МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Навчально-науковий інститут інноваційних освітніх технологій
Кафедра безпеки, правоохоронної діяльності та фінансових розслідувань

КРАВЕЦЬ Сергій Анатолійович

Механізм запобігання та протидії кіберзлочинності в міжнародному вимірі / Mechanism of prevention and counteraction of cybercrime in the international dimension

спеціальність: 262 - Правоохоронна діяльність
освітньо-професійна програма - Економічна безпека та фінансові розслідування

Випускна кваліфікаційна робота

Виконав студент групи
ПДЕБзмхм-21
С. А. Кравець

Науковий керівник:
к.е.н., доцент О. М. Карапетян

Випускну кваліфікаційну роботу
допущено до захисту:

"___" _____ 20___ р.

Завідувач кафедри
_____ **Н. Б. Москалюк**

561
29.11.19

ТЕРНОПІЛЬ - 2019

ЗМІСТ

ВСТУП

Кіберзлочинність не є традиційним злочином, а відносно молодим явищем, яке пов’язується із появою та поширенням глобальної мережі Інтернет. Із самого моменту виникнення даний вид злочинності проявив себе зручним для зловмисників. Особлива природа Всесвітньої мережі забезпечила глобальність та анонімність для її користувачів, що безсумнівно постало у якості передумов для появи даного виду злочинності. У свою чергу із поширенням кіберзлочинів пов’язано виникнення потреби правового регулювання цього питання як у світі, так і в Україні. Протидія будь-якому негативному впливу вимагає формування розуміння сутності проблеми та знання її генезису. Оскільки швидкість розвитку суспільства нерозривно пов’язана з досягненнями науково-технічного прогресу та злочинними проявами, важливим є також звернення до питання історичного розвитку впровадження правових механізмів для боротьби з кіберзлочинністю в світі та Україні.

Питання боротьби із кіберзлочинністю розглядали такі видатні вчені, як Дж. Арас, О.О. Баєв, Г.Р. Бєляков, Дж. Блумбекер, В.Л. Бурячок, В.М. Бутузов, Г.П. Власова, В.Я. Вовк, А.В. Войціховський, В.Д. Гавловський, Р.Є. Джансараєва, В.Б. Дзюндзюк, Д.В. Дубов, О.Є. Користін, М.О. Кравцова, М.Ю. Літвінов, Р.В. Лук’янчук, О.В. Манжай, В.В. Марков, М.А. Ожеван, Ю.М. Онищенко, О.В. Орлов, А.А. Протасевич, П.І. Пушкаренко, К.М. Рудой, Є.Д. Скулиш, В.Г. Хахановський, В.В. Чернєй та інші. Варто зазначити, що практично більшість науковців у тій чи іншій мірі досліджували проблематику правового регулювання боротьби із кіберзлочинністю в різних аспектах, однак ними не було досліджено комплексно саме ретроспективний аналіз даного правового явища, тенденцій розвитку та механізму правового регулювання боротьби із кіберзлочинністю.

Мета і задачі дослідження. Метою дослідження є концептуальне розуміння специфіки та тенденцій розвитку і механізму боротьби із кіберзлочинністю. Для досягнення зазначеної мети поставлено такі задачі:

Об'єкт дослідження – кіберзлочинність як суспільне явище та методи боротьби з нею.

Предмет дослідження – теоретико-правові засади регулювання боротьби із кіберзлочинністю.

Методи дослідження. Наукове дослідження побудовано на застосуванні загального системно-структурного методу, основні елементи якого забезпечили високий ефект побудови моделей розв'язання поставлених задач. В основі системи методології наукового аналізу генезису та тенденцій розвитку і механізму правового регулювання боротьби із кіберзлочинністю лежать наступні методи: діалектичний метод, історичний метод, системний метод порівняльно-правовий метод, логічні методи і прийоми – дедукція, індукція, аналогія, аналіз, синтез простежуються впродовж здійснення усього наукового аналізу.

Теоретико-методологічною основою дослідження є праці класиків економіко-правової науки, наукові дослідження вітчизняних і закордонних вчених з протидії кіберзлочинам та забезпечення кібербезпеки.

Інформаційну та емпіричну основу дослідження становлять норми міжнародно-правових актів, Конституції України, законодавчих та інших нормативно-правових актів, що визначають правові засади протидії кіберзлочинності в Україні, узагальнення діяльності державних суб'єктів протидії кіберзлочинності, форм та методів взаємодії між ними, довідкові видання, статистичні матеріали.

Наукова новизна одержаних результатів полягає в тому, що магістерська кваліфікаційна робота спробою комплексно, з використанням сучасних методів пізнання, з урахуванням новітніх досягнень науки теорії і права дослідити ретроспективу і тенденції розвитку, а також механізм правового регулювання боротьби із кіберзлочинністю. За результатами дослідження сформульовано

авторські основні положення: розкрито детально зміст ознак правового регулювання боротьби із кіберзлочинністю у Європейському Союзі, якими є наступні: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну; удосконалено: – характеристику підтенденцій тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні, якими є наступні: 1) ратифікація окремих міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю, які на сьогодні ще не є джерелом вітчизняного права; 2) укладення міжнародних двосторонніх чи багатосторонніх угод з іншими державами; 3) правова допомога іншим державам у питаннях боротьби із кіберзлочинністю.

Практичне значення. Основні положення магістерської кваліфікаційної роботи можуть бути враховані при подальшому коригуванні державної політики протидії кібертерзлочинності, виявленні найбільш ефективних напрямків попередження і нейтралізації кібератак. Матеріали магістерської роботи можуть використовуватися у науково-дослідній діяльності для подальших загальних і спеціальних наукових досліджень теоретико-правових аспектів правого регулювання боротьби із кіберзлочинністю.

Структура роботи. Магістерська кваліфікаційна робота складається з вступу, трьох розділів, висновків, переліку використаних джерел.

Основний зміст магістерської роботи викладено на 75 сторінках. Робота містить 4 аналітичних таблиці та 2 рисунки. Перелік використаних джерел складається із 60 найменувань.

РОЗДІЛ 1
ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

1.1. Теоретико-правові основи боротьби з кіберзлочинністю

Донедавна рівень кіберзлочинності в нашій країні був мінімальним, оскільки рівень розвитку інформаційних технологій був нижчим, ніж у розвинених країнах світу. Однак сьогодні нашу країну можна охарактеризувати за наявністю освіченого молодого покоління, високим рівнем безробіття та обмеженими можливостями працевлаштування, а події минулого року показали, що існує загроза цьому явищу у більш глобальному масштабі. В Україні проблема боротьби з нею ускладнюється тим, що термін "кіберзлочинність" не визначений в офіційних нормативно-правових документах, хоча поняття є загальним як для лексикону правоохоронних органів України, так і для держав світу , і за юридичну доктрину нашої держави. Використання сучасних інформаційних технологій майже у всіх сферах суспільного життя, включаючи державні та недержавні структури, ставить проблему боротьби з кіберзлочинністю серед основних. Окрім прямої шкоди від несанкціонованого доступу до інформації, її розповсюдження, зміни, знищення тощо, кіберзлочинність є джерелом загрози національній безпеці, економіці, правам людини та інтересам. Ступінь загрози комп’ютерних злочинів не повністю зрозуміла в суспільстві через відсутність наукової розробки фундаментальних понять, пов'язаних з цим. Тому вітчизняний законодавець та дослідники повинні враховувати досвід в Україні та розвинених країнах світу, оскільки це є свідченням існування такої загрози в майбутньому для будь-якої країни світу.

Тому ми пропонуємо трактувати кіберзлочинність як сукупність злочинних діянь, викладених у кримінальному законі, або на будь-якій території чи об’єктах, розташованих у них, вчинених у віртуальному просторі

руйнівно впливаючи на комп'ютерні системи, комп’ютерні мережі та комп'ютерні дані. На сучасному етапі поняття "боротьба з кіберзлочинністю" є досить незвичним для вітчизняної науки, незважаючи на те, що злочинні дії, які використовують всесвітню павутину, несуть високий рівень суспільної небезпеки. Сам термін не вперше з'явився в науковому обігу, але в основному автори неохоче пояснюють його сутність та особливості, орієнтуючись насамперед на значення та алгоритми реалізації. Тому один із способів вирішення проблеми боротьби з кіберзлочинністю вбачається у розробці теоретичної основи цього деструктивного соціального явища. Для аналізу концепції протидії кіберзлочинності звернемося до законодавчих актів, що становлять правову базу протидії кіберзлочинності - Конституції України, Конвенції про кіберзлочинність, Кримінального кодексу України, Кримінально-процесуального кодексу України тощо. У Основному законі взагалі немає поняття "боротьба з кіберзлочинністю". У статті 17 Конституції законодавець зазначав, що забезпечення інформаційної безпеки України є найважливішою функцією держави та справою всього українського народу, але йдеться не про протистояння небезпекам, а про забезпечення безпеки. Норми Конвенції про кіберзлочинність від 23.11.2001 р., Ратифікованої Верховною Радою України 7 вересня 2005 р. [8], містять поняття "боротьба з кіберзлочинністю", але вони не мають визначення. Кримінальний кодекс України передбачає відокремлення окремих видів кіберзлочинності у розділі XVI спеціального розділу "Злочини у використанні електронних комп'ютерів (комп'ютерів), систем та комп'ютерних мереж" - статті 361, 362 та 363, розділ V Спеціальної У розділі "Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина" перераховано певні види злочинів, у яких комп'ютерна продукція ідентифікується як злочин - статті 163, 176, 177 та розділ VII "Злочини у сфері бізнесу" – стаття 200 [3], але розумію, тітка "боротьба з кіберзлочинністю" також не визначена. Подібним чином дане питання врегульоване і нормами Кримінального процесуального кодексу України – стаття 263 врегульовує питання зняття інформації з транспортних телекомунікаційних мереж, стаття

264 – зняття інформації з електронних інформаційних систем, стаття 268 установлення місцезнаходження радіоелектронного засобу тощо, проте про «боротьбу із кіберзлочинністю» мова також не йде [9]. Отже, відсутність належного законодавчого закріплення поняття «боротьба із кіберзлочинністю» є однією із причин наявності проблем у його теоретичному розумінні та неоднозначності наукового тлумачення. За таких обставин важливо проаналізувати, як нормативно-правові джерела розкривають пов'язані з нашим дослідженням поняття. Посилаючись на нормативно-правові акти, які регламентують діяльність суб'єктів кіберзлочинності, у положенні управління кіберполіції Національної поліції України використовується термін "протидія кіберзлочинності", але також без уточнення його сутності. Звернемо увагу на термін «протидія», який на перший погляд є синонімом поняття «боротьба», але аналіз наукової доктрини показав труднощі реалізації їх поділу. Таким чином, вітчизняні вчені висловили думку щодо недоцільності використання терміна держава для боротьби зі злочинністю терміна "боротьба" - зокрема, пропонується використовувати інші терміни, такі як "запобігання", "протидія", "вплив", "запобігання", "запобігання", "подолання", "війна" або, власне, "протидія". Такі позиції в основному виправдовуються тим, що в боротьбі обов'язково треба перемогти і перемогти, а об'єктивна реальність свідчить про те, що повна перемога над явищем злочину неможлива [10, с. 31]. Однак ми все ще залишимось у позиції тих, хто вважає використання терміна «боротьба» більш доцільним. У загальнотеоретичному розумінні боротьба - це активне протиставлення, сутички між протилежними соціальними групами, державами, протилежні течії в суспільстві тощо [11, с. 93]. Тобто, боротьба з кіберзлочинністю - це активне протистояння деструктивній діяльності осіб, які здійснюють злочинні дії, використовуючи всесвітню павутину правоохоронними органами України - Службою безпеки України, відділом кіберполіції Національного управління кіберполіції, штат проблеми законодавців та інших зацікавлених сторін. Боротьба - це активна, цілеспрямована, науково обґрунтована діяльність держави, спрямована на

подолання негативного соціального явища кіберзлочинності, а термін «боротьба» позначає та підкреслює активний характер цієї діяльності, який не притаманний іншим термінам. Тому, незважаючи на її недоступність, подолання кіберзлочинності є одним із важливих завдань держави і таким і залишиться. На відміну від наших висновків, аналізуючи інтерпретацію поняття «протидія», зазначимо, що саме дія проти іншої дії перешкоджає цьому [11]. Тобто, порівнюючи терміни «боротьба» та «протидія», зазначимо, що, незважаючи на їх спорідненість, їх не слід ототожнювати. Боротьба ведеться незалежно від вчинення певних руйнівних дій, тобто ця концепція не виникає безпосередньо у відповідь на кіберзлочинність - вона здійснюється постійно, з метою повного подолання певного негативного явища. У свою чергу, виходячи зі значення терміна "протидія", ми робимо висновок, що "спрямування проти іншої перешкоджаючої дії" означає, що ця дія виникає у відповідь на вжиті дії. Тобто, переносячи це питання у сферу кіберзлочинності, ми наголошуємо, що обов'язковою умовою протидії кіберзлочинності є наявність юридичного факту у формі кіберзлочинності. У тлумаченні терміна «протидія злочинності» у науковій літературі це не є однозначним. У свою чергу, протидія є більш імпульсивною і залежить від конкретних вжитих дій. Тому слід зазначити, що боротьба з кіберзлочинністю проявляється у двох напрямках: перший - попередження злочинності, другий - розкриття злочинів, виявлення злочинців та їх покарання. Злочинність, у свою чергу, включає лише другий напрямок. Так, позначення державної політики більш доцільно описує термін "боротьба з кіберзлочинністю", але використання терміна "протидія кіберзлочинності" або "запобігання кіберзлочинності" в контексті діяльності компетентних правоохоронних органів є виправданим, оскільки це суть їх діяльності - порядок, пошук винних та притягнення їх до відповідальності. Юридична енциклопедія розглядає термін "запобігання злочинності" як протидію злочинності із застосуванням репресивних та нерепресивних засобів двома взаємопов'язаними способами: 1) запобігання злочинності та забезпечення неминучості покарання; 2) виправлення та перевиховання винних у злочинах

[14]. Зауважимо, що укладачі енциклопедії фактично ідентифікували поняття "боротьба" та "протидія", оскільки одне поняття пояснюється через інше. Ми бачимо такий підхід не зовсім вдалим, але ми залишаємось у розумінні цих явищ як двох окремих. Він також потребує подальшого уточнення неповного використання засобів запобігання злочинності - використання термінів "запобігання", "впевненість у неминучості" чи "перевиховання" не повністю описує процес боротьби та коло діяльності компетентного права правоохоронні органи. Тому варто додати до цього переліку вказівки щодо виявлення злочинів та виявлення злочинців, а також законодавчий напрям. Відзначимо розподіл дослідників заходів впливу на репресивні та не репресивні. Репресія - міра державного примусу, покарання [11]. Отже, "репресивний" - це той, який має на меті покарати. Це свідчить про те, що це визначення більш точно описувало б процес боротьби зі злочинцями. Злочинність є більш загальним і глобальним явищем, і тому методи впливу та протидії набагато конкретніші. Характеризуючи це визначення крізь призму пояснення суті боротьби з кіберзлочинністю, зазначимо, що воно потребує значного уточнення. По-перше, запобігання кіберзлочинності є надто абстрактним, оскільки кіберзлочинці часом частіше, ніж більш "традиційні" злочинці, тому запобігання виникненню та поширенню кіберзлочинності є непростим завданням для держави сьогодні. По-друге, санкції, введені сьогодні Кримінальним кодексом України за комп’ютерні злочини, є недостатньо суворими. Наприклад, створення чи продаж шкідливого програмного забезпечення або обладнання, призначених для посягань на електронні комп’ютери (комп'ютери), автоматизовані системи, комп’ютерні мережі або телекомунікаційні мережі, караються штрафом від п'ятисот до тисячі мінімумів, що не обкладаються податком. громадяни, виправні роботи на строк до двох років або позбавлення волі на той самий строк [3].

Законодавець розробляє фактичну нормативно-правову базу, компетентні правоохоронні органи здійснюють попередження злочинів, розслідування та притягнення до відповідальності винних осіб. Індивіди або групи осіб також

можуть сприяти цій боротьбі якнайкраще. За таких обставин ознака самоврядування означає, що незважаючи на неоднорідність, кожен із суб'єктів-учасниць зосереджений на досягненні спільної мети. Що стосується боротьби з кіберзлочинністю в Україні, то, як правило, вона проводиться відділом кіберполіції Національної кіберполіції, національним законодавцем та іншими соціальними групами, зацікавленими у подоланні цієї проблеми.

