МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного права та порівняльного правознавства

ДОПУСТИТИ ДО ЗАХИСТУ
Т.в.о. Завідувача кафедри
_____ Р.О. Максимович
«____»_____2023 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«БАКАЛАВР»
спеціальності 293 «Міжнародне право»

Тема: **МІЖНАРОДНО-ПРАВОВЕ СПІВРОБІТНИЦТВО ДЕРЖАВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ**

Виконавець: Ремарчук Артем Ігорович
Науковий керівник: д.ю.н., доцент, професор кафедри міжнародного права та порівняльного правознавства Нуруллаєв Ількін Садагат огли
Нормоконтролер: викладач Головатенко Марина Юріївна

Київ, 2023

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Кіберзлочинність – це не традиційний злочин, а відносно молоде явище, яке виникло разом із появою та поширенням глобальної мережі Інтернет. З самого початку цей злочин полегшив справу злочинцям. Специфіка Всесвітньої павутини забезпечує глобальність та анонімність її користувачів, що, безсумнівно, є передумовами для виникнення подібних злочинів. У свою чергу, необхідність правового врегулювання цього питання у світі та в Україні пов'язана з поширенням кіберзлочинності.

Боротьба з будь-яким негативним впливом вимагає розвитку розуміння природи проблеми та знання її походження. Оскільки швидкість суспільного розвитку нерозривно пов'язана з досягненнями технічного прогресу та діяльністю злочинців, важливо також звернутись до історичного розвитку запровадження правових механізмів боротьби з кіберзлочинністю у світі та в Україні.

Зростання кількості кіберзагроз у нашій країні робить все більш актуальною оптимізацію правового регулювання у цій сфері. З огляду на процес євроінтеграції, Україна має продемонструвати, що ми готові протистояти загрозі найшвидше зростаючого виду злочинності. Крім того, в сучасних умовах важливо бути готовим прийняти необхідні зміни, щоб відповідати стандартам, встановленим на європейському та світовому рівнях.

Ступінь наукової розробленості дослідження. Розробкою питання щодо співробітництва держав у сфері боротьби із кіберзлочинністю розглядали такі вчені як Р.В. Лук'янчук, О.В. Манжай, В.В. Марков, Ю.М. Онищенко, П.І. Пушкаренко, Є.Д. Скулиш, В.Г. Хахановський, В.В. Чернєй, М.Ю. Яцишин та інші.

Мета і завдання дослідження. Метою даного дослідження є концептуальне розуміння конкретної ситуації міжнародно-правового співробітництва у сфері протидії кіберзлочинності та тенденції розвитку

механізмів правового нагляду за протидією кіберзлочинності.

Для досягнення поставленої мети визначені наступні завдання дослідження:

- дослідити генезис визначення та основний зміст кіберзлочинності;
- охарактеризувати видову та складову характеристику кіберзлочинності;
- розкрити та конкретизувати універсальні та регіональні механізми боротьби з кіберзлочинністю;
- з’ясувати специфіку правових механізмів боротьби з кіберзлочинністю спеціалізованих установ ООН;
- виділити особливості специфіка міжнародно – правового співробітництва у боротьбі з кіберзлочинністю;
- виокремити тенденції та перспективи розвитку правового регулювання боротьби з кіберзлочинністю в Україні.

Об’єктом дослідження є система міжнародно - правових відносин у сфері правового регулювання боротьби із злочинністю.

Предметом дослідження є міжнародно – правове співробітництво держав у сфері боротьби з кіберзлочинністю.

Методи дослідження. Для виконання поставлених цілей і завдань дослідження в дипломній роботі використовується комплексний загальнонауковий метод пізнання та спеціальний метод пізнання.

Отже, діалектика - дає можливість досліджувати внутрішню природу речей у процесі розвитку, а також внутрішні та зовнішні суперечності, особливо цей метод дає можливість досліджувати кіберзлочинність; історичний метод - допомагає зрозуміти походження законів і нормативних актів для боротьби з кіберзлочинністю; системний підхід - дозволяє всебічно та об'єктивно досліджувати відповідно конкретно окреслену тему, зокрема дозволяє дослідити структуру правових і нормативних механізмів боротьби з кіберзлочинністю; порівняльно-правовий метод - використовується для аналізу характеристик іноземних законів і нормативних актів для боротьби з

кіберзлочинністю; логічні методи та прийоми - дедукція, індукція, аналогія, аналіз і синтез весь процес наукового аналізу.

Структура та обсяг дипломної роботи. Дипллomна робота складається із переліку умовних скорочень, вступу, трьох розділів, якими охоплюються шість підрозділів, висновків та списку використаних джерел (70 найменувань). Загальний обсяг дипломної роботи – 70 сторінки, у тому числі список використаних джерел – 8 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИКО-ПРАКТИЧНІ ОСНОВИ ВИЗНАЧЕННЯ ПОНЯТТЯ КІБЕРЗЛОЧИННІСТЬ

1.1. Генезис визначення та основний зміст кіберзлочинності

Сьогодні кіберзлочинність стала гострою проблемою, з якою стикаються країни 21 століття. Випадки кіберзлочинності збільшують свій зріс як за своїм розміром, так і за ступенем шкоди, яку завдає. Кіберзлочинцям вдалося продовжити діяти в кіберпросторі, незважаючи на комплексні заходи з боку фізичних та юридичних осіб, а також держав. У зв’язку з цим на даний момент особливо важливо переглянути всі існуючі заходи та активно розробляти нові заходи для отримання більшої вигоди та формування надійної системи реалізації національних інтересів у кіберпросторі.

Перш за все, можна зазначити, що в офіційних національних нормативно-правових документах термін «кіберзлочинність» не визначений, незважаючи на те, що він використовується в окремих нормативно-правових актах, які регулюють суспільні відносини в кіберпросторі. Водночас це поняття укорінилося в лексиконі правоохоронних органів розвинених країн Європи та світу. Під ним узагальнено розуміють види злочинів у сфері комп'ютерної інформації та телекомунікацій, незаконне розповсюдження радіоелектронних і спеціальних технічних засобів, розповсюдження неліцензійного програмного забезпечення для ЕОМ та деякі інші види злочинів.

