МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Навчально-науковий інститут новітніх освітніх технологій
Кафедра менеджменту, публічного управління та персоналу

НІМЧУК Василь Павлович

Удосконалення діяльності органу влади в питаннях запобігання кіберзлочинності. / Improving the activity of the authority in matters of cybercrime prevention

спеціальність: 281 - Публічне управління та адміністрування
освітньо-професійна програма - Публічне управління та адміністрування

Кваліфікаційна робота

Виконав студент групи ПУАзм-24
В. П. Німчук
_____

Науковий керівник:
к.е.н., доцент, Ю. А. Богач
_____

Кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **М. М. Шкільняк**

ЗМІСТ

ВСТУП

Кіберзлочинність є відносно новим явищем, яке виникло разом із появою та поширенням глобальної мережі Інтернет, і відрізняється від традиційних видів злочинів. Вона з самого початку стала зручною формою для зловмисників, оскільки особливості Інтернету забезпечують глобальність та анонімність користувачів. Ці фактори стали ключовими передумовами для її появи. Разом із зростанням кількості кіберзлочинів зросла й необхідність правового регулювання цього питання як у світі, так і в Україні. Ефективна протидія кіберзлочинності вимагає розуміння її сутності та генезису, а також аналізу історичного розвитку правових механізмів боротьби із цим явищем.

Значний внесок у вивчення кіберзлочинності зробили такі вчені, як В.М. Бутузов, Г.П. В.Я. Вовк, А.В. Гавловський, Р.Є. Джансараєва, В.Б. Дзюндзюк, Д.В. Дубов, О.Є. Літвінов, В.В. Марков, М.А. Ожеван, К.М. Рудой, Є.Д. Скулиш, В.Г. Хахановський, В.В. Чернєй та інші. Більшість із них досліджували різні аспекти правового регулювання боротьби з кіберзлочинністю, але питання ретроспективного аналізу, тенденцій розвитку та механізмів правового регулювання залишаються недостатньо комплексно вивченими.

Метою дослідження є формування концептуального розуміння специфіки, тенденцій розвитку та механізмів боротьби з кіберзлочинністю. Для досягнення цієї мети визначено такі завдання:

Об’єктом дослідження є кіберзлочинність як суспільне явище та методи боротьби з нею.

Предмет дослідження охоплює теоретико-правові основи регулювання боротьби із кіберзлочинністю.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ДІЯЛЬНОСТІ ОРГАНІВ ВЛАДИ В ПИТАННЯХ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

1.1. Теоретико-правові основи діяльності органів влади в питаннях запобігання кіберзлочинності

Рівень кіберзлочинності в нашій країні довгий час залишався відносно низьким через недостатній розвиток інформаційних технологій порівняно з передовими державами світу. Проте нині ситуація змінюється. Зростання рівня освіти серед молоді, значний рівень безробіття та обмежені можливості працевлаштування створюють умови для збільшення масштабів цього явища. Останні події також продемонстрували потенційну загрозу кіберзлочинності у ширшому контексті.

В Україні проблема ускладнюється тим, що термін «кіберзлочинність» досі не має чіткого визначення в офіційних нормативно-правових документах. Хоча це поняття широко використовується як у правоохоронних органах, так і в юридичній доктрині, відсутність точного визначення створює перешкоди для ефективної боротьби з цим явищем. Розвиток інформаційних технологій у всіх сферах суспільного життя, включаючи державні та приватні інституції, підкреслює необхідність пріоритетного вирішення цієї проблеми.

Крім очевидних втрат, пов'язаних з несанкціонованим доступом до інформації, її модифікацією чи знищенням, кіберзлочинність становить загрозу національній безпеці, економіці, правам людини та інтересам громадян. Водночас суспільство ще недостатньо усвідомлює серйозність цієї загрози, що частково пояснюється браком наукових досліджень у цій сфері. Це підкреслює необхідність використання досвіду як українських, так і міжнародних практик для розробки ефективних підходів до боротьби з кіберзлочинністю.

Пропонуємо трактувати кіберзлочинність як сукупність протиправних дій, передбачених кримінальним законодавством, які здійснюються у

віртуальному просторі і спрямовані на шкоду комп'ютерним системам, мережам чи даним. У сучасній українській науці термін «боротьба з кіберзлочинністю» залишається новим, незважаючи на те, що злочини, пов'язані з використанням Інтернету, мають високий рівень суспільної небезпеки. Хоча цей термін неодноразово згадувався в науковій літературі, автори рідко зосереджуються на його сутності та особливостях. Тому розробка теоретичної бази для вивчення цього соціального явища є одним із ключових завдань.

Для аналізу концепції протидії кіберзлочинності важливо звернутися до законодавчих актів, таких як Конституція України, Конвенція про кіберзлочинність, Кримінальний кодекс України та Кримінально-процесуальний кодекс України. У Конституції, наприклад, не згадується термін «боротьба з кіберзлочинністю». У статті 17 підкреслюється значення інформаційної безпеки, але відсутні положення, які безпосередньо регулюють протидію кіберзагрозам.

Конвенція про кіберзлочинність 2001 року, ратифікована Україною в 2005 році, також не містить чіткого визначення цього поняття. У Кримінальному кодексі України виділені окремі статті, присвячені комп’ютерним злочинам (статті 361–363), однак термін «боротьба з кіберзлочинністю» залишається невизначеним. Подібна ситуація спостерігається і в Кримінально-процесуальному кодексі, де певні статті стосуються кіберзагроз (наприклад, статті 263–268), але без узагальненого визначення.

Відсутність чіткого законодавчого закріплення поняття «боротьба з кіберзлочинністю» породжує теоретичну невизначеність і складнощі у його науковій інтерпретації. Зокрема, у законодавстві України термін «протидія кіберзлочинності» частіше використовується, ніж «боротьба». Хоча ці поняття мають спільні риси, вони не є тотожними. Протидія має реактивний характер, тобто передбачає дії у відповідь на конкретні загрози. Натомість боротьба охоплює активну діяльність, спрямовану на усунення проблеми, незалежно від

того, чи є конкретна загроза в даний момент.

Таким чином, боротьба з кіберзлочинністю має два основні напрями: попередження злочинів та розкриття вже скоєних правопорушень із притягненням винних до відповідальності. Використання терміна «боротьба» у державній політиці є доцільним, оскільки підкреслює активний і цілеспрямований характер діяльності. Водночас для правоохоронних органів доречними є такі поняття, як «протидія» та «запобігання» кіберзлочинності, які відображають їхню практичну роботу.

Юридична енциклопедія визначає «запобігання злочинності» як сукупність репресивних і нерепресивних заходів. До них відносять як забезпечення невідворотності покарання, так і виправлення осіб, які скоїли злочини. Однак цей підхід вимагає розширення, щоб включити виявлення злочинів та їхніх виконавців, а також удосконалення законодавства.

Зважаючи на специфіку кіберзлочинності, запобігання їй стає складним завданням для сучасної держави. На жаль, санкції, передбачені Кримінальним кодексом України за кіберзлочини, нерідко є недостатньо суворими. Наприклад, створення або продаж шкідливих програм карається штрафом або позбавленням волі на строк до двох років, що не відповідає серйозності завданої шкоди. Враховуючи глобальний характер кіберзлочинності, необхідно посилити покарання і вдосконалити механізми протидії цьому явищу.