За таких умов законодавець здійснює свою діяльність у законодавчому та організаційному напрямках, а Департамент кіберполіції Національної кіберполіції у профілактичному. Інші соціальні групи, зацікавлені у боротьбі із кіберзлочинністю, сприяють даному процесу у міру своїх можливостей. Останньою ознакою є комплексність боротьби із злочинністю, яка виявляється у поєднанні репресивних та не репресивних заходів для досягнення окреслених цілей. Ознаки збірності та комплексності є близькими за своєю сутністю, проте розрізняються за наступними критеріями: 1) збірністю є поєднання підсистем, які значно відрізняються за своїми функціями та призначенням, у свою чергу комплексність полягає у взаємодії усіх елементів єдиного цілого із метою досягнення спільної мети; 2) метою збірності є об'єднання низки елементів у єдине ціле, комплексності – встановлення між ними таких взаємозв'язків, завдяки яким сам процес набуде дієвості; 3) збірність є структурним поняттям, а комплексність – функціональним. На відміну, від дослідженого поняття «боротьби зі злочинністю», «боротьба із кіберзлочинністю» є в меншій мірі висвітленою у наукових джерелах.

Увагу вітчизняних дослідників привертають різноманітні аспекти даного явища, процесуальні моменти, нормативно-правова основа його існування, проте понятійний апарат залишається поза увагою. У процесі дослідження нами встановлено, що дефініція поняття «боротьба із кіберзлочинністю» є новою для вітчизняної юридичної науки. Аналіз російських наукових джерел продемонстрував, що їх вчені концентрують свою увагу у цілому на тих самих проблемах, що й українські, а отже визначення поняття «боротьба із кіберзлочинністю» також залишається невстановленим. Щодо наближених до

боротьби із кіберзлочинністю понять, В. Л. Бурячок оперує терміном «кіберборотьба» [25, с. 11]. Дане поняття не у повній мірі є тотожним об’єкту нашого дослідження, оскільки дане явище позбавлене головної деструктивної риси – воно не стосується злочинності. Проте аналіз сутності терміну «кіберборотьба» дозволить вдаліше розібратись у специфіці такого протистояння та виділити специфічні ознаки боротьби із кіберзлочинністю. З точки зору ученого, кіберборотьбу становить комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань [25, с. 11]. Дана позиція не є правовою, тому дослідник оперує галузевою термінологією, проте безсумнівно при аналізі зазначеної дефініції можливо провести співвідношення із визначенням поняття «боротьба із злочинністю», сформульованим нами.

Спочатку зверніть увагу на вибір вченим складного характеру явища. По-друге, дослідник встановив наявність двох сторін, що повністю відповідає нашому аналізу сутності терміна "боротьба". Що стосується специфічних особливостей, то вони такі: 1) насамперед при розгортанні бою слід вжити всіх необхідних заходів для запобігання руйнівного впливу на власні автоматизовані системи; 2) кібер-боротьба здійснюється за допомогою використання спеціально розробленого програмного забезпечення, а також після проведення системи спеціалізованого навчання. Загальне, тобто характерне для явища боротьби зі злочинністю загалом, ми включаємо: 1) діяльність; 2) зобов'язання; 3) командна робота; 4) всебічність. У процесі аналізу правової доктрини ми виділили як особливу, а саме, виключно характерну для боротьби з кіберзлочинністю: 1) ознаку можливості контратаки з боку кіберзлочинців; 2) вказівка на здійснення виключно компетентними суб'єктами, що володіють спеціалізованими знаннями та необхідними ресурсами; 3) ознака міждержавної; 4) ознака згуртованості держав. Ознака можливості контратаки

кіберзлочинцями характерна лише для цього виду злочинів. Суть його полягає в тому, що в процесі боротьби з кіберзлочинністю, суб’єкти, представлені правоохоронними органами зі спеціальними знаннями та необхідними ресурсами, законодавча влада за сприяння осіб або груп, зацікавлених у подоланні цієї проблеми, повинна піклуватися про своє. руйнівний вплив на безпеку кіберзлочинців за рахунок використання спеціально розробленого програмного та апаратного забезпечення, а також проведення системи спеціалізованого навчання. Часто державні органи розглядаються як об'єкти кібератак, і ці ситуації також характерні для недавньої історії України. Наприклад, у грудні 2015 року було здійснено кібератаку на енергокомпанії України, внаслідок якої було закрито близько 30 підстанцій, близько 230 тис. Жителів залишилися без світла на одну-шість годин. 6 грудня 2016 року хакерська атака на урядові сайти (Державне казначейство України та інші) та на внутрішні мережі урядових установ призвела до великих затримок з бюджетними платежами [26]. Це вказує на те, що будь-яка суб'єкт кіберзлочинності може бути ідентифікований як об'єкт кіберзлочинності. Тому важливо не лише вжити заходів для її подолання, але і завжди бути готовими до контр-дій, оскільки інструменти кіберзлочинності дозволяють нам робити деструктивні дії проти будь-якого об’єкта.

Тому слід підкреслити, що міжнародна співпраця у боротьбі з кіберзлочинністю здійснюється за такими напрямками: 1) прийняття міжнародно-правових механізмів регулювання та співпраця правоохоронних органів у боротьбі з кіберзлочинністю; 2) гармонізація національного законодавства з міжнародним законодавством; 3) безпосереднє співробітництво, як формальне, так і неформальне; 4) координація повноважень у боротьбі з кіберзлочинністю. Таким чином, рівень та темпи зростання кіберзлочинності потребують адекватного реагування не лише на законодавчому та правоохоронному рівнях, але й на науковому рівні.

Згідно з нашим дослідженням, вченим слід приділяти більше уваги теоретичним проблемам досліджуваного явища. Занадто багато складних

досліджень було присвячено боротьбі з кіберзлочинністю, тому не дивно, що немає розуміння реальних загроз, спричинених поширенням цього руйнівного процесу в суспільстві. Кіберзлочинність – специфічне і унікальне явище, тому логічно, що боротьба з нею також набула особливих особливостей. Для ефективної боротьби з кіберзлочинністю слід надати адекватну та об'єктивну оцінку її природи, особливостей, вимог до часу та потреб у практиці. Кіберзлочинність набуває нових можливостей та досягнення кращого організаційного рівня, а враховуючи тенденції розвитку інформаційних технологій, соціальний ризик цього руйнівного явища постійно зростає. Для України ця проблема раніше не була такою гострою, але зі зміною курсу держави та приєднанням до світового інформаційного простору кібербезпека постійно існує. Таким чином, оскільки кіберзлочинність у нашій країні як і раніше є переважно потенційною загрозою, на цьому етапі важливо вжити профілактичних заходів. Все це зумовлює необхідність створення ефективної системи запобігання, виявлення та припинення такої діяльності, яка гарантуватиме успіх боротьби з кіберзлочинністю в Україні.

1.2. Генезис протидії кіберзлочинності на міжнародному та національному рівнях

Наразі відбувається останній етап розвитку кіберзлочинності – етап появи нових форм комп’ютерних злочинів. Як відзначає В. Б. Дзюндзюк, серед них варто відзначити наступні: 1) Інтернет-війна – уперше групи комп’ютерних активістів, засуджуючи військові дії Югославії та НАТО, здійснювали злом урядових комп’ютерів та поширювали антивоєнну Інтернет-пропаганду; 2) Інтернет-страйк – групова діяльність, яка призводить до перевантаження Інтернет-сайту на неможливість його відвідування іншими користувачами тощо [29, с. 5-6].

Очевидно, такий перелік нових форм далеко не вичерпний, але його основна мета – продемонструвати, що питання правового регулювання кіберзлочинності у світі потребує постійної еволюції та вдосконалення,

оскільки комп’ютерні злочинці постійно змінюють напрями та методи своєї діяльності. Тому основними рисами сучасного етапу є: 1) еволюція кіберзлочинності, поява її нових форм; 2) спроби законодавців адекватно реагувати на ці зміни. Тому завдяки аналізу юридичної доктрини ми виділили наступні етапи процесу розвитку явища кіберзлочинності:

1. Підготовча фаза (початок 60-х - початок 70-х рр. XX ст.) – першими випадками слід вважати перші випадки злочинів із застосуванням електронних комп'ютерів, врешті-решт комп’ютерні зловмисники вже були організованими злочинними групами, які використовували власні знання незаконного збагачення та порушення встановленого порядку;

2. Етап розповсюдження кіберзлочинності (початок 1970-х - 1986 рр.) – початком слід вважати появу хакерів та їх організованих груп, а кінцем, пов’язаним з прийняттям першого регуляторного акта про кіберзлочинність та першого в історії арешту хакер;

3. Етап транснаціональної кіберзлочинності та кібертероризму (1994 - початок 21 століття) – початок цього етапу пов'язаний із "справою Володимира Левіна", першою великою міжнародною транснаціональною кіберзлочинністю, а кінцева дата була обрана умовно – ми попередньо зробили це до початку нового століття, в якому не було значних історичних подій у розвитку кібертероризму, але в яких відбувається систематична еволюція кіберзлочинності;

4. Сучасна стадія кіберзлочинності (21 століття) - це стадія виникнення нових форм комп'ютерних злочинів. Таким чином, ми встановили, що генезис розвитку кіберзлочинності та генезис правового регулювання боротьби з кіберзлочинністю неможливо ідентифікувати. Кіберзлочинність розвивається відповідно до еволюції новітніх технологій, тому сьогодні це область, яка постійно знаходиться на крок попереду своєї регуляторної бази. Беручи до уваги стадію розвитку кіберзлочинності, зазначимо, що на перших двох етапах законодавче регулювання цього інституту практично не було здійснено.

Так, нами наведено приклад кіберзлочину, внаслідок якого відбулось перше затримання хакерів, проте їх умовне покарання свідчить про відсутність на той момент адекватних інструментів боротьби із комп’ютерними злочинцями. Відповідно, на другому та третьому етапах правове регулювання боротьби з кіберзлочинністю в світі вже відбувалось повноцінно.

Таким чином, перший етап генезису правового регулювання боротьби з кіберзлочинністю буде обмежений періодом з 1986 року, тобто прийняттям першого комп'ютерного закону в історії, до 1989 року, коли Рекомендація № R (89) 9 була прийнято, що суттєво вплинуло на подальший розвиток законодавства. про кіберзлочинність і послужив поштовхом до змін у кримінальному законодавстві в європейських країнах. Так, після 1989 року почалася швидка еволюція кримінального права європейських держав у частині посилення боротьби з комп’ютерними злочинами, яка триває певною мірою і донині. Підсумовуючи, перший етап генезису правового регулювання кіберзлочинності у світі характеризується такими особливостями: 1) прийняття першого в історії «комп’ютерного» закону; 2) внесення змін до національного кримінального законодавства в деяких країнах; 3) прийняття рекомендацій європейським країнам щодо боротьби з кіберзлочинністю, що згодом значно вплинуло на швидкий розвиток європейського законодавства. Важливість початкової фази полягає в тому, що до моменту свого виникнення кіберзлочинність вже зростала з тривожною швидкістю і швидко розвивалася. Прийняття перших регламентів не вплинуло на зменшення кіберзлочинності, проте воно продемонструвало волю провідних країн боротися з цим негативним явищем. Тому, на нашу думку, 1989 рік є початковою датою для наступного етапу генезису правового регулювання кіберзлочинності у світі – внесення змін до кримінального законодавства європейських країн, що тривало до 2000 року. Використання терміна "умовно" є обумовлюється тим, що цей процес загалом триває і донині. Однак, в першу чергу, враховуючи аналіз динаміки прийняття державами змін до вітчизняного кримінального законодавства на зазначеному етапі, слід зробити висновок, що це було у 2000 році, після прийняття змін у

кримінальному законодавстві Бельгія, що подальші зміни до національних законів вже не мають настільки масштабного характеру. По-друге, 2000 рік означає початок прийняття важливих міжнародно-правових актів, які сьогодні складають основу європейського та світового законодавства про кіберзлочинність. Такими міжнародно-правовими інструментами щодо регулювання міжнародних відносин у цій галузі є Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 р. [40], Віденська декларація про злочинність та правосуддя: Відповідь на виклики 21 століття (ООН) 17.04.2000 [41], Конвенція про взаємодопомогу у кримінальних справах між державами-членами Європейського Союзу, Конвенція про кіберзлочинність, Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації, її расистських та ксенофобських дій через комп'ютерні системи, Пакт про співробітництво між державами-учасницями Співдружності Незалежних Держав у сфері кіберзлочинності, ряд інших інструментів, таких як рекомендації Ради Європи.

Таким чином, фактично за останні два роки у міжнародному праві з’явилася низка актів, які мали значний вплив на боротьбу з кіберзлочинністю. Ось чому ми назвали третю стадію генезису правового регулювання боротьби з кіберзлочинністю у світі "консолідацією європейської спільноти" та хронологічно обмежили її лише двома роками – 2000 та 2001 роками. Сьогодні цей етап слід розглядати як найважливіше, оскільки кіберзлочинці завжди випереджали попередні, коли співвідносили темпи кіберзлочинності та інструменти правового регулювання проти неї. Однак з початку 21 століття розвинені країни та європейська спільнота виявили готовність вживати жорстких заходів щодо боротьби з кіберзлочинністю як явищем. Таким чином, третій етап генезису правового регулювання боротьби з кіберзлочинністю у світі характеризується такими ознаками: 1) динамічна еволюція національних законів провідних держав Європи та світу з точки зору посилення кримінальної відповідальності за вчинення комп’ютерних злочинів; 2) прийняття основних міжнародних правових актів щодо співробітництва та взаємодопомоги

провідних країн світу у питаннях кібербезпеки, які сьогодні становлять правову основу сфери протидії кіберзлочинності; 3) законодавці виходять на новий рівень у боротьбі з кіберзлочинцями внаслідок посилення міждержавних відносин та розширення змісту поняття кіберзлочинності. Що стосується наступного періоду, який є останнім, ми вважаємо, що це сучасний етап правового регулювання боротьби з кіберзлочинністю, який триває і сьогодні. Цей період не можна охарактеризувати з урахуванням конкретних основних подій, що відбулися або відбуваються – його головна характеристика – вдосконалення законодавства про кіберзлочинність державами, які на кілька кроків відстають від розвинених країн. До таких держав, зокрема, відноситься і Україна. Виділяючи специфічні особливості сучасного етапу, зазначимо наступне: 1) міжнародне право суттєво не змінилося, а поступово розвивається; 2) Збільшення кількості країн світу для боротьби з кіберзлочинністю. Таким чином, вивчення генезису правового регулювання боротьби з кіберзлочинністю у світі вимагає виділення власної історичної класифікації. У процесі аналізу наукової доктрини ми встановили, що дослідницьке питання слід класифікувати наступним чином:

1. Етап правового регулювання боротьби з кіберзлочинністю (1986 - 1989) – від прийняття першого в історії комп'ютерного закону до прийняття Рекомендації № R (89) 9, яка мала вирішальне значення для подальшого розвитку законодавства, спрямованого на боротьба з кіберзлочинністю та діяла як поштовх для розвитку кримінального права в європейських країнах;

2. Етап змін до кримінального закону європейських країн (1989-2000 рр.) Після 1989 р. Почалася швидка еволюція кримінального права європейських держав з точки зору активізації боротьби з кіберзлочинністю, яка певною мірою триває і донині. і кінцевий термін цього періоду ми умовно пов'язуємо з 2000 роком, після якого подальші зміни до національних законів вже не характеризуються масовим характером;

3. Етап консолідації Європейського співтовариства в кіберзлочинності (2000-2001 рр.) - За останні два роки в міжнародному праві з'явилася низка

актів, які мали значний вплив на боротьбу з кіберзлочинністю. Ось чому цей етап хронологічно обмежений лише двома роками; 4. Сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 - донині) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, що перебувають на нижчих рівнях розвитку. Наша держава перебуває на ранніх стадіях боротьби з кіберзлочинністю, але цілеспрямована політика щодо кіберзлочинності все ще проводиться. Тому важливо проаналізувати цей відносно короткий шлях вітчизняного законодавця до вирішення існуючих проблем із виникненням та поширенням нових форм злочинності та співвіднесення історії розвитку цього явища на світовому рівні. В рамках дослідження генезису правового регулювання боротьби з кіберзлочинністю доцільно було б Україна почати аналіз історії розвитку кіберзлочинності в нашій країні, але аналіз праць вітчизняних вчених показав, що це насправді відсутня. Варто зазначити так звану "справу Вінниці" 1998 року, в якій зловмисник незаконно перерахував понад 80 мільйонів гривень, використовуючи електронну платіжну систему, і на той момент сума становила близько 20 мільйонів доларів, за рахунок одного з латвійські банки [45]. Однак ця справа не була включена в історію комп'ютерної злочинності в Україні, оскільки її не відносили до кіберзлочинності через недосконаліть вітчизняного законодавства. Це підтвердження того, що на той час законодавство України у сфері боротьби з кіберзлочинністю було недосконалим, точніше фактично відсутнім. Ми виявляємо, що, в той же час, у 1998 р. Розвиток правового регулювання проти кіберзлочинності у світі був на етапі внесення змін до кримінального законодавства європейських країн, на якому відбувалася швидка еволюція кримінального права європейських держав. місце в рамках активізації боротьби з комп'ютерними злочинами.

