мереж ENISA, EU-CyCLONe, CERT-EU та EDA, орієнтованих на військову діяльність, ЄС інституціоналізував структуру, яка прагне досягти узгодженості між кількома рівнями управління та різноманітними операційними контекстами.

Більш широкий погляд на систему кібербезпеки Європейського Союзу вказує на те, що її стратегічна основа кодифікована через законодавчі акти, такі як Закон про кібербезпеку та Директива NIS, які визначають обов'язки та передбачають співпрацю між державами-членами. Роль ENISA у керуванні технічними стандартами посилюється завдяки створенню загальноєвропейської системи сертифікації кібербезпеки, тоді як циклічні оцінки загроз і широкомасштабні навчання підкреслюють постійну адаптацію до мінливих ризиків. Поєднуючи нормативні цілі з готовністю на місцях, система кібербезпеки Європейського Союзу прагне зменшити ризики в спосіб, який є гнучким і надійним, визнаючи, що кіберзагрози розвиваються з тривожною швидкістю, і їм неможливо ефективно протистояти за допомогою ізольованих, нескоординованих ініціатив.

Закон про кіберсолідарність демонструє значний прогрес у підході ЄС до кібербезпеки [256]. Розвиваючи солідарність, посилюючи можливості виявлення та реагування, а також розглядаючи мінливість кіберзагроз, Регламент підкреслює відданість Європейського Союзу захисту свого цифрового суверенітету та забезпеченню безпечної та стійкої цифрової екосистеми для всіх стейкхолдерів.

Концепція транскордонних кіберхабів є критично важливим компонентом стратегії ЄС щодо посилення архітектури кібербезпеки, як це сформульовано в Законі про кіберсолідарність [240]. Кіберхаби передбачаються як платформи для співпраці, які виходять за межі національних кордонів, сприяючи співпраці в реальному часі та обміну інформацією між державами-членами. Виконуючи роль вузлів у ширшому Європейському кіберщиті, транскордонні кіберхаби відіграють ключову роль в уніфікації підходу Європейського Союзу до виявлення та подолання кіберзагроз.

Однією з основних функцій в роботі центрів є підвищення обізнаності Європейського Союзу щодо ситуації загроз кібербезпеці. Інтеграція передових технологій, включаючи штучний інтелект і машинне навчання, дозволяє здійснювати раннє виявлення аномалій і потенційних кіберзагроз. Проактивна здатність відіграє важливе значення для боротьби зі зростаючою складністю кібератак, які часто використовують вразливі місця не лише однієї країни, що може особливо негативно вплинути на стабільність всієї системи Європейського Союзу.

Транскордонні кіберхаби діють як координаційні центри під час кіберкриз. Пов'язуючи національні центри безпеки (SOC) та інші критично важливі об'єкти, центри сприяють швидкому розповсюдженню розвідувальних даних про загрози та координованої реакції на них. Така координація особливо важлива у випадках, коли кіберінциденти мають транскордонні наслідки, наприклад атаки на взаємопов'язану інфраструктуру чи ланцюги поставок. На додаток до своїх операційних функцій транскордонні кіберхаби служать інноваційними центрами та центрами нарощування потенціалу. Вони надають державам-членам платформу для обміну передовим досвідом, розробки гармонізованих протоколів і проведення спільних навчань. Такий спільний підхід не тільки зміцнює індивідуальні національні можливості, але й сприяє розвитку культури взаємодопомоги та довіри між членами Європейського Союзу.

Створення центрів передбачає значні інвестиції з боку Європейського Союзу, як зазначено в поправках до Положення про програму «Цифрова Європа» [242]. Фінансування підтримує розвиток

технічної інфраструктури, необхідної для роботи центрів, а також ініціативи, спрямовані на підвищення сумісності та стандартизації в державах-членах. Крім того, очікується, що центри будуть тісно співпрацювати з партнерами з приватного сектору, інтегруючи досвід лідерів галузі, щоб залишатися серед лідерів технологічних досягнень.

Незважаючи на потенціал трансформації, транскордонні кіберхаби стикаються з кількома проблемами. Забезпечення сумісності між різними національними системами вимагає подолання технічних і нормативних відмінностей, зберігаючи надійні стандарти захисту даних і конфіденційності. Сприяння довірі та рівноправній участі між державами-членами має важливе значення для успіху центрів. Вирішення цих викликів вимагатиме постійної політичної волі, постійних фінансових інвестицій і відданості колективній безпеці. По суті, транскордонні кіберхаби втілюють бачення Європейського Союзу стійкого та об'єднаного цифрового простору. Покращуючи можливості виявлення, координації та інновацій, ці центри є зв'язуючим елементом в системі Союзу щодо захисту свого цифрового суверенітету та забезпеченні безпечного середовища для громадян, бізнесу та державних установ. Оскільки кіберзагрози продовжують розвиватися, роль цих центрів, безсумнівно, розширюватиметься, посилюючи їхнє значення в ширшій системі кібербезпеки Європейського Союзу.

Основні положення Директиви NIS2 [208] пов'язані з забезпеченням надійних механізмів управління кіберкризами в Європейському Союзі. Як частина комплексної основи для посилення кібербезпеки в країнах Європейського Союзу, Директива зобов'язує кожну державу призначати або створювати один або декілька органів управління кіберкризою. На ці органи влади покладено особливі обов'язки щодо забезпечення скоординованої та ефективної протидії загрозам та інцидентам кібербезпеці.

Директива визнає, що інциденти кібербезпеки часто мають широкомасштабні наслідки, впливаючи на численні сектори та, у деяких випадках, перетинаючи національні кордони. Очікується, що для вирішення цих проблем органи управління кіберкризами будуть виконувати функції центральних координаційних органів у відповідних державах-членах. Їх основні функції включають нагляд за

підготовкою до серйозних кіберінцидентів, реагуванням на них і відновленням після них. Реалізація цих функцій передбачає тісну співпрацю з державними та приватними організаціями, установами для забезпечення узгодження зусиль і ресурсів.

З метою забезпечення Агентства з кібербезпеки ефективного виконання своїх обов'язків, Директива вимагає відповідні ресурси. Це не тільки гроші, але доступ до передових технологій, кваліфікований персонал і операційна підтримка. Наявність відповідних ресурсів має вирішальне значення, щоб ці агентства могли бути в курсі нових загроз, звітувати про інциденти та координувати реагування в багатьох секторах, включаючи критичну інфраструктуру, державну адміністрацію та постачальників цифрових послуг. Очікується, що ці органи управління кіберкризою працюватимуть у ширшій європейській структурі. Їм доручено робити внесок у загальноєвропейські ініціативи, такі як Європейський кіберщит і Мережа організацій зв'язку з кіберкризою (CyCLONe). Об'єднуючи зусилля з цими транскордонними механізмами, влада зміцнює колективний захист Європейського Союзу від кіберзагроз. Інтеграція передбачає обмін розвідувальними даними про загрози, участь у спільних навчаннях і узгодження національних протоколів зі стандартами Європейського Союзу.

На додаток до своїх оперативних функцій органи влади відіграють ключову роль у впровадженні та забезпеченні політики кіберзахисту. Вони контролюють застосування правил кібербезпеки в межах своєї юрисдикції, забезпечуючи дотримання організаціями вимог щодо управління ризиками та звітування про інциденти. Подвійна роль як координатора та виконавця покладає на ці організації значну відповідальність за досягнення балансу між проактивною підтримкою та регулятивним наглядом.

Серед проблем у створенні органів управління кіберкризою є те, що держави-члени повинні усунути розбіжності в можливостях, ресурсах і досвіді в різних регіонах. Забезпечення узгоджених стандартів і зміцнення довіри між заінтересованими сторонами є

важливими для ефективного функціонування органів влади. Динамічний характер кіберзагроз вимагає постійної адаптації, інновацій та нарощування потенціалу в цих організаціях.

Директива NIS2 є важливим етапам на шляху створення гармонізованого та стійкого середовища кібербезпеки в ЄС. Директива гарантує, що держави-члени спроможні реагувати на складні сучасні кіберзагрози. Досягнення цієї спроможності передбачається через створення добре забезпечених ресурсами та проактивних органів управління кіберкризами. Саме органи управління відіграватимуть вирішальну роль у захисті цифрової інфраструктури та сприянні безпеці та стабільності цифрової економіки та суспільства Європейського Союзу.

Резерв кібербезпеки Європейського Союзу є ключовим компонентом стратегічної структури Європейського Союзу, спрямованої на посилення його стійкості проти значних і масштабних кіберзагроз [256]. Резерв, запроваджений у рамках таких ініціатив, як Закон про кіберсолідарність, призначений для того, щоб Європейського Союзу мав доступні необхідні ресурси для ефективного реагування на критичні інциденти кібербезпеки. Використовуючи попередньо укладені послуги та досвід надійних приватних постачальників, резерв являє собою проактивний підхід до управління складністю та масштабом кіберзагроз, що зростає.

Основною метою Резерву кібербезпеки Європейського Союзу є надання швидкої, скоординованої та ефективної підтримки під час кіберкриз. Метою роботи Резерву є об'єднання ресурсів, які держави-члени можуть використати, коли їхні національні можливості перевантажені або коли інциденти мають транскордонні наслідки. Резерв включає низку послуг, таких як реагування на інциденти, пом'якшення загроз, цифрова криміналістика та операції з відновлення. Послуги призначені для вирішення як безпосередніх загроз, так і довгострокових наслідків кібератак.

Відмінною рисою Резерву кібербезпеки Європейського Союзу є його залежність від попередньо укладених послуг. Заздалегідь укладаючи угоди з перевіреними та надійними постачальниками з приватного сектору, Резерв гарантує, що ресурси будуть миттєво використані під час кризи. Такий підхід не тільки скорочує час відповіді, але й сприяє

інтеграції спеціалізованого досвіду та передових технологій у систему кібербезпеки Європейського Союзу. Очікується, що ці постачальники будуть дотримуватись суворих стандартів безпеки та якості, забезпечуючи надійність і ефективність своїх внесків.

Окрім реагування на кризу, Резерв відіграє ключову роль у зміцненні загального стану кібербезпеки Європейського Союзу. Через стимулювання державно-приватного партнерства зміцнюється співпраця між державами-членами, установами Європейського Союзу та стейкхолдерами галузі. Існування саме такої моделі співпраці підтримує розробку інноваційних рішень і постійне вдосконалення можливостей кібербезпеки не лише в межах держави, але на рівні Європейського Союзу.