Законодавець формує нормативно-правову базу, а компетентні правоохоронні органи займаються запобіганням злочинам, їх розслідуванням і притягненням винних осіб до відповідальності. У свою чергу, окремі громадяни або групи також можуть активно сприяти цій боротьбі. У таких умовах принцип самоврядування полягає в тому, що, незважаючи на різноманітність учасників, кожен з них працює задля досягнення спільної мети. У контексті боротьби з кіберзлочинністю в Україні ця діяльність зазвичай здійснюється Департаментом кіберполіції Національної поліції, законодавцями та іншими соціальними групами, зацікавленими у вирішенні

цієї проблеми.

За таких обставин законодавець виконує функції у законодавчій та організаційній сферах, тоді як Департамент кіберполіції зосереджується на профілактичних заходах. Інші соціальні групи, які прагнуть допомогти у боротьбі з кіберзлочинністю, сприяють цьому процесу в межах своїх можливостей. Комплексність боротьби з кіберзлочинністю полягає у поєднанні репресивних та превентивних заходів задля досягнення поставлених цілей. Хоча збірність і комплексність є близькими за змістом, вони мають відмінності:

– збірність передбачає об'єднання підсистем, які відрізняються своїми функціями та призначенням, тоді як комплексність полягає у взаємодії всіх елементів для досягнення єдиної мети;

– мета збірності — це створення єдиної структури, тоді як комплексність спрямована на встановлення зв'язків між елементами, які підвищують ефективність процесу;

– збірність є поняттям структурним, а комплексність — функціональним.

На відміну від загального поняття «боротьби зі злочинністю», поняття «боротьба з кіберзлочинністю» є менш вивченим у науковій літературі.

Увага вітчизняних дослідників зосереджується на різноманітних аспектах цього явища, зокрема на процесуальних питаннях і нормативно-правовій базі його існування. Однак понятійний апарат часто залишається поза увагою. У ході нашого дослідження було встановлено, що дефініція поняття «боротьба з кіберзлочинністю» є новим терміном для української юридичної науки. Аналіз російських наукових джерел показав, що їхні дослідники також приділяють увагу схожим проблемам, проте визначення поняття «боротьба з кіберзлочинністю» залишається невизначеним і у них.

Варто підкреслити, що міжнародна співпраця у сфері боротьби з кіберзлочинністю здійснюється за такими основними напрямами: 1) розробка міжнародно-правових механізмів регулювання та співпраця правоохоронних органів; 2) гармонізація національного законодавства з міжнародними

нормами; 3) формальне та неформальне співробітництво між країнами; 4) координація повноважень у боротьбі з кіберзлочинністю. Таким чином, зростаючий рівень і темпи поширення кіберзлочинності вимагають адекватної реакції не лише на законодавчому чи правоохоронному рівнях, але й у науковій сфері.

1.2. Види та загрози кіберзлочинності для інформаційної безпеки

Кіберзлочини можна розподілити за різними критеріями, такими як мета, виконавець або спосіб вчинення. На сьогодні найбільш поширеною є класифікація, що базується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація вважається своєрідним «еталоном», оскільки вона використовується у більшості міжнародних, регіональних документів та наукових досліджень.

1) «Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

- Несанкціонований доступ - умисний несанкціонований доступ до всієї або частини комп'ютерної системи, з метою отримання комп'ютерних даних або з будь-якою іншою неналежною метою;
- Втручання в дані - навмисне пошкодження, знищення, спотворення, зміна або приховування комп'ютерних даних без належних на те прав;
- Системне втручання - навмисне і суттєве втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, спотворення, зміни або приховування комп'ютерних даних без належних на те прав;
- Незаконне використання пристрою, тобто його виготовлення, продаж, придбання з метою використання, розповсюдження або надання в користування іншим способом» [2];

2) «Правопорушення, пов'язані з комп'ютером

3) Правопорушення, пов'язані з контентом

4) Правопорушення, пов'язані з порушенням авторського права та суміжних прав» [2];

5) «Акти расизму та ксенофобії, вчинені через комп'ютерні мережі» [5].

«Основними видами кіберзлочинів є розповсюдження шкідливих програм, злам паролів, крадіжка номерів кредитних карток та іншої банківської інформації, а також поширення незаконної інформації через

Інтернет» [15].

«Групи кіберзлочинів поділяються за метою правопорушення на: злочини, що порушують конфіденційність, цілісність і доступність комп'ютерних даних та комп'ютерних мереж; економічні комп'ютерні злочини; комп'ютерні злочини проти недоторканності прав особи та приватного простору; комп'ютерні злочини проти суспільних та державних інтересів проти комп'ютерних злочинів. Однак варто зазначити, що багато кіберзлочинів впливають на декілька об'єктів одночасно. Ще однією категорією правопорушень, яка окремо не згадується в Конвенції Ради Європи, є крадіжка особистих даних, тобто викрадення, передача або використання персональних даних у злочинних цілях» [15].

Кіберзлочини у сучасному світі класифікуються наступним чином:

1) наступальні: кібертероризм, погрози фізичного насильства (наприклад, через електронну пошту), кіберпереслідування, кібersталкінг (незаконні сексуальні домагання або переслідування осіб через інтернет), дитяча порнографія (створення, розповсюдження та отримання доступу до порнографічних матеріалів із зображеннями дітей);

2) неагресивні: кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусів.

«Водночас, беручи до уваги мотиви правопорушників, кіберзлочини можна класифікувати наступним чином:

- кібершахрайство, спрямоване на отримання коштів;
- кібершахрайство, спрямоване на отримання інформації (для особистого використання або продажу); та втручання в інформаційні системи для отримання доступу до автоматизованих систем управління (з метою отримання винагороди або нанесення шкоди конкуренту);
- кіберзлочини, які стосуються інформаційної безпеки держави;
- кіберзлочини, що направлені на знищення даних;
- кіберзлочини, що направлені на порушення роботи інформаційних систем у приватному секторі;

- кіберзлочини, що трактуються як несанкціонований доступ на приватні сторінки користувачів соціальних мереж, тощо;
- інші злочини» [32].

Сьогодні кіберзлочини можна умовно розділити на дві категорії. До агресивних належать кібертероризм, погрози фізичною розправою через електронні повідомлення, кіберпереслідування, кіберсталкінг, що включає незаконні сексуальні домагання або переслідування осіб через Інтернет, а також дитяча порнографія, яка охоплює створення, розповсюдження та доступ до матеріалів із зображеннями дітей. Неагресивні кіберзлочини охоплюють кіберкрадіжки, цифровий вандалізм, шахрайство в Інтернеті, шпигунство із застосуванням кіберзасобів, а також поширення спаму і комп'ютерних вірусів.

«Кіберзлочини вчиняються до комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних, використання комп'ютерних систем або доступу до комп'ютерних мереж кіберпростору. Тому комп'ютери можуть бути як знаряддям вчинення злочину, так і об'єктом злочину» [14].

«Особливості кіберзлочинності:

- важливість віднесення деяких злочинів у сфері новітніх інформаційних технологій до комп'ютерних полягає у знарядді вчинення злочину - комп'ютерній техніці. Об'єктом злочину є суспільні відносини у сфері автоматизованої обробки інформації;
- значення віднесення окремих правопорушень у сфері новітніх інформаційних технологій до кіберзлочинів полягає в особливому середовищі, в якому вчиняється правопорушення - кіберпросторі. При цьому предмет злочинної агресії може стосуватися будь-якої сфери людської діяльності, яка проявляється в кіберпросторі. При цьому дослідник посилається на перелік протиправних діянь, передбачених Конвенцією та Додатковими протоколами до неї. За його словами, лише діяння з цього переліку класифікуються як кіберзлочини» [8].