Проте Україна ще не була частиною даного процесу. До нормативно-правових актів, які врегульовують суспільні відносини у сфері кібербезпеки в Україні слід віднести: Конституцію України, Кримінальний кодекс України, Конвенцію про кіберзлочинність, закони України «Про інформацію» № 2657-

XII від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 , «Про державну таємницю» № 3855-XII від 21.01.1994 [48], «Про основи національної безпеки України» № 964-IV від 19.06.2003; численні укази Президента України та інші нормативно-правові акти. Також вагоме значення має новоприйнятий Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. Із аналізу нормативно-правої бази боротьби із кіберзлочинності в Україні, можемо встановити певні закономірності, які дозволять нам здійснити вдалу етапізацію генезису правового регулювання боротьби з кіберзлочинністю.

Із початку 90-х років XX століття зазначеній проблемі у багатьох країнах світу приділялась значна увага. Проте, Україна у даному контексті в цілому не відноситься до таких держав. Аналізуючи норми прийнятих у 90-х роках минулого століття нормативно-правових актів, відзначаємо, що увага питанню захисту від кіберзлочинів законодавцем не приділялась у належному обсязі. Тому перший етап хронологічно обмежимо 1991 та 2000 роками, періодом від моменту здобуття Україною незалежності і до початку нового століття, коли почали бути помітними тенденції до розвитку законодавства про кіберзлочини. Отже, початковий етап генезису правового регулювання боротьби з кіберзлочинністю в Україні у цілому характеризується наступними ознаками: 1) прийняття нормативно-правових актів, присвячених захисту інформації, які втім фактично не врегульовували сферу кіберзлочинів; 2) відсутність імплементації норм міжнародного законодавства у кіберсфері; 3) брак в Україні гучних справ, пов'язаних із вітчизняними кіберзлочинцями, що в певній мірі може слугувати поясненням ігнорування законодавцем даного питання. Вважаємо, що поштовхом для стрімкої еволюції стали взяті Україною зобов'язання щодо інтеграції у міжнародну та світову спільноту, наприклад прийняті згідно до Програми інтеграції України в Європейський Союз [50]. Так, Розділ 13 Програми було присвячено інформаційному суспільству. У 2001 році було прийнято новий Кримінальний кодекс України, у якому: 1) окремі види кіберзлочинів було виділено у Розділі XVI Особливої частини «Злочини у сфері

використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж – статті 361, 362 та 363; 2) Розділом V Особливої частини «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину – статті 163, 176, 177; 3) Розділом VII «Злочини у сфері господарської діяльності» – стаття 200 [3]. Значення прийняття Кримінального кодексу України можна виразити наступними аспектами: 1) незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства; 2) за кіберзлочини було встановлено конкретні санкції; 3) прийняття Кодексу послужило поштовхом для настання наступного етапу генезису правового регулювання боротьби з кіберзлочинністю – етапу прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю. Паралельно із даним процесом, актуальність проблеми кібербезпеки було зокрема відмічено Указами Президента: «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891 [51], «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000 [52], «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001 [53] тощо. Разом з тим, відмічаємо, що не зважаючи на значне поліпшення нормативно-правової бази щодо запобігання та регулювання відносин у сфері кіберзлочинності, у цілому її стан залишався та залишається недосконалим, у першу чергу через безсистемність. У 2003 році було прийнято Закон України «Про основи національної безпеки» від 19.06.2003 № 964-IV, у якому, зокрема, були закріплені поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» та їх віднесення до основних реальних та потенційних загроз національній безпеці України [49]. Тож, підсумуємо закінчення другого етапу генезису правового регулювання боротьби з кіберзлочинністю в Україні саме 2003 роком. По-перше, на даному етапі було здійснено віднесення незаконної

діяльності у кіберпросторі до злочинів та встановлено конкретні санкції за їх вчинення. По-друге, була значно розширена нормативно-правова база правового регулювання боротьби з кіберзлочинністю. По-третє, в законодавчий обіг було введено поняття «комп'ютерна злочинність» та «комп'ютерний тероризм». По-четверте, наступні події щодо правового регулювання боротьби з кіберзлочинністю в Україні пов’язані із ратифікацією міжнародного законодавства, які логічно виділити окремим етапом. У 2005 році Україною ратифіковано Конвенцію про кіберзлочинність і таким чином імплементовано положення міжнародного акту у вітчизняне законодавство [1]. Норми Конвенції вже частково були розглянуті нами у межах даного підрозділу, тож доцільно відмітимо, що її прийняття послужило початком нового етапу генезису правового регулювання боротьби з кіберзлочинністю в Україні, який триває і по сьогоднішній день. Курс України до євроінтеграції свідчить про подальшу інтеграцію міжнародних правових норм у вітчизняну систему. Стан розвитку законодавства про кіберзлочинність свідчить про те, що дана сфера однозначно потребує удосконалення, а застосування європейського досвіду є доцільним з огляду на рівень його розвитку. Відзначимо, що на сучасному етапі розвиток кіберзлочинності в нашій державі ще не досяг значних масштабів. Серед суттєвих кібератак варто виділити нещодавнє застосування невідомими зловмисниками вірусу «Petya.A» проти значної кількості стратегічних об’єктів нашої держави. Зокрема, відомо, що одним із шляхів потрапляння вірусу до комп’ютерних мереж було оновлення бухгалтерського програмного забезпечення «M.E.Doc» [54]. Проте, на сьогодні у даних справах все ще ведеться слідство, а винні особи не встановлені. Аналіз судової практики засвідчує, що на сьогодні в Україні є поширеними такі кіберзлочини, як несанкціоноване втручання в роботу автоматизованих систем, шахрайство, із використанням електронно-обчислювальної техніки, розповсюдження відеопродукції порнографічного характеру у кіберпросторі та інші незаконні операції з використанням електронно-обчислювальної техніки. Тобто, кібертероризм ще не набув значних масштабів в нашій державі, проте останні

негативні тенденції свідчать про необхідність переходу правового регулювання боротьби з кіберзлочинністю на наступний етап.

Щодо прикладів вітчизняної судової практики, 21 січня 2016 року Стрийським міськрайонним судом Львівської області було розглянуто справу щодо несанкціонованого втручання в роботу автоматизованих систем, зокрема банкомату. Зловмисники встановили два несанкціоновані пристрої, які мають умовну назву «накладка на банкомат» і призначені для прихованого розміщення на банкоматі з метою отримання інформації з магнітних стрічок банківських карт користувачів та здійснення відеофіксації виконання ними операцій на цифровій клавіатурі банкомату, що призвело до проникнення в автоматизовану систему вказаного банкомату та витоку інформації 45 клієнтів вказаної вище банківської установи, на яких містилась інформація з магнітних стрічок карт та пінкодів клієнтів банку [55]. Оскільки, статтею 361 Кримінального кодексу України передбачено відповідальність за незаконне втручання в роботу електронних обчислювальних машин, зробимо висновок, що вітчизняний законодавець адекватно реагує на подібні загрози. Оскільки правове регулювання подібних питань передбачено нормами вітчизняного законодавства, основною проблемою існування зазначеного негативного явища є недосконаліть систем захисту банків, у результаті чого зловмисники знаходять можливості незаконного збагачення. Тому, зробимо висновок, що законодавець адекватно реагує на наявність проблеми можливості несанкціонованих втручань у кіберпросторі. Поширеними на сьогодні є випадки шахрайства із використанням електронно-обчислювальної техніки. Так, 22.05.2017 року Першотравневим районним судом міста Чернівці було винесено вирок по справі № 725/85/17 щодо вчинення із корисливих мотивів ряду дій, спрямованих на підготовку та реалізацію шахрайства. Зловмисниця розмістила на Інтернет-сайті \ оголошення про здачу в оренду кімнати, достовірно знаючи, що житла за вказаною адресою у неї не має та наміру здавати кімнату в оренду вона не мала. Особа повідомила потерпілому завідомо неправдиву інформацію, та отримала грошову суму у якості завдатку [56]. У

даному випадку злочин кваліфікувався за статтею 190 Кримінального кодексу України. У даному випадку законодавець не відокремив окремо шахрайство за допомогою електронно-обчислювальної техніки, проте у даному випадку все ж основоположну роль відіграє факт заволодіння чужим майном шляхом обману. Тому, не зважаючи на наявні ознаки кіберзлочину, подібні правопорушення варто кваліфікувати як шахрайство. Наступним прикладом є вирок Ленінського райсуду міста Кіровограда (нині м. Кропивницький) у справі № 405/1660/14-к. Зловмиснику було пред'явлено обвинувачення у вчиненні розповсюдження відеопродукції порнографічного характеру за допомогою веб-сайту «http://vk.com» [57]. Не зважаючи на те, що даний злочин було кваліфіковано за статтями 300 та 301 Кримінального кодексу України, а саме ввезення, виготовлення, збут і розповсюдження порнографічних предметів та творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, даний проступок все ж має чіткі ознаки кіберзлочинів, адже його вчинення пов’язується із Всесвітньою мережею. Тому, зробимо наступний висновок: не зважаючи на те, що деякі із проступків, які містять ознаки кіберзлочинів, не кваліфікуються як останні, законодавцем все ж на належному рівні здійснюється правове регулювання тих загроз, які є актуальними на сьогодні. Водночас, останні тенденції свідчать про те, що в подальшому існуючий механізм потребує значного вдосконалення із урахуванням нещодавніх викликів. Отже, на сучасному етапі правове регулювання боротьби з кіберзлочинністю в Україні характеризується такими особливими рисами: 1) ратифікація міжнародних правових актів; 2) курс України до євроінтеграції зумовлює необхідність подальшого приведення вітчизняного законодавства у відповідність до європейських стандартів; 3) поява тенденції до збільшення загрози кібертероризму в Україні; 4) належне правове регулювання тих кіберзагроз, які на сьогодні є найбільш поширеними в Україні.

Дослідження генезису правового регулювання боротьби з кіберзлочинністю в Україні дозволяє виділити його наступні етапи:

1. Початковий етап (1991 рік – 2000 рік) – не зважаючи на те, що у даний період було прийнято декілька нормативно-правових актів, спрямованих на врегулювання проблем кібербезпеки, питанню захисту від кіберзлочинів законодавцем увага не приділялась у належному обсязі, проте у 2000 році почали бути помітними тенденції до розвитку законодавства про кіберзлочини;

2. Етап прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю (2001 рік – 2005 рік) – його початок пов’язується із прийняттям Кримінального кодексу України, у нормах якого незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства, а за кіберзлочини було встановлено конкретні санкції. Відповідно, закінчення етапу віднесемо до введення у правовий обіг понять «комп'ютерна злочинність» та «комп'ютерний тероризм»;

3. Етап відповідності правового регулювання боротьби з кіберзлочинністю існуючим загрозам (2005 рік – до 27.06.2017 року) – не зважаючи на те, що на даному етапі зроблено небагато, курс України до євроінтеграції вимагає імплементації європейських правових норм у вітчизняне законодавство. Існуючі кіберзагрози були врегульовані належним чином. У цілому, зазначений період характеризується відсутністю вагомих подій у сфері боротьби із кіберзлочинністю;

4. Новітній етап (від 27.06.2017 року) – вірус «Petya.A» продемонстрував неготовність України до боротьби із сучасними кіберзагрозами. Тому, щойно розпочатий етап пов’яжемо із подальшою розробкою інструментів для боротьби із кібертерроризмом. Отже, комп’ютерна злочинність є проблемою, з якою суспільство зіштовхнулось порівняно нещодавно, проте яка обіцяє постійно зростати та вдосконалюватись. Незважаючи на усі заходи, які приймаються державами, їх усе ще недостатньо. Тому на сьогодні важливим є перегляд усіх існуючих інструментів та розробка нових, які дозволять надійніше захиститись від кіберзлочинців. Дослідження розвитку правового регулювання боротьби з кіберзлочинністю в світі та Україні засвідчило, що жодна держава не в змозі протистояти кіберзлочинності самостійно. Аналіз

історичних процесів генезису європейського законодавства засвідчив, що основні поштовхи у еволюції правового регулювання боротьби з кіберзлочинністю в зарубіжних країнах були спричинені прийняттям колективних рішень чи рекомендацій. Тому Україна, як держава, яка в світлі нещодавніх подій фактично вперше зіштовхнулась із масовими організованими кібератаками потребує значної активізації діяльності у зазначеній сфері.

Висновки до розділу 1

1. Боротьбою зі злочинністю є комплексна активна система заходів, що застосовується у якості реакції держави на протиправну діяльність осіб чи їх груп та входить до компетенції правоохоронних органів та органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми.

2. Виділено наступні етапи процесу розвитку явища кіберзлочинності: 1) Підготовчий етап (початок 60-років - початок 70-х років XX століття) – початковим моментом варто вважати перші випадки злочинів, вчинених із використанням електронних обчислювальних машин, наприкінці комп'ютерні зловмисники вже представляли із себе організовані злочинні групи, які використовували власні знання для незаконного збагачення та порушення встановленого порядку; 2) Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік); 3) Етап транснаціональних кіберзлочинів та кібертероризму (1994 рік – початок XXI століття) – початковий момент даного етапу пов'язується із «справою Володимира Льовіна», першим великим міжнародним транснаціональним мережевим комп'ютерним злочином, а кінцева дата обрана умовно – нами здійснено її прив'язку до початку нового століття, у якому не відбулось вагомих історичних подій у розвитку

кібертероризму, проте у якому відбувається планомірна еволюція комп'ютерної злочинності; 4) Сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп'ютерних злочинів.

3. Генезис правового регулювання боротьби з кіберзлочинністю в світі етапізований наступним чином: 1) Етап зародження правового регулювання боротьби з кіберзлочинністю (1986 рік – 1989 рік) – від прийняття першого в історії комп'ютерного закону, до прийняття Рекомендації № R(89)9, яка мала ключове значення для подальшого розвитку законодавства, спрямованого на боротьбу з кіберзлочинністю та виступила у якості поштовху для еволюції кримінального законодавства європейських країн; 2) Етап внесення змін до кримінального законодавства європейських країн (1989 - 2000 рік) - після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день, а кінцевий термін даного періоду ми умовно пов'язуємо із 2000 роком, після якого подальші зміни до національних законодавств уже не характеризувались масовим характером; 3) Етап консолідації європейської спільноти для боротьби із кіберзлочинністю (2000 рік – 2001 рік). Саме тому даний етап хронологічно обмежений лише двома роками; 4) Сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 рік – наші дні) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, які перебувають на нижчих рівнях розвитку.

РОЗДІЛ 2
МЕХАНІЗМ РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1. Аналіз стану кіберзлочинності в Україні

В Україні відсутня офіціальна державна статистика, яка б містила відомості про кіберзлочини, що негативно позначається на запобіжних заходах, які мають фрагментарний характер, зумовлюючи труднощі у протидії та боротьбі з таким видом суспільно небезпечних діянь.

Серед причин зазначеного, зокрема, те, що терміном “кіберзлочинність” (визначений лише 2017 р. у Законі України “Про основні засади забезпечення кібербезпеки України” [5]) охоплюється широкий спектр правопорушень, ускладнюючи тим самим розробку системи типології або класифікації кіберзлочинності. Під поняттям “кіберзлочини” ми розуміємо кримінальні правопорушення, передбачені розділом XVI КК України (“Злочини у сфері використання електроннообчислювальних машин (комп’ютерів, систем та комп’ютерних мереж і мереж електрозв’язку”), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – “з використанням високих інформаційних технологій і телекомунікаційних мереж”. На сьогодні офіційна державна статистика містить лише відомості про вчинені кримінальні правопорушення, передбачені Розд. XVI КК України, що відображаються у звітах Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення; Єдиний звіт про осіб, які вчинили кримінальні правопорушення). У Державній судовій адміністрації України готуються звіти судів першої інстанції про розгляд матеріалів кримінального провадження (форма № 1-к), про осіб, притягнутих до кримінальної відповідальності, та види кримінального покарання (форма № 6) і про склад засуджених (форма № 7). Варто визначити, що до 2018 р. складалися

піврічні й річні звіти. Але з метою вдосконалення звітності про стан здійснення правосуддя місцевими та апеляційними судами Державною судовою адміністрацією України видано наказ “Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами” від 23 червня 2018 р. № 325 [6]. Зараз періодичність цих звітів річна. Термін підготовки і подання звітів Державною судовою адміністрацією України до Державної служби статистики України – не пізніше 40-го дня після звітного періоду (для порівняння – Генеральна прокуратура України подає звіти до Державної служби статистики України до 5 числа після звітного періоду). Статистичні дані про кіберзлочини відображаються також у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України, де, крім кримінальних правопорушень, охоплених Розд. XVI КК України, зазначається ще низка кримінальних правопорушень, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 КК України “Порушення авторського права і суміжних прав” і ст. 185 КК України “Крадіжка”, чч. 3 і 4 ст. 190 КК України “Шахрайство”, ст. 200 КК України “Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення”, ст. 229 КК України “Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару” і ст. 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю”, чч. 3, 4 і 5 ст. 301 КК України “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів”. Але цей перелік статей неповний. Варто відмітити, що зважаючи на високий рівень латентності кіберзлочинності (наразі обліковується тільки 10 – 20 % вчинених злочинів, а решту становить латентна злочинність), а також низький рівень звітно-реєстраційної дисципліни, сьогодні говорити про будь-яку офіційну статистику, яка повно й достовірно відображає стан і структуру кіберзлочинності, проблематично. Можливо проаналізувати тільки динаміку

цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів. Протягом 2018 р., згідно зі статистичними даними Генеральної прокуратури України (табл. 2.1), обліковано 2017 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Їх питома вага ще незначна і становить усього 0,5 % від усіх облікованих кримінальних правопорушень у 2018 р., але за останні п'ять років зросла в 5,6 раза (у 2014 р. становила – 0,09 %).