Перш за все, можна зазначити, що в офіційних національних нормативно-правових документах термін «кіберзлочинність» не визначений, незважаючи на те, що він використовується в окремих нормативно-правових актах, які регулюють суспільні відносини в кіберпросторі. Водночас це поняття укорінилося в лексиконі правоохоронних органів розвинених країн Європи та світу. Під ним узагальнено розуміють види злочинів у сфері комп'ютерної інформації та телекомунікацій, незаконне розповсюдження радіоелектронних і

спеціальних технічних засобів, розповсюдження неліцензійного програмного забезпечення для ЕОМ та деякі інші види злочинів.

Хочемо зазначити, що масштаби кіберзлочинності як транснаціонального явища породжують багато практичних і наукових питань, вирішення яких може забезпечити усунення негативних наслідків та мінімізацію швидкості та форми її розвитку.

Зараз кіберзлочинність становить ще більшу загрозу для України, в умовах війни, яку веде російська федерація проти нашої країни. Проте наукового осмислення цих питань у рамках наукових досліджень недостатньо. Незважаючи на окремі та фрагментарні зусилля правоохоронних органів у боротьбі з окремими кіберзлочинцями, на жаль, їх кількість не зменшується, а навпаки, постійно збільшується. Однією з причин є те, що не виконано виконання завдання побудови національної системи безпеки мережі.

У 2008 році експерти визначили мережі ботів як десятку найнебезпечніших загроз — «цілеспрямовані» атаки на державні веб-сайти, приватні підприємства та кінцевих користувачів. А в 2013 році, за прогнозами експертів McAfee, почали з'являтися загрози, пов'язані з використанням мобільного доступу до мережі.

Злочинність у кіберпросторі є однією з найгостріших проблем, з якими стикається міжнародне співтовариство в розвитку інформаційних технологій за останні десятиліття [1].

Впровадження та розвиток сучасних інформаційно-комунікаційних технологій значно випереджає швидкість, з якою законодавчі та правоохоронні органи можуть адекватно реагувати на їх зростання.

Термін «кіберзлочинність» часто вживається разом із терміном «комп'ютерна злочинність», і ці поняття часто використовуються як синоніми. Насправді ці терміни дуже близькі один до одного, але не є синонімами. Поняття «кіберзлочинність» (англійський варіант – cybercrime) є ширшим за поняття «комп'ютерна злочинність» і точніше відображає природу явищ кіберзлочинності.

Відповідно, Оксфордські словники визначають приставку «cyber» як компонент складних слів. Його значення пов'язане з інформаційними технологіями, Інтернетом і віртуальною реальністю. Кембриджський словник дає майже таке саме визначення. Отже, «кіберзлочинність» — це злочин, пов’язаний із використанням комп’ютерів та використанням інформаційних технологій і глобальної мережі. Тим часом термін «комп'ютерна злочинність» в основному відноситься до злочинів, скоєних проти комп'ютерів або комп'ютерних даних. Ідея поділу термінів «кіберзлочинність» і «комп’ютерна злочинність» і використання першого терміну була закріплена в міжнародному праві. У листопаді 2001 року Рада Європи прийняла Конвенцію про кіберзлочинність, замінивши термін «комп’ютерна злочинність» на термін «кіберзлочинність». Наразі на міжнародному рівні немає офіційного визначення кіберзлочинності [2].

Хоча аналіз національного законодавства України, яке регулює публічно-інформаційні відносини, може стверджувати, що в нашій державі вжито необхідних заходів, спрямованих на запобігання та протидію комп’ютерним злочинам. Прикладом цього є Указ Президента від 31 липня 2000 р. «Про заходи щодо розвитку національної частини глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до неї в Україні» та розділ 16 «Використання комп’ютерів, систем і комп’ютерних мереж» » чинного Кримінального кодексу України. Але цього недостатньо, щоб повністю перемогти кіберзлочинність у нашій країні.

Таким чином, одним із питань, яке пропонується висвітлити, є питання концептуального та категоріального обладнання. Термін «кіберзлочинність», який зараз використовується в науковому середовищі для позначення окремого виду злочинності, що відноситься до так званої «кібернетичної сфери», набув досить широкого вжитку на пострадянському просторі і не має загальновизнаного юридичного значення. Питання залишається невирішеним, мало того, що «Кіберзлочинність» буде пов’язана з такими юридичними категоріями, як «комп’ютерна злочинність», «злочинність у сфері комп’ютерної

інформації», «системи та комп’ютерні та телекомунікаційні мережі», а визначення місця «кіберзлочину» в системі протиправних діянь, передбачених національним законодавством: як окремого виду цих діянь, як специфічної форми їх скоєння, як того й іншого. Усе це ставить під великий сумнів нормативне визначення кіберзлочинності та її легкості та можливості вчинення як окремого кримінально-правового виду злочину [3, с. 189].

Відповідно, «кіберзлочинність» означає:

- протиправні дії, які здійснюються людьми, які використовують інформаційні технології у злочинних цілях, це визначення є досить абстрактним і незрозумілим. Крім того, використання терміна «людина» в юридичній науці є неприпустимим, особливо в цьому визначенні. Людина – це перш за все живий організм, але не кожен має можливість користуватися інформаційними технологіями. Крім того, комп’ютеризація суспільних відносин, подальше поширення ботів створюють умови для вчинення ними певних протиправних дій [4, с. 33];

- неправомірне втручання в роботу кібернетичних систем, основною ланкою управління якими є комп'ютер (наприклад, спотворення інформації про стан об'єктів у каналах зворотного зв'язку, спотворення сигналів керування та каналів зв'язку, використання шкідливого програмного забезпечення тощо), створення конкретних кібернетичних (комп’ютерних) систем і злочинне використання, злочинне використання існуючих кібернетичних (комп’ютерних) систем (наприклад, комп’ютерних або телекомунікаційних мереж для шахрайства, вимагання тощо), зазначена дефініція може бути прийнята за приклад під час прийняття відповідних нормативно-правових актів [5, с.85];

- правопорушення, вчинені за допомогою або через комп'ютерні системи або конкретно пов'язані з комп'ютерними системами, тобто злочини, пов'язані з групою пристроїв, один або більше з яких здійснюють автоматичну обробку даних відповідно до певних процедур [6];

- злочини у сфері комп’ютеризованої інформації, тобто під час використання текстової, графічної чи будь-якої іншої інформації (даних), яка

існує в електронній формі, зберігається на відповідному носії та може бути створена, змінена чи використана за допомогою АЕОМ [6, с. 89];

- злочинні діяння проти суспільства, передбачені Кримінальним кодексом, у тому числі незаконне використання інформаційно-комунікаційних технологій, відповідальність за які встановлено законодавством про кримінальну відповідальність;

- сукупність злочинів, вчинених у комп'ютерних мережах та у віртуальному просторі проти комп'ютерних систем, мереж і даних за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуальних просторів;

- злочинність у кібернетичному (віртуальному) просторі - комп'ютерний і телекомунікаційний кіберпростір [7, с. 190].