«Питання запобігання кіберзлочинності в Україні є комплексним.

Сьогодні законодавство має бути адаптоване до сучасних реалій, а не до рівня розвитку науки чи розуміння правлячою групою пріоритетності тих чи інших національних інтересів. Технологічний розвиток, кібернетизація та подальше впровадження штучного інтелекту в наше життя - це вже не майбутнє, а сьогодення» [14].

Оскільки кіберзлочинність має транснаціональний характер, науковці вказують на високий рівень затримки як одну з ключових характеристик цього явища. Цьому сприяють декілька факторів. По-перше, складність і масштабність механізмів кіберзлочинності, широкий спектр її наслідків, а також низький рівень «комп'ютерної грамотності» серед багатьох потенційних жертв і нехтування питаннями кібербезпеки. По-друге, небажання жертв або свідків повідомляти про злочини. Потерпілі чи особи, які мають інформацію про вчинені правопорушення, часто утримуються від звернення до правоохоронних органів. Нарешті, недоліки у роботі правоохоронних органів, які не завжди ефективно реагують на заяви або повідомлення про кіберзлочини, також впливають на рівень затримки.

«Існує три різні напрямки заходів боротьби з кіберзлочинністю: загально соціальні заходи, специфічні кримінологічні заходи та індивідуальні заходи.

Заходи протидії на загально соціальному рівні кіберзлочинності включає комплекс перспективних соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на розв'язання нагальних соціальних проблем і протиріч у країні. Саме реалізація загально соціальних профілактичних заходів здатна усунути або мінімізувати дію криміногенних факторів, що детермінують кіберзлочинність та гальмують розвиток особистості злочинців» [12].

«Розробка належних заходів протидії злочинності, в тому числі кіберзлочинності, потребує належної регламентації діяльності як правоохоронних органів, так і вищих органів державної влади, що, в свою чергу, відповідає вимогам правової, незалежної та демократичної держави.

Також необхідно усунути фактори, які сприятливо впливають на існування та розвиток злочинності» [10].

Професійна діяльність із запобігання злочинності тісно пов'язана з роботою Національної поліції України та орієнтована на окремі соціальні групи, які є об'єктами профілактичної діяльності. Одним із основних напрямків у сфері запобігання кіберзлочинності є розробка та затвердження Міністерством внутрішніх справ стратегії боротьби з цим видом правопорушень. Ця стратегія повинна охоплювати концепцію профілактичної діяльності, стратегічні й тактичні заходи, спрямовані на запобігання злочинам, а також механізми моніторингу ефективності їх впровадження. Крім того, необхідно збільшити кількість планових і позапланових перевірок компаній, діяльність яких може бути пов'язана з кіберзлочинністю, що здійснюються відповідними підрозділами поліції.

Особливу увагу слід приділити ідентифікації потенційно небезпечних осіб, зокрема шахраїв, чия діяльність проявляється у систематичному внесенні незначних змін до даних, їх модифікації або видаленні, а також у створенні неправдивих записів. Така поведінка має бути врахована як важливий аспект протидії кіберзлочинності.

«Ще одним заходом запобігання кіберзлочинності є виявлення та запобігання діяльності кібертерористів, тобто тих, хто використовує комп'ютерне обладнання, пристрої та мережі для вчинення терористичних актів. В умовах інформаційної війни під час діючої військової агресії з боку росії, найбільш вразливі до кібератак є державні установи, великі корпорації, оборонні підприємства та підприємства критичної інфраструктури, а також компанії, які забезпечують все необхідне для населення та оборони у воєнний час» [38].

У умовах воєнного стану важливо впроваджувати ефективні інструменти протидії кіберзлочинності. По-перше, державні органи та підприємства повинні мати у своєму штаті висококваліфікованих ІТ-

спеціалістів, які здатні оперативно виявляти та нейтралізувати кіберзагрози. Такі професіонали також мають інформувати інших працівників про правила безпечної поведінки у комп'ютерних мережах. По-друге, особам, які знаходяться в зоні кіберризику, рекомендується регулярно відстежувати повідомлення на офіційних ресурсах Адміністрації Державної служби спеціального зв'язку та захисту інформації України та CERT-UA, де публікуються попередження про можливі загрози і рекомендації щодо мінімізації ризиків.

У разі виявлення кібератаки важливо негайно повідомити спеціалізовані органи, відповідальні за протидію кіберзлочинності, зокрема CERT-UA та Кіберполіцію. Це дозволить не лише притягнути винних до відповідальності, але й швидко вжити заходів для блокування шкідливих ресурсів. Особи, які здійснюють дії, спрямовані на кібератаки проти ворожих держав або займаються багхантингом для зміцнення кібербезпеки України, мають бути готові надати докази того, що їхня діяльність відповідає національним інтересам. Це дозволить уникнути непорозумінь з правоохоронними органами.

Тобто, з розвитком комп'ютерних технологій одночасно еволюціонували і злочини в мережах. Поширення Інтернету створило нові можливості для шахраїв здійснювати різноманітні види кіберзлочинів. Узагальнюючи дослідження вітчизняних та іноземних вчених, можна визначити, що термін «кіберзлочинність» охоплює правопорушення у сфері комп'ютерної інформації та телекомунікацій, незаконну торгівлю бездротовими електронними та спеціальними технічними засобами, несанкціоноване розповсюдження програмного забезпечення та інші види правопорушень.

Кіберзлочини можуть здійснюватися різними способами, серед яких шахрайські дії через Інтернет або телефонні мережі, спрямовані на отримання прибутку шахраями або завдання шкоди державним органам, підприємствам чи фізичним особам для їх дискредитації. В умовах війни з РФ та активної

інформаційної протидії агресору, українські ІТ-спеціалісти постійно виявляють та ліквідовують подібні загрози. Проте слід розуміти, що ці ризики залишаються актуальними цілодобово.

Для ефективної протидії кіберзлочинам необхідно впроваджувати спеціальні інструменти та заходи. Перш за все, потрібні кваліфіковані спеціалісти, які будуть інформувати про правила поведінки у кіберпросторі в умовах інформаційної війни. Важливу роль у створенні таких інструментів відіграє держава.

РОЗДІЛ 2.
АНАЛІЗ ІНСТРУМЕНТАРІЮ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1. Аналіз стану кіберзлочинності в Україні

В Україні термін «кіберзлочинність» охоплює широкий спектр правопорушень, що ускладнює розробку системи типології або класифікації кіберзлочинів. Поняття «кіберзлочини» охоплює як кримінальні правопорушення, так і зареєстровані кримінальні провадження, що мають кваліфікуючу відмітку в картці про правопорушення — «з використанням високих інформаційних технологій і телекомунікаційних мереж». Це створює труднощі для державних інституцій та науковців у співставленні вітчизняних статистичних даних із інформацією про протидію кіберзлочинності в Європі, США або інших країнах. У зв'язку з цим аналіз стану кіберзлочинності здійснюється за різними методиками з використанням результатів як українських, так і зарубіжних аналітичних інститутів.

Говорячи про глобальні цілі кібертероризму, варто зазначити його політичне забарвлення. Дослідження показують, що з початку століття найбільше політично вмотивованих кібератак здійснено з Китаю — майже 12% від загальної кількості. Росія займає друге місце з часткою 11,6%, за нею йде Іран з 5,3%, а Північна Корея відповідальна за 4,7% таких інцидентів. Україна з часткою 2,6% закриває п'ятірку країн, з яких здійснюються політично вмотивовані кібератаки (рис. 2.1).