Таблиця 2.1.

Обліковані кримінальні правопорушення, передбачені статтями Розд. XVI КК України (за даними Генеральної прокуратури України) [12]

Статті КК України	2017 р.	2018 р	У порівнянні 2017 і 2018 рр.	
			+/–	%
361	1795	1023	-772 %	-43,0
361^1	35	134	99	282,9 %
361^2	64	52	-12	-18,8 %
362	670	1070	400	59,7 %
363	6	12	6	100,0 %
363^2	3	10	7	233,3 %
Усього	2573	2301	-272	-10,6 %

Порівняно із 2017 р. кількість кримінальних правопорушень, передбачених статтями Розд. XVI КК України, зменшилася на 10,6 % (у 2017 р. – 2573). При цьому кількість кримінальних правопорушень, за якими особам вручено повідомлення про підозру, збільшилася на 26,4 % (1272 у 2017 р. проти 1608 у 2018 р.), зокрема передбачених ст. 362 КК України "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", на 58,2 % (607 у 2017 р. проти 960 у 2018 р.). Також збільшилася

кількість кримінальних правопорушень, за якими провадження направлені до суду з обвинувальним актом, – на 31,0 % (1015 у 2017 р. проти 1220 у 2018 р.). Спостерігається незначне (на 1,3 %) зменшення кількості тяжких кримінальних правопорушень – 1591 у 2017 р. проти 1270 у 2018 р. Збільшилася кількість майже всіх кримінальних правопорушень цієї категорії, крім передбачених ст. 361 КК України "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку", чисельність яких зменшилася на 772 кримінальні правопорушення, завдяки чому зменшилася кількість кримінальних правопорушень, передбачених статтями розд. XVI КК України. Водночас кількість кримінальних правопорушень, передбачених розділом XVI КК України, що вчинені групою осіб, за якими провадження направлено до суду, зросла на 4,8 % (42 у 2017 р. проти 44 у 2018 р.). На 45,9 % (142 у 2017 р. проти 771 у 2018 р.) зменшилася чисельність кримінальних правопорушень, щодо яких наприкінці 2018 р. рішення не прийнято (про закінчення або припинення).

Таблиця 2.2

Облікові у 2018 р. кримінальні правопорушення, передбачені статтями Розд. XVI КК України та ст. 362 КК України з наростаючим підсумком та помісячно [12]

Розділ XVI	**січ.**	**лют.**	**бер.**	**квіт.**	**трав.**	**черв.**	**лип.**	**серп.**	**вер.**	**жовт**	**лист.**	**груд.**
з наростаючим підсумком	272	597	982	1275	1487	1637	1726	1885	2017	2130	2245	2301
щомісячно	272	325	385	293	212	150	89	159	132	113	115	56
ст. 362												
з наростаючим підсумком	190	363	564	700	780	806	836	909	951	1027	1062	1070
щомісячно	190	173	201	136	80	26	30	73	42	76	35	8

Найбільшу частку правопорушень в зазначеній сфері становлять кримінальні правопорушення, передбачені ст. 362 КК України (47 %) та ст. 361 КК України КК України (44 %).

Із табл. 2.2. прослідковується, що найбільшу кількість кримінальних правопорушень було обліковано в березні – 385, найменшу – в грудні – 56, що майже в 7 разів менше. При цьому кримінальних правопорушень, передбачених ст. 362 КК України у грудні, обліковано у 25 разів менше порівняно з березнем (8 у грудні проти 201 у березні). Варто відзначити, що у січні 2019 року обліковано 218 кримінальних правопорушень, передбачених статтями Розд. XVI КК України, а передбачених ст. 362 КК України – 90. На час вчинення кримінального правопорушення 45 осіб були у віці від 18 до 28 років, 47 – від 29 до 39 років, 22 – від 40 до 54 років, 15 – 60 і більше років. Таким чином, за віковою ознакою неможливо виокремити якусь явну категорію правопорушників. Виявлено 42 жінки (30,9 %), що вчинили кримінальні правопорушення, тобто третина виявлених правопорушників – жінки. За освітою на час вчинення кримінального правопорушення найбільшу кількість становили особи з повною вищою і базовою вищою освітою – 77 (56,6 %), з професійно-технічною – 27 осіб, з повною загальною середньою та базовою загальною середньою освітою – 31 особа. Із 136 виявлених осіб, які вчинили правопорушення, передбачені Розд. XVI КК України, всі є громадянами України, майже половина осіб є працездатними, які не працювали і не навчалися, – 46 та 21 – безробітні, 8 учнів і студентів навчальних закладів. Групою осіб у 2018 році у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп’ютерних мереж і мереж електрозв'язку вчинено 44 кримінальних правопорушення, що становить 3,3 % від облікованих і на 4,8% більше порівняно з 2017 роком. Найбільше групою осіб вчинено кримінальних правопорушень, передбачених ст. 361 КК України, – 37. Розглянемо судову статистику. У судах першої інстанції у 2018 році перебували на розгляді 198 проваджень (справ) за статтями Розд. XVI КК України, з них 135 надійшли протягом року, що на 70,9 % більше у порівнянні з 2017 роком

(надійшло 79). У 2018 році розглянуто 96 проваджень, що майже у два рази більше ніж у 2017 році (50) [16].

З них 63 – із постановленням вироку, 23 із закриттям провадження у справі, 5 – повернуто прокурору. На кінець 2018 року залишилося 102 нерозгянутих провадження, що на 64,5 % більше у порівнянні з 2017 роком (62). Кількість осіб, провадження щодо яких перебували в суді, складала 224, що на 57,7 % більше у порівнянні з 2017 роком (142). Кількість осіб, судові рішення щодо яких набрали законної сили складає 70 (у 2017 році – 56), з них 49 осіб засуджено (70 %), 28,6 % (20) складають особи, матеріали кримінального провадження у відношенні яких закрито. Призначено покарання у вигляді позбавлення волі на певний строк 3 особам (у 2017 році – 7), 23 особи оштрафовано, 20 осіб звільнено від покарання з випробувальним строком і 3 унаслідок амністії. За сукупністю злочинів призначено покарання 15 особам. Найбільше засуджено осіб за статтею 361 КК України – 26. Варто вказати, що лише 4,3 % (3 з 70 осіб) становлять особи, яких позбавили волі на певний строк: понад 2 роки до 3 років включно – 1 і понад 3 років до 5 років включно – 2. Також слід відзначити, що всі із 49 засуджених осіб є громадянами України, кожен п’ятий із засуджених – жінки (10). Найбільше засуджених – це особи в віці від 30 до 50 років –18 (36,7 %), від 18 до 25 років – 30,6 % (15), від 25 до 30 років – 22,4 % (11). Більш повний аналіз стану кіберзлочинності можна зробити, використавши відомчу звітність Національної поліції України, зокрема Звіт про результати роботи підрозділів Національної поліції України за 2018 р [5]. Аналізуючи дані статистичних звітів, слід звертати увагу на можливі розбіжності між ідентичними показниками різних звітів. Як приклад, відповідно до статистичного звіту Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення), у 2018 р., обліковано 2241 кримінальне правопорушення у сфері використання електроннообчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку (Розд. XVI КК України), а у відомчому звіті Національної поліції України кількість вчинених кримінальних правопорушень, передбачених статтями Розд. XVI КК

України, становить 2374 (різниця – 133). При цьому, відповідно до звітності Генеральної прокуратури України, зменшення кількості облікованих кримінальних правопорушень порівняно з 2017 роком складає 10,94 %, а відповідно до звітності Національної поліції України – 2,9 % [8].

Також, зокрема за статистичним звітом Генеральної прокуратури України, обліковано 1007 кримінальних правопорушень, передбачених ст. 361 КК України, а у відомчому звіті Національної поліції України кількість вчинених кримінальних правопорушень, передбачених цією статтею, за цей же період становить 1108 (різниця – 101 кримінальне правопорушення). З порівняльного аналізу злочинів, учинених із використанням високих інформаційних технологій (за даними Національної поліції України), випливає, що кількість кримінальних правопорушень, вчинених у 2018 р., зменшилася на 14,0 % порівняно з 2017 р. (6974 у 2017 р. проти 6001 у 2018 р.). При цьому, варто зазначити, що на 22,4 % збільшилася кількість кримінальних правопорушень, досудове розслідування за якими не закінчено: з 4930 у 2017 р. до 6035 у 2018 р. [43]. Аналіз динаміки даного виду злочинності свідчить про те, що відбулося різке зниження кількості злочинів, передбачених чч. 3 і 4 ст. 190 КК України, – на 1200 (42,9 %) (2798 у 2017 р. проти 1598 у 2018 р.). На 10,8 % зменшилася чисельність крадіжок, вчинених із використанням електронно-обчислювальної техніки (860 у 2017 р. проти 767 у 2018 р.). Слід звернути увагу на значне (у 3,8 раза) збільшення кількості кримінальних правопорушень, передбачених ст. 231 КК України, – на 275,9 % (58 у 2017 р. проти 218 у 2018 р.). На 28,9 % збільшилася кількість злочинів, передбачених чч. 3, 4 і 5 ст. 301 КК України (463 у 2017 р. проти 597 у 2018). У 2 рази зросла чисельність злочинів, передбачених ст. 176 КК України (29 у 2017 р. проти 59 у 2018 р.).

В Україні серед злочинів, учинених із використанням високих інформаційних технологій у 2018 р., за даними Національної поліції, найбільшу питому вагу становлять кримінальні правопорушення, передбачені чч. 3 і 4 ст.

190 КК України – 27 %, ст. 361 КК України – 18 %, ст. 362 КК України – 17 %, чч. 3, 4 і 5 ст. 301 КК України – 10 %.

Таблиця 2.3

Обліковані кримінальні правопорушення, вчинені з використанням високих інформаційних технологій [7]

Статті КК України	**2017 р.**	**2018 р.**	**У порівнянні 2017 і 2018 рр.**	
			+/–	**%**
176	29	59	30	103,4 %
185	860	767	-93	-10,8 %
чч. 3 і 4 ст. 190 - -	2798	1598	1200	28,9 %
361	1618	1108		
361^1	28	142		
361^2	57	49		
362	729	1049		
363	11	15		
3631	2	11		
Розд. XVI -	2445	2374	71	-2,9 %
Усього	6974	6001	-973	-14,0 %

Пропорційно зменшенню кількості правопорушень, вчинених із використанням високих інформаційних технологій, зменшилася й чисельність осіб, яким повідомлено про підозру у вчиненні кримінального правопорушення (980 у 2017 р. проти 803 у 2018 р.), що становить 18,1 %. Також на 12,8% зменшилася кількість осіб, яким пред'явлені обвинувальні акти: з 764 у 2017 р. до 666 у 2018 р. Кіберзлочини вчиняють переважно індивідууми або невеликі злочинні групи хакерів. Працівники підрозділів кіберполіції Національної поліції України порівняно з попереднім періодом виявили на 4 організовані групи і злочинні організації більше (7 у 2017 р. проти 11 у 2018 р.). Вони вчинили 142 кримінальних правопорушень, з яких 140 – тяжкі. Найбільше – передбачених ст. 190 КК України (100), у сфері обігу наркотичних засобів,

психотропних речовин, їх аналогів або прекурсорів (7). У 2018 р. виявлено 196 фактів збуту наркотичних засобів, психотропних речовин або їх аналогів, а також отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів із використанням всесвітньої мережі Інтернет, що на 37,1 % більше порівняно з 2017 р. (143), і в 7,5 рази порівняно з 2016 р. (26). При цьому, варто відзначити, що у ЗМІ ці показники подаються як кількість виявлених груп, які збували наркотичні засоби з використанням Інтернету [7]. У сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку організованими групами вчинено 9 кримінальних правопорушень: із них 6 – виявили працівники підрозділів кіберполіції, 3 – підрозділів захисту економіки. Виявлено 41 особу, яка вчинила кримінальні правопорушення у складі ОГ і ЗО, що на 51,9 % більше порівняно з 2017 р. (27 осіб). Слід зазначити, що у 2018 р. 72 кримінальних правопорушення у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виявили працівники підрозділів карного розшуку (проти 163 у 2017 р.). У 2018 р. кримінальними правопорушеннями, вчиненими з використанням високих інформаційних технологій, завдано матеріальних збитків на суму 38 713 тис. грн.., що на 51 674 тис. грн./ менше, ніж у попередньому періоді (90387 тис. грн). При цьому у 2017 р. відшкодовано (з урахуванням накладеного арешту та вилученого майна) 71,8 % коштів, а у 2018 р. – лише 57,2 %. У 2018 р. найбільших матеріальних збитків завдано шахрайством – 21 194 тис. грн, при цьому відшкодовано лише 53,1 % (11 250 тис. грн) [16].

У 2018 р. збільшення кількості кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій, відзначалося у 8 областях. Найбільше зростання відбулося в Миколаївській (106,9%), Рівненській (93,5%), Харківській (85,5%) областях (табл. 2.4).

Найбільше кримінальних правопорушень вчинено в м. Києві (845), Миколаївській (776), Одеській (647) та Львівській (591) областях, найменше – у Волинській області (51). Рівень кіберзлочинності в Україні на 10 000 населення

невисокий і у 2018 р. складав 2,1 проти 2,4 у 2017 р. При підрахунку використовувалися показники Державної служби статистики України, зокрема статистичного збірника “Розподіл постійного населення України за статтю та віком (на 1 січня 2018 року) ”. Вікова категорія населення складала 15 – 64 років. У 5 областях України рівень злочинності на 10 000 населення вищий ніж загалом по Україні. Найвищий – у Миколаївській області – 10,0 [5].

Таблиця 2.4.

Найбільше зростання і найбільше зменшення кількості вчинених кримінальних правопорушень, вчинених з використанням високих інформаційних технологій [5]

	2017	**2018**	**+ /-**	**%**
Миколаївська	375	776	401	106,9 %
Рівненська	77	149	72	93,5 %
Харківська	117	217	100	85,5%
Полтавська	94	145	51	54,3 %
Вінницька	122	149	27	22,1 %
Івано-Франківська	235	122	-113	-48,1 %
Чернівецька	298	125	-173	-58,1 %
Волинська %	133	51	-82	-61,7
Кіровоградська	252	94	158	-62,7 %

Дещо нижчий – у м. Києві (4,2), Одеській (4,0), Львівській (3,4) та Черкаській областях. Найнижчий у Закарпатській, Волинській та Донецькій (3,1) областях менше 1.

Найбільше злочинів, передбачених чч. 3 і 4 ст. 190 КК України, вчинено в Одеській (280), Дніпропетровській (191), Луганській (174), Харківській (149) областях; крадіжок із використанням електронно-обчислювальної техніки – в Миколаївській області (145), м. Києві (112), Дніпропетровській і Сумській областях (81 і 73 відповідно); передбачених чч. 3, 4 і 5 ст. 301 КК України – у м.

Києві (299), Івано-Франківській (82) та Донецькій (55) областях; несанкціонованих втручань у роботу електроннообчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, відповідальність за які передбачена ст. 361 КК України – в Одеській (141), Львівській (140), Миколаївській (126) областях; у Миколаївській області – злочинів, передбачених ст. 362 КК України – 241, в Одеській області – 207, в м. Києві – 125. Варто звернути увагу на деякі особливості вчинення кримінальних правопорушень за регіонами. Так, у Львівській області – 34 з 59 вчинених по Україні кримінальних правопорушень, передбачених ст. 176 КК України, що становить 57,6 %. 36,3 % кримінальних правопорушень, передбачених ст. 200 КК України, вчинено в м. Києві (132 із 364). Кримінальні правопорушення, передбачені ст. 231 КК України, мали місце лише в Миколаївській (117) і Львівській (101) областях. У м. Києві вчинено 50,1 % кримінальних правопорушень, передбачених ст. 301 КК України (299 із 597). У Запорізькій області вчинено 8 із 11 кримінальних правопорушень, передбачених ст. 3631 КК України. Висновки. Дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів. Згадані вище звіти розроблені без врахування подальшого аналізу кіберзлочинності [7]. І якщо у звіті Національної поліції України містяться дані про певну кількість злочинів, які можна віднести до кіберзлочинів, в офіційних статистичних звітах, крім Розділу XVI КК України, такі показники відсутні. Тож, про офіційну статистику, яка повно й достовірно відображає стан і структуру кіберзлочинності, сьогодні говорити проблематично. Можливо проаналізувати тільки динаміку цього виду злочинності, структуру злочинності на основі облікованих злочинів. Вказане може свідчити про необхідність визначення критеріїв щодо віднесення кримінальних правопорушень до категорії кіберзлочинів із подальшою розробкою статистичної звітності про зареєстровані кіберзлочини, про осіб, які їх вчинили, та результати боротьби з кіберзлочинністю.