Резерв кібербезпеки ЄС продовжує принцип солідарності, який лежить в основі Закону про кібербезпеку, оскільки втілює в собі зобов'язання держав-членів підтримувати одна одну в часи потреби, зміцнюючи колективну стійкість. Дія принципу поширюється на фінансові механізми, оскільки заповідник частково фінансується через ініціативи ЄС, такі як Програма цифрової Європи. Фінансування забезпечує достатнє фінансування резерву та його стійкість у довгостроковій перспективі. Однак впровадження та функціонування Резерву кібербезпеки ЄС не позбавлене проблем. Забезпечення справедливого доступу до ресурсів, підтримка взаємодії між різними національними системами та інтеграція внесків приватного сектору в єдину структуру ЄС вимагають ретельного планування та управління. Крім того, резерв повинен постійно адаптуватися до динаміки кіберзагроз, що вимагає постійних інвестицій в інновації та нарощування потенціалу. По суті, Резерв кібербезпеки ЄС є рамковим інструментом зі створення безпечного та стійкого цифрового середовища. Поєднуючи попередній досвід, державно-приватну співпрацю та відданість солідарності, резерв забезпечує надійний механізм для вирішення складних завдань сучасних кіберзагроз. Його створення відображає проактивну позицію ЄС щодо захисту свого цифрового суверенітету та забезпечення безпеки громадян, підприємств і критичної інфраструктури.

Академія кібернавчання є ключовою ініціативою в рамках ширшої стратегії Європейського Союзу, спрямованої на підвищення

можливостей кібербезпеки та задоволення зростаючого попиту на кваліфіковану робочу силу в цій галузі [198]. Оскільки цифрова економіка продовжує розвиватися, потреба у висококваліфікованих професіоналах для захисту критичної інфраструктури, цифрових послуг і діяльності приватного сектора стає дедалі гострішою. Академія кібернавчання прагне подолати цю прогалину в знаннях та вміннях, інвестуючи в передання досвіду, інновації та співпрацю між державами-членами. Основна мета Академії кібернавчання полягає в тому, щоб розробити надійну групу спеціалістів у сфері кібербезпеки, які зможуть вирішувати як поточні, так і нові виклики. Ініціатива зосереджена на забезпеченні комплексних навчальних і освітніх програм, адаптованих до різних рівнів знань, від практиків початкового рівня до досвідчених спеціалістів. Програми розроблено для вирішення різноманітних сфер кібербезпеки, включаючи розвідку про загрози, реагування на інциденти, управління ризиками, розробку безпечного програмного забезпечення та дотримання норм ЄС, таких як Директива NIS2 і GDPR.

Особливістю роботи Академії кібернавчання є акцент на гармонізації та стандартизації підходів до навчання в усіх країнах ЄС [198]. Узгодивши навчальні програми з загальноєвропейськими стандартами, Академія здатна забезпечувати узгодженість компетенцій і кваліфікації фахівців з кібербезпеки. Стандартизація сприяє транскордонному співробітництвута мобільності, дозволяючи професіоналам ефективно сприяти колективним зусиллям Союзу з кібербезпеки незалежно від їхнього місцезнаходження. Академія надає пріоритет інклюзивності та доступності, визнаючи важливість формування різноманітної та рівноправної робочої сили в галузі кібербезпеки.

Державно-приватне партнерство здійснює суттєвий вплив для розвитку Академії кібернавчання. Академія інтегрує передові технології та реальний досвід у свої навчальні програми через співпрацю з лідерами галузі, академічними установами та дослідними організаціями. Співпраця гарантує, що навчальна програма залишається актуальною для середовища кібербезпеки, що швидко змінюється, і озброює професіоналів практичними навичками, які можна оперативно впроваджувати на практиці. Окрім тренінгових та освітніх функцій,

Академія кібернавчання служить платформою для інновацій та обміну знаннями, що сприяє обміну дослідженнями, інструментами та методологіями між державами-членами, сприяючи розвитку культури постійного навчання та вдосконалення. Середовище співпраці підтримує розробку нових рішень і найкращих практик, що зміцнює позицію ЄС як світового лідера в галузі кібербезпеки.

Створення Академії підтримується механізмами фінансування ЄС, зокрема Програмою Digital Europe Programme [199], яка надає ресурси для розвитку та масштабування її діяльності. Ці інвестиції відображають визнання Союзом кібербезпеки як важливого фактора цифрової трансформації та економічного зростання. Незважаючи на свої амбітні цілі, Академія кібернавчання стикається з проблемами, зокрема необхідністю йти в ногу зі стрімким технологічним прогресом і розглядати різні рівні існуючого досвіду кібербезпеки в країнах-членах. Академія кібернавчання представляє трансформаційну спробу зміцнити можливості ЄС у сфері кібербезпеки через освіту, співпрацю та інновації. Усуваючи прогалину в навичках і сприяючи сталому розвитку робочої сили, Академія підтримує ініціативи ЄС щодо захисту свого цифрового суверенітету та просування безпечного, інклюзивного та розвинутого цифрового майбутнього.

Система органів взаємодії ЄС у сфері кібербезпеки має вагомий потенціал впливу на трансформацію української національної системи кіберзахисту, оскільки демонструє комплексний підхід, де кожен інститут виконує чітко окреслені функції та водночас тісно співпрацює з іншими структурами. Екосистема ЄС включає спеціалізовані установи на кшталт Європейського агентства з кібербезпеки (ENISA), мережі обміну оперативною інформацією (CERT-EU, EU-CyCLONe) та секторні платформи (ISACs), а також військові та оборонні елементи у межах Європейського оборонного агентства чи відповідних мереж (MICNET). Така модель стає прикладом, за яким Україна може оптимізувати розподіл відповідальності між державними органами, військовими структурами, приватними компаніями та громадськими інституціями.

Насамперед, українські відомства, які відповідальні за виявлення, оцінку й реагування на кібератаки, отримають зразок ефективного функціонування, де вертикальна ієрархія поєднується з горизонтальними

контактами та взаємною підтримкою між різними ланками, що сприятиме активнішому залученню України в загальноєвропейські механізми обміну інформацією про загрози і у взаємні навчальні ініціативи. Запровадження більш тісної інтеграції з ENISA та іншими структурами ЄС дозволить отримувати оновлені аналітичні дані щодо вразливостей і методів зловмисників, а також впроваджувати найкращі практики щодо протидії сучасним кіберзагрозам.

Окрім взаємодії з європейськими партнерами, українська держава зіткнеться з необхідністю внутрішньої реорганізації та оновлення нормативної бази, аби забезпечити сумісність з координаційними механізмами ЄС. Інституції, які відіграють роль Національних центрів кібербезпеки, а також військові комп'ютерні групи реагування (milCERT), імовірно, об'єднають зусилля для спільного відстеження складних багатоетапних кібератак. У такій системі держава отримує більш повну «оперативну картину» кіберзагроз і може оперативно ухвалювати рішення, у тому числі з урахуванням міжнародних рекомендацій. Гармонізація процедур із системою ЄС також позитивно вплине на рівень довіри між різними секторами й іноземними партнерами. Коли приватний бізнес бачить, що уряд слідує чітким європейським стандартам і приєднується до міжнародних ініціатив з обміну досвідом, це стимулює компанії впроваджувати власні програми безпеки та брати участь у секторальних ISACs. Такий обмін інформацією і найкращими практиками, зокрема, дозволяє краще розуміти специфіку атак на конкретні галузі та швидше розгортати ефективні заходи захисту.

Подальша інтеграція з оборонним сегментом ЄС, зокрема через механізми Європейського оборонного агентства чи подібні мережі, підштовхне реформування військового блоку кіберзахисту України. Це включатиме підвищення кваліфікації військових фахівців та уніфікацію протоколів реагування на гібридні загрози, що охоплюють і військову, і цивільну інфраструктуру. З часом такий процес дозволить уникнути дублювання функцій у різних державних структурах і сприятиме більш оперативному обміну інформацією між цивільними та оборонними відомствами. У рамках проведеного дослідження нами

запропоновано потенційну структуру системи кібербезпеки України, яка враховує необхідність інтеграції в європейську систему кібербезпеки (рис. 5.2).

Структура базується на адаптації європейських стандартів, передбачених Директивою (EU) 2022/2555 (NIS2), а також інших ключових нормативно-правових актів ЄС, таких як GDPR, Cybersecurity Act та Cyber Resilience Act. Запропонована модель включає три основні рівні: стратегічний, операційний та секторальний. На стратегічному рівні передбачено функціонування таких органів, як Офіс Президента, Кабінет Міністрів та Рада національної безпеки і оборони, які забезпечуватимуть координацію та розробку загальної стратегії кібербезпеки. Операційний рівень представлений Національним центром управління кіберкризами, Центром сертифікації кібербезпеки та Національним кіберрезервом, що забезпечуватимуть реагування на інциденти, сертифікацію IT-продуктів та послуг, а також готовність до масштабних кібератак. На секторальному рівні пропонується створення локальних офісів кібербезпеки, підтримка публічно-приватних партнерств і функціонування Академії кібернавичок для підготовки кваліфікованих кадрів. Модель орієнтована на зміцнення національної стійкості до кіберзагроз, ефективну координацію з європейськими органами кібербезпеки, а також дотримання високих стандартів кіберзахисту в усіх секторах економіки та державного управління.

Загалом, система органів взаємодії ЄС у галузі кібербезпеки вплине на трансформацію української системи передусім через демонстрацію прикладу багаторівневого, скоординованого та стандартизованого підходу до захисту цифрового простору. Впровадження споріднених процедур і методологій має на меті не лише підвищити загальний рівень безпеки критичної інфраструктури, але й стимулювати більш тісну інтеграцію України в європейський політико-правовий простір, створюючи умови для сталої співпраці та міжнародного визнання українських компетенцій у сфері кіберзахисту.