Конвенція про кіберзлочинність також не дає визначення поняття «кіберзлочинність». Водночас у її преамбулі зазначено, що Конвенція необхідна для припинення дій, спрямованих на конфіденційність, цілісність і доступність комп’ютерних систем, мереж і комп’ютерних даних, а також неправомірне використання таких систем, мереж і даних, шляхом встановлення конфіденційності, цілісності. наявність комп’ютерних даних і кримінальна відповідальність за такі дії, необхідні для зловживання такими системами, мережами та даними, шляхом встановлення кримінальної відповідальності за такі дії, наприклад, Конвенція, передбачає достатню кількість злочинів, щоб полегшити виявлення, розслідування та переслідування таких злочинів на національному та міжнародному рівнях, а також укладати угоди про оперативне та надійне міжнародне співробітництво [8].

Таким чином, у цьому контексті кіберзлочин – це дія, а саме: незаконний доступ; незаконне перехоплення; підробка даних або систем; неправомірне використання обладнання; шахрайство; правопорушення, пов’язані з дитячою порнографією; конфіденційність, цілісність і доступність комп’ютерних даних, а також неправомірне використання таких систем, мереж і даних, які тягнуть за собою кримінальну відповідальність [9].

Підсумовуючи, можемо зазначити, що, насамперед, засобами кіберзлочинності є комп’ютер, тобто комп’ютерна мережа чи комп’ютерна система. З точки зору кримінального права воно має ознаки прямого умислу, що майже виключає можливість необережності. Крім того, суб'єкт є осудною фізичною особою. Метою таких злочинів є порушення інформаційно-комп’ютерних систем, порушення авторських і суміжних прав, використання документів на переказ, платіжних карток та інших засобів доступу до банківських рахунків, їх виробничого обладнання тощо для здійснення протиправної діяльності.

Наслідки кіберзлочинності зачіпають інтереси не лише окремих жертв, а й компаній, організацій, урядів і суспільства в цілому. Кіберзлочинність найчастіше ставить під загрозу життєво важливу інформацію та загалом критичну інфраструктуру, яка не перебуває під контролем державного сектора в багатьох країнах, і такі злочини можуть мати дестабілізуючий вплив на всі сектори суспільства. Тому можна стверджувати, що кіберзлочинність є загрозою національній безпеці в кіберсфері.

Аналізуючи теоретичні та практичні дослідження щодо визначення сфери поняття «кіберзлочинність», можна зробити висновок, що сучасні українські вчені не мають єдиного визначення поняття «кіберзлочинність». Крім того, методології значно відрізняються, що може призвести до неправильного тлумачення та, отже, неправильної кваліфікації злочинної поведінки, що може спричинити проблеми не лише на теоретичному, а й на практичному рівні.

Кіберзлочинність поділяється на різні види за об’єктом злочину, суб’єктом злочину та способом вчинення злочину.

Найпоширеніші сьогодні класифікації кіберзлочинності базуються на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація наразі використовується як «стандарт», оскільки вона використовується в наявних міжнародних і регіональних документах, а також у науковій практиці.

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

• Незаконний доступ - відсутність права свідомого доступу до всієї комп'ютерної системи або її частин з метою отримання комп'ютерних даних або інших нечесних цілей;

• Втручання в дані, навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це;

• Втручання в роботу системи - навмисне і серйозне втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

• Неналежне використання пристрою, тобто виготовлення, продаж, придбання пристрою для використання, розповсюдження або будь-яким іншим доступним для використання способом;

2) злочини, пов'язані з комп'ютером;

3) протиправні дії, пов'язані зі змістом;

4) правопорушення, пов'язані з порушенням авторського права і суміжних прав[45];

5) расистські та ксенофобські дії, вчинені з використанням комп'ютерних мереж [10].

До основних видів кіберзлочинності належать розповсюдження шкідливих програм, злом паролів, викрадення номерів кредитних карток та інших банківських реквізитів, а також поширення незаконної інформації через Інтернет.

Залежно від об'єкта атаки кіберзлочинність поділяється на такі категорії: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і комп'ютерних мереж, економічні комп'ютерні злочини, комп'ютерні злочини проти прав особи та недоторканності приватної сфери, комп'ютерні злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і комп'ютерних мереж, комп'ютерні злочини проти прав людини та проти недоторканності приватної сфери. сфери комп'ютерної злочинності та національні інтереси. Однак варто зазначити, що багато кіберзлочинців

атакують кілька цілей одночасно. Ще одна категорія злочинів, окремо не включена в Конвенцію Ради Європи (яка стала загальною після її прийняття) – крадіжка особистих даних, викрадення, передача та використання персональних даних для вчинення злочинів [11, С. 173].

В даний час досить поширеними є такі класифікації кіберзлочинності:

1) Агресивний – кібертероризм, погрози фізичного насильства (наприклад, електронною поштою), кіберпереслідування, кіберпереслідування (незаконні сексуальні домагання та переслідування інших через Інтернет), дитяча порнографія (створення порнографічних матеріалів із зображеннями дітей, розповсюдження таких матеріалів, їх отримання) ;

2) Неагресивні – кіберкрадіжка, кіберсаботаж, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [12, С. 156].