2.2. Універсальні інструменти правового регулювання боротьби з кіберзлочинністю

Законодавство Європейського Союзу у сфері інформаційної безпеки розвивалося у руслі міжнародних ініціатив Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку, Організації Об'єднаних Націй. Законодавчі заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програм Європейського Союзу – «Безпечний Інтернет» (1999-2004 рр.), «Безпечний Інтернет Плюс» (2005– 2008 рр.), «Безпечний Інтернет 2009-2013 рр.», прийнятих рішеннями Європейського Парламенту і Ради, і переважно були спрямовані на захист персональних даних, сприяння безпечному користуванню Інтернетом, формуванню сприятливого середовища для розвитку європейської Інтернетіндустрії, захист дітей, що користуються Інтернетом і новими 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 [21].

Провідне місце серед відповідної групи міжнародно-правових документів відведено Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року (Будапешт) [99]. Наша країна ратифікувала цю Конвенцію 7 вересня 2005 року. На сьогодні це один з найважливіших документів, які регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний

документ такого рівня [19]. Нею на держави покладаються зобов'язання щодо вживання законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за злочини в кіберпросторі.

Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги, зокрема відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації, так всі злочини в кіберпросторі вона поділяє на 4 групи:

1) у першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в ст.ст. 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

2) до другої групи входять злочини, пов'язані з використанням комп'ютерних засобів: підлог і шахрайство з використанням комп'ютерних технологій (ст. 7, 8 Конвенцій).

3) третю групу складають злочини, пов'язані з контентом (змістом) даних.

4) до четвертої групи увійшли порушення авторського права і суміжних прав [19]. На початку 2002 року до Конвенції ухвалили протокол, що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Другий розділ Конвенції освітлює процесуальні аспекти боротьби з кіберзлочинністю. Конвенція пропонує традиційне рішення проблеми юрисдикції: карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави). Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином (підданим) 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 уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування [19]. Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, рахом з тим, й вона не позбавлена недоліків.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі [19]. Прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується, навіть ті країни, які з якихнебудь причин не підписали Конвенцію можуть використовувати досвід, що

накопичується, по правовому регулюванню нової предметної області – кіберпростір.

Отже, Конвенція про кіберзлочинність є одним із найважливіших документів у сфері глобальної комп'ютерної мережі, роль якої у регулюванні боротьби з кіберзлочинністю у державах всього світу є вирішальною. Щодо України, значення даного міжнародного нормативно-правового акту можна виразити наступним чином. По-перше, Конвенцією здійснено розмежування кіберзлочинів залежно від об'єкта посягання на 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, 2) правопорушення, пов'язані з комп'ютерами, 3) правопорушення, пов'язані зі змістом, 4) правопорушення, пов'язані з порушенням авторських та суміжних прав. Схожим чином, класифікують такі правопорушення і у національних законодавствах країн-учасниць, зокрема в Розділі XVI Кримінального кодексу України [13]. По-друге, Конвенцією регламентовано процедурні аспекти, такі як умови, запобіжні заходи, обшук і арешт комп'ютерних даних, які зберігаються, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації, юрисдикція тощо. Така систематизація значним чином полегшує діяльність правоохоронних органів держави. По-третє, даним документом встановлено принципи співробітництва країн-учасниць у сфері боротьби з кіберзлочинністю, зокрема – екстрадиції та взаємодопомоги. Відзначимо, що реалізація цього аспекту здійснюється шляхом укладення державами двосторонніх угод. Як вже засвідчив їх аналіз, на практиці Україна надає перевагу реалізації принципу взаємодопомоги. По-четверте, Конвенція надає право учасникам здійснювати доступ до публічно доступних комп'ютерних даних, які зберігаються, не отримуючи дозволу від іншої сторони, що значним чином полегшує розслідування злочинів та дозволяє уникати надмірного затягування оперативно-розшукової діяльності.

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 [13]. 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.

Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40] не є нормативно-правовим актом, яким безпосередньо врегульовується питання боротьби із кіберзлочинністю. Проте, комп'ютерна злочинність переважно має транснаціональний характер, є організованою та може набувати ознак тероризму. А отже, прийняття Конвенції, спрямованої на попередження та боротьбу із даними видами злочинних діянь є важливим інструментом у боротьбі з кіберзлочинністю. Конвенцією Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40] запропоновано ухвалення законодавчих та інших заходів, спрямованих на заходи проти корупції і відповідальності юридичних осіб за участь останніх у серйозних злочинах, до яких причетна організована злочинність; заходи які можуть забезпечувати можливості конфіскації та арешту доходів від злочинів і розпорядження конфіскованими доходами від злочинів тощо. С. А. Шепетько в

даному контексті зазначає, що норми Конвенції не застосовуються щодо правопорушень, які не відносяться до організованої злочинності, розглядаючи, як виняток, лише окремі сфери – особливо комп'ютерних правопорушень, оскільки дана проблема потребує більшої уваги з боку міжнародної спільноти [10]. Тобто, у разі якщо кіберзлочин має транснаціональний характер, а саме, планується чи вчиняється в кількох державах, або вчиняється в одній державі, а має істотні наслідки в іншій, можуть бути застосовані норми Конвенції.

Варто відзначити, що загальна кількість міжнародних договорів у сфері співробітництва у кримінальних справах є значною. Ще з моменту проголошення незалежності, Україна активно укладала подібні угоди і на сьогодні співпрацює з кількома десятками держав різних континентів. Проте, більшість із них ніяким чином не регламентують співпрацю у сфері боротьби з кіберзлочинністю, що у цілому не виключає такої можливості у разі виникнення необхідності. Наприклад, Угода між Кабінетом Міністрів України і Урядом Турецької Республіки про співробітництво передбачає надання взаємної допомоги в попередженні й розкритті кіберзлочинів [10]. Це означає, що у разі виникнення такої необхідності правоохоронні органи обох держав зобов'язані всебічно та двосторонньо сприяти діяльності один одному. Для порівняння аналогічна угода із Сполученими Штатами Америки взагалі не містить посилання на сфери співпраці, обмежуючись формулюванням «взаємна допомога у розслідуванні, переслідуванні та запобіганні злочинам, а також у судовому розгляді кримінальних справ» [10]. Це свідчить про те, що конкретна співпраця у сфері боротьби із кіберзлочинністю не передбачена, проте і не виключена у разі виникнення таких проблемних питань. Також відмітимо наявність міждержавних угод Генеральної прокуратури України із головними органами прокуратури інших держав. Зокрема, в 2015 році було укладено Угоду про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія у боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом [18]. Подібні угоди були укладені зокрема і з Національною прокуратурою

Королівства Нідерланди [10] та державами пострадянського простору. Текст кожного з договорів фактично є тотожним – сторони беруть на себе зобов'язання здійснювати співробітництво в сфері боротьби з кіберзлочинністю шляхом обміну інформацією і документами стосовно таких злочинів. Не зважаючи на дещо усічений перелік напрямів співробітництва, значення таких угод варто виразити наступним чином: 1) Україну як порівняно новоутвореного суб'єкта міжнародних відносин поступово залучають до міждержавних процесів; 2) ураховуючи специфіку злочинності у кіберпросторі, нашій державі гарантована допомога у разі виникнення такої необхідності; 3) іноземні держави вважають вітчизняні правоохоронні органи такими, що можуть посприяти вирішенню їх внутрішніх проблем. Разом з тим, сама сфера реалізації таких угод потребує розширення. Аналіз їх змісту засвідчив, що основною формою співробітництва є надсилання запитів про інформацію. В умовах швидкості вчинення кіберзлочинів даний інструмент може бути неефективним, адже потребує значної кількості часу. А отже, порядок укладення Україною міжнародних угод у сфері взаємної правової допомоги в розслідуванні кіберзлочинів також потребує подальшого удосконалення.

Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації від 1 червня 2001 року [44] покладає на держави зобов'язання щодо визнання у відповідності з національним законодавством в якості кримінальних злочинів:

1) здійснення неправомірного доступу до комп'ютерної інформації, що охороняється законом, якщо це потягло знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхньої мережі;

2) створення, використання або поширення шкідливих програм;

3) порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі особою, що має доступ до ЕОМ, системи ЕОМ або їхньої мережі, що потягло знищення, блокування або модифікацію інформації ЕОМ, що охороняється законом, якщо це спричинило суттєву шкоду або тяжкі наслідки;

4) протизаконне використання програм для ЕОМ та баз даних, що є об’єктами авторського права, так само як і присвоєння авторства [44]. Однак для повноцінної реалізації відповідних завдань необхідно було узгодити чіткий перелік відповідних злочинних діянь та покарання за них. На практиці не всі держави, які є учасницями СНД реалізували відповідні завдання, що суттєво знижує протидію інформаційній злочинності, яка потребує комплексного транснаціонального співробітництва.

В Угоді між урядами держав-членів Шанхайської організації співробітництва про співробітництво в області забезпечення міжнародної інформаційної безпеки, прийнятій 16 червня 2009 року [10], питання інформаційної злочинності розглянуто в загальному контексті з основними напрямами, принципами, формами і механізмами міжнародного співробітництва. Варто зазначити, що на відміну від попередніх,Угода передбачає новий концептуальний підхід до питань забезпечення міжнародної інформаційної безпеки. Його суть полягає у комплексному забезпеченні міжнародної інформаційної безпеки держав від усіх інформаційних загроз, що можуть бути спричинені злочинним використанням ІКТ. Виходячи з цих позицій, інформаційна злочинність, разом із п’ятьма іншими, визнана сторонами Угоди в якості основної загрози в області забезпечення міжнародної інформаційної безпеки. Джерелом цієї загрози, відповідно до Угоди, є особи або організації, що здійснюють неправомірне використання інформаційних ресурсів або несанкціоноване втручання в такі ресурси у злочинних цілях [10].

З метою протидії інформаційній злочинності, сторони Угоди погодились співробітничати і проводити свою діяльність у інформаційному просторі таким чином, щоб така діяльність сприяла соціальному і економічному розвитку і була сумісною з задачами підтримки міжнародної безпеки і стабільності, відповідала загальновизнаним принципам міжнародного права. Така діяльність повинна бути сумісною з правом кожної сторони Угоди шукати, отримувати і поширювати інформацію з урахуванням можливих обмежень з причин захисту інтересів національної та суспільної безпеки (ст. 4). Сторони визнали право на

захист інформаційних ресурсів і критично важливих структур від неправомірного використання і несанкціонованого втручання, погодились не проводити одна проти одної подібних дій та сприяти одна одній в реалізації цього права [10]. Істотним недоліком відповідного міжнародно-правового документу було те, що не зважаючи на декларування необхідності боротьби з кіберзлочинністю, він не містить реальних заходів. Тобто відсутні зобов'язання держав-учасниць внести зміни в національне законодавство, які би сприяли реальній протидії інформаційний злочинам. Сутність відповідного документу зводиться до характеристик загроз інформаційних злочинів, необхідності консолідації зусиль держав тощо.

В рамках Азійсько-Тихоокеанської економічної співдружності у 2002 році була прийнята «Стратегія кібербезпеки АТЕС», передбачається прийняття зводу законів щодо кібербезпеки та кіберзлочинності, а також створення національних підрозділів з кіберзлочинності та центрів технологічної допомоги. Ліги арабських держав і Організації американських держав розвивають співробітництво у боротьбі із комп'ютерними злочинами з урахуванням рекомендацій ООН, МСЕ, Ради Європи.

Діяльність Організації економічного співробітництва і розвитку, розпочата за тематикою комп'ютерної злочинності ще 1983 року, спрямовується на проведені досліджень, пов'язаних із можливістю гармонізації кримінального законодавства щодо комп'ютерних злочинів. У 1992 році радою ОЕСР було прийнято «Керівні принципи з інформаційної безпеки». У 2002 році нова версія принципів «Керівні принципи ОЕСР із забезпечення безпеки інформаційних систем і мереж: до культури безпеки» була рекомендована Радою ОЕСР. Останні доповіді були присвячені темам боротьби зі спамом (2005 рік), та законодавчих рішень держав щодо проблеми кібертероризму (2007 рік).

Особливостями регіонального міжнародно-правового регулювання протидії кіберзлочинності можна визначити таке: 1) значна увага з боку різноманітних регіональних міжнародних організацій до питань протидії

кіберзлочинам; 2) розробка численних регіональних угод про співробітництво у сфері протидії інформаційним злочинам; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. – на початку 2000-х рр.; 4) така діяльність є складовою частиною як міжнародних інформаційних відносин, так і кримінального судочинства.

Проведене доктринальне дослідження дає підстави стверджувати, що для створення умов щодо належної й ефективної діяльності по протидії кіберзлочинності недостатньо ресурсів одного правоохоронного орану або правоохоронних оранні певної держави. Така діяльність повинна мати комплексний характер й передбачати участь багатьох країн, що вимагає необхідного нормативно-правового базису на міжнародному рівні. На сьогодні відбуваються дії стосовно встановлення засад міжнародної співпраці у сфері протидії кіберзлочинності у рамках як універсальних, так і регіональних договорів. Разом з тим, таких заходів для повноцінної діяльності недостатньо, що вимагає пожвавлення діяльності з боку кожного суб’єкта міжнародного співтовариства з метою створення дієвого механізму міжнародно-правового регулювання протидії кіберзлочинності.

2.3. Легалізація доходів, одержаних у сфері кіберзлочинності

Під приводом "традиційно" відмивання грошей, для якого використовується банківська система, вбивство базується на використанні різних видів операцій та постачальників фінансових послуг, починаючи з банківських переказів, депонування / вилучення готівки, використання електронних грошей, і закінчуючи "грошовими мулами" та послугами від грошових переказів. Тож правило, ланцюжок перериваєтся касовими операціями, які зазвичай здійснюються за допомогою "грошових мулів", за якими слідує використання традиційної платіжної системи. Якщо відповідна

платіжна послуга інтегрована з послугами онлайн-платежів, гроші можуть бути переведені на електронну та без затримки, майже анонімно переведені в іншу державу. Таким чином, виявлення та переслідування злочинних грошових потоків є надзвичайно складним завданням для правоохоронних органів. Такі заплутані схеми є викликом потужному, але традиційному збиранню даних про відмивання коштів та фінансуванню тероризму, що базується на поведінці клієнтів, якщо частина "відмивання" ланцюга здійснюється повністю в іншому фінансовому становищі. Методи здійснення платежів в Інтернеті також можуть розділити джерело, звідки було отримано інструкції щодо здійснення операцій з фактичного місця переказу коштів. Це ще одна перешкода для правоохоронних органів у виявленні та переслідуванні злочинних доходів.

Основні механізми легалізації злочинних доходів від злочину зароблені гроші вимагають від злочинців оперативно та ефективно здійснювати легалізацію. Більше того, через специфіку кіберзлочинності організатори та виконавці схем переважно освічені та технічно компетентні, відповідно, методи, використані ними для легалізації отриманих коштів, також можуть бути досить складними та нестандартними. Інструменти та механізми, що використовуються злочинцями для відмивання надходжень від кіберзлочинів, досить різноманітні, зокрема, характерні для відмивання доходів від кіберзлочинів такі механізми:

- користування рахунками, відкритими особами за втрачені документи;
- використання альтернативних платіжних систем (електронних платежів), як національних, так і міжнародних;
- ведення ланцюга фінансових операцій через декілька банківських рахунків за допомогою віддаленого доступу;
- користування грошовими коштами на останньому етапі фінансової операції;
- придбання електронних грошей та використання платіжних систем через електронні гаманці;

– перетворення незаконних доходів на товари через придбання останнього через Інтернет [2].

Введення вкрадених коштів у грошові кошти широко поширене, оскільки подальше рух грошових коштів поза банківською системою практично неможливо відслідковувати. Широке практикується виведення грошових коштів через банкомати, щоб уникнути участі учасників з працівниками банківських установ. Надала готівкові кошти через кур'єрів (грошові мули) можуть бути вільно передані анонімному організатору кіберзлочинів. Виловлені злочинними доходами використовуються для придбання високоліквідних товарів або передплаченого карток для їх перепродажу та зняття готівки. Крім того, кошти можуть бути використані для придбання інтернет-квитків, проїзних документів, товарів для дому та інших товарів для подальшого використання, перепродажу та зняття готівки. Частину доходів, одержаних злочинним шляхом, використовується для придбання нового обладнання та розробки більш ефективної шкідливої програму для обходу безпеки. Слід також зазначити, що підставами платежів, пов'язаними з несанкціонованим списанням коштів, можуть бути різні призначення, які не дозволяють їм розділяти їх від інших фінансових операцій:

– оплата за ТМК (обладнання, пристрої, нафтопродукти, обладнання, будівельні матеріали, побутові товари, офісні меблі, соняшник, соняшникова олія);
– оплата послуг (рекламні та поліграфічні послуги, роботи з контролю якості продукції, експедирування вантажів, перевезення вантажів, спортивні заходи);
– оплата за контрактом;
– надання / повернення фінансової допомоги (позики);
– поповнення карткового рахунку;
– виплата заробітної плати або заробітної плати;
– оплата за рішенням суду;
– повернення гарантійного платежу покупцеві за контрактом.