«Майже третина проаналізованих кібератак здійснили держави або афілійовані групи й така сама частка окремими суб'єктами з політичними цілями. Близько половини зафіксованих атак були спрямовані на політичні цілі, а майже 20% — на об'єкти критичної інфраструктури.

З 2020 року кількість політизованих кібератак почала зростати у рази та досягла піка у 2023 році — тоді хакери провели 666 атак» [36].

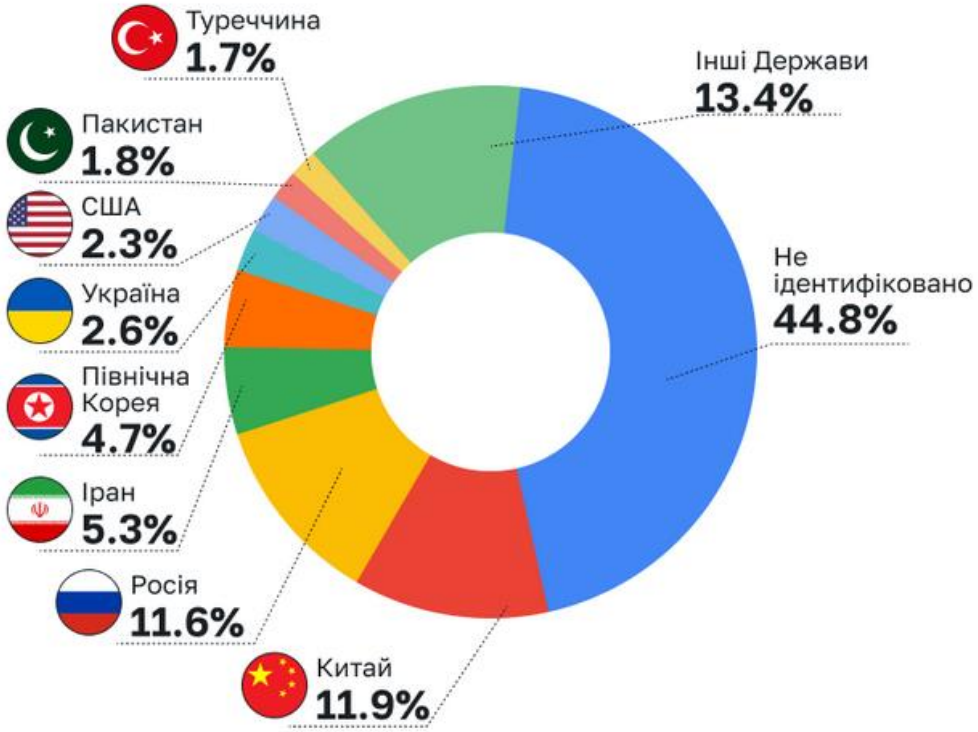

Рис. 2.1. Країни, відповідальні за найбільшу кількість кібератак у 2020-2023 рр.

Примітка. Наведено за [36]

«Протягом останніх років найбільше від політично вмотивованих кібератак постраждали Сполучені Штати Америки, на які у 2023 році було спрямовано 262 такі атаки. Росія зазнала 63 кібератак, Німеччина — 59, Велика Британія — 42, а Україна — 37. Ці дані свідчать про те, що держави з розвиненою інфраструктурою та активною політичною позицією стають основними мішенями для кібератак з політичним підтекстом» [39]. Однак в загальному, найбільша активність даних злочинів припало саме на 2023 рік (Рис. 2.2)

«Світовий рейтинг кіберзлочинності очолила Росія. Україна посіла друге місце. У першу п’ятірку також увійшли Китай, США та Нігерія.

Перший в історії світовий рейтинг кіберзлочинності, складений у рамках дослідження Оксфордського університету та Університету Нового Південного Вельсу, очолила Росія» [36].

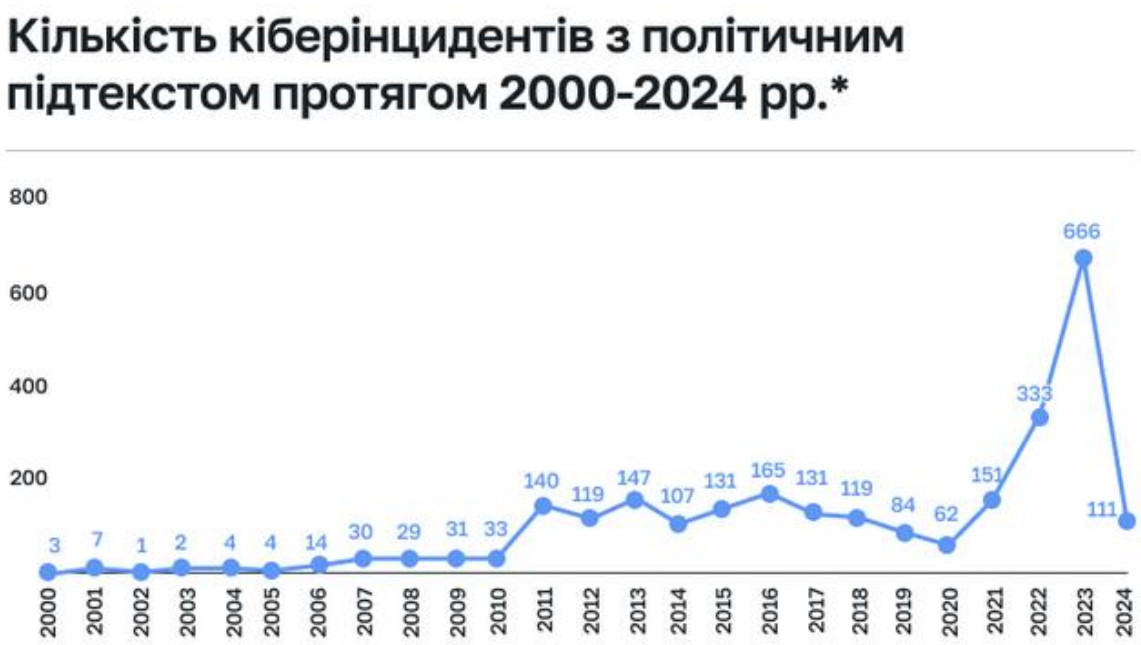

Рис. 2.2. Світова динаміка кількості кібератак з 2000 по 2024 (9 місяців) рр.

Примітка. Наведено за [37]

Науковці вказують на нерівномірний розподіл джерел загрози кіберзлочинності по всьому світу. Лідером у рейтингу кіберзлочинності є Росія, яка набрала 58,39 бала. На другому місці з великим відривом розташувалася Україна з результатом 36,44 бала. До списку також входять Китай із 27,86 бала, Сполучені Штати Америки з 25,01 бала, Нігерія, яка отримала 21,28 бала, та Румунія з показником 14,83 бала. Велика Британія опинилася на восьмому місці з 9,01 бала.

«В Оксфордському університеті зауважили, що російські кіберзлочинці вважаються найбільш професійними та технічно кваліфікованими у світі. Їхні злочини мають найбільший вплив» [37].