Водночас, враховуючи мотиви злочинців, видається можливим умовно поділити кіберзлочинність на кілька категорій:

• Інтернет-шахрайство з метою отримання коштів;

• Інтернет-шахрайство з метою отримання інформації (для особистого використання чи подальшого продажу);

• Втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (диверсія або травмування конкурента за винагороду);

• Інші злочини.

Кіберзлочин — це акт несанкціонованого вторгнення в комп’ютерні мережі, комп’ютерні системи та програми з метою зміни комп’ютерних даних і може каратися кримінально. Водночас, оскільки об’єктом злочину є комп’ютер, об’єктом є й інформаційна безпека. Варто зазначити, що кіберзлочинність спрямована на особисті дані, банківські рахунки, паролі та іншу особисту інформацію окремих осіб і компаній, а також державного сектора. Кіберзлочинність є загрозою не лише національного, а й глобального рівня.

Найпоширенішими видами кіберзлочинів є: кардинг, фішинг, онлайн-шахрайство, піратство, кардшерінг, соціальна інженерія, зловмисне програмне

забезпечення, незаконний контент, повторне архівування тощо [13].

Акцентуємо увагу на таких ознаках кіберзлочинності:

1. Ці злочини вчиняються у віртуальному просторі чи комп'ютерній мережі. Кіберпростір – модульований за допомогою комп'ютерів кібернетичний простір, що містить дані про людей, факти, явища, процеси, представлені в математичній, символьній чи іншій формах. Ця інформація переміщується через локальні та глобальні комп'ютерні мережі та зберігається в пам'яті будь-якого фізичного чи віртуального пристрою, спеціально призначеного для її зберігання, обробки та передачі.

2. Під кіберзлочинністю розуміються засоби проникнення в кіберпростір за допомогою комп'ютерних систем або комп'ютерних мереж, а також злочини, вчинені проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювальна техніка може бути використана як засіб, так і як об'єкт злочину.

Цікава та змістовна думка інформаційного спеціаліста В.М. Бутузова висвітлює свій повний список ознак кіберзлочинності:

1) Символом віднесення окремих злочинів у сфері високих інформаційних технологій до комп'ютерних є засіб злочину – комп'ютерна техніка. Причому об'єктом порушення є суспільні відносини у сфері автоматизованої обробки інформації;

2) Специфічне злочинне середовище – кіберпростір (комп'ютерна система та мережеве середовище) є ознакою того, що злочини у сфері високих інформаційних технологій відносять до кіберзлочинів. Причому об'єктами злочинних посягань можуть бути відносини в будь-якій сфері людської діяльності, що проявляються в кіберпросторі. Дослідник посилався на перелік протиправних дій, викладених у Конвенції та Додаткових протоколах до неї. На його думку, лише діяння з цього переліку можна кваліфікувати як кіберзлочин [14, С. 119].

Відсутність чіткого визначення в законі викликала певні дискусії на теоретичному рівні. На сьогоднішній день нормативно-правові норми

кіберзлочинності не адаптовані до розвитку сучасних інформаційних технологій, що загострює проблему кіберзлочинності та робить її реальною загрозою національній безпеці України. Для фізичних осіб кіберзлочинність пов'язана з використанням піратського програмного забезпечення: злочинці отримують доступ до персональних даних користувачів. Піратство також створює надзвичайно сприятливі умови для виникнення та розвитку кіберзлочинності.

В Україні до кіберзлочинності належать порушення авторського права та суміжних прав, шахрайство, використання документів на переказ, платіжних карток та інших засобів доступу до банківських рахунків, незаконні дії щодо його виробництва обладнання; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографії, незаконне збирання чи використання з метою використання відомостей, що становлять комерційну чи банківську таємницю .

Терміни, які використовуються в Конвенції та Додаткових протоколах до неї, не знаходять свого визначення у національному законодавстві. Так, терміни «комп'ютерна злочинність» та «комп'ютерний тероризм» згадуються в «Основних засадах національної безпеки України», але закон не дає визначення цих понять, як і інші нормативні акти. Поняття «кібертероризм» не визначено в Законі України «Про боротьбу з тероризмом», а питання, які може охоплювати це поняття, описані частково як складові поняття «технотероризм» [15, С. 414].

Варто зазначити, що в «Доктрині інформаційної безпеки України» йдеться про поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», а також питання захисту інформації від «кібератак». Проте визначення цих понять не знайшли відображення в жодній із перерахованих дій.

Зауважу, що деякі з цих порушень зазначені як злочини у розділі XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку». Водночас суспільні відносини у цій сфері регулюються рядом підзаконних актів.

В Указі Президента України про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку системи безпеки та оборони» неодноразово вживаються поняття «кіберзагрози», «кібербезпека», «кібер шпигунство» тощо, однак не дається визначення жодному з цих понять.

4 червня 2013 року було зареєстровано проект закону «Про кібербезпеку в Україні», але в ньому також не було ні визначення «кіберзлочинності», ні поняття «кіберзлочинність». Пізніше, у проекті Закону № 2126а «Про основи забезпечення кібербезпеки в Україні», зареєстрованому 19 червня 2015 року, кіберзлочин було визначено як небезпечне для суспільства злочинне діяння в кіберпросторі, передбачене законодавством України про кримінальну відповідальність, а під кіберзлочинністю - сукупність кіберзлочинів.

На даний момент питання кіберзлочинності є першочерговим на державному рівні. У більшості випадків кіберзлочинність зачіпає критичну інфраструктуру, особливо інформаційну: об’єкти енергетики, транспорту та банківського сектору.

Тому протидія та запобігання кіберзлочинності та підвищення рівня кібербезпеки наразі є одними з пріоритетних напрямів політики нашої держави. Але комплексне вирішення проблеми вимагатиме об’єднання зусиль держав, громадян і всього міжнародного співтовариства.

Питання протидії кіберзлочинам в Україні є складним. Зараз закон має відповідати сучасним реаліям, а не рівню наукового розвитку чи розуміння правлячою групою пріоритетів тих чи інших національних інтересів. Подальший прогрес технологій, робототехніки та штучного інтелекту в наше життя – це не майбутнє, це сьогодення. Тому будь-які подальші роздуми над цим питанням потребуватимуть часу лише тоді, коли відносини в кіберпросторі розвиватимуться швидко та нелінійно.