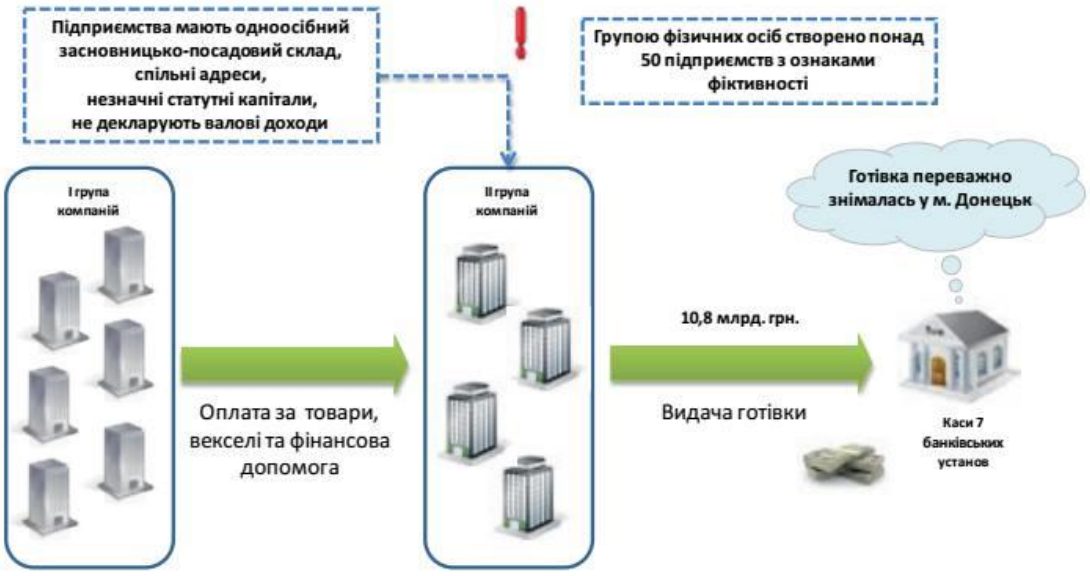

Рис. 2.1. Схема легалізації коштів від кіберзлочинів [12]

У той же час іноді злочинці вказали підстави для здійснення іноземних грошових переказів та сумнівних призначень, зокрема виграшів у казино, продажу об'єктів права інтелектуальної власності, веб-сайти або інтернет-магазини, віртуальні казино та ін

З метою швидкого переказу коштів, отриманих у сфері кіберзлочинності, злочинцям широко використовується можливість використання платіжних систем або систем передачі.

Українське законодавство передбачає функціонування внутрішніх та міжнародних платіжних систем в Україні. Внутрішня платіжна система – це платіжна система, в якій платіжна організація є резидентом та здійснює свою діяльність та забезпечує переказ коштів виключно в межах України. Міжнародна платіжна система – це платіжна система, в якій платіжна організація може бути як резидентом, так і нерезидентом і працює на території двох або більше країн, і передбачає переказ коштів в рамках цієї платіжної системи, в тому числі з однієї країни до іншої . За даними Національного банку України, станом на 01.07.2017 на території України на території України було здійснено дев'ять внутрішніх та міжнародних систем грошових переказів, створені резидентами України, з яких п'ять систем були введені банки та чотири системи були впроваджені небанківськими установами України. Є

також 22 системи міжнародних грошових переказів, встановлені нерезидентами на території України. Учасниками таких систем є понад 150 банків України, ПАТ "Українська фінансова група" та національний поштовий оператор "УкрПост". У першій половині 2017 р. З використанням внутрішніх та міжнародних трансферних систем фондів, створених як резидентами, так і нерезидентами, було перевизначено:

-в межах України – 7 915,0 млн. Грн. і 4,5 млн. дол США (в еквіваленті);

- в Україні – 2 203,0 млн. грн. США (в еквіваленті);

- за межами України – 384,0 млн. грн. США (в еквіваленті) [16].

Платіжні системи мають ряд незаперечних переваг, які також визначають їх стрімкий розвиток, а саме:

Доступність – відкриття власного електронного рахунку є безкоштовним для будь-якого користувача;

простота використання – відкриття та використання електронного рахунку є інтуїтивно зрозумілим і не вимагає спеціальних знань;

мобільність – користувач через Інтернет може керувати своїм рахунком з будь-якого місця;

ефективність – операції з рахунками відбуваються протягом декількох секунд;

безпека – передача інформації здійснюється за допомогою криптографічного захисту [3].

Щоб стати учасником та користуватися послугами платіжної системи, вам потрібно пройти процес реєстрації та відкрити в ньому електронний рахунок як електронний гаманець. Електронний кошель зберігає інформацію про суму коштів на рахунку користувача в платіжній системі. Для фінансових операцій необхідно ввести гроші в платіжну систему, тобто поповнити електронний рахунок. Різні платіжні системи пропонують різні способи поповнення електронних гаманців. Це може бути банківський переказ, поштове замовлення, придбання передплаченої картки, поповнення через термінал платежу тощо. Крім того, грошові перекази між учасниками схеми можуть

використовуватися для термінових переказів через системи міжнародних грошових переказів. Механізм таких переказів досить простий і зручний. Для цього до відділу системи або його партнера звертається особа (яка потребує документа, що посвідчує особу), яка робить необхідні кошти та заповнює форму з ім'ям бенефіціара та країни походження переказу. У майбутньому оператор отримає номер передачі, який повинен бути повідомлений одержувачу. Бенефіціар (із документом, що посвідчує особу) поширюється на філію системи або її партнера та заповнює форму видачі готівки з номером переказу, прізвищем та ім'ям відправника, країною переказу, сумою та валютою від переказу. Трансфери та зняття готівкових коштів займає всього кілька хвилин [8].

Використання електронних грошей для відмивання грошей. Відповідно до законодавства України електронні гроші є одиницею вартості, що зберігається на електронному пристрої, приймається як спосіб оплати особами, які не є емітентом, і є грошовим зобов'язанням емітента. Тільки банки (емітенти) мають право випускати електронні гроші в Україні. Емітенти мають право випускати електронні гроші, виражені в гривнях. Сума електронних грошей на електронному пристрої, яка не може бути поповнена, не повинна перевищувати 2 тис. грн. Сума електронних грошей на електронному пристрої, яку можна поповнити, не повинна перевищувати 8 тис. грн. Погашення електронних грошей, принесених користувачами – фізичними особами, можна здійснити готівкою або шляхом перерахування на банківський рахунок носія. Погашення електронних грошей, принесених користувачами – суб'єктами господарської діяльності, дилерами, агентами, емітент зобов'язаний здійснювати виключно шляхом перерахування на їхні банківські рахунки. За допомогою електронних грошей ви можете здійснити такі платежі:

- платежі в середині системи на рахунки фізичних та юридичних осіб;
- оплата товарів в інтернет-магазинах;
- оплата послуг мобільних операторів;

- оплата комунальних послуг;
- оплата інтернет-послуг;
- сплата державних зборів, мита та штрафів;
- придбання залізничних / авіаквитків;
- Закупівля палива та замовлення скретч-карт для палива;
- бронювання готелів та інше [1].

Для злочинців безсумнівною перевагою використання електронних грошей є можливість анонімного відкриття та поповнення електронних гаманців, а також цілодобової доступності та швидкості операцій (протягом декількох секунд). Електронний гаманець фізичної особи найчастіше має легкість посилання на майже або номер мобільного телефону.

Висновки до розділу 2

Відповідно до проведеного у другому розділі дослідження аналізу кримінальних доходів та схем легалізації злочинних надходжень можемо зробити такі висновки та узагальнення:

По-перше, у магістерській роботі встановлено, що стосовно до структури досліджуваного злочину найбільша частка (40-60% від усіх зареєстрованих злочинів у цій сфері) є діями, пов'язаними з несанкціонованим втручанням у роботу електронних комп'ютерів (комп'ютерів), автоматизованих систем, комп'ютерних мереж або телекомунікаційних мереж що призвело до витоку, втрати, втручання, блокування інформації, викривлення обробки інформації або порушення встановленого порядку його маршрутизації (стаття 361 Кримінального кодексу України) та дій, передбачених ст. 362 КК України, а саме: несанкціоновані дії з інформацією, яка обробляється на електронних комп'ютерах (комп'ютерах), автоматизованих системах, комп'ютерних мережах

або зберігається на носіях такої інформації, вчинених особою, яка має право на це (25 - 45%).

По-друге, в системі даного дослідження кіберзлочинність – шахрайство з використанням комп'ютерів, комп'ютерних мереж, включаючи використання Інтернету. Слід зазначити, що в сучасних умовах значна частина традиційного бізнесу йде в віртуальне середовище, що пояснюється швидким розвитком Інтернету. Це, зокрема, стосується розміщення в Інтернеті реклами товарів та послуг та Інтернет-торгівлі, що є досить широким поширенням в Україні та, у певних сферах, являє собою значну конкуренцію з традиційною торгівлею. Шахраї також використовують сучасні засоби для доступу до Інтернету.

По-третє, основні механізми легалізації злочинних доходів, одержаних злочинним шляхом, вимагають від злочинців швидкого та ефективного їх легалізації. Більше того, через специфіку кіберзлочинності організатори та виконавці схем переважно освічені та технічно компетентні, відповідно, методи, використані ними для легалізації отриманих коштів, також можуть бути досить складними та нестандартними.

РОЗДІЛ 3
ОПТИМІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ ТА СВІТІ

3.1.Особливості боротьби з кіберзлочинністю у міжнародному вимірі

Масштабність Інтернету вказує на те, що певні елементи кіберзлочинності не можуть бути обмежені лише територією певної країни, тому в будь-якому випадку національне законодавство повинне відповідати загальновизнаним стандартам у цій галузі, щоб мати можливість продовжувати міжнародне співробітництво. Більше того, процес встановлення системи правового регулювання боротьби з кіберзлочинністю неможливий без урахування досягнень та помилок, допущених іноземними державами при формуванні цього інституту. Розвиток правового регулювання проти кіберзлочинності в Україні знаходиться на активному етапі протягом останніх двох десятиліть. У багатьох зарубіжних країнах ця система працює давно і дала позитивні результати, хоча кіберзлочинність все ще випереджає рівень розвитку інструментів протидії їй. Тому, аналізуючи сучасні вітчизняні реалії, ми можемо відзначити незавершеність цього процесу в Україні та необхідність подальших трансформацій. За таких умов актуальними стають питання позитивного та негативного досвіду інших держав, що є дуже відповідним вектором розвитку науково-дослідного інституту [21].

Почнемо з досвіду Сполучених Штатів Америки як держави, яка зазнала негативного впливу кіберзлочинців і є однією з перших в історії, яка розробила відповідні норми. Серед норм Національної стратегії національної безпеки США, прийнятих у 2015 році, особливий інтерес представляє розділ Кібербезпека, який підкреслює необхідність захисту від кібератак у кіберпросторі. Сполучені Штати Америки, проголосивши себе батьківщиною Інтернету, взяли на себе відповідальність за весь інтернет-світ за кібербезпеку. Крім того, було оголошено курс на зміцнення законодавчої бази та підвищення

стандартів захисту прав та інтересів громадян [11]. Тому Сполучені Штати Америки є однією з провідних країн-дослідників у галузі досвіду. У цій країні триває активна діяльність з протидії таким негативним явищам, як кіберзлочинність, і багато уваги приділяється безпеці громадян в цілому. США є однією з головних мішеней кіберзлочинців у всьому світі, тому досвід цієї країни корисний для розробки правових інструментів протидії цьому негативному явищу. Незважаючи на вищесказане, в Сполучених Штатах Америки переважає концепція саморегуляції Інтернету, а тому спеціальне законодавство у цій галузі представлено лише кількома регуляторними актами. Наприклад, до них належить Закон про електронний підпис, прийнятий у 2000 році [19]. Основна його мета – забезпечити правовий режим електронного підпису в комерційних відносинах. У Сполучених Штатах Америки прийнято давати цьому регламенту символ вступу людства в нову еру - еру електронної комерції. Тому слід зробити висновок, що боротьба з кіберзлочинністю повинна бути складною, а відповідне галузеве законодавство - лише один елемент. Найбільша кількість нормативно-правових актів прийнята у сфері випуску цінних паперів, захисту інтелектуальної власності, захисту від несанкціонованого доступу до інформації, авторських прав тощо [11]. Загалом, до недавнього часу американські юристи дотримувались думки, що для регулювання кіберзлочинності важливіші міждержавні, а не національні норми, оскільки накладення певних обмежень на один суб'єкт господарювання може негативно впливати на інтереси інших сторін [5]. Однак теракти 11 вересня 2001 року суттєво посилили боротьбу з тероризмом, однією з яких є кібертероризм. В тому ж році урядом США було прийнято Закон «Про об’єднання та зміцнення США», згідно норм якого будь-яка дія, яка спричиняє порушення в роботі чи призводить до незаконного проникнення в комп’ютер, класифікується як тероризм. В свою чергу провайдер зобов’язаний надати всю відому йому інформацію про користувача на першу вимогу Федерального бюро розслідувань [15]. Таким чином, на сьогоднішній день вектор правового регулювання боротьби з кіберзлочинністю асоціюється з протидією

кібертероризму як найнебезпечнішому прояву кіберзлочинності. Деструктивна діяльність в кіберпросторі США санкціонується набагато суворіше, ніж у Європі. Наприклад, у США кримінальна відповідальність за неналежне зберігання та обробку особистої інформації або знищення особистої інформації іншим чином, ніж передбачено законодавством. Для порівняння, у країнах Європейського Союзу кримінальні справи можуть бути порушені лише у випадку шкоди національній безпеці та основним правам громадян [15]. Це вказує на те, що соціальний аспект правового регулювання кіберзлочинності в США не нехтується, оскільки він має велике значення не лише для захисту державних інтересів, але і для кожної людини. Тому дослідження сучасного стану боротьби з кіберзлочинністю показали, що ця сфера є одним із пріоритетів державної політики США. Позитивними тенденціями є активна боротьба з кібертероризмом та оперативність заходів щодо вирішення існуючих проблем. Негативні відповіді - це насамперед відповідь на загрози лише в тому випадку, коли вони виникають, але в той же час США залишаються однією з найбільш захищених країн світу. У контексті боротьби з кіберзлочинністю важливо проаналізувати нормативно-правові акти, які закріплюють повноваження органів державної влади та правоохоронних органів щодо протидії кіберзлочинності. У 2009 році Сенат США зареєстрував Закон про кібербезпеку 2009 року [15], розроблений Національним агентством розвідки США, в якому пропонувалося значно розширити федеральну владу в галузі кібербезпеки та призначити її користувачем кіберпростору в інтересах національної безпеки. Цей законопроект, якщо його буде прийнято, може мати суттєвий вплив на суть сьогоднішнього Інтернету, оскільки він мав на меті встановити нові стандарти комп'ютерної безпеки, зокрема шляхом встановлення стандартів, які вимагатимуть від користувачів обов'язкової ідентифікації та згоди на легітимний уряд. Причини перевірки вмісту електронних листів, завантажених файлів, пошуку користувачів кіберпростору тощо [15]. Крім того, звертається увага на систему органів влади, що борються з кіберзлочинністю: 1) Кіберкомандування США (USCYBERCOM) - підрозділ

Збройних сил США, основними завданнями якого є централізоване ведення операцій з кібервійни, управління та захист військова комп'ютерна мережа США 2) Команда з готовності до надзвичайних ситуацій США (CERT) США - частина національного відділу кібербезпеки Міністерства національної безпеки США, яка оприлюднює інформацію про поточні проблеми безпеки, вразливі до кібератак, і працює з постачальниками програмного забезпечення, що надають програмне забезпечення для створення спеціальних програмних програм, що усувають прогалини в безпеці; 3) Відділ комп'ютерної злочинності та інтелектуальної власності (CCIPS), відділ кримінального розслідування та інтелектуальної власності Міністерства юстиції США, що спеціалізується на галузі пошуку та захоплення цифрових доказів, комп'ютерів та мереж [15].

Для того, щоб в Україні на сьогоднішній день існував той самий орган, - Департамент кіберполіції Національної поліції України, який намагається відійти від кіберзлочинності, повинен бути представлений у правоохоронному просторі, і сьогодні він є недоступним. У США таких рівнів троє - найважливіші, правоохоронніші та юстиційні, при яких існують ті, хто має особливі особливості. Тому, ми маємо на увазі боротьбу із кіберзлочинністю, що досягає ефективних результатів.

Право регулювання боротьби із кіберзлочинністю у європейському Союзі проводиться наступними ознаками: 1) використання як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю;

2) діяльність з протидіями кіберзлочинців, що займаються одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників;

3) реалізувавши бойові дії, втілюючи теоретичні питання, таким чином, як експертне оцінювання кіберзлочинів, розсилка переходів методів ефективності та розширення роботи;

4) фактично активного інформаційного обміну.