Глобальний індекс кіберзлочинності формується на основі аналізу, проведеного 92 провідними експертами у сфері кіберзлочинності. Ці фахівці оцінюють країни за кількома основними параметрами. Вони враховують здатність створювати шкідливі продукти та послуги, зокрема написання шкідливого коду, використання ботнетів і створення інструментів для злому. До уваги беруться також атаки та вимагання, як-от DoS-атаки та використання

програм-вимагачів, крадіжки даних, включаючи фішинг та викрадення банківських рахунків. Крім цього, експерти аналізують шахрайство в інтернеті, зокрема на онлайн-аукціонах або через зламані облікові записи компаній, а також відмивання грошей, як-от підробка кредитних карток. Оцінювання також охоплює професіоналізм і технічні навички злочинців, а також вплив місцевих злочинних угруповань на глобальну кіберзлочинність. У рейтинг включено 97 країн, про які вдалося зібрати достатньо даних. Одна зі співавторок дослідження, Міранда Брюс, зазначила, що дослідження дало можливість краще зрозуміти географію кіберзлочинності. Лідером за рівнем загрози стала Росія, яка отримала 58,39 бала. На другому місці опинилася Україна з результатом 36,44 бала, а третє місце посів Китай із 27,86 бала. До першої п'ятірки також увійшли США з 25,01 бала та Нігерія з 21,28 бала (рис. 2.3-2.4)

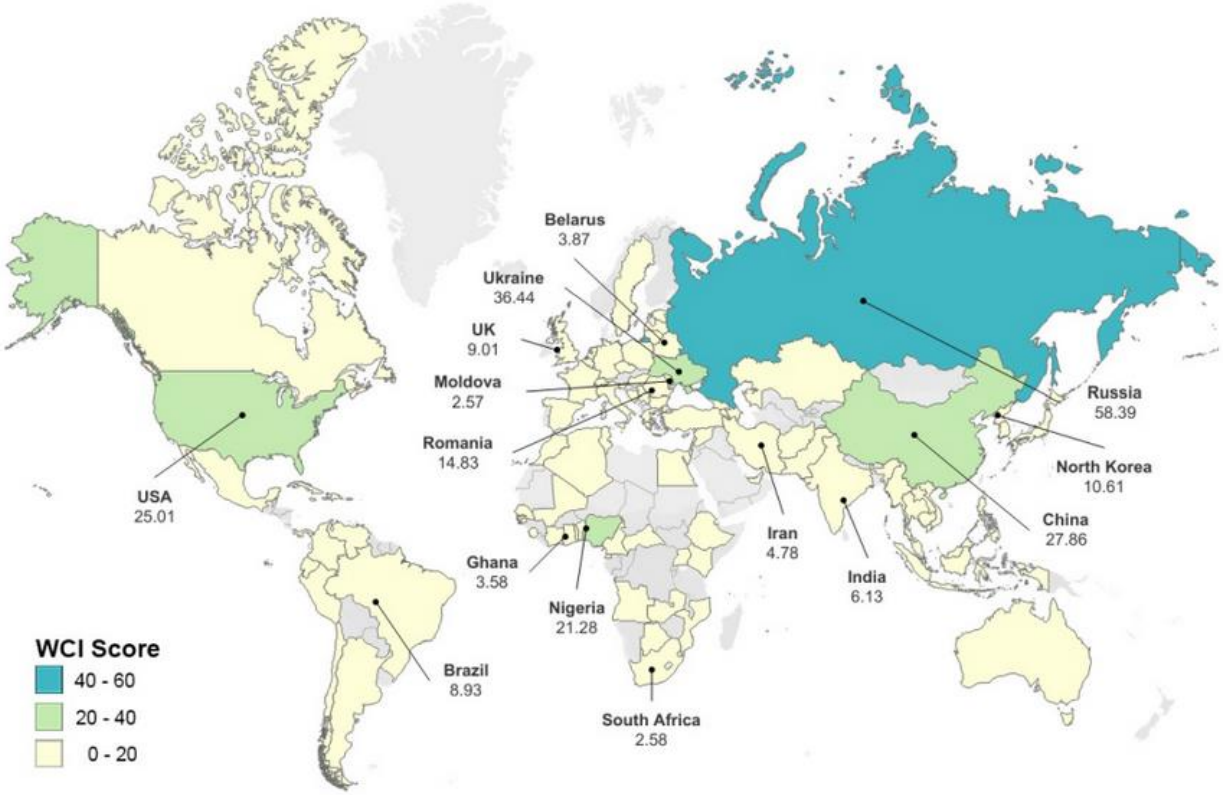

Рис. 2.3. Наглядна мапа глобального індексу кіберзлочинності.

Примітка. Наведено за [36]

Рис. 2.4. Рейтинг країн з найвищим глобальним індексом кіберзлочинності.

Примітка. Наведено за [37]

«В Україні активність кібершахраїв значно зросла від початку повномасштабного вторгнення. За результатами опитування, проведеного компанією Опендатабот спільно з Національним банком, 11% респондентів повідомили, що стали жертвами шахраїв у цей період. Найчастіше шахраї обманювали жінок, ніж чоловіків, а серед постраждалих за віковими категоріями переважали молодь віком 18–24 роки — 14% та люди у віці 65 років і старше — 11,5%» [30].

«Збитки банків, торговців та клієнтів від шахрайських дій із платіжними картками за 2022 рік зросли на 46% і склали 481 мільйон гривень. Понад половина цих збитків — 53%, стала наслідком використання методів соціальної інженерії. Це означає, що жертви самі надають шахраям інформацію про свої картки, одноразові паролі для підтвердження операцій або дані для входу до інтернет-банкінгу» [30].

Рис. 2.5. Зміна структури кіберзлочинів в Україні у 2022 році в порівнянні з2017 роком

Примітка. Наведено за [30]

Структура кіберзлочинності в Україні включає кілька основних напрямів, які домінують серед зареєстрованих правопорушень. Одним із найпоширеніших видів є шахрайство в інтернеті, що охоплює фішингові атаки, створення підроблених вебсайтів для збору персональних або фінансових даних, а також обманні схеми на платформах оголошень та в онлайн-магазинах. Значне місце займають злочини, спрямовані на банківські системи, такі як використання шкідливого програмного забезпечення для крадіжки банківських даних, злам акаунтів клієнтів та здійснення незаконних транзакцій. Зростає кількість випадків кібертероризму, спрямованого на державні органи та критично важливу інфраструктуру, включаючи енергетичні компанії, комунікаційні мережі та фінансові установи. Розповсюдження шкідливого програмного забезпечення також залишається серйозною проблемою, адже Україна виступає як джерелом, так і мішенню для вірусів-шифрувальників, троянів та інших шкідливих кодів. Часто застосовуються методи соціальної інженерії, коли шахраї змушують жертв розголошувати конфіденційну інформацію, паролі чи дані платіжних карток.

Водночас викрадення особистих даних залишається актуальною загрозою, що реалізується через фішинг, злам баз даних або використання шкідливих програм. У 2023 році кіберполіція України фіксує постійне зростання кіберзлочинів, що вимагає посилення заходів кібербезпеки та активізації міжнародної співпраці. Топ шахрайських схем в Україні за 2023 рік наведено на рис. 2.6.