Пріоритетним напрямком також є організація взаємодії та координації правоохоронних органів, спеціальних служб, судової системи, забезпечення їх не лише найсучаснішою матеріально-технічною базою, а й розвиток

екологічної основи навчання з кібербезпеки, навчання відповідні спеціалісти. Наразі жодна країна не може боротися з кіберзлочинністю поодинці. В інтересах національної безпеки Україні необхідно терміново посилити свою участь у різних міжнародних і глобальних системах інформаційної безпеки, посилити співпрацю зі світовими інформаційними гігантами: Facebook, Apple, Google, залучити широкий спектр аналітичних центрів, особливо недержавних. та інститути громадянського суспільства.

Експерти впевнені, що найближчим часом хакерство стане загрозою номер один, прийшовши на зміну тероризму. Незважаючи на віртуальний характер злочинів, вони завдають миттєвої шкоди в реальному світі. Яскравим прикладом є масштабна атака на українські ресурси вірусом Petya, під час якої були скомпрометовані численні інформаційні системи органів державної влади України.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння правових аспектів регулювання інформаційних мереж. Аналіз зв'язку між технічними характеристиками мереж і правовими та соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, що виникають у зв'язку з цими характеристиками, є першим кроком до можливої розробки механізмів для адекватної боротьби з розвитком і зростанням кіберзлочинності. Механізми контролю, запобігання та розслідування вторгнень у кіберпростір соціально та технологічно обмежені.

1.2. Видова та складова характеристика кіберзлочинності

Питання криміналізації кіберзлочинних діянь є самостійною науково-практичною проблемою, яка може бути вирішена лише шляхом формування універсального поняття кіберзлочинності шляхом уніфікації міжнародно-правових норм. При цьому слід врахувати аналіз національного законодавства групою експертів ООН і відповідно скласти перелік кримінальних злочинів. Серед таких правопорушень, на які не поширюються положення договорів, що розглядаються, експерти ООН рекомендували встановити кримінальну

відповідальність за: комп'ютерні злочини, пов'язані з використанням персональних даних; комп'ютерні злочини, пов'язані з авторським правом і товарними знаками; комп'ютерні злочини, пов'язані з нанесенням тілесних ушкоджень; комп'ютерні злочини, пов'язані з використанням персональних даних; злочини, пов'язані з расизмом і ксенофобією, використання комп'ютерів для заманювання та виховання дітей, комп'ютерні злочини, пов'язані зі спамом [16, С.9].

Кіберзлочинність базується на обмеженому діапазоні дій, спрямованих на конфіденційність, цілісність і доступність комп'ютерних даних або систем. Однак, без обмежень, дії, пов'язані з використанням комп'ютерів для отримання особистої вигоди чи отримання фінансової вигоди або для заподіяння особистої чи економічної шкоди, включаючи форми злочину у зв'язку з використанням особистого широкого поняття «кіберзлочинність»), непросто знайти вичерпне юридичне визначення. Стосовно злочинів, які складають основу кіберзлочинності, необхідні деякі визначення.

Дослідження віктимізації показують, що люди значно більше потерпають від кіберзлочинності, ніж від «звичайних» форм злочинності. Онлайн-шахрайство з кредитними картками, викрадення особистих даних, фішингові відповіді та неавторизований доступ до облікових записів електронної пошти є жертвами від 1% до 17% користувачів Інтернету в 21 країні світу, що можна порівняти з типовими випадками, такими як крадіжка зі зломом, пограбування та викрадення автомобіля, що становлять для цих же країн менше 5 відсотків. Більш високий рівень віктимізації, пов'язаної з кіберзлочинністю, у країнах з низьким рівнем доходу підкреслює необхідність посилення заходів із запобігання в цих країнах.

Залежно від об'єкта злочину виділяємо види інформації, яка має певну форму і міститься на різноманітних носіях, комп'ютерах (документи), веб-сторінках (персональні дані) чи банківських рахунках (реквізити рахунків, банківських карток) тощо. У цьому контексті ми не можемо розглядати вторгнення в комп'ютер як повноцінний злочинний об'єкт, тому що якщо

комп’ютер атакує, наприклад, вірус, злочинець націлюється не на фізичний носій, а на інформацію, розміщену на цьому носії. До основних властивостей кіберзлочинності вчені відносять такі: інтелектуальний характер кіберзлочинності; відсутність вікових обмежень та соціального статусу; анонімність та об’єктивність; віддаленість кіберзлочинності; транснаціональний характер кіберзлочинності. Одним із головних чинників кіберзлочинності є зловживання програмним забезпеченням та інструментами Інтернету. Є багато способів, якими злочинці можуть втручатися в особистий простір людини, такі як електронна пошта, особисті веб-сторінки тощо. У цьому випадку зловмисники використовують коди доступу та засоби віддаленого доступу. Останні були створені для вирішення системних проблем, але їх також можна використовувати як засіб незаконного доступу до інформації. Кіберзлочинці можуть використовувати мікрофон і камеру на комп’ютері користувача, щоб стежити за тим, що він робить.

Іншою характерною ознакою кіберзлочинності є видавання себе за іншу особу, що дозволяє злочинцям проникнути та отримати інформацію. Вони ховаються за акціями, подарунковими сертифікатами, безкоштовними пропозиціями. Вони також вміють видати себе за відому організацію чи інституцію, щоб їхня пропозиція чи запитання виглядали цілком законними й не викликали підозр. Так, наприклад, один із способів отримати доступ до особистих даних — попросити підтвердити пароль або номер рахунку онлайн-банкінгу під виглядом проблеми з обліковим записом клієнта в Інтернеті [17, С. 56].

Законодавча невизначеність щодо цих понять досі розпалює дебати щодо тлумачення того, що саме є кіберзлочинністю, і загалом розділяє вчених на дві групи. Перша група вчених відносить до кіберзлочинності дії, в яких комп’ютер використовується як об’єкт або засіб проникнення. Інша група визначає кіберзлочин як злочин, що об’єктом посягання бере електронні обчислювальні машини або інформацію, що обробляється в комп’ютерних системах, а засобом

реалізації є електронні обчислювальні машини (ЕОМ), тобто протизаконні дії у сфері автоматичної обробки інформації [18, С. 416].