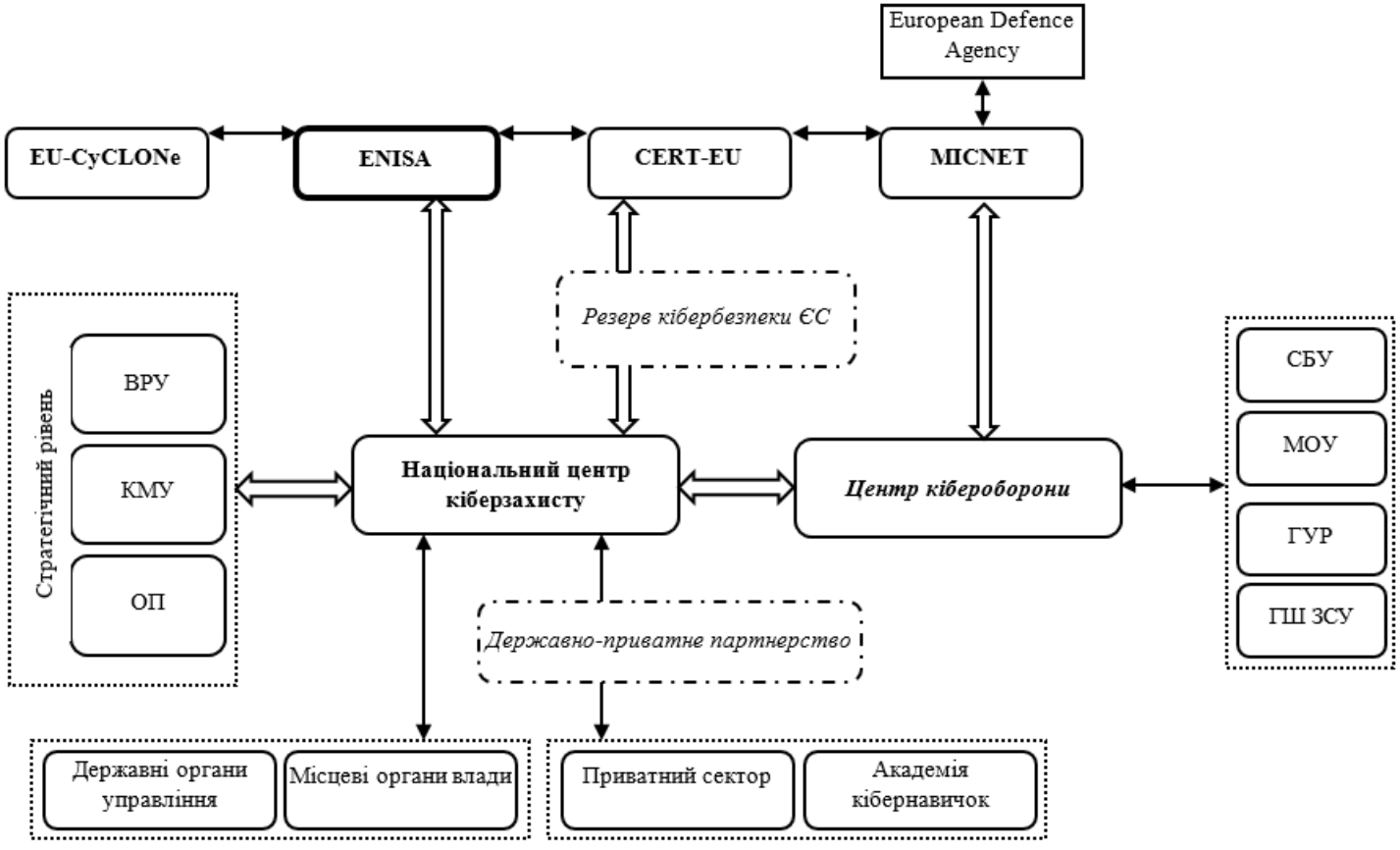

Рис. 5.2. Модель кібербезпекової системи України інтегрованої до системи ЄС

Джерело: створено на основі [240].

Проведене дослідження довело, що побудова ефективної системи кібербезпеки України потребує адаптації європейських стандартів, таких як Директива (EU) 2022/2555 (NIS2), Загальний регламент про захист даних (GDPR), Cybersecurity Act та CyberResilience Act. Гармонізація національного законодавства відповідно до цих стандартів дозволяє створити багаторівневу структуру, яка включає стратегічний, операційний і галузевий рівні з чітким розподілом функцій. Такий підхід сприяє підвищенню рівня кіберзахисту в державному управлінні, а також відповідає інтеграційним пріоритетам України в європейський економічний політико-правовий простір й має особливе значення в умовах сучасних цифрових трансформацій та глобалізації.

Запропоновано модель підвищення національної стійкості до кіберзагроз через ефективну координацію між державними органами та міжнародними організаціями. Ця модель включає створення ключових інституцій, таких як Національний центр управління кіберкризами, Центр сертифікації кібербезпеки та Національний кіберрезерв, які задні забезпечити оперативне реагування на кіберінциденти та підтримку високих стандартів сертифікації. Важливим елементом моделі є підготовка фахівців через Академію кібернавичок, яка забезпечує тривале зміцнення національного потенціалу в сфері протидії кіберзлочинам.

Доведено, що запровадження сучасних методологій та процедур забезпечує рівень безпеки критичної інфраструктури, одночасно зміцнюючи позицію України як надійного партнера в міжнародній кібербезпековій спільноті. Інтеграція з європейськими структурами, обмін досвідом та використання інноваційних підходів до управління ризиками сприяють побудові стійкої системи захисту цифрового простору. Взаємодія з міжнародними інституціями дозволяє посилити правові, технічні та організаційні механізми, що є ключовими для забезпечення безпечного цифрового середовища України та ЄС.

ВИСНОВКИ

Розроблено сукупність теоретичних положень, що є підґрунтям для формування та реалізації державної кримінально-правової політики у сфері протидії кіберзлочинності. Запропоновано багаторівневу класифікацію, що дозволило виявити більшість ознак кіберзлочинностіне лише з позиції права, криміналістики, кримінології, а й державного управління та державної політики. Обґрунтовано необхідність щодо наявності двох підходів стосовно тлумачення поняття «кіберзлочинності», а саме: 1) суспільно-небезпечне протиправне діяння, що полягає у виготовленні, фінансуванні, використанні, реалізації, обміні та розповсюдженні шкідливих програмних продуктів (на матеріальних і на нематеріальних носіях), елементів комп'ютерних систем, для зміни та підробки інформації, перехоплення інформації, втручання в дані, отримання незаконного доступу до інформації, створення неправдивої інформації, розповсюдження незаконно здобутої інформації та інших дій, що заборонено кримінальним законодавством України; 2) суспільно-небезпечне протиправне діяння, що скоєне із використанням інформаційно-комп'ютерних технологій проти особи, підприємства, органу державної влади, держави, міжнародних організацій, органів державного управління інших держав, що призводить до сукупності негативних наслідків економічного, соціального, політичного, інфраструктурного та іншого характеру та становить загрозу інформаційній, економічній, соціальній, продовольчій, енергетичній, воєнній, екологічній та політичній безпеці.

Це стало основою для визначення підходів щодо характеристики напрямків розвитку державної кримінально-правової політики, зокрема: 1) формування правового поля з використання інформації щодо функціонування джерел його утворення, зберігання, розповсюдження, обміну; 2) формування системи регулювання виробництва, використання, реалізації та обміну інформаційними технологіями, системами та їх елементами; 3) модернізації кримінального законодавства на предмет протидії кіберзлочинності, встановлення кримінальної відповідальності та інше; 4) формування

суб'єктної структури державного управління у сфері протидії кіберзлочинності; 5) активізація діяльності у сфері міжнародної співпраці щодо протидії кіберзлочинності.

Розроблено комплексну теоретико-методологічну складову державної кримінально-правової політики, що складається з наступних послідовних етапів: 1) визначення суспільної проблеми та її ключових ознак, які згруповано за детермінантами розвитку кіберзлочинності, системними проблемами правоохоронної діяльності та впливом кіберзлочинності на складові національної безпеки); 2) ідентифікація стейкхолдерів, здійснена на основі обґрунтування впливу на носіїв публічних, приватних та суспільних інтересів; 3) окреслення вихідних положень державної кримінально-правової політики у сфері протидії кіберзлочинності; 4) визначення напрямів розвитку державної політики (реформування кримінального законодавства щодо протидії кіберзлочинності; 5) трансформація суб'єктної структури системи державного управління у сфері протидії кіберзлочинності; 6)розширення міжнародно-правового механізму реалізації державної кримінально-правової політики); 7) визначення об'єктів державної політики; 8) обґрунтування суб'єктного складу; 9) визначення методів та принципів реалізації державної політики; 10) запропоновано ключові механізми її реалізації;

На основі проведеного аналізу глобального стану кіберзлочинності встановлено, що кількість здійсненних кібератак щорічно зростає, а їх характер стає складнішим, фішингові атаки є лідерами серед кіберзлочинів у світі, із тенденцією до подальшого збільшення. У 2023 р. кількість атак із використанням зловмисного програмного забезпечення досягла 6,06 млрд дол. США, це відображає масштабність проблеми. Глобальні фінансові втрати від кіберзлочинності у 2023 р. склали понад 7,1 трлн. доларів США та до 2029 р. ці втрати можуть досягти 15,63 трлн дол. Основні наслідки для організацій від втрати конфіденційної інформації є втрата доходу (56,6%), погіршення репутації(38,9%) та послаблення конкурентних позицій (35,8%). Доведено, що боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Зокрема, діяльність таких міжнародних інституцій, як Інтерпол та Європол, є одним з ефективних засобів протидії кіберзлочинності на

міжнародному рівні. Захист від кіберзагроз залежить від усвідомлення всіх учасників цифрового простору того, що забезпечення безпеки є спільною відповідальністю. Відсутність обміну інформацією про кібератаки між державними організаціями, приватними підприємствами, бізнесом та фізичними особами, а також глибоких досліджень, ефективних інструментів протидії та організованих консультацій значно підвищує ризик виникнення кіберзагрози. Для протистояння хакерським діям необхідна тісна співпраця між компаніями, організаціями та урядовими структурами, зокрема у сфері обміну інформацією про загрози та новітні методи захисту. Крім того, впровадження освітніх програм з кібербезпеки для широкої аудиторії сприятиме підвищенню рівня відомості користувачів і зниженню ризиків, пов'язаних із людським фактором.

Вивчення досвіду Республіки Узбекистан, Республіки Таджикистан та Грузії дозволило встановити напрямки трансформації кримінального законодавства України в частині розширення видів кіберзлочинів та кримінальної відповідальності за їх скоєння. Є потреба у запозиченні досвіду тих підходів, які розглядають механізми встановлення кримінальної відповідності щодо незаконного поводження з криптоактивами. Є необхідність передбачити кримінальну відповідальність або ж визначити обставину, пов'язану із критичною інфраструктурою, як таку, що обтяжує покарання за скоєні кіберзлочини. Щодо розширення обставин, які обтяжують зміст покарання, пропонується визначити наступні: завдавання значних фінансових збитків державі або суб'єктам господарювання чи фізичним особам; скоєння кіберзлочину посадовою особою або за її посередництва.