Щоправда, виділимо наступні шляхи затримання позитивного результату Європейського Союзу в Україні: 1) еволюція вітчизняного законодавства серед

європейських стандартів. Варто визначити, що в даному випадку діяльності України є активною. Найголовніший нормативно-правовий акт у даному бізнесі, Конвенція про кіберзлочинність [1], ратифікований на державній державі, діючий реабілітація на вказівці Ради Європи з питань еволюції вітчизняного законодавства у відповідних сферах. Цей єдиний вірний напрямок стосується даного вектору, що зафіксував необхідну кількість представників європейських стандартних та імплементаційних європейських програм, що розробляють нові інститути у вітчизняних стратегіях. Іншими словами, євроінтеграція України дозволяє використовувати лише норми вітчизняного законодавства європейських стандартів. Втілення даного натиску можна в першу чергу створити, щоб зафіксувати необхідні результати.

2) відповідність діяльності європейських міжнародних організацій щодо боротьби із кіберзлочинністю на українській місцевості.

3) запропоновано конкретизувати поняття «кіберзлочинності» у вітчизняному законодавстві для використання норм європейського законодавства. Розмежовуючи із-за правового регулювання боротьбу із кіберзлочинністю у Франції, залишається зберегти одну із перших у Європі, але вона перетворилася на кроки, доки не з'явилися в регуляції кіберпростору. Так, на сьогоднішній день у даному державі виявлено наступні форми кіберзлочинності: 1) громадсько небезпечні дії, які залишаються за рахунок надійного тиражування комп’ютера, необхідного для програмування, впевнені в роботі, до автоматизованих системних даних, введення в систему веб-сайтів, створення та надання необхідних послуг; 2) пропоновані сайти, підтримувані з дитячою порнографією, збудження наркотиків, расистською, ксенофобною або антисемітською найсучаснішими, терористичними, які використовуються, про замовлення приватного життя, із застосуванням вимог щодо отримання вищої інформації, реклами в шахрайських цілях [21]. Даний досвід є актуальним для втілення в Україні з огляду на недосконаліть вироблення та формулювання суттєвого поняття «кіберзлочинність» у своєму державі.

Крім того, важливо чіткий розподіл злочинів, оскільки вони впливають на соціальні процеси в країні та негативні наслідки. У сфері активної боротьби з кіберзлочинністю 14 лютого 2008 року була прийнята Французька стратегія боротьби з кіберзлочинністю. кіберзлочинність. Цікавим моментом Стратегії є курс на встановлення співпраці між провайдерами та поліцією та жандармерією та створення національної комісії з питань професійної етики у зв'язках з громадськістю [16]. Особливо доцільним є останній напрямок. Будь-яке обмеження прав і свобод громадян вимагає належного роз'яснення та двостороннього конструктивного діалогу з громадянами. З цією метою у Франції проводяться інші дії, крім наміру створити спеціальну комісію. Зверніть увагу на запуск веб-сайту Charte de'Internet, який визначає принципи добровільних зобов'язань користувачів та Інтернет-провайдерів. Ще одна подібна тенденція – створення інтернет-ресурсу Mineurs.org, який надає інформацію про проекти у сфері безпечного використання кіберсетей. Тобто укладення міжнародних угод у Франції передбачає можливість дозволу на віддалений пошук інформаційних ресурсів без отримання попереднього дозволу країни, де розміщується сервер [16]. У цій роботі перспективи розвитку правового регулювання боротьби з кіберзлочинністю пояснюються потенційною потребою скасування державних кордонів у питаннях кіберзлочинності. Для втілення цього напрямку в Україні доцільно вивчити досвід Франції, оскільки можливість такої "вільної" співпраці не передбачена чинним законодавством України.

Таким чином, особливості правового регулювання боротьби з кіберзлочинністю у Франції є: 1) істотною роллю держави в регулюванні суспільних відносин в Інтернеті; 2) контроль над користувачами шляхом встановлення вимоги щодо авторизації авторів веб-сайтів; 3) налагодження співпраці між правоохоронними органами та Інтернет-провайдерами з метою оперативного реагування на появу загроз; 4) наявність двостороннього діалогу з громадянами та належне роз'яснення їх прав та обов'язків як користувачів Інтернету, надання інструкцій; 5) встановлення курсу на вільну співпрацю з

іншими країнами шляхом надання доступу до власних кібермереж у разі вчинення кіберзлочинності у Франції. Практично кожна з обраних характеристик була б доречною для впровадження в сучасних українських реаліях.

Розглянемо досвід Республіки Білорусь, як однієї з перших держав колишнього СРСР, якої було утворено спеціальний орган для боротьби із кіберзлочинністю – управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ Республіки Білорусь. 27 лютого 2001 року у структурі кримінальної міліції МВС з'явилося управління оперативно-організаційної роботи, у складі якого до листопада 2002 року активно діяло спеціалізоване відділення по розкриттю злочинів у сфері високих технологій, а вже 28 листопада 2002 року на підставі наказу Міністра внутрішніх справ, з метою вдосконалення організації роботи названих підрозділів, в МВС було створено самостійне управління, що здійснює практичну діяльність по розкриттю злочинів у сфері високих технологій [16]. Даний орган має статус самостійного оперативно-розшукового підрозділу Міністерства, яке здійснює координацію підрозділів головного управління кримінальної міліції МВС і органів внутрішніх справ при виявленні ними злочинів проти інформаційної безпеки Для здійснення взаємодії з іншими правоохоронними органами і організаціями застосовується умовне найменування Управління «К» МВС Республіки Білорусь [16].

Аналізуючи законодавчу базу боротьби із кіберзлочинності в Білорусі, вона представлена незначною кількістю норм та законів: Глава Кримінального кодексу Республіки Білорусь, Закон про електрозв'язок, Закон про інформацію, інформатизації і захист інформації, Конвенція про кіберзлочини, Додатковий протокол до Конвенції про кіберзлочини, Указ «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», Указ «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову

діяльність» [163, 169, 170]. У цілому відзначаємо тотожність законодавчої бази Республіки Білорусь та України, проте звернемо особливу увагу на Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність».

Аналізуючи моделі правового регулювання боротьби із кіберзлочинністю, нами встановлено тенденцію до спроб встановлення контролю за Всесвітньою мережею, проте наявні заборони все ж не містять ознак суттєвого порушення прав та свобод людини і громадянина. У досліджуваних державах існує двосторонній діалог влади та громадян, завдяки якому у суспільстві формується вірне розуміння необхідності встановлення обмежень, заборон чи регламентів. В той же час, ми звернули увагу на незначну кількість нормативно-правових актів, які при цьому належним чином врегульовують даний інститут, тобто в них переважає саморегулювання сфери кібербезпеки. Також доцільно відзначити роль міжнародного законодавства та міждержавних угод, які значним чином мають вплив на суспільні відносини всередині держав. Очевидно, що їх роль у вітчизняному праві необхідно виводити на новий рівень.

3.2. Державні механізми боротьби з кіберзлочинністю та методи їх покращення

На сучасному етапі розвитку суспільства все більше відчувається значущість інноваційних процесів, що відбуваються в нашому суспільстві у зв’язку з глобальною інформатизацією. Але разом з позитивними досягненнями, інформатизація супроводжується побічними, негативними явищами криміногенного характеру, до яких відносять комп’ютерну злочинність. Це, безумовно, вимагає негайного створення системи протидії даному різновиду злочинності на державному рівні. Для сучасного суспільства

(в період його переходу від індустріального етапу розвитку до нового – постіндустріального, інформаційного) актуальність цієї проблеми не викликає сумнівів. За різними експертними оцінками у всьому світі втрати від діяльності кіберзлочинців складають щорічно від 300 до 800 млрд. євро. На міжнародному рівні у ряді нормативно-правових актів визнано, що кіберзлочинність погрожує не лише національній безпеці окремих країн, але і безпеці людства та міжнародному правопорядку. Стратегія державних підходів та механізмів з поліпшення інформаційних систем повинна сприяти скороченню масштабів кіберзлочинності та створити основні принципи національної політики протидії кіберзлочинності в міжнародному кіберпросторі. Протидія кіберзлочинності в широкому розумінні включає у себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності. Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею життєво важливе значення має гармонізація національних законодавств. Проте, гармонізація повинна враховувати регіональні вимоги і можливості. Велике значення регіональних аспектів в здійсненні стратегій боротьби з кіберзлочинністю підкреслює той факт, що багато правових і технічних стандартів було погоджено між країнами світу. Глобальна програма кібербезпеки заснована на п’яти основних принципах: 1) правові заходи; 2) технічні й процедурні заходи; 3) організаційні структури; 4) створення потенціалу; 5) міжнародна співпраця. Зрозуміло, що українська система державних механізмів боротьби з кіберзлочинністю повинна використовувати всі ці принципи. Серед п’яти принципів, при розгляді стратегії боротьби з кіберзлочинністю, ймовірно, правові заходи є найбільш важливими. По-перше, ці заходи вимагають прийняття основних положень кримінального законодавства, що передбачають кримінальну відповідальність за такі дії, як комп’ютерне шахрайство, незаконний доступ, спотворення даних, порушення авторських прав, розповсюдження дитячої порнографії тощо. Механізми й інструменти, необхідні для розслідування кіберзлочинів, можуть істотно

відрізнятися від тих, що використовуються для розслідування загальних злочинів. У зв'язку з міжнародним масштабом кіберзлочинності необхідно додатково доробити основи національного законодавства, з тим, щоб мати можливість спільної співпраці з правоохоронними органами за кордоном. Ефективна боротьба з кіберзлочинністю вимагає розвиненої організаційної структури. Не маючи правильно створеної системи відповідних органів, яка дозволяє уникнути дублювання та чітко розподіляє повноваження, навряд чи можна чекати на комплексне вирішення юридичних, технічних та соціальних аспектів даної проблеми. Кіберзлочинність є глобальним явищем. Для того, щоб мати можливість ефективно розслідувати кіберзлочини, необхідно не тільки гармонізувати законодавство, але й розробити відповідні механізми міжнародної співпраці. Рівень довіри повинен зрости не лише між державами, але й між приватним і державним секторами. Одним з найбільш важливих елементів в попередженні кіберзлочинів є навчання користувача. Деякі кіберзлочини, особливо ті, які пов'язані з шахрайством типу «спуфінг», як правило, обумовлені не відсутністю засобів технічного захисту, а непоінформованістю або простою безвідповідальністю. Існують різні програмні продукти, що дозволяють автоматично визначати деякі шахрайські веб-сайти, хоча, на жаль, не всі. Попри те, що засоби технічного захисту продовжуватимуть розвиватися і доступні програмні продукти регулярно оновлюватимуться, такі продукти поки ще не можуть замінити інші підходи. Стратегія захисту користувача, що заснована тільки на програмних продуктах, ще не дає гарантії повного захисту користувачів [19].

Важливу роль відіграє також беззаперечне дотримання встановлених правил і процедур інформаційної безпеки. Наприклад, якщо користувачі знають, що їх фінансові установи ніколи не зв'язуватимуться з ними по електронній пошті з проханням повідомити пароль або деталі банківського рахунку, вони не стануть жертвами фішингу або атаки з метою крадіжки ідентифікації. Навчання користувачів Інтернету скорочує кількість потенційних жертв кіберінцидентів. Держава повинна розробити відповідну інформаційну

програму розумної поведінки щодо попередження кіберзлочинності. До її поширення слід долучити громадські кампанії, школи, інформаційні центри і ВНЗ, реалізовуючи приватно-державні партнерства. Проблема протидії комп'ютерної злочинності – це комплексна проблема. Закони України та інші нормативні документи у сфері кібербезпеки повинні відповідати сучасному рівню розвитку інформаційних технологій. З цією метою необхідно проводити цілеспрямовану роботу з гармонізації й удосконалення законодавства, що регулює поширення інформації в телекомунікаційних мережах. Одним з пріоритетних напрямків є також організація взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою, а також розвиток державно-приватного партнерства [21].

Кіберзлочинність – за своєю природою транскордонне явище, що дозволяє більшості вчених вказувати на те, що для кіберзлочинів є характерним максимальний рівень латентності. Факторами латентності кіберзлочинів виступають такі: 1) складність механізму вчинення кіберзлочинів, поєднана з дуже різноманітними сферою та наслідками їх учинення, а також «комп'ютерна безграмотність» більшості потенційних жертв кіберзлочинів, їх нехтування своєю безпекою; 2) негативна поведінка жертв (очевидців) злочину – незвернення жертви та осіб, яким відомо про злочин, до правоохоронних органів і неповідомлення про факт вчинення кіберзлочину; 3) недоліки в роботі правоохоронних органів стосовно реагування на звернення та повідомлення про кіберзлочини. Розглядаючи питання протидії кіберзлочинності, доцільно приєднатися до тих науковців-кримінологів, які виокремлюють загальносоціальні, спеціально-кримінологічні й індивідуальні напрями протидії. Протидія кіберзлочинності на загальносоціальному рівні (напрямі) передбачає комплекс перспективних соціально-економічних, організаційноуправлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на вирішення нагальних соціальних проблем і суперечностей у країні. Саме реалізація загальносоціальних заходів запобігання

дає змогу усунути чи мінімізувати вплив криміногенних факторів детермінації кіберзлочинності, запобігти формуванню особистості злочинця. Задля належної розробки відповідних заходів протидії злочинності, в тому числі кіберзлочинності, є необхідною належна організація діяльності як правоохоронних органів, так і вищих органів держави, яка відповідає вимогам, що висуваються до правової, незалежної та демократичної держави. Крім того, необхідно усувати фактори, що позитивно впливають на існування та розвиток злочинності [5]. Спеціально-кримінологічне запобігання стосується безпосередньо діяльності Національної поліції України і спрямовується головним чином на окремі соціальні групи, які привертають увагу суб'єктів превентивної діяльності. Основними заходами запобігання кіберзлочинності, що повинні реалізовувати ОВС та Національною поліцією (в особі Департаменту кіберполіції), слід визнати такі: розроблення та затвердження МВС Стратегії протидії кіберзлочинності, що повинна містити концепцію кримінально-превентивої діяльності, науково обґрунтовані стратегічні й тактичні заходи антикримінального впливу й моніторингові механізми забезпечення якості останнього; збільшення кількості планових і позапланових перевірок відповідними органами поліції підприємств, установ та організацій, діяльність яких прямо пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг, з метою виявлення випадків використання нелегального (нерегламентованого) програмного забезпечення; посилення відповідальності уповноважених осіб підприємств, установ або організацій, діяльність яких пов'язана із зазначеною сферою, які за своїми посадовими або функціональними обов'язками відповідають за безпеку функціонування комп'ютерів та комп'ютерних мереж; установлення жорсткого контролю за обігом будь-яких технічних засобів, заборонених для використання у вільному обігу або використання яких є обмеженим (технічні засоби для негласного зняття інформації з каналів зв'язку, прослуховування, перехоплення кодованих сигналів, добору паролів тощо); використання позитивного досвіду діяльності правоохоронних органів інших країн у цій сфері (в першу чергу аналізуються

стан технічного забезпечення й технології, що використовуються для запобігання вчиненню зазначених злочинів); участь працівників «кіберполіції» у міжнародних семінарах, круглих столах тощо, присвячених указаній проблематиці, та ініціювання відповідними органами нашої держави проведення таких заходів на території України. Напрямом діяльності щодо протидії вчиненню кіберзлочинів слід також визначити виявлення осіб, які вчиняють або схильні до вчинення кіберзлочинів, індикаторами поведінки яких є систематичний перезапис даних без необхідності, заміна або видалення даних, поява фальшивих записів, випадків, коли оператор системи без об'єктивних підстав починає працювати наднормово, персонал заперечує проти здійснення контролю за записом даних, фіксуються постійні скарги користувачів баз даних або власників щодо помилок та затримок у роботі системи тощо. Окремим заходом запобігання вчиненню кіберзлочинів є виявлення та запобігання діяльності кібертерористів, тобто осіб, які використовують комп'ютерну техніку, пристрої та мережі для вчинення терористичних актів [11].

Висновки до розділу 3

Виділено три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні: 1) тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні; 2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні; 3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

2. Деталізовано перелік основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні підтенденціями, які розкривають їх зміст.

3. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки є такі: 1) США вважають себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) дана держава має значний вплив на прийняття відповідного законодавства у країнах Європейського Союзу; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам.

4. Правове регулювання боротьби із кіберзлочинністю у Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

5. Особливостями боротьби із кіберзлочинністю у Франції є: 1) суттєва роль держави у регулюванні суспільних відносин в Інтернеті; 2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів;

3) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз.

6. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Республіці Білорусь є: 1) наявність спеціального органу із значним досвідом протистояння кіберзлочинності; 2) перелік повноважень даного органу є значно ширшим, ніж у Департаменту кіберполіції Національної поліції України; 3) невелика кількість нормативно-правових актів у сфері правового регулювання боротьби із кіберзлочинністю; 4) встановлення співпраці операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність.