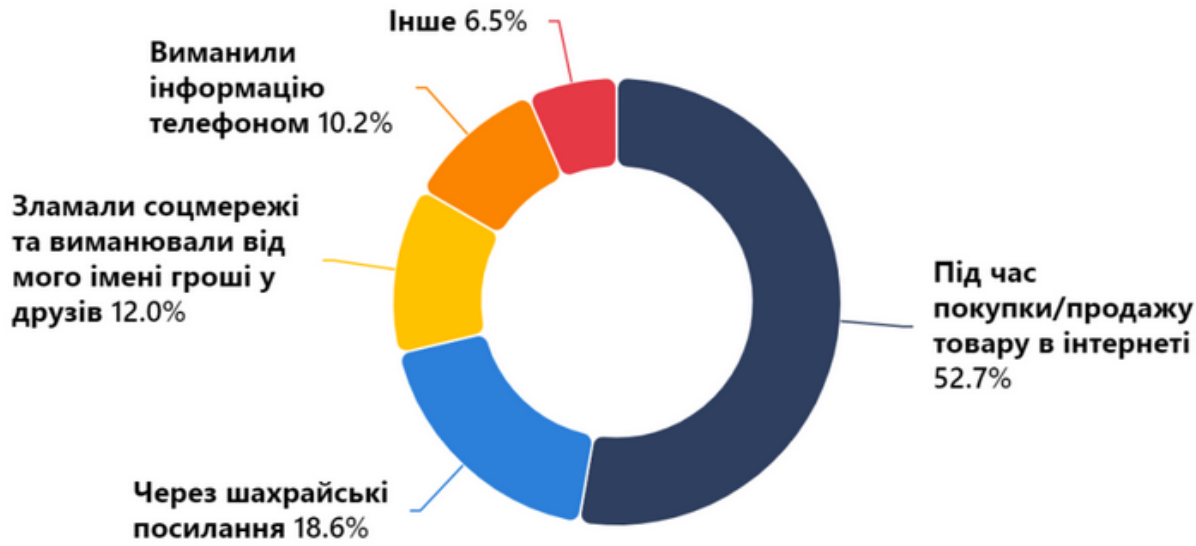

Рис. 2.6 Топ шахрайських схем в Україні за 2023 рік

Примітка. Наведено за [30]

2.2. Оцінка інструментарію боротьби з кіберзлочинністю та його результативності

Законодавство Європейського Союзу у сфері інформаційної безпеки формувалося під впливом міжнародних ініціатив, таких як діяльність Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку та Організації Об'єднаних Націй. Законодавчі заходи щодо боротьби з кіберзлочинністю впроваджувалися в межах програм Європейського Союзу, серед яких програма Безпечний Інтернет, що діяла у періоди з 1999 до 2004 року, Безпечний Інтернет Плюс з 2005 до 2008 року, а

також Безпечний Інтернет у період з 2009 до 2013 року. Ці заходи, прийняті рішеннями Європейського Парламенту і Ради, були спрямовані на захист персональних даних, забезпечення безпечного користування Інтернетом, створення сприятливих умов для розвитку європейської Інтернет-індустрії, а також на захист дітей, які користуються Інтернетом і новітніми інформаційними технологіями. «Найважливіші заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програми Європейського Союзу *Попередження і боротьба із злочинністю* і передбачали співробітництво в протидії кіберзлочинності. Складність та чисельність питань інформаційної безпеки сформувала в законодавчих органах Європейського Союзу концептуальне бачення майбутнього міжнародно- правового регулювання виключно на рівні, спрямованому на вирішення кримінальних аспектів, пов'язаних із використанням інформаційно- комунікаційних технологій. В Європейському Союзі не було сприйнято концепцію міжнародної інформаційної безпеки, яка передбачала б комплексне розв'язання проблеми на трьох рівнях міжнародно-правового регулювання - військовому, терористичному і кримінальному» [24].

«Провідне місце серед відповідної групи міжнародно-правових документів відведено Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року у Будапешті» [41]. Наша країна ратифікувала цю Конвенцію 7 вересня 2005 року. Сьогодні це один з ключових документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі, і поки що єдиний документ такого рівня. Вона зобов'язує держави вживати законодавчих та інших заходів для встановлення кримінальної відповідальності за злочини у кіберпросторі відповідно до внутрішнього законодавства. До підписання Конвенції деякі групи із захисту громадянських прав та провайдери інтернет-послуг висловлювали серйозні аргументи проти укладення цієї угоди. На їхню думку, її положення мають нечіткі формулювання, покладають на провайдерів надмірні вимоги, створюють ризик для норм захисту прав особи, розширюють поліцейські функції урядів і

знижують відповідальність держав у правоохоронній діяльності.

Перший розділ Конвенції визначає види діянь, які підлягають криміналізації, поділяючи злочини в кіберпросторі на кілька груп. До першої групи входять злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Сюди належать незаконний доступ, незаконне перехоплення, вплив на комп'ютерні дані чи системи, а також протизаконне використання спеціальних технічних пристроїв. Об'єктами злочину є комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, а також паролі, коди доступу та їхні аналоги, які забезпечують доступ до комп'ютерної системи. Норми Конвенції застосовуються лише за наявності злочинного наміру і у випадках, коли використання технічних пристроїв спрямоване на протиправну діяльність. До другої групи належать злочини, пов'язані з використанням комп'ютерних засобів, як-от підробки та шахрайство з використанням комп'ютерних технологій. Третя група охоплює злочини, пов'язані зі змістом даних, а четверта зосереджена на порушеннях авторських і суміжних прав. У 2002 році до Конвенції було додано протокол, який розширив перелік злочинів, включивши поширення інформації, що підбурює до насильства, ненависті або дискримінації за расовою, національною, релігійною чи етнічною ознакою.

«Другий розділ Конвенції освітлює процесуальні аспекти боротьби з кіберзлочинністю. Конвенція пропонує традиційне рішення проблеми юрисдикції: карна юрисдикція визначається відповідно до територіальної ознаки. Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином якої є злочинець. Тут виникає неясність: незрозумілий статус кіберпростору - чи поширюється на нього національне законодавство або ні? Таким чином, проблема визначення підвідомчості і осудності злочинів в кіберпросторі як і раніше залишається відкритою. Щоб уникнути можливих подальших суперечок в Конвенції передбачається, що внутрішні закони держав можуть містити інші норми про юрисдикцію. Зважаючи на відсутність кордонів в

глобальних мережах. Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, разом з тим, й вона не позбавлена недоліків» [40].

Розділ ІІІ Конвенції, присвячений міжнародній співпраці, охоплює питання екстрадиції, взаємодії держав-учасників у боротьбі з комп'ютерними злочинами та узгодження дій для збору доказів в електронному вигляді. Ця Конвенція створює основу для розвитку міжнародного законодавства у цій сфері. Навіть ті країни, які з певних причин не стали її підписантами, можуть скористатися накопиченим досвідом у правовому регулюванні кіберпростору.

«Конвенція про кіберзлочинність є важливою основою діяльності Національної поліції України, проте, деякі її положення так і не знайшли відображення у вітчизняному кримінальному законодавстві. Наприклад, виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів, придбання дитячої порнографії через комп'ютерну систему та володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних не знайшли свого втілення у вітчизняному кримінальному законодавстві» [15]. «Проблема полягає у тому, що з однієї сторони правоохоронці наділені правом керування у своїй діяльності нормами Конвенції про кіберзлочинність, проте з іншої - на практиці вони майже не використовують їх, тож перенесення міжнародних стандартів на вітчизняну практику боротьби з кіберзлочинністю є не в повній мірі коректним твердженням. Проте, не зважаючи на такі суперечності, Конвенція про кіберзлочинність все ще залишається одним із найважливіших інструментів національного правового регулювання боротьби із кіберзлочинністю» [27].