Ідентифіковано особливості еволюції кримінального права країн Європейського Союзу (Литви, Болгарії, Чехії, Польщі), які були складі Радянського Союзу або соціалістичного табору. Здійснено структурний та змістовний аналіз основних нормативних документів, що встановлюють кримінальну відповідальність за злочини. Визначено, що кіберзлочинам, у Кримінальних Кодексах зазначених вище країн приділено окремі розділи, зокрема в: зокрема в Польщі – Розділ XXXIII «Злочини проти охорони інформації»; у Чехії – Розділ V «Злочини проти власності»; у Болгарії – Главу 9 а «Комп'ютерні злочини». Варто зазначити, що в Польщі досліджувані злочини

визначають як злочини проти охорони інформації, а в Чехії як злочини проти власності. Натомість, у Кримінальних кодексах Болгарії ці злочини є відокремленими. Встановлено, що в досліджуваних країнах, незважаючи на їх членство в Європейському Союзі, відсутні єдині підходи щодо механізму покарання та поняття «кіберзлочину», що можна пояснити національними правовими традиціями та особливою увагою політиків до інформаційної безпеки держави.

При реформуванні кримінального права в Україні в умовах євроінтеграційних процесів є потреба у врахуванні лише часткового досвіду зазначених країн. Адже, вже майже десятиліття точиться дискусія щодо необхідності прийняття нового Кримінального Кодексу, який має врахувати сучасні методи скоєння злочинів, їхню класифікацію та механізми групування. Це зумовлено тим, що кіберзлочини можуть бути скоєні в різних сферах суспільного життя та можуть мати різноманітні наслідки соціального, економічного, політичного, правового характеру.

Для ефективної реалізації державної кримінально-правової політики у сфері протидії кіберзлочинності є необхідність у змістовній та структурній модернізації суб'єктів державного управління. Встановлено напрями розширення завдань та повноважень суб'єктів, що реалізують державну політику у сферах: забезпечення економічної безпеки, фінансового моніторингу, міжнародної співпраці у сфері інформаційної безпеки; захисту критичної інфраструктури; правоохоронної діяльності. Запропоновано напрямки розширення суб'єктної структури правоохоронної системи щодо протидії кіберзлочинності. Зокрема, запропоновано створення Національного бюро з розслідувань кіберзлочинів та забезпечення кібернетичної безпеки (державний правоохоронний орган, на який покладаються завдання щодо попередження, запобігання, протидії, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, скоєних у віртуальному (кібернетичному) просторі та інших сферах із застосуванням інформаційно-комп'ютерних технологій та забезпечення кібернетичної безпеки України). Визначено ключові завдання та повноваження зазначеної структури та сформовано напрями взаємодії з іншими суб'єктами, що реалізують

правоохоронну функцію. Запропоновано підпорядкувати Національне бюро розслідувань кіберзлочинів та забезпечення кібернетичної безпеки Кабінетові Міністрів України та визначити необхідність звітування перед Верховною Радою України.

Визначено специфічні риси кримінальної відповідальності за кіберзлочини, відповідно до чинного кримінального законодавства (Кримінальний Кодекс України 2001 р.). Вивчення Проєкту Кримінального Кодексу України від 01.08.2024 р., що був розроблений Робочою групою із питань розвитку кримінального права, сприяло встановленню ряду відмінностей і в частині визначення міри покарання, і в розділі, який регламентує формулювання правового положення. Зокрема, такі поняття, як: автоматизовані системи та мережі електрозв'язку не згадуються, натомість наявні поняття кіберзлочинів, пов'язаних із діями щодо інформаційних систем, комп'ютерних даних та програмних продуктів. Крім того, важливого значення в умовах війни мають кібератаки на критичну інфраструктуру, про що також не згадується в Проєкті нового Кримінального Кодексу. Відповідно, зазначене дослідження є підґрунтям для розробки векторів розвитку кримінального законодавства в частині протидії кіберзлочинам.

Запропоновано внести зміни до Кримінального Кодексу України, які стосуються: а) розширення переліку основних понять (кримінальні правопорушення у сфері кібернетичного простору та кримінальні правопорушення із використанням інформаційно-комп'ютерних технологій та систем, спрямованих проти суспільних відносин); б) передбачення окремого розділу в Кримінальному Кодексі України, під назвою «Кримінальні правопорушення у сфері кібернетичного простору»; в) передбачення ознак щодо тих обставин, які обтяжують покарання, внаслідок скоєння кримінального правопорушення у сфері кібернетичного простору; г) передбачення у частині розділу «Кримінальні правопорушення проти економіки» кримінальної відповідальності за діяльність у сфері криптовалюти та криптоактивів; д) передбачення статті, яка регулюватиме кримінальні правопорушення із використанням інформаційно-комп'ютерних

технологій та систем, спрямованих проти суспільних відносин різних видів. Визначено напрями правового регулювання щодо модернізації суб'єктної структури з питань реалізації державної кримінально-правової політики.

Акцентовано, що запровадження принципів євроінтеграції в сфері кібербезпеки насамперед вимагає законодавчих змін, які врегулюють обов'язки операторів критичної інфраструктури, забезпечать прозорий та своєчасний інцидент-репортинг, створять незалежний і ефективний координаційний орган, узгодять систему сертифікації та гармонізують підходи до захисту персональних даних із європейськими стандартами. Усі ці кроки є першочерговими, тому що становлять основу для побудови комплексної, дієвої та прозорої системи кіберзахисту, що відповідає сучасним викликам і стандартам ЄС. Для цього в роботі розроблено організаційно-методичні положення формування та реалізації стратегії гармонізації державної політики протидії кіберзлочинності системою кібербезпеки Європейського Союзу, що грунтується на вимогах Європейського Союзу.

Запропоновано модель кібербезпекової системи України інтегрованої до системи ЄС, що включає три основні рівні: стратегічний, операційний та секторальний. На стратегічному рівні передбачено функціонування таких органів, як Офіс Президента, Кабінет Міністрів та Рада національної безпеки і оборони, які забезпечуватимуть координацію та розробку загальної стратегії кібербезпеки. Операційний рівень представлений Національним центром управління кіберкризами, Центром сертифікації кібербезпеки та Національним кіберрезервом, що забезпечуватимуть реагування на інциденти, сертифікацію ІТ-продуктів та послуг, а також готовність до масштабних кібератак. На секторальному рівні пропонується створення локальних офісів кібербезпеки, підтримка публічно-приватних партнерств і функціонування Академії кібернавичок для підготовки кваліфікованих кадрів. Модель орієнтована на зміцнення національної стійкості до кіберзагроз, ефективну координацію з європейськими органами кібербезпеки, а також дотримання високих стандартів кіберзахисту в усіх секторах економіки та державного управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аніщук В. В. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2024. Вип. 83(3). С. 19-23. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2024_83(3)__4

2. Аніщук В., Зицик С. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. Науковий вісник Ужгородського Національного Університету. 2024. Т. 3, № 83. С. 19–23. URL: https://doi.org/10.24144/2307-3322.2024.83.3.2.

3. Атамась В. Р., Сокуренко О. М. Щодо проблеми визначення поняття «кіберзлочини» та «кіберзлочинність». *Актуальні проблеми формування громадянського суспільства та становлення правової держави* : збірник матеріалів IV Всеукраїнської науково-практичної інтернет-конференції, 21 травня 2021 р., Черкаси. С. 106-110.

4. Бабанін С. В. Кіберзлочинність. Комп'ютерна злочинність. Велика українська юридична енциклопедія : у 20 т. Харків, 2019. Том 18. 544 с.

5. Бабанін С. В. Кіберзлочинність. *Вісник Асоціації кримінального права*. 2016. № 1 (6). С. 468–470.

6. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. 2021. № 1 (49). С. 85-90.

7. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. № 2(42). С. 54-62.

8. Бельській Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414–418.

9. Біленчук Д. П. Кібершахраї – хто вони? *Міліція України.* 1999. № 7–8. С. 32–34.

10. Білоброва Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 121-126. URL: http://nbuv.gov.ua/UJRN/Pis_2020_3_20

11. Близнюк І. Л. Характеристика типових способів вчинення кіберзлочинів в умовах воєнного. *Наука і правоохорона*. 2022. № 3. С. 82-94. URL: http://nbuv.gov.ua/UJRN/Nip_2022_3_11

12. Борисенко В. О. Методологічні основи формування методики розслідування кіберзлочинів. Європейський правничий часопис. 2024. Вип. 3. С. 102-106. URL: http://nbuv.gov.ua/ UJRN/elj_2024_3_17

13. Боровиків В. Б. Кримінальне право. 2015 р. URL: https://stud.com.ua/53995/pravo/kriminalne_pravo

14. Бортнік П., Воєводін І. Правова природа та сутність кіберзлочинності. Протидія кіберзагрозам та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф., 26 лист. Харків : ХНУВС. 2019. С. 36–38. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/8.pdf.

15. Буяджи С. А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. Право України. 2017. № 9. С. 245-251. URL: http://nbuv.gov.ua/UJRN/prukr_2017_9_28.

16. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.

17. Вакула І. Ю. Стадії вчинення злочину за кримінальним правом України та Республіки Польща: порівняльно-правове дослідження. Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Львівський державний університет внутрішніх справ Міністерства внутрішніх справ України, Львів, 2019.

18. Васильковський І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. Прикарпатський юридичний вісник. 2017. Т. 2. № 1 (16). С. 196–201. URL: http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf.

19. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. Вип. 1–2 (10–11). С. 276-282.

20. Вілкул Т. Л. Закон судний людєм. (Уклад)**.** *Енциклопедія історії України: Т. 3: Е-Й.* НАН України. Інститут історії України. «Наукова думка». 2005. URL: http://www.history.org.ua/?termin=Zakon_sudny_ljudem.

21. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і Безпека*. 2011. № 4. С. 107–112.

22. Всесвітній огляд економічних злочинів. URL: https://www.pwc.com/ua/uk/Україна.

23. Гавриш С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії. URL: http://www.irbis-nbuv.gov.ua.

24. Голін І. В. Боротьба з кіберзлочинами: досвід окремих зарубіжних країн. *Аналітично-порівняльне правознавство*. 2024. № 4. С. 497-501. URL: http://nbuv.gov.ua/UJRN/anpopr_2024_4_85

25. Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / За ред. О. Денькович, Г. Шмельцер. Львів. ЛНУ ім. Івана Франка. 2022. 298 с.

26. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. Ресурсний центр ГУРТ. Ресурсний центр ГУРТ. URL: https://www.gurt.org.ua/articles/34602/ .

27. Горлинський В., Горлинський Б. Кібербезпека як складова інформаційної безпеки України. *Information Technology and Security*. July-December 2019. Vol. 7. Iss. 2 (13). P. 136-148.

28. Грицишен Д. О., Абрамова І. В. Міжнародні імперативи фінансового забезпечення сталого розвитку сільських громад. *Проблеми економіки*. 2024. № 2. С. 31-38. https://doi.org/10.32983/2222-0712-2024-2-31-38

29. Грицишен Д. О., Абрамова І. В. Формування та реалізації фінансових механізмів ЄС щодо сталого розвитку сільських громад. *Таврійський науковий вісник. Серія: Економіка*. 2024. № 20. С. 67-78. DOI: https://doi.org/10.32782/2708-0366/2024.20.8

30. Грицишен Д. О. Державна політика в сфері запобігання та протидії економічній злочинності: монографія. Житомир: Вид. О.О. Євенок. 2020. 384 с.

31. Грицишен Д. О., Євдокимов В. В., Савчук С. О., Корзун С. В. Стратегія інтеграції державної політики протидії кіберзлочинності в європейську систему кібербезпеки: монографія. Житомир: ТОВ «Видавничий дім “Бук-Друк”». 2024. 312 с.

32. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права.* 2014. № 4. С. 312–317.

33. Грубінко А. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. Актуальні проблеми правознавства. 2021. № 1. С. 5–10. URL: http://dspace.wunu.edu.ua/handle/316497/42023.

34. Дерещук Т. М. Виклики на шляху до ефективної протидії кіберзлочинності в Європейському Союзі. Філософія та політологія в контексті сучасної культури. 2022. Т. 14. № 2. С. 110-118. URL: http://nbuv.gov.ua/UJRN/filipol_2022_14_2_17

35. Державна служба спеціального зв'язку та захисту інформації України. Access Denied. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti.

36. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text .

37. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.

38. Діденко А. С. Державна політика у сфері протидії кіберзлочинності як об'єкт адміністративно-правового регулювання. *Матеріали конференції «Харківський національний університет внутрішніх справ:* 25 років досвіду та погляд у майбутнє (1994–2019 рр.)». Харків. 2019. С. 154. URL: https://univd.edu.ua/general/publishing/konf/22_11_2019/pdf/73.pdf

39. Діденко А. С. Мета, завдання та принципи державної політики у сфері протидії кіберзлочинності. *Право і безпека*. 2020. № 1(76). С. 53-59. URL: http://nbuv.gov.ua/UJRN/Pib_2020_1_9

40. Діордіца І. В. Поняття та зміст кіберзлочинності. *Глобальна організація союзницького лідерства.* URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti.

41. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki.

42. Довженко О. Поняття кіберзлочину з криміналістичної позиції. Юридичний вісник. 2018. №3. С. 79-83.

43. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. South Ukrainian Law Journal. 2019. Т. 1. С. 19–22. URL: https://doi.org/10.32850/sulj.2019.1-5.

44. Довженко О. Ю. Особливості проведення допиту у справах про кіберзлочини. *Право та державне управління.* 2019. № 3(2). С. 56-60. URL: http://nbuv.gov.ua/UJRN/Ptdu_2019_3(2)__11

45. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Протокол Ради Європи (від 28.01.2003 р.). Законотворчість: база даних Верховної Рада України.: https://zakon.rada.gov.ua/laws/show/994_687#Text.

46. Думчиков М. О. Кримінально-правова характеристика поняття та видів кіберзлочинів. *Науковий вісник Міжнародного*

гуманітарного університету. Сер.: Юриспруденція. 2022. С. 55. С. 65–68.

47. Думчиков М. О. Кримінально-правова характеристика поняття та видів кіберзлочинів. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2022. № 55. С. 65-68.

48. Думчиков М., Каріх І. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на тернах України. *Юридичний науковий електронний журнал*. 2022. № 5. С. 476–478. URL: https://doi.org/10.32782/2524-0374/2022-5/113.

49. Економічна правда. Протидія кіберзлочинам: правила корпоративного захисту. *Економічна правда*. URL: https://epravda.com.ua/columns/2019/05/15/647756/.

50. Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *LIGA ZAKON*: оф. вебсайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-21–49-ix.

51. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. *Часопис Академії адвокатури України.* 2012. № 17. С. 1–6.

52. Заворуєв Р., Резніченко В. Протидія кіберзлочинності в Україні. Актуальні досягнення в галузі кібербезпеки : Матеріали всеукр. науково-практ. конф. 23-25 листоп. 2016 р., м. Кропивницький. 2016. С. 49–50. URL: https://dspace.kntu.kr.ua/handle/123456789/5113.

53. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk.

54. Загуменний О. О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини». Процесуальне та техніко-криміналістичне забезпечення досудового розслідування : тези доп. всеукр. наук.-практ. конф. 28 листоп. 2019 р., м. Харків. 2019. С. 67-70.

55. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172–177.

56. Карчевський Н. В. Кіберзлочин або злочин у сфері використання інформаційних технологій. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф. 21 жовтня 2016 р. Одеса. 2016. С. 10–15.

57. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. *Актуальні проблеми міжнародних відносин.* 2015. № 126 (II). С. 77–90.

58. Кіберзлочинність: проблеми боротьби і прогнози. *Антикібер. Національне антикорупційне бюро.* URL: http://anticyber.com.ua/article_detail. php?id=140.

59. Ковальчук А. Ю. Кіберзлочини як загроза державній безпеці: кримінологічні та організаційні особливості обліку. Інформація і право. 2023. № 4. С. 187-196. URL: http://nbuv.gov.ua/UJRN/Infpr_2023_4_20.

60. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.

61. Конституція України: Закон України від 28.06.1996 №254к/96-ВР URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

62. Контрольний текст проєкту Кримінального кодексу України. URL: https://newcriminalcode.org.ua/upload/media/2024/08/02/kontrolnyj-tekst-proyektu-kk-stanom-na-01-08-2024.pdf.

63. Копан О. Словник термінів з кібербезпеки. К.: Аванпост-Прим. 2012. 214 с.

64. Користін О. Є., Бутузов В. М., Василевич В. В. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. К.: Скіф. 2012. 722 с.

65. Косиця О. Актуальні питання вдосконалення законодавства у сфері протидії кіберзлочинності. Національний юридичний журнал: теорія і практика. 2017. № 2. С. 81–84. URL: https://ibn.idsi.md/sites/default/files/imag_file/81_84_Aktual'ni%20pitannja%20vdoskonalennja%20zakonodavstva%20u%20sferi%20protidiї%20kiberzlochinnosti.pdf.

66. Коцман І. Державне регулювання протидії кіберзлочинності в Україні: поняття та основні напрямки. *Публічне управління та адміністрування в Україні*. 2024. Вип. 40. С. 245–252. URL: https://doi.org/10.32782/pma2663- 5240-2024.40.41

67. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.

68. Кривенко К. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika.

69. Криза правоохоронної системи України: монографія / За загальною редакцією В. В. Євдокимова, Д. О. Грицишена. Житомир: Видавничий дім «Бук-друк», 2023. 584 с.

70. Кримінальний кодекс Республіки Болгарія / Переклад на українську мову – О. В. Коротюк. К.: ОВК. 2024. 294 с.

71. Кримінальний кодекс Республіки Польща / Під ред. В. Л. Менчинського. Переклад на українську мову – В. С. Станіч. К.: ОВК. 2022. 164 с.

72. Кримінальний кодекс Республіки Таджикистан / Під ред. О. В. Коротюк. Переклад на українську мову – В. С. Станіч. К.: ОВК. 2019. 288 с.

73. Кримінальний кодекс Республіки Узбекистан / Під ред. В. Л. Менчинського. Переклад на українську мову – В. С. Станіч, О. В. Іванов. К.: ОВК. 2019. 194 с.

74. Кримінальний кодекс України: Кодекс України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text .

75. Кримінальний кодекс Чеської Республіки / Переклад на українську мову – О. В. Коротюк. К.: ОВК. 2020. 264 с.

76. Кришганович М. Правове забезпечення діяльності правоохоронних органів в Галичині (1772 р. – початок XX ст.). *Ефективність державного управління.* 2011. № 29.

77. Кундеус В. Г. Поняття та види кіберзлочинів. Держава і злочинність. Нові виклики в епоху постмодерну: зб. тез доп. наук.-практ. конф., присвяч. пам'яті віце-президента Кримінологічної асоціації України, професора, О. М. Литвака (м. Харків, 23 квітня 2020 р.). Харків: ХНУВС. 2019. С. 44-45. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/7723

78. Леган І. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2021. № 50. С. 118–121. URL: https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc50/27.pdf.

79. Лефтеров Л. В. Кримінологічна характеристика осіб, підозрюваних у кіберзлочинах. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція*. 2018. Вип. 35 (2). С. 65-68. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2018_35(2)__18

80. Лисеюк А. М. Застосування методів кримінального аналізу під час розслідування кіберзлочинів правоохоронними органами. Науковий вісник публічного та приватного права. 2021. Вип. 4. С. 191-194. URL: http://nbuv.gov.ua/UJRN/nvppp_2021_4_35

81. Лисько Т. Д. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права*. 2022. Вип. 96. С. 44–49. URL: http://nbuv.gov.ua/UJRN/apdp_2022_96_6

82. Ліпкан В. Національна система кібербезпека як складові частина системи забезпечення національної безпеки. *Підприємництво, господарство і право.* 2017. № 5. С. 174–180.

83. Логінова Н. І. Правові основи кібербезпеки в Україні. *Правові та інституційні механізми забезпечення розвитку держави та прав в умовах євроінтеграції*: матеріали міжнар. наук.-практ. конференції. Одеса: 2016. Т. 1. С. 575–577.

84. Лугіна Н. А. Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. *Соціологія права*. 2022. Вип. 1-2. С. 58–60. URL: http://nbuv.gov.ua/UJRN/sprav_2022_1-2_13

85. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 180–186. URL: https://doi.org/10.33244/2617-4154-1(10)-2023-180-186.