Криміналістичною особливістю кіберзлочинів є те, що їх розслідування та розкриття неможливо без застосування та використання комп'ютерних технологій. Тому держава має приділяти більше уваги вихованню нових професіоналів для боротьби з подібними злочинами, перепідготовці старих кадрів, і далі йти попереду злочинців. Підготовка кваліфікованих спеціалістів насамперед пов'язана з необхідністю точного, швидкого реагування та електронного пошуку, фіксації, виїмки та збирання доказів та проведення оперативно-розшукових заходів [19].

Вважається, що момент вчинення злочину у сфері комп'ютерної інформації слід ідентифікувати як момент натискання клавіші керування комп'ютером, запуску та подання останньої команди. При цьому неважливо, скільки часу потрібно для настання прогнозованих небезпечних наслідків. Розділивши результати та дії, можна мінімізувати часові інтервали, еквівалентні хвилинам, які необхідні комп'ютеру для аналізу, прийняття та виконання завантаженої команди. Навпаки, в деяких випадках цей проміжок часу може бути дуже тривалим, тому що, наприклад, деякі шкідливі програми спочатку запускаються не відразу, а через деякий час. Шкідливий код може розпочинати деструктивні дії лише після того, як користувач виконає певну дію, наприклад, після запуску програми або після закінчення певного часу після використання програми. Тобто кіберзлочинність має особливі кримінально-правові ознаки у визначенні сукупності та повторності протиправних діянь.

Набагато складніше визначити, де відбуваються комп'ютерні злочини. Більшість комп'ютерних злочинів відбувається в комп'ютерних мережах. При цьому передбачається, що місце вчинення порушення знаходиться на відстані кількох кілометрів від місця настання суспільно небезпечних наслідків або навіть на території іншої країни. Швидке зростання його «поширеності» в кримінальному середовищі пояснюється особливостями цього виду злочинності: високою латентністю, що пояснюється загальною

комп’ютеризацією суспільного та приватного життя, а також транскордонним характером і пов’язаними з цим способами злочинності. для комп’ютерних злочинців важко вловити та відносно легко вчинити злочини. Поширення комп’ютерних технологій та їх збочений динамізм змушують законодавців і правоохоронні органи, які борються з комп’ютерними злочинами, прискорювати реакцію на нові методи використання комп’ютерних технологій для ведення незаконної діяльності [20, С. 52].

Зарубіжні вчені виділяють наступні ознаки кіберзлочинності, які відрізняють їх від «звичайних» кримінальних правопорушень і значно підвищують їх суспільну небезпеку:

● Кіберзлочин не вимагає фізичної близькості жертви та суб’єкта злочину під час злочину.

● Кіберзлочинність є «автоматичним» злочином. Це означає, що за допомогою комп’ютерних технологій злочинці мають можливість збільшити кількість протиправних дій до тисяч за короткий проміжок часу.

● Предмет кіберзлочинності не залежить від існуючих сучасних обмежень. Як наслідок, кіберзлочин може бути скоєний миттєво і, отже, вимагає негайного реагування.

● Кіберзлочинність все ще є новим явищем, і ця дисципліна не змогла нормалізувати географічний і демографічний розподіл різних типів злочинів, скоєних у фізичному, а не у віртуальному світі.

Предметом таких злочинів є врегульовані законом суспільні відносини щодо забезпечення безпеки сфери та повноцінного функціонування електронно-обчислювальних машин (ЕОМ), комп’ютерних мереж і систем.

Об’єктивні аспекти визначаються таким чином: кіберзлочин зазвичай вчиняється шляхом активних дій, незважаючи на об’єктивні аспекти того, що є злочином, як це передбачено ст. 363 Кримінального кодексу України (недодержання вимог законодавства про електронно-обчислювальну техніку, автоматизовану техніку, комп’ютерні мережі чи мережі електрозв’язку чи системи захисту інформації чи обробку в них), також через бездіяльність [21].

Суб’єкт кіберзлочинності, який як норма означає, що засуджені особи, які досягли вікової межі кримінальної відповідальності, в окремих випадках є винятковими – а саме особи, які мають можливість доступу до автоматизовано оброблених даних, комп’ютерних мереж (ст. 362 КК України), або осіб, відповідальних за використання електронно-обчислювальних машин, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (ст. 363 КК України).

Класифікація кіберзлочинності здійснюється за різними критеріями. Залежно від мети атаки можна виділити такі категорії кіберзлочинності:

- зочини проти конфіденційності, одноманітності та доступності комп'ютерних даних і комп'ютерних мереж;

- фінансова комп'ютерна злочинність;

- комп'ютерні злочини проти прав особи та недоторканності її особистої сфери;

- комп'ютерні злочини проти суспільних інтересів і національних інтересів.

Однак варто зазначити, що багато кіберзлочинів порушують кілька предметів одночасно: наприклад, незаконне перехоплення приватних електронних комунікацій порушує недоторканність приватної сфери та конфіденційність комп’ютерних даних, а комп’ютерне шахрайство порушує право власності та цілісність комп'ютерні дані.

Розглянемо деякі види кіберзлочинності:

1. Фінансова кіберзлочинність – це суспільно небезпечна поведінка, яка порушує фінансово-економічні відносини, тобто шахрайство з кредитними картками, привласнення коштів банківських операцій тощо.

2. Фішинг — це отримання інформації від довірливих громадян для доступу до банківських рахунків. Це поширене явище в країнах, де популярні онлайн-банкінгові послуги. Ще одна незаконна діяльність, яка широко поширена в сучасних умовах, – це цільовий фішинг.

Цільовий фішинг спрямований на невелику кількість користувачів і включає соціально-контекстуальні повідомлення, які закликають потенційних

жертв відкрити виконувані файли або відвідати сайти, що містять шкідливий код.

3. Фармінг - програма, яка таємно перенаправляє жертв на підроблені IP-адреси, є більш технічно складним методом шахрайства.