ВИСНОВКИ

У магістерській кваліфікаційній роботі наведено теоретичне узагальнення та нове вирішення наукового завдання, що полягає у визначенні теоретико-правових засад боротьби із кіберзлочинністю. Основними науковими та практичними результатами роботи є такі висновки й пропозиції:

1. Кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов'язане із використанням комп'ютерної техніки через комп'ютерні системи, або із комп'ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність. Систему ознак боротьби із кіберзлочинністю визначено дворівнево. До загальних, тобто характерних явищу боротьби із злочинністю загалом, віднесено такі: 1) активність; 2) цілеспрямованість; 3) збірність; 4) комплексність. У якості спеціальних, а саме характерних виключно боротьбі із кіберзлочинністю, у процесі аналізу правової доктрини виділено: 1) ознака можливості зустрічної атаки зі сторони кіберзлочинців; 2) ознака здійснення виключно компетентними суб'єктами, володіючими спеціальними знаннями та необхідними ресурсами; 3) ознака міждержавності; 4) ознака згуртування держав.

2. У рамках генезису правового регулювання боротьби з кіберзлочинністю в Україні виділено наступні етапи: 1) початковий етап (1991 рік – 2000 рік) – не зважаючи на те, що у даний період було прийнято декілька нормативно-правових актів, спрямованих на врегулювання проблем кібербезпеки, питанню захисту від кіберзлочинів законодавцем увага не приділялась у належному обсязі, проте у 2000 році почали бути помітними тенденції до розвитку законодавства про кіберзлочини; 2) етап прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю (2001 рік – 2005 рік) – його початок пов'язується із прийняттям Кримінального кодексу України, у нормах якого незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства, а за кіберзлочини було

встановлено конкретні санкції. Відповідно, закінчення етапу автор відносить до введення у правовий обіг понять «комп'ютерна злочинність» та «комп'ютерний тероризм»; 3) етап відповідності правового регулювання боротьби з кіберзлочинністю існуючим загрозам (2005 рік – до 27.06.2017 року) – не зважаючи на те, що на даному етапі зроблено небагато, курс України до євроінтеграції вимагає імплементації європейських правових норм у вітчизняне законодавство. Існуючі кіберзагрози були врегульовані належним чином. У цілому, зазначений період характеризується відсутністю вагомих подій у сфері боротьби із кіберзлочинністю; 4) новітній етап (від 27.06.2017 року) – вірус «Petya.A» продемонстрував неготовність України до боротьби із сучасними кіберзагрозами. Тому, щойно розпочатий етап автор пов'язує із подальшою розробкою інструментів для боротьби із кібертерроризмом.

3. Механізм правового регулювання боротьби з кіберзлочинністю – це чітко визначена й організована система юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

4. Особливостями універсального міжнародно-правового регулювання боротьби з кіберзлочинністю є наступні: 1) відповідна діяльність акумулюється навколо ООН та її органів або створених за її підтримки суб'єктів; 2) на сьогодні наявні виключно програмні та інші стратегічні документи, які повинні закласти основи міжнародно-правового регулювання відповідного кола відносин; 3) основними напрямами діяльності має бути створення й розробка організаційних та законодавчих заходів протидії кіберзлочинності, а також питання взаємодії у даній сфері діяльності; 4) наявна необхідність у створенні міжнародних спільних органів оперативно-розшукової діяльності для забезпечення фіксування слідів вчинених злочинів; 5) удосконалення взаємодії між компетентними органами різних держав; 6) існує нагальна потреба

розробки й прийняття універсальних конвенцій з відповідних питань, які би забезпечили участь більшості держав у відповідних заходах проти кіберзлочинності. Особливостями регіонального міжнародно-правового регулювання протидії кіберзлочинності є такі: 1) значна увага з боку різноманітних регіональних міжнародних організацій до питань протидії кіберзлочинам; 2) розробка численних регіональних угод про співробітництво у сфері протидії інформаційним злочинам; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. – на початку 2000-х рр.; 4) така діяльність є складовою частиною як міжнародних інформаційних відносин, так і кримінального судочинства.

5. Особливостями нормативно-правової бази національного правового регулювання боротьби з кіберзлочинністю є наступні: 1) наявність системи національного правового регулювання боротьби з кіберзлочинністю, проте недостатній рівень єдності її елементів, що полягає у відмінностях в термінології, наявності розбіжностей у формулюваннях, прогалин та інших проблем; 2) комбінування у правовій системі норм вітчизняного законодавства та міжнародних правових актів, ратифікованих нашою державою; 3) наявність міжнародних договорів щодо двосторонньої співпраці у сфері правового регулювання боротьби з кіберзлочинністю; 4) існування Стратегії кібербезпеки України, що визначає подальший розвиток національного правового регулювання боротьби із кіберзлочинністю.

6. Виділено три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні: 1) тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні; 2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні; 3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

7. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки є такі: 1) США вважають

себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) дана держава має значний вплив на прийняття відповідного законодавства у країнах Європейського Союзу; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам. Правове регулювання боротьби із кіберзлочинністю у Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинам здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

9. Рівень кіберзлочинності на початок 2018 р. склав 2573 злочинів і має тенденцію до зростання. Показники динаміки кіберзлочинності в цілому відповідають показникам загальної злочинності в країні, що свідчить про специфічність детермінаційного комплексу кіберзлочинності та про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності. Найбільш ефективними заходами, безпосередньо спрямованими на протидію кіберзлочинності, є такі: збільшення кількості планових і позапланових перевірок; установлення жорсткого контролю за обігом технічних засобів, заборонених або обмежених у вільному цивільному обігу; перейняття досвіду діяльності правоохоронних органів інших країн у цій сфері; співробітництво з відповідними органами інших країн щодо розкриття, розслідування та запобігання злочинам в аналізованій сфері, обмін досвідом правозастосування; виявлення осіб, схильних до вчинення злочинів в аналізованій сфері, тощо. Указані заходи потребують подальших наукових розробок для створення дієвих інструментів протидії сучасним викликам кіберзлочинності.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» *Правова інформатика*. 2014.№ 2. С. 54-62.
2. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». Інформаційна безпека людини, суспільства, держави. 2010. № 1 (3). С. 16–18.
3. Буяджи С.А. Тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія"*. 2017. № 2. С. 21-32.
4. Великий енциклопедичний юридичний словник. НАНУ; Ін-т держави і права ім. В.М. Корецького; редкол.: Шемшученко Ю.С., Горбатенко В.П., Касяненко Ю.Я., Авер"янов В.Б. та ін. Київ : Юридична думка, 2007. 992 с.
5. Вінер О. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2018 році. URL https://defence-ua.com/index.php/statti/562-v-tenetakh-svitovoyipavutyny-tendentsiyi-rozvytku-kiberbezpeky-u-2016-r (дата звернення: 14.06.2019)
6. Горова С.В. Кіберпрофесіонали і кіберзлочинність *Боротьба з організованою злочинністю і корупцією (теорія і практика*): науковопрактичний журнал. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ, 2014. № 2 (33), спецвипуск. С. 170-173.
7. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. *Вісник Харківського національного університету внутрішніх справ*: *збірник наукових праць.* Харківський національний університет внутрішніх справ. Харків, 2014. № 4 (67). С. 65-75.
8. Денькович О. Поняття кіберзлочину у зарубіжній кримінології. Проблеми державотворення і захисту прав людини в Україні: матеріали XXIII звіт.

наук.-практ. конф., 7-8 лют. 2017 р. / Львів. нац. ун-т ім. Івана Франка, Юрид. ф-т ; [редкол.: В.М. Бурдін (голова) та ін.]. Львів: Львівський національний університет імені Івана Франка, 2017. Ч. 2. С. 130-133

9. Єгоричева С. Б. Організація фінансового моніторингу в банках. Навч. росіб. К.: Центр учбової літератури, 2014. 292 с.
10. Єфименко Т. І. Розвиток національної системи фінансового моніторингу: монографія. Держ. навч.-наук. установа "Акад. фін. упр.". Київ: ДННУ "Акад. фін. упр.", 2013. 378 с.
11. Кіберзлочинність та відмивання коштів. Департамент фінансових розслідувань. Державна служба фінансового моніторингу. 2018. URL http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pd (дата звернення: 5.09.2019)
12. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Офіційний вісник України. 2007 р. № 65. стор. 107. стаття 2535. код акту 40846/2007.
13. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. ст. 141. 7. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України (ВВР). 2013. № 910. № 11-12. № 13. ст.8.
14. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР). 2001. № 25-26. ст.131.
15. Луньова О. С. Окремі аспекти правового регулювання розслідування кіберзлочинів в Україні. *Актуальні питання розслідування кіберзлочинів*. Харків, 2013. С. 106-110.
16. Лук"янчук Р.В. Сучасний формат державного регулювання процесів забезпечення кібернетичної безпеки: досвід європейського союзу. *Вісник Київського національного університету імені Тараса Шевченка*. Київський національний університет імені Тараса Шевченка. Київ , 2016. (Державне управління; вип. 2 (6)). С. 34-38.

17. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. *Форум права*. 2017. № 1. С. 646-650.
18. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації. *Південноукраїнський правничий часопис*. 2013. № 1. С. 112-115.
19. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект. *Право і безпека*. 2015. № 2. С. 136-140.
20. Науково-практичний коментар до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення". Київ: Ваіте, 2015. 816 с.
21. Офіційний сайт Державної служби фінансового моніторингу України. URL http://www.sdfm.gov.ua/ (дата звернення: 1.06.2018)
22. Офіційний сайт Євразійської групи з протидії легалізації злочинних доходів і фінансуванню тероризму (ЄАГ). URL Режим доступу: http://www.eurasiangroup.org/ (дата звернення: 10.07.2018)
23. Офіційний сайт FATF. URL http://www.fatf-gafi.org/ (дата звернення: 4.06.2019)
24. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 14 жовтня 2014 р. № 1702 (зі змінами та доповненнями) *Відомості Верховної Ради*. 2014. № 39. ст. 2057.
25. Про судову експертизу. Закон України від 25.02.1994 № 4038-XII *Відомості Верховної Ради України (ВВР)*. 1994. № 28. ст.232.
26. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України». Указ президента України від 06.12.2001 № 1193/2001. *Урядовий кур'єр*. 18.12.2001. № 235.

27. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Указ Президента України від 15.03.2016 № 96/2016. *Урядовий кур'єр.* 18.03.2016. № 52.
28. Основні завдання Департаменту кіберполіції Національної поліції України. URL https://www.cybercrime.gov.ua/contacts (дата звернення: 02.06.2017) 118. Про Національну поліцію. Закон України від 02.07.2015 № 580-VIII. Відомості Верховної Ради (ВВР). 2015. № 40-41. ст.379.
29. Про Службу безпеки України. Закон України від 25.03.1992 № 2229-XII. *Відомості Верховної Ради України (ВВР*). 1992. № 27. ст.382.
30. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради України (ВВР).* 2006. № 30. ст.258.
31. Про Національний банк України. Закон України від 20.05.1999 № 679-XIV. *Відомості Верховної Ради України (ВВР).* 1999. № 29. ст.238.
32. Про утворення територіального органу Національної поліції. Постанова Кабінету Міністрів України від 13.10.2015 № 831. *Урядовий кур'єр*. 21.10.2015. № 195
33. Про затвердження Штату Департаменту кіберполіції Національної поліції України. Наказ Національної поліції України від 07.11.2015 № 10. URL https://www.npu.gov.ua/uk/publish/printable_article/1816252 (дата звернення: 03.06.2017).
34. Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів по суші, морю і повітрю). Закон України від 04.02.2004 № 1433-IV. *Відомості Верховної Ради України (ВВР).* 2004. № 19. ст.263.
35. Сорокин В. Д. Правовое регулирование: предмет, метод, процесс. *Правоведение.* 2000. №4 (231). С. 35-44.

36. Погорецький М. Кіберзлочини: до визначення поняття. *Вісн. прокуратури.* 2012. № 8. С. 89-96.
37. Поляруш О. О. Використання мережі Інтернет як каналу інформаційнопсихологічного впливу *Боротьба з організованою злочинністю і корупцією (теорія і практика).* К.: МНДЦ, 2015. № 21. С. 218-227.
38. Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року №47/2017. URL http://zakon3.rada.gov.ua/laws/show/47/2017 (дата звернення: 03.06.2018)
39. Про національну безпеку України: Закон України від 8 липня 2018 року №8068 // Верховна Рада України. URL http://zakon2.rada.gov.ua/laws/show/964-15 (дата звернення: 03.06.2019).
40. Рафал Канія Розвиток правової кібернетики у Польщі в XX-му сторіччі // Інформація і право : науковий журнал / Н.-д. ін-т інформатики і права Нац. акад. правових наук України ; Нац. б-ка України ім. В.І. Вернадського Нац. акад. наук України ; Відкритий міжнар. ун-т розвитку людини "Україна" ; голов. ред. Пилипчук В.Г. Київ, 2018. № 1 (24). С. 81-88.
41. Ращенко Є. Кримінально-правове забезпечення боротьби зі злочинами у сфері використання комп'ютерних технологій. *Право України*. 2015. № 10. С. 87-91.
42. Розенфельд Н. Віртуальний предмет злочинів, пов'язаних з порушенням авторського права і суміжних прав. *Право України*. 2012. № 5. С. 105-109.
43. Рудик М. В. Суб'єкт злочину, передбаченого ст. 362 КК України. *Роль та місце ОВС у розбудові демократичної правової держави*. Одеса, 2012. С. 323-324.
44. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. *Публічне право : науково-практичний*

юридичний журнал. Всеукр. громадська організація "Майбутнє країни"; Ужгород. нац. ун-т. Київ, 2015. № 3 (19). С. 144-149.

45. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки: збірник наукових праць*. МОНУ; КНУ імені Тараса Шевченка; Ін-т конкурентного суспільства. Київ, 2009. Вип. 19. С. 338-342.
46. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки: зб. наук. пр*. К.: Видав.-поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338–342.
47. Семенов Г. Криминалистическая классификация преступлений против информации в системе сотовой святи. Закон и жизнь. 2015. № 5. С. 24-28.
48. Семенов Г. Система сотовой связи как основополагающий фактор, детерминирующий способы совршения мошеничества в системе сотовой святи. *Закон и жизнь*. 2014. № 3. С. 20-24.
49. Сервецький І. В. Деякі проблеми захисту персональних даних в Україні *Боротьба з організованою злочинністю і корупцією (теорія і практика*). К. : МНДЦ, 2014. № 9. С. 193-199.
50. Симкин Л. Как бороться с «сетевыми пиратами» Л. Симкин *Рос. юстиция.* 2012. № 7. С. 62-64.
51. Скалозуб Л. П. Інтелектуалізація злочинності. Варіант стримування *Боротьба з організованою злочинністю і корупцією (теорія і практика*). К.: МНДЦ, 2012. № 1. С. 295-307.
52. Солодка О. М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави:* зб. матеріалів наук.-практ. конф., 17 берез. 2010 р., м. Київ. К.: Нац. акад. СБУ України, 2010. С. 126-128.
53. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення Протидія кіберзлочинності в фінансово-банківській сфері: матеріали

Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. Х. : ХНУВС, 2013. С. 144-147.

54. Струков В. М. Деякі технічні аспекти побудови кіберпростору в контексті протидії кіберзлочинності. *Протидія кіберзлочинності в фінансово-банківській сфері*: матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. Х. : ХНУВС, 2013. С. 65-68.
55. Струков В. М. Технічні аспекти побудови кіберпростору, що сприяють кіберзлочинності. *Боротьба з інтернет-злочинністю*: матеріалиміжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). Донецьк: Донец. юрид.ін-т, 2013. – С. 234-235.
56. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом «Властивості та ознаки операцій, пов'язаних з відмиванням коштів шляхом зняття готівки. Тактичне дослідження та практичне розслідування». Державна служба фінансового моніторингу України. http://www.sdfm.gov.ua/articles.php?cat_id=114&art_id=1890&lang=uk
57. Хакерська атака в Україні: як працює вірус Petya.A і що робити? URL http://24tv.ua/hakerska_ataka_v_ukrayini_virus_petya_a_yak_pratsyuye_i_shho_r obiti_n835033 (дата звернення: 18.05.2017)
58. Харко Д. М. Кримінологічні проблеми щодо визначення поняття та ознак сучасної економічної злочинності як фактора тінізації економіки України URL http://www.apdp.in.ua/v55/119.pdf (дата звернення: 11.09.2019)
59. Якубівська Ю. Є. Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі. *Вітчизняна система охорони і захисту інтелектуальної власності в умовах приєднання до Європейського Союзу*: Збірник тез доповідей Всеукраїнської науково-практичної конференції, м. Тернопіль, 24-25 квітня 2015 р., ТНЕУ. Тернопіль, 2015. С. 164-166.
60. National Security Strategy. The White House, February 2015. Washington D.C., 2015. 29 p. URL http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf (дата звернення: 05.07.2017)