86. Малишев К. В. Державна політика в сфері трансформації правоохоронної системи: теорія, методологія, організація: монографія. Житомир: Вид. О.О. Євенок. 2022. 300 с .

87. Марисюк К. Б. Кримінально-правова політика у сфері майнових покарань на українських землях у складі Австрії (1772–1848 рр.). *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2011. № 3. С. 288–296

88. Марків С. Кіберзлочинність. Нова кримінальна загроза. Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід : матеріали ІІ Міжнар. наук.-практ. конф., м. Тернопіль. 2017. С. 360–362.

89. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека*. 2015. № 2. С. 107–113.

90. Матвійчук М. П. Кіберзлочини: поняття та види. *Кримінальне право в умовах глобалізації : матер. Міжнар. наук.-практ. конфер*. 25 травня 2018 р. Одеса, 2018. С. 236–238.

91. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави:* зб. матер. наук.-практ. конф., Київ, 22 березня 2011 р. К. : Вид-во НА СБ України, 2011. Ч. 2. С. 43-48.

92. Микитчик А. Заходи запобігання кіберзлочинності в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. 2019. С. 137–139. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf.

93. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки : монографія : електрон. наук. вид. / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька. Харків : Право, 2023. 152 с.

94. Мокляк А., Бабенко О. Теоретичний аналіз дослідження психологічного портрета кіберзлочинця. *Теорія та практика сучасної психології*. 2018. № 2. С. 89–93.

95. Мордань Є. Ю. Удосконалення вітчизняної системи протидії кіберзлочинності та кібершахрайству на основі впровадження міжнародного досвіду. *Ефективна економіка*. 2023. № 10. URL: http://nbuv.gov.ua/UJRN/efek_2023_10_40

96. Найдьон Я. П. Порнографічні діпфейки як сучасний прояв кіберзлочинності. *Соціологія права*. 2021. Вип. 1. С. 34-37. URL: http://nbuv.gov.ua/UJRN/sprav_2021_1_9

97. Никончук Н., Маслова О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. 2021. № 9. С. 202–205. URL: https://doi.org/10.32782/2524-0374/2021-9/49.

98. Нізовцев Ю. Установлення особи, підозрюваної у скоєнні кіберзлочину з використанням Wi-Fi-технологій. *Теорія та практика судової експертизи і криміналістики.* 2023. Вип. 4. С. 23-38. URL: http://nbuv.gov.ua/UJRN/Tpsek_2023_4_5

99. Нізовцев Ю. Ю. Використання можливостей WI-FI маршрутизаторів для встановлення мобільного терміналу та його мережевої активності під час розслідування кіберзлочинів. *Інформація і право*. 2023. № 4. С. 124-135. URL: http://nbuv.gov.ua/UJRN/Infpr_2023_4_14

100.Орлов О. В., Онищенко Ю. М. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління.. 2013. Вип. 3. С. 3–9. URL: http://nbuv.gov.ua/UJRN/Tpdu_2013_3_3

101.Орлов О. В., Онищенко Ю. М. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. *Теорія та практика державного управління*. 2013. № 4 (43). С. 1–6.

102.Орлов О. В., Онищенко Ю. М. Державна політика підготовки кадрів з попередження кіберзлочинності в Україні. Актуальні проблеми державного управління, 2014. № 1. С. 230-236.

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?Z21ID=&I21DBN=UJRN&P21DBN=UJRN&S21STN=1&S21REF=10&S21FMT=njuu_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21COLORTERMS=0&S21P03=I=&S21STR=%D0%9669634:%D0%A5.%D1%84./2014/1

103.Остапець А. О. Вплив ризику кіберзлочинності на діяльність технологічних підприємств. Наукові записки Національного університету «Острозька академія». Серія : Економіка. 2024. № 32. С. 37-46. URL: http://nbuv.gov.ua/UJRN/Nznuoa_2024_32_8

104.Павленко В. С. Сутність кібербезпеки у теорії інформаційного права. Право та державне управління. 2021. № 2. С. 28-33.

105.Передумови розробки нового Кримінального кодексу України. EUAM Ukraine. URL: https://newcriminalcode.org.ua/about-us#block1.

106.Пивоваров В. В., Лисенко С. Ю. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3(2). С. 177-182. URL: http://nbuv.gov.ua/UJRN/Pis_2016_3%282%29__32

107.Питання діяльності Міністерства інформаційної політки України: Постанова КМУ від 14 січня 2015 р. № 2. URL: https://zakon.rada.gov.ua/laws/show/2-2015-п#Text

108.Питання Міністерства цифрової трансформації: Постанова КМУ від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text.

109.Піцик Ю. Класифікація кіберзлочинів проти власності. Науковий вісник Міжнародного гуманітарного університету. 2017. Т. 2. № 30. С. 65–68. URL: http://vestnik-pravo.mgu.od.ua/archive/juspradenc30/part_2/18.pdf.

110.Піцик Ю. Напрями протидії кіберзлочинам проти власності. Національний юридичний журнал. 2018. № 3 (2). С. 52–54. URL: http://www.jurnaluljuridic.in.ua/archive/2018/3/part_2/11.pdf.

111.Погорецький М. А. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.

112.Полігенько О. Держустанови й банки під шквалом кібератак. Хто ще в зоні підвищеного ризику у 2025-му і яка стратегія захисту спрацює? Поради від експерта у сфері кібербезпеки. Forbes. 2025. URL: https://forbes.ua/innovations/kiberriziki-na-ponad-10-trln-zbitkiv-yaki-galuzi-biznesu-naybilshe-atakuyut-kiberzlochintsi-ta-yak-minimizuvati-naslidki-instruktsiya-vid-eksperta-u-sferi-kiberbezpeki-olega-poligenko-23012025-26534

113.Полякова О. Цифрові соціально-педагогічні технології профілактики кіберзлочинів щодо дітей: досвід України Ввічливість. 2021. Вип. 3. С. 76-83. URL: http://nbuv.gov.ua/UJRN/humit_2021_3_13

114.Посилено кримінальну відповідальність за кіберзлочини. КАПІТАЛ Юридична компанія. URL: https://capital-ukraine.com/posyleno-kryminalnu-vidpovidalnist-za-kiberzlochyny/.

115.Про Бюро економічної безпеки України : Закон України від 28.01.2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text.

116.Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. № 2938-VI. URL: https://zakon.rada.gov.ua/laws/show/2938-17#Text .

117.Про Державне бюро розслідувань : Закон України від 12.11.2015 р. № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text.

118.Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

119.Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

120.Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-р#Text.

121.Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова Кабінету Міністрів України від 03.09.2014 р. № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text .

122.Про затвердження Положення про Державну службу фінансового моніторингу України : Постанова Кабінету Міністрів України від 29.07.2015 р. № 537. URL: https://zakon.rada.gov.ua/laws/show/537-2015-п#Text .

123.Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінету Міністрів України від 28.10.2015 р. № 878. URL: https://zakon.rada.gov.ua/laws/show/878-2015-п#Text.

124.Про затвердження Положення про Міністерство закордонних справ України : Постанова Кабінету Міністрів України від 30.03.2016 р. № 281. URL: https://zakon.rada.gov.ua/laws/show/281-2016-п#Text.

125.Про затвердження Положення про Міністерство оборони України : Постанова Кабінету Міністрів України від 26.11.2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-п#Text.

126.Про затвердження Положення про Міністерство фінансів України : Постанова Кабінету Міністрів України від 20.08.2014 № 375. URL: https://zakon.rada.gov.ua/laws/show/375-2014-п#Text.

127.Про затвердження Положення про Міністерство юстиції України : Постанова Кабінету Міністрів України від 02.07.2014 р. № 228. URL: https://zakon.rada.gov.ua/laws/show/228-2014-п#Text.

128.Про затвердження Положення про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів : Постанова Кабінету Міністрів України від 11.07.2018 р. № 613. URL: https://zakon.rada.gov.ua/laws/show/613-2018-п#Text.

129. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

130.Про Кабінет Міністрів України: Закон України від 27.02.14 р. № 794-VII. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text.

131.Про Національне агентство з питань запобігання корупції. URL: https://nazk.gov.ua/uk/pro-nazk/.

132.Про Національне антикорупційне бюро України : Закон України від 14.10.2014 р. № 1698-VII. URL: https://zakon.rada.gov.ua/laws/show/1698-18#Text.

133.Про національну безпеку України: Закон України 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

134.Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

135.Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

136.Про Раду національної безпеки і оборони України: Закон України від 05.03.98 р. № 183/98. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр#Text.

137.Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

138.Про регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI. URL: https://zakon.rada.gov.ua/laws/show/1861-17/ed20100210.

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

140.Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/ laws/show/2229-12#Text.

141.Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 14.05.2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0055525-21#Text.

142.Продан Т. Кіберзлочинність: виклики часу. *Chernivtsi law school*. URL: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/.

143.Пфо О.М. Основні поняття і класифікація кіберзлочинності. Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф. 23-25 листопада. м. Кропивницький. КНТУ. 2016. С. 33–34.

144.Рибальченко Л. В. Кіберзлочинність в глобальному просторі. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 2. С. 524-530. URL: http://nbuv.gov.ua/ UJRN/nvdv_s_2022_2_80

145.Рудий Т. В. Організаційно-правові, криміналістичні та технічні аспекти протидії кіберзлочинності в Україні. Н*ауковий вісник Львівського державного університету внутрішніх справ*. серія юридична. 2018. Вип. 1. С. 283-301. URL: http://nbuv.gov.ua/ UJRN/Nvlduvs_2018_1_35

146.Рульов І. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник*. 2021. № 3. С. 178-185. URL: http://nbuv.gov.ua/ UJRN/urid_2021_3_24

147.Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять кіберзлочин і кіберзлочинність. *Право і безпека*. 2017. №1 (64). С. 74–78.

148.Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки. 2009. Випуск 19. С. 338-342. URL: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf .

149.Савчук С. О. Аналітичний вимір кібербезпеки та кіберзлочинності у світовому просторі. Тези Всеукраїнської науково-практичної онлайн-конференції аспірантів, молодих учених та студентів, присвяченої Дню науки. Житомир: «Житомирська політехніка». 2024. С. 704-705.

150.Савчук С. О. Архітектура кібербезпеки Європейського Союзу. Національна безпека в умовах війни, післявоєнної відбудови та

глобальних викликів XXI століття: збірник тез доповідей Всеукраїнської науково-практичної конференції, 7-8 грудня 2023 р. Житомир: Житомирська політехніка. 2023. С. 596-600.