4. Віддалений злом комп'ютерів є окремим і небезпечним видом кіберзлочинності, що дає злочинцям можливість читати та редагувати документи, що зберігаються на файлових серверах і робочих столах комп'ютерів, запроваджувати власні шкідливі програми, а також збирати різну інформацію, використовувати аудіо та відеоспостереження. Нещодавно з'явився вірус як кіберзброя, спрямована на руйнування промислової інфраструктури. Серед них такі віруси, як Duqu, Stuxnet, Gauss, Flame тощо. За цими вірусами стоять уже не низькокваліфіковані айтішники, а суперпрофесіонали.

Інформаційний веб-сайт People and Progress, який вивчає вплив технологічного прогресу на людину, містить перелік таких видів кіберзлочинності:

- «Кібер-порнографія»- стосується порнографічних веб-сайтів, які дозволяють відвідувачам розміщувати порнографічні фільми, відео та фотографії неповнолітніх громадян.
- Кібер-торгівля наркотиками — це використання новітніх технологій шифрування для здійснення наркотрафіку на основі інформації, надісланої клієнтами електронною поштою. У таких повідомленнях наркоторговці в зашифрованому вигляді вказують, де і як можна обміняти товар на гроші [21].
- Кібертероризм - це терористична діяльність, яка здійснюється в кіберпросторі. До таких злочинів можна віднести просте поширення через Інтернет інформації про терористичний акт, який може бути здійснений у визначений час у майбутньому.

Розрізняють також види кіберзлочинності, такі як азартні ігри в Інтернеті та кіберпереслідування.

До найбільш відомих видів таких злочинів відносяться:

- Кардинг – в операції використовувалися реквізити платіжних карток, придбаних на зламаних серверах мереж інтернет-торгових центрів, платіжно-розрахункових систем, персональних комп’ютерів.

- Фішинг — це шахрайство, за допомогою якого покупці платіжної концепції отримують електронний лист нібито від адміністративної служби або служби безпеки системи з проханням ввести свої особисті дані та пароль під час телефонної розмови.

- Інтернет-шахрайство - шахрайські мережі інтернет-аукціонів, інтернет-магазинів в Інтернеті, взаємний обмін веб-сайтами та телекомунікаційними ресурсами.

- Піратство - незаконне розповсюдження копій об'єктів або об'єктів інтелектуальної власності в Інтернеті.

- Кард-шарінг - надає незаконний доступ до перегляду супутникового та кабельного телебачення.

- Соціальна інженерія - метод управління людьми в Інтернеті.

- Мальваре - створення та поширення вірусів і шкідливих програм.

- Протизаконний контент - пропагує екстремізм, гангстеризм, наркоманію, порнографію, бездушність і насильницьке поклоніння.

- Рефайлінг – незаконна заміна телефонного трафіку [22].

Найпоширеніші види кіберзлочинності в поточний період базуються на положеннях Конвенції Ради Європи про кіберзлочинність. Ця типологія є найбільш обґрунтованим способом класифікації кіберзлочинності, прийнятим різними державами та їх групами та включеним у їхні правові системи. Конвенція РЄ про кіберзлочинність визначає наступні види кіберзлочинності:

1) злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (так звані «CIA-злочини»):

● незаконний доступ - навмисний несанкціонований доступ до всієї комп'ютерної системи або її частин з метою отримання комп'ютерних даних або в інших нечесних цілях;

● несанкціоноване втручання в дані, навмисне пошкодження, знищення, погіршення, зміна або приховування комп’ютерної інформації;

● втручання в систему - навмисне та серйозне втручання у функціональність комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

● використовувати пристрій не за призначенням, тобто виготовляти, продавати, придбавати для використання, розповсюджувати або надавати для використання будь-яким іншим способом;

2) злочини, пов'язані з комп'ютером;

3) протиправні дії, пов'язані зі змістом;

4) протиправні дії, пов'язані з порушенням авторського права і суміжних прав;

5) расистські та ксенофобські дії, вчинені з використанням комп'ютерних мереж.

Окрім наведених вище класифікацій кіберзлочинності в науковій літературі знаходимо ще один підхід, згідно з яким виділяють:

а) Агресивний – кібертероризм, погрози фізичного насильства (наприклад, електронною поштою), кіберпереслідування, кіберпереслідування (незаконні сексуальні домагання та переслідування інших через Інтернет), дитяча порнографія (виробництво порнографічних матеріалів із зображеннями дітей), розповсюдження цих матеріалів, отримання їх);

б) Неагресивні – крадіжка в Інтернеті, саботаж в Інтернеті, шахрайство в Інтернеті, шпигунство в Інтернеті, спам і розповсюдження вірусних програм.

Залежно від мотивів злочинців кіберзлочинність можна умовно поділити на такі категорії:

● Інтернет-шахрайство з метою отримання коштів;

● Інтернет-шахрайство з метою отримання інформації (для особистого використання чи подальшого продажу);

● Втручання в роботу інформаційних систем для отримання доступу до автоматизованих систем управління (з метою винагороди за вандалізм або заподіяння шкоди конкурентам);

● Інші злочини [23].

Кіберзлочинність можна систематизувати на два види: класичні, що здійснюються за допомогою комп'ютерних технологій та Інтернету (використання комп'ютерів для вчинення шахрайства, незаконний збір даних, що становлять комерційну таємницю, несанкціонований доступ до комп'ютерних даних тощо), а також нові злочини, які стали можливими завдяки новим комп'ютерним технологіям (злочини включені до глави XVI Кримінального кодексу України). Загалом з використанням комп'ютерів та мережі Інтернет переважно вчиняються такі типові злочини: порушення авторського права та суміжних прав (ст. 176); шахрайство (ст. 190); доступ до банківських рахунків, виробничого обладнання з використанням переказних документів, платіжних карток та інших способів (ст. 200); ухилення від сплати податків, ухилення від сплати податків (обов'язкових платежів) (ст. 212); ввезення, виготовлення, збут і розповсюдження порнографії (ст.301); відомості, що становлять комерційну чи банківську таємницю, з метою використання або використання та незаконне збирання (ст. 231).

Тому слід зазначити, що відсутність єдиного визначення поняття «кіберзлочинність» створила сприятливі умови для виникнення та вирішення ряду проблем. Невідповідність чинного законодавства сучасним загрозам і небезпекам у кіберсфері також сприяє появі та зростанню кіберзлочинності. Суб'єктом даного виду злочинів є фізична осудна людина, об'єктом є, перш за все, кібербезпека. Кіберзлочинність часто ставить під загрозу критичну інфраструктуру. Кіберзлочини здійснюються за допомогою комп'ютерних систем або комп'ютерних мереж та інших засобів проникнення у віртуальний простір, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [23].