Законодавство Європейського Союзу у сфері інформаційної безпеки формувалося під впливом міжнародних ініціатив, таких як діяльність Ради

Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку та Організації Об'єднаних Націй. «Законодавчі заходи щодо боротьби з кіберзлочинністю впроваджувалися в межах програм Європейського Союзу, серед яких програма Безпечний Інтернет, що діяла у періоди з 1999 до 2004 року, Безпечний Інтернет Плюс з 2005 до 2008 року, а також Безпечний Інтернет у період з 2009 до 2013 року. Ці заходи, прийняті рішеннями Європейського Парламенту і Ради, були спрямовані на захист персональних даних, забезпечення безпечного користування Інтернетом, створення сприятливих умов для розвитку європейської Інтернет-індустрії, а також на захист дітей, які користуються Інтернетом і новітніми інформаційними технологіями» [16].

«Наша країна ратифікувала цю Конвенцію 7 вересня 2005 року. Сьогодні це один з ключових документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі, і поки що єдиний документ такого рівня. Вона зобов'язує держави вживати законодавчих та інших заходів для встановлення кримінальної відповідальності за злочини у кіберпросторі відповідно до внутрішнього законодавства. До підписання Конвенції деякі групи із захисту громадянських прав та провайдери інтернет-послуг висловлювали серйозні аргументи проти укладення цієї угоди. На їхню думку, її положення мають нечіткі формулювання, покладають на провайдерів надмірні вимоги, створюють ризик для норм захисту прав особи, розширюють поліцейські функції урядів і знижують відповідальність держав у правоохоронній діяльності» [4].

Перший розділ Конвенції визначає види діянь, які підлягають криміналізації, поділяючи злочини в кіберпросторі на кілька груп. До першої групи входять злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Сюди належать незаконний доступ, незаконне перехоплення, вплив на комп'ютерні дані чи системи, а також протизаконне використання спеціальних технічних пристроїв. Об'єктами злочину є комп'ютерні програми, розроблені або адаптовані для скоєння

злочинів, а також паролі, коди доступу та їхні аналоги, які забезпечують доступ до комп'ютерної системи. Норми Конвенції застосовуються лише за наявності злочинного наміру і у випадках, коли використання технічних пристроїв спрямоване на протиправну діяльність. До другої групи належать злочини, пов'язані з використанням комп'ютерних засобів, як-от підробки та шахрайство з використанням комп'ютерних технологій. Третя група охоплює злочини, пов'язані зі змістом даних, а четверта зосереджена на порушеннях авторських і суміжних прав. У 2002 році до Конвенції було додано протокол, який розширив перелік злочинів, включивши поширення інформації, що підбурює до насильства, ненависті або дискримінації за расовою, національною, релігійною чи етнічною ознакою.

«Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, прийнята 15 листопада 2000 року, не є нормативним актом, що безпосередньо регулює питання боротьби з кіберзлочинністю. Однак більшість комп'ютерних злочинів має транснаціональний характер, є організованими та часто включають ознаки тероризму. У цьому контексті прийняття Конвенції стало важливим кроком у попередженні таких правопорушень. Документ передбачає ухвалення законодавчих і практичних заходів, спрямованих на боротьбу з корупцією, залучення юридичних осіб до відповідальності за серйозні злочини, пов'язані з організованою злочинністю, а також конфіскацію та арешт доходів, отриманих злочинним шляхом. Норми цього документа здебільшого не застосовуються до правопорушень, що не пов'язані з організованою злочинністю, хоча окремі сфери, зокрема комп'ютерні злочини, все ж залишаються у полі уваги міжнародної спільноти. У випадках, коли кіберзлочин має транснаціональний характер, а саме здійснюється або має наслідки у кількох державах, норми Конвенції можуть бути застосовані» [43].

Загальна кількість міжнародних договорів у сфері кримінального співробітництва є значною. Від часу проголошення незалежності Україна активно укладала такі угоди і нині співпрацює з багатьма країнами. Хоча

більшість з них не містить прямих положень про боротьбу з кіберзлочинністю, це не виключає можливості взаємодії у разі потреби. Наприклад, Угода між урядом України та Туреччиною передбачає обмін інформацією і допомогу у виявленні та розкритті кіберзлочинів. Подібні угоди існують також з Бельгією, Нідерландами та іншими державами, що підкреслює важливість міжнародної співпраці у цій сфері. Однак механізми реалізації таких угод потребують вдосконалення, зокрема через спрощення процедур і підвищення оперативності обміну інформацією.

РОЗДІЛ 3.
НАПРЯМКИ ОПТИМІЗАЦІЇ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Зі зростанням кількості економічних кіберзагроз в Україні питання боротьби з ними стає дедалі актуальнішим. У контексті євроінтеграції важливо демонструвати готовність протидіяти найдинамічніше зростаючому виду злочинності та підтверджувати, що національне законодавство забезпечує належне регулювання у сферах економічного, фінансового та банківського кіберпростору. Крім того, у сучасних умовах пріоритетом є готовність приймати необхідні зміни, які відповідатимуть міжнародним стандартам.

З огляду на постійний розвиток віртуального простору в економіці та злочинності, що з ним пов'язана, питання перспектив та тенденцій правового регулювання боротьби з кіберзлочинністю в Україні набуває першочергового значення. Розвиток правового регулювання у цій сфері визначається кількома ключовими факторами. Перш за все, практично всі розрахункові процеси в державному та приватному секторах здійснюються із застосуванням кібертехнологій. По-друге, в умовах війни, яка триває, економічний віртуальний простір стає одним із важливих фронтів, де Україна через відставання у сфері інформаційних технологій ще не досягла значних успіхів. По-третє, рівень усвідомлення небезпеки економічних кіберзлочинів у суспільстві залишається низьким. У таких умовах питання перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні потребує першочергового дослідження.

Ключовими факторами, які визначають розвиток правового регулювання у цій сфері, є зростання активності громадян в інтернет-просторі, посилення діяльності кіберзлочинців та необхідність імплементації міжнародних правових норм у національне законодавство. Разом із цим варто зазначити, що наукова доктрина поки що приділяє недостатньо уваги цьому питанню. Більшість наукових праць охоплюють тенденції поширення

кіберзлочинів або є лише частково актуальними. Це створює проблему, адже дослідження правового регулювання боротьби з економічною кіберзлочинністю є постійно актуальним завданням для вітчизняних науковців.

Тож, «постійний розвиток інформаційних технологій та нормативно-правової бази їх реалізації, а також важливість дослідження тих тенденцій, які є доцільними саме на даному етапі розвитку нашої держави, зумовлюють важливість дослідження виділеної проблеми. Оскільки на світовому рівні боротьба із економічною кіберзлочинністю розпочалась майже на десятиліття раніше, ніж в Україні, перейняття досвіду розвинутих країн очевидно ще довгий час передуватиме в переліку основних тенденцій розвитку правового регулювання боротьби з економічною кіберзлочинністю в нашій державі» [12].

«До виконання частини з них Україна вже приєдналась шляхом ратифікації, проте ряд угод, протоколів та рекомендацій все ще не є джерелами вітчизняного законодавства. Щодо питання співробітництва також доцільно відзначити, що необхідність координації питань співробітництва кожною країною відповідно до розробленої та чинної у ній стратегії економічної кібербезпеки» [29].

Перспективи та тенденції розвитку правового регулювання боротьби з економічною кіберзлочинністю в Україні стосуються ключових аспектів забезпечення кібербезпеки у фінансовій і банківській сферах. Рада національної безпеки і оборони України визначила основні напрямки кіберзахисту, які включають захист державних електронних інформаційних ресурсів, критичної інфраструктури та розвиток потенціалу сектору безпеки у сфері кібербезпеки і боротьби з кіберзлочинністю. Ці заходи носять організаційний, процесуальний і технологічний характер, тому не завжди їх можна віднести до сфери правового регулювання.