151.Савчук С. О. Виклики гармонізації законодавства ЄС в галузі кібербезпеки для України. Економіка, управління та адміністрування. 2024. № 1 (107). С. 207–213. URL: https://ema.ztu.edu.ua/article/view/319745

152.Савчук С. О. Вимоги ЄС до забезпечення кібербезпеки. Правова політика України: історія та сучасність: матеріали IV Всеукраїнського науково-практичного семінару, 6 жовтня 2023 р. Житомир: Житомирська політехніка. 2023. С. 249-250.

153.Свірко С. В. Механізми державного управління бюджетною безпекою: монографія. Житомир: ТОВ «Видавничий дім «Бук-Друк»», 2021. 436 с.

154.Семенюк О. О. До питання про міжнародно-правове розуміння кіберзлочину. *Європейський правничий часопис*. 2023. № 1. С. 117-121. URL: http://nbuv.gov.ua/UJRN/elj_2023_1_21

155.Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету "Львівська політехніка"*. Серія: "Юридичні науки". № 1 (41), 2024 . С.314-320.

156.Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Справедливість у юриспруденції : теорія та практика : збірник матеріалів Міжнародної юридичної науково-практичної конференції : тези наукових доповідей. 23 лютого 2017 р. Київ : АртЕк. 2017. С. 54-58

157.Сілантьєв О. І. Інститути як складова суспільного багатства та чинник синтезу його складових. *Бізнес Інформ*. 2017. № 9. С. 128–135.

158.Словник термінів з кібербезпеки: за заг. ред. О. Копана, Є. Скулиша. К. : ВБ «Аванпост-Прим», 2012. 214 с.

159.Степлюк К. В. Кримінологічна характеристика кіберзлочинності: сучасний стан та тенденції розвитку. *Міжнародний науковий журнал «Інтернаука»*. 2018. № 22(3). С. 33-36. URL: http://nbuv.gov.ua/UJRN/mnj_2018_22(3)__9

160.Столяр О. Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів». Jurnalul juridic naţional: teorie şi practică. 2017. № 4. С. 190–193. URL: https://ibn.idsi.md/vizualizare_articol/54445.

161.Ткачова О. К. Теоретичні основи інституційних механізмів державного управління митною справою. *Державне управління: удосконалення та розвиток.* 2013. № 6. http://www.dy.nayka.com.ua/?op=1&z=587

162.Тощакова А. Проблеми боротьби з кіберзлочинністю: міжнародний досвід. *Міжнародне право в період турбулентності міжнародних відносин : зб. матеріалів Всеукр. наук. студент. інтернет-конф.* 19 листопада 2021 р. Одеса. 2021. С. 64–66.

163.Фоменко О. В. Кіберзлочинність: сучасний стан та особливості віктимологічної профілактики. *Юридичний науковий електронний журнал.* 2017. № 6. С. 328–330.

164.Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162-169.

165.Харитоненко І. О. Причини та умови вчинення кіберзлочинів. *Економіка. Фінанси. Право*. 2023. № 7. С. 67-72.

166.Хахановський В. Г. Кримінально-правове забезпечення протидії кіберзлочинності, особливості кваліфікації кіберзлочинів в Україні. *Європейський правничий часопис*. 2023. № 1. С. 38-45. URL: http://nbuv.gov.ua/UJRN/elj_2023_1_8

167.Хахановський В. Г., Гавловський В. Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право.* 2020. № 2 (33). С. 99-109. URL: http://il.ippi.org.ua/article/view/208101

168.Храпенко В. С. Протидія нотаріусів кіберзлочинам, що вчиняються в процесі державної реєстрації прав на нерухоме майно. *Актуальні проблеми вітчизняної юриспруденції*. 2017. Спец. вип. 2. С. 205-208. URL: http://nbuv.gov.ua/UJRN/apvu_2017_Spets

169.Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник.* 2018. № 3. С. 158-162. URL: http://www.pjv. nuoua.od.ua/v3_2018/34.pdf

170.Чубоха Н. Ф. Співвідношення інтересу та суб'єктивного цивільного права. *Юридичний науковий електронний журнал.* 2019. № 4. С. 56–59.

171.Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 1 (27). С. 312–320.

172.Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки.* 2018. Том 29 (68) № 6. С. 119–124. URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf.

173.Шинкарук О., Сеник В., Зачек О. Стан та особливості протидії кіберзлочинності в Україні в умовах пандемії COVID-19. *Соціально-правові студії.* 2021. № 3. С. 68–76. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/3975.

174.Шуп'яна М. Ю. Кодифікація Австрійського кримінального законодавства у другій половині XIX ст. – на початку XX ст. *Науковий вісник Ужгородського національного університету. Серія ПРАВО.* 2016. № 37 (1). С. 47–50.

175.Янґ Е. Як написати дієвий аналітичний документ у галузі державної політики. Практичний посібник для радників з державної політики Центральної і Східної Європи / пер. з англ. С. Соколик ; наук. ред. пер. О. Кілієвич. Київ : К.І.С., 2003. 120 с.

176.Яценко С. С. Основні питання загальної частини кримінального права іноземних держав. *Навчальний посібник*. К.: ВД «Дакор». 2013. 168 с.

177.Яцишин М. Криміналізація кіберзлочинів в міжнародному праві: порівняльний аналіз. Форум права. 2018. № 53 (5). С. 92–99. URL: https://doi.org/10.5281/zenodo.2009191.

178.Яцишин М. Порівняльний аналіз українського та польського кримінально-виконавчого законодавства в контексті європейських вимог. *Науковий вісник Волинського національного університету імені Лесі Українки*. 2009. № 3. С. 149–153. URL: http://evnuir.vnu.edu.ua/handle/123456789/2032.

179.Яцишин М. М., Куренда Л. Д. Злочин та покарання за Кримінальним кодексом Литовської Республіки. *Публічне право*. 2012. № 3. С. 115–121.

180.Ahram T., Sargolzaei A., Sargolzaei S., Daniels J., Amaba B. Blockchain technology innovations. *In Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON)*. 2017. P. 137–141.

181.Analytics CyberHubs. URL: https://data.cyberhubs.eu/.

182.Aria M., Cuccurullo C. Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*. 2017. Vol. 11(4). P. 959-975

183.Bequai A. High-tech security and the failings of president Clinton's commission on critical infrastructure protection. *Computers & Security*. 1998. Vol. 17, no. 1. P. 19–21. URL: https://doi.org/10.1016/s0167-4048(97)80244-1.

184.Boiko A., Shendryk V., Boiko O. Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia Computer Science*. 2019. Vol. 149. P. 65–70. URL: https://doi.org/10.1016/j.procs.2019.01.108.

185.Brito C. R., Andrade A. O. Advances in Science, Technology & Innovation (ASTI): Smart Innovation, Systems and Technologies. *Springer*. 2019. p. 45-48.

186.Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, no. 2. P. 1153–1176. URL: https://doi.org/10.1109/comst.2015.2494502.

187.Bührer S., Seus S., Walz R. Potentials and limitations of program-based research funding for the transformation of research systems. *Handbook of Public Funding of Research, chapter* 9, 2023. P. 139-155. URL: https://ideas.repec.org/h/elg/eechap/20558_9.html

188.Burlingame D. Patricia L. Rosenfield: A World of Giving: Carnegie Corporation of New York: A Century of International Philanthropy. *Nonprofit Policy Forum*. 2015. Vol. 6, no. 1. P. 121–123. URL: https://doi.org/10.1515/npf-2015-0001

189.Business Acceleration Services. *European Innovation Council*. URL: https://eic.ec.europa.eu/eic-funding-opportunities/business-acceleration-services_en.

190.CCDCOE. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/

191.CERT-EU. About us. URL: https://cert.europa.eu/about-us.

192.Chen H., Chung W., Xu J.J., Wang G., Qin Y., Chau M. Crime data mining: a general framework and some examples. *Computer*. 2004. Vol. 37. No. 4. P. 50–56. URL: http://dx.doi.org/10.1109/MC.2004.1297301.

193.Chiara P. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. International *Cybersecurity Law Review*. 2022. 3. 1-18. 10.1365/s43439-022-00067-6.

194.CSIRTs Network. URL: https://csirtsnetwork.eu/

195.Cyber Dimensions of the Armed Conflict in Ukraine | CyberPeace Institute. Cyber Attacks in Times of Conflict. *CyberPeace Institute*. URL: https://cyberconflicts.cyberpeaceinstitute.org/report.

196.Cyber incidents targeting governments global by attack vector 2023. *Statista*. URL: https://www.statista.com/statistics/1428581/government-worldwide-targeted-cyber-incidents-by-attack-vector/.

197.Cyber Resilience Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

198.Cyber Skills Academy. Knowledge and training. Digital Skills and Jobs Platform. URL: https://digital-skills-jobs.europa.eu/en/cyber-skills-academy-knowledge-and-training.

199.Cybercrime to Cost the World $9.5 Trillion USD Annually In 2024. eSentire. URL: https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in 2024?utm_medium=email& utm_source=pardot&utm_campaign=autoresponder.

200.Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU. Council of the EU. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/

201.Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013, 02 February). *European Comission. High representative of the European Union for foreign affairs and security policy. Brussels*. Join. URL: http:// www.enisa.europa.eu.

202.Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security.

203.Data explorer – ITU DataHub. The worldâs richest source of ICT statistics and regulatory information – ITU DataHub. URL: https://datahub.itu.int/dashboards/idi/?y=2024&e=UKR.

204.Deep Learning Approach for Intelligent Intrusion Detection System. *R. Vinayakumar et al. IEEE Access*. 2019. No 7. P. 41525–41550. URL: https://doi.org/10.1109/access.2019.2895334

205.Dema D., Abramova I., Nedilska L. Financial and Economic Conditions of Rural Development in Ukraine. *Eastern Journal of European Studies*. Volume 10. Issue 1. 2019. pp. 199-220. https://ejes.uaic.ro/articles/EJES2019_1001_DEM.pdf

206.Digital Operational Resilience Act (DORA). URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

207.Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: http://data.europa.eu/eli/dir/2016/1148/oj

208.Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014

and Directive (EU) 2018/1972. URL: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

209.Dr. Mike McGuire and Samantha Dowling. Cybercrime: A review of the evidence Summary of key findings and implications. *Home Office Research Report 75*. University of Surrey. 2013

210.EDA-led network of cyber defence teams starts with 18 EU countries. URL: https://eda.europa.eu/news-and-events/news/2023/02/10/eda-led-network-of-cyber-defence-teams-starts-with-18-eu-countries.