Міжнародне співробітництво у цій сфері поєднує різні тенденції. Хоча

використання зарубіжного досвіду є важливим, розвиток вітчизняного законодавства має спиратися на власну стратегію, яка враховує нагальні потреби держави. Ознайомлення із практикою інших країн дозволяє адаптувати механізми боротьби до українських реалій, проте повне копіювання цих підходів через специфіку кожної держави є неможливим.

Пріоритетним завданням залишається гармонізація нормативних документів зі стандартами Європейського Союзу і НАТО. Це сприяє розвитку вітчизняної нормативно-правової бази, оскільки міжнародні акти, ратифіковані Україною, виступають важливим джерелом права. За останні роки дискусії стосовно доповнення Кримінального кодексу України статтями про злочини у комп'ютерній сфері та посилення покарань за економічні кіберзлочини стали особливо актуальними. До Розділу XVI Кримінального кодексу вже вносилися зміни, зокрема щодо санкцій за відповідні злочини.

Зважаючи на безперервний розвиток інформаційних технологій та нові форми економічної кіберзлочинності, існує ризик, що чинні санкції не відповідатимуть шкоді, завданій фінансовій сфері. Тому одним із напрямів розвитку є доповнення Кримінального кодексу новими статтями, які враховуватимуть специфіку кіберзлочинів, і посилення відповідальності за такі діяння.

«Міжнародне співробітництво в боротьбі з кіберзлочинністю також потребує переходу на новий якісний рівень. Наприклад, прийняття Конвенції ООН проти транснаціональної організованої злочинності у 2000 році пов'язане з тим, що у 90-х роках XX століття кіберзлочинність набула транснаціонального характеру. Цей документ став адекватною відповіддю на зростання масштабів злочинності у кіберпросторі. Віденська декларація про злочинність і правосуддя, прийнята того ж року, підкреслила необхідність об'єднання зусиль держав для боротьби із серйозними злочинами глобального характеру» [8].

Аналіз цих документів свідчить, що увага міжнародної спільноти до

нових форм злочинності стала поштовхом для суттєвих змін у міжнародному правовому регулюванні боротьби з кіберзлочинністю. Такий підхід є важливим для ефективного протистояння загрозам у сучасному світі.

«Розвиток системи перспектив та тенденцій правового регулювання боротьби з економічною кіберзлочинністю в Україні повинен враховувати кілька важливих аспектів. По-перше, в Україні розпочато інтеграцію міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю у національне законодавство. По-друге, Україна співпрацює із зарубіжними державами у питаннях розслідування економічних кіберзлочинів, але ця взаємодія поки що недостатньо активна. По-третє, спостерігається тенденція посилення контролю за користувачами мережі Інтернет» [12].

Подальший розвиток цього інституту слід пов’язати із вдосконаленням законодавчої бази та розширенням міжнародної співпраці. Це передбачає посилену взаємодію органів внутрішніх справ з правоохоронними органами інших країн для ефективного протистояння економічній кіберзлочинності. Негативною тенденцією є зростання рівня контролю за користувачами Інтернету, що вимагає обережного підходу для забезпечення балансу між безпекою та правами громадян.

Для більш детального визначення напрямків розвитку необхідно акцентувати увагу на таких аспектах. У рамках розвитку нормативно-правової бази важливими є розширення розуміння поняття кіберзлочинності, посилення кримінальної відповідальності за кіберзлочини та створення єдиного термінологічного апарату у відповідних нормативно-правових актах. У межах тенденції контролю за кіберпростором актуальними є встановлення чітких правил користування та створення спеціальних органів контролю для моніторингу й виявлення порушників.

«Враховуючи, що суспільні відносини, як у реальному, так і у віртуальному світі, повинні бути регламентовані законодавством, успіхи у боротьбі з кіберзлочинністю залежать від вдосконалення правової бази. Наразі Україна перебуває на третьому етапі розвитку правового регулювання

економічної кіберзлочинності, але існує багато нерозв'язаних проблем. Основними викликами є недосконаліть законів, що регламентують кіберпростір, і невідповідність кримінального законодавства сучасним формам кіберзлочинності. Наприклад, у контексті гібридної війни Україна регулярно зазнає атак на банківський сектор.

Ще однією проблемою є відсутність єдиного понятійного апарату, що призводить до різного трактування ключових понять, таких як кіберзлочинність, кібербезпека та кіберпростір. Це особливо актуально для економічної сфери, де термінологічна невизначеність ускладнює правозастосування і боротьбу з новими формами злочинів у сфері інформаційних технологій» [34].

«Посилення міжнародного співробітництва у сфері боротьби з економічною кіберзлочинністю в Україні є однією з ключових тенденцій. Потреба у такій співпраці має кілька аспектів. По-перше, формування правового регулювання у цій сфері вимагає врахування досвіду тих держав, які успішно впровадили подібні механізми, з акцентом на сильних сторонах та можливих проблемах цього процесу. По-друге, масова поява транснаціональних комп'ютерних злочинів, скоєних із метою фінансової наживи, свідчить про необхідність об'єднання зусиль, адже жодна країна не може ефективно боротися з такими злочинами самостійно. По-третє, прагнення України до євроінтеграції неможливе без побудови міцних зв'язків з європейськими державами, зокрема у сфері економічної кібербезпеки» [27].

Водночас існують певні проблеми, які стримують розвиток міжнародного співробітництва України у цій сфері. До них належать недостатній рівень розвиненості національного законодавства, яке потребує вдосконалення відповідно до міжнародних стандартів, а також обмежена кількість міждержавних угод і ратифікованих міжнародних актів, що стосуються боротьби з кіберзлочинністю.

«Значну увагу привертає питання контролю за користувачами Інтернету. Ця тенденція характеризується пошуком балансу між правоохоронними

інтересами та правами людини, але її реалізація може викликати суперечності. Наприклад, рішення Ради національної безпеки і оборони України від 2017 року про заборону доступу до деяких російських ресурсів стало одним із перших кроків у цьому напрямі. Попри виконання цих вимог, користувачі Інтернету все ще мають можливість обходити обмеження, що демонструє складність повного контролю» [9].

«Важливим аспектом є гармонізація національного законодавства із міжнародними стандартами. Це включає розробку правил користування кіберпростором, створення спеціальних органів для моніторингу та виявлення порушень. Наприклад, Департамент кіберполіції Національної поліції України вже виконує ці функції, але збільшення обсягу контролю може вимагати розширення таких структур» [35].

Перспективою міжнародного співробітництва є ліквідація кордонів між державами у боротьбі з економічною кіберзлочинністю. Кіберпростір не має географічних обмежень, тому ефективна протидія цим злочинам можлива лише за участі всіх країн, незалежно від їхнього рівня розвитку. Більш технологічно розвинені держави повинні допомагати іншим у запобіганні та розслідуванні кіберзлочинів.

Розвиток економічної кіберзлочинності та поява нових методів протиправного впливу можуть кардинально змінити підходи до їх регулювання. Специфіка кіберзлочинів полягає у можливості швидкого знищення доказів, що ускладнює розслідування. Тому швидкість дій і координація зусиль на міжнародному рівні є надзвичайно важливими. Ліквідація юридичних кордонів у цій сфері стане вагомим кроком до глобального забезпечення кібербезпеки.

ВИСНОВКИ