211.ENISA. Threat Landscape 2024. ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

212.EU CyCLONe. ENISA. URL: https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone.

213.EUR-Lex – Access to European Union law. *For a European Industrial Renaissance. Commission Communication. COM(2014) 14 final.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014 DC0014&amp.

214.European Commission, Directorate-General for Research and Innovation, Key findings from the Horizon 2020 interim evaluation, Publications Office. 2017. P. 3-4. URL: https://data.europa.eu/doi/10.2777/46837.

215.European Innovation Council and SMEs Executive Agency. EIC pathfinder challenges in the EIC work programme 2024. *Publications Office of the European Union*. 2023. URL: https://data.europa.eu/doi/10.2826/449500.

216.European Research Area. *European University Association*. URL: https://www.eua.eu/our-work/topics/european-research-area.html.

217.Funding by management mode. *European Commission*. URL: https://commission.europa.eu/funding-tenders/find-funding/funding-management-mode_en.

218.Gareth Corfield. 'Russian cyberattacks on Ukraine halved with help from Amazon and Microsoft', The Telegraph, 7 January 2023. URL: https://www.telegraph.co.uk/business/2023/01/07/russian-cyberattacks- ukraine-halved-help-amazon-microsoft/

219.Gruodytė E. Reform of Lithuanian Criminal Law: Tendencies and Problems. *Baltic Journal of Law & Politics*. 2008. No 1. P. 18–40.

220.Haines J. and Johnstone P. Global Cybercrime: New Toys for the Money Launderers, *Journal of Money Laundering Control*. 1999. No 2 (4). P. 317–325. URL: https://doi.org/10.1108/eb027198.

221.Holt T. J., Bossler A. M. Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant*

Behavior. 2008. No 30 (1). P. 1–25. URL: https://doi.org/10.1080/01639620701876577.

222.Home – Grant Writing USA. *Grant Writing USA*. URL: https://www.grantwritingusa.com.

223.Html Publication. ITU: Committed to connecting the world. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

224.Ievdokymov V., Frikel A., Polishchuk V., Savchuk S., Klimova I. Cybercrime and Information Protection in the Field of State Security: Current Threats and Measures for their Prevention. *Economic Affairs (New Delhi)*. 2024. Volume 69, P. 61-69.

225.Isaak J., Hanna M. J. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*. 2018. No 51 (8). P. 56–59. URL: https://doi.org/10.1109/mc.2018.3191268.

226.Isaksen A., Trippl M. Exogenously Led and Policy-Supported New Path Development in Peripheral Regions: Analytical and Synthetic Routes. *Economic Geography*. 2016. Vol. 93, no. 5. P. 436–457. URL: https://doi.org/10.1080/00130095.2016.1154443.

227.Jara Antonio J., Martinez, Iris, Sanchez Jaime. CyberSecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2. 2024. URL: 10.1109/SCFC62024.2024.10698057.

228.Johnstone P. Financial Crime: Prevention and Regulation in the Intangible Environment. *Journal of Money Laundering Control*. 1999. No 2 (3). P 253–263. URL: https://doi.org/10.1108/eb027191.

229.LAB – FAB – APP. *Publications Office of the EU*. URL: https://data.europa.eu/doi/10.2777/477357.

230.Lietuvos Respublikos baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Baudžiamasis kodeksas. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/JYbvMjklSa.

231.Meng-Hsuan Ch. The evolution of the Europe-an Research Area as an idea in European integration. In Meng-Hsuan Chou and Åse Gornitzka (Eds.), *Build-ing the knowledge economy in Europe*. 2014. p. 27-50.

232.Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. April 27, 2022. URL: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc.

233.Microsoft, Defending Ukraine: Early Lessons from the Cyber War, 22 June 2022. URL.: https://query.prod.cms.rt. microsoft.com/cms/api/am/binary/RE50KOK.

234.MilCERT Interoperability Conference talks strategy. EDA. URL: https://eda.europa.eu/news-and-events/news/2021/06/08/milcert-interoperability-conference-talks-strategy.

235.NCSI: Ranking. Index. URL: https://ncsi.ega.ee/ncsi-index/

236.Norton Cyber Security Insights Report: Global Results, Harris Poll. 2023. URL: https://www.gendigital.com/media/ qcymrc1i/2023-ncsir-us-global-report_final.pdf

237.Obnovené zřízení zemské: Zákoník, ústava nebo základ absolutismu. URL: https://www.stoplusjednicka.cz/.

238.OECD database. URL: https://stats.oecd.org/

239.Policy Observatory. ENISA. URL: https://www.enisa.europa.eu/ topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/policy-observatory.

240.Potentials and challenges for EU cybersecurity cooperation. Institutt for informatikk. Forside. Det matematisk-naturvitenskapelige fakultet. URL: https://www.mn.uio.no/ifi/studier/masteroppgaver/ informasjonssikkerhet/potential-and-challenges-for-cybercooperation-in-e.html.

241.Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). URL: http://data.europa.eu/eli/reg/2019/881/oj.

242.Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. URL: http://data.europa.eu/ eli/reg/2021/694/oj

243.Reyns B. W., Henson B., Fisher B. S. Being Pursued Online. *Criminal Justice and Behavior*. 2011. Vol. 38. No. 11. P. 1149–1169. URL: https://doi.org/10.1177/0093854811421448.

244.Robust Intelligent Malware Detection Using Deep Learning / *R. Vinayakumar et al. IEEE Access*. 2019. Vol. 7. P. 46717–46738. URL: https://doi.org/10.1109/access.2019.2906934 .

245.Romanchuk L., Abramova I., Moroz Yu., Poplavskyi P. Svitlyshyn I. Funding for sustainable development of rural communities: European experience. *Agricultural and Resource Economics*. 2024. Vol. 10. No. 4. Pp. 203–234. https://doi.org/10.51599/are.2024.10.04.09

246.Samuelson P. A. The Pure Theory of Public Expenditure. *The Review of Economics and Statistics*. 1954. Vol. 36, no. 4. P. 387. URL: https://doi.org/10.2307/1925895

247.Savchuk S. Challenges and prospects for the formation of state policy in the field of cybersecurity and combating cybercrime. Public Policy and Accounting. 2024. № 1 (9). P. 30–38. URL: https://ppa.ztu.edu.ua/article/view/321575

248.Savchuk S. Institutional and legal model for the formation and implementation of the state policy of combating cybercrime. Public Policy and Accounting. 2023. № 2 (8). P. 56–60. URL: https://ppa.ztu.edu.ua/article/view/321327.

249.State Service of Special Communications and Information Protection of Ukraine, 'Ukraine has signed an agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence', 19 January 2023. URL: https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato.

250.StatPlanet. *EC-OECD STIP Compass*. URL: https://stip.oecd.org/stats/SB-StatTrends.html?i=TOP10_X&v=3&t=2006,2020&s=UKR.

251.Stephanie Pell. 'Private-Sector Cyber Defense in Armed Conflict', Lawfare, 1 December 2022. URL: https://www.lawfareblog.com/private-sector-cyber-defense-armed-conflict.

252.Susan Landau. 'Cyberwar in Ukraine: What You See Is Not What's Really There', Lawfare, 30 September 2022. URL: https://www.lawfareblog.com/cyberwar-ukraine-what-you-see-not-whats-really-there.

253.The Digital Europe Programme. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

254.The Digital Markets Act. URL: https://digital-markets-act.ec.europa.eu/index_en.

255.The Digital Services Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

256.The EU Cyber Solidarity Act. Shaping Europe's digital future. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

257.The European Commission's response to the coronavirus crisis. *European Commission*. URL: https://commission.europa.eu/strategy-and-policy/coronavirus-response_en.

258.Transforming our world: the 2030 Agenda for Sustainable Development. Department of Economic and Social Affairs. *Sustainable Development*. URL: https://sdgs.un.org/2030agenda.

259.UN Human Rights Monitoring Mission in Ukraine. URL: https://ukraine.ohchr.org.

260.USTAWA z dnia 6 czerwca 1997 r. Kodeks karny1. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf.

261.Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022. Cambridge : Harvard Kennedy School, 2022. 66 p. URL: https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

262.World Bank. *World Bank Open Data*. URL: https://data.worldbank.org/indicator/SP.POP.SCIE.RD.P6?locations=UA.

263.Yar M. The Novelty of «Cybercrime». *European Journal of Criminology*. 2005. No. 2(4). P. 407–427. URL: https://doi.org/10.1177/147737080556056.

264.Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). URL: https://www.zakonyprolidi.cz/cs/2009-40.

265.ЎЗБЕКИСТОН РЕСПУБЛИКАСИНИНГ ЖИНОЯТ КОДЕКСИ. URL: https://www.lex.uz/docs/111453.

266.საქართველოს სისხლის სამართლის კოდექსი. სსიპ ”საქართველოს საკანონმდებლო მაცნე”.b URL: https://matsne.gov.ge/ka/document/view/16426?publication=264.

Наукове видання

Колектив авторів:
Євдокимов В. В., Грицишен Д. О., Свірко С. В., Дикий А. П.,
Сергієнко Л. В., Кіблик Д. В., Соха С. І., Сьомак О. М.,
Токарчук О. Й., Умрихіна І. О., Харченко О. А., Корзун С. В.,
Савчук С. О., Михаленко Д. Д., Бовсунівський С. І., Здибель Р. О.,
Порохнавець В. В., Соха А. І.

СТРАТЕГІЯ ІНТЕГРАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ЄВРОПЕЙСЬКУ СИСТЕМУ КІБЕРБЕЗПЕКИ

МОНОГРАФІЯ

За загальною редакцією
Віктора Євдокимова, Димитрія Грицишена

Віддруковано з готових оригінал-макетів

Підписано до друку 23.04.2024 р.
Папір офсетний. Формат 70x100/16
Гарнітура "Таймс". Друк офсетний. Ум. др. арк. 24,4
Наклад 300 прим. Зам. № 906

ТОВ «Видавничий дім "Бук-Друк"»
м. Житомир, вул. М. Бердичівська, 17А.
тел.: 063 101 22 33

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції України серія ДК № 7412 від 27.07.2021 р.

Друк та палітурні роботи ФОП О.О. Євенок
м. Житомир, вул. Мала Бердичівська, 17А
тел.: 063 101 22 33, e-mail: printinzt@gmail.com

Свідоцтво *про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції України серія ДК № 3544 від 05.08.2009*