Щодо класифікації кіберзлочинності можна зробити висновок, що

більшість дослідників, які досліджують проблеми кіберзлочинності, пропонують поділяти кіберзлочинність на види відповідно до об'єкта та суб'єкта атаки. Найпоширенішим варіантом є поділ на комп'ютерні злочини та злочини, вчинені за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв, які мають доступ до кіберпростору. Організація Об'єднаних Націй використовує цю класифікацію для поділу вищезазначених типів злочинної діяльності на «широку» та «вузьку» кіберзлочинність. У цьому контексті кіберзлочинність відноситься до злочинів, які порушують основні цілі конфіденційності, цілісності, доступності та безпечної роботи комп'ютерних даних і систем. Інші кіберзлочини, окрім комп'ютерних систем, посягають на інші об'єкти (як основні): безпеку суспільства і людини (кібертероризм), майно і майнові права (крадіжки, шахрайства, здійснені за допомогою комп'ютерних систем або в кіберпросторі), авторські права (піратство).

РОЗДІЛ 2.
МІЖНАРОДНИЙ МЕХАНІЗМ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1. Універсальні та регіональні механізми боротьби з кіберзлочинністю

На одинадцятому (18-25 квітня 2005 р., Таїланд) і дванадцятому (12-19 квітня 2010 р., Бразилія) Конгресі ООН із запобігання злочинності та кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися міжнародні партнерства для боротьби з кіберзлочинністю. Учасники Конгресу обговорили заходи щодо зміцнення міжнародного партнерства та вдосконалення національного законодавства у сфері боротьби з відмиванням грошей, торгівлею наркотиками, тероризмом та кіберзлочинністю. Тобто Організація Об'єднаних Націй ставить комп'ютерну злочинність і тероризм в один список, показуючи, що міжнародна спільнота приділяє цьому питанню особливу увагу [24, С. 109].

У 2010 році 12-й Конгрес із запобігання злочинності та кримінального правосуддя завершився створенням міжурядової експертної групи відкритого складу для вивчення кіберзлочинності та реагування держав-членів, міжнародної спільноти та приватного сектору. У 2013 році Управління ООН з наркотиків і злочинності підготувало комплексне дослідження кіберзлочинності.

Норми матеріального права гармонізовані за допомогою цілого ряду директив, зокрема, Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії (Directive2011 / 93 / EUof the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework – Decision 2004/68 / JHA), Директива щодо атак проти інформаційних систем (Directive 2013/40 / EU of the European Parliament and the Council of 12 August 2013 on attacks against information systems and replacing Council Framework

Decision 2005/222 / JHA), Директива про безпеку мереж та інформаційних систем (Directive (EU) 2016/1148 of the European Parliament a nd of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). Норми матеріального права гармонізовано за допомогою низки директив, зокрема щодо боротьби з сексуальним насильством над дітьми та їх експлуатацією в Інтернеті та дитячою порнографією.

У 2013 році керівництво Організації Об'єднаних Націй у боротьбі з наркотиками та злочинністю заявило у своїй доповіді «Комплексний аналіз проблем кіберзлочинності та зустрічних граней з краю країн — членів міжнародного співтовариства та приватного сектору», що термін «кіберзлочинність» залежить від контекст, у якому використовується цей термін. Ефективний моніторинг несприятливих явищ у кіберпросторі, особливо протиправної поведінки, вимагає більш активного міжнародного партнерства, ніж існуючі заходи для боротьби з різними іншими формами міжнародної злочинності.

Тому на практиці, крім гармонізації кримінально-правових норм, необхідна гармонізація процесуальних важелів і формування нових елементів міжнародного партнерства. Міжнародні договори у відповідних сферах є значним внеском у боротьбу з кіберзлочинністю, наприклад, Конвенція Ради Європи про кіберзлочинність, Рішення Європейської комісії, Модельний закон Карибського басейну про кіберзлочинність (проєкт HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв`язку для держав Тихоокеанського регіону (проект ICB4PAC), проєект ООН з розробки кіберзлочинного законодавства у сфері кіберзлочинності в країнах Африки (проєкт ESCWA) тощо [25].

20 травня 2015 року під час паралельного заходу, що відбувся в рамках 24-ї сесії Комісії з питань запобігання злочинності та кримінального правосуддя, УНП ООН відкрило архів кіберзлочинності – базу даних, яка містить законодавство, судову практику, витягнуті з досвіду боротьби з

кіберзлочинністю та електронні докази. Механізм допоможе країнам у запобіганні та ефективному переслідуванні кіберзлочинів [26].

Починаючи з 1990-х років багато міжнародних організацій визнали важливість розробки та прийняття міжнародних правових актів, спрямованих на боротьбу з комп'ютерними злочинами. Враховуючи роль і значення інформації, розвиток інформаційно-комунікаційних технологій, створення глобальних баз даних, глобальних інформаційних мереж і систем, їх захист, Організація Об'єднаних Націй відіграла координуючу роль у розробці концептуальних і правових основ регулювання ключових питання, зокрема: боротьба із злочинним використанням інформаційних технологій (Резолюції Генеральної Асамблеї ООН 55/63 від 4 грудня 2000 р., 56/121 від 19 грудня 2001 р. «Боротьба зі злочинним використанням інформаційних технологій»); міжнародна інформаційна безпека (Резолюції ГА ООН «Досягнення в сфері інформації та комунікації в контексті міжнародної безпеки» № 53/70 від 4 грудня 1998 року, № 54/49 від 1 грудня 1999 року, № 55/28 від 20 листопада 2000 року, № 56/19 від 29 листопада 2001 року, № 57/53 від 22 листопада 2002 року, № 58/32 від 8 грудня 2003 року, № 59/61 від 3 грудня 2004 року, № 60/45 від 8 грудня 2005 року, № 61/54 від 6 грудня 2006 року, № 62/17 від 5 грудня 2007 року, № 63/37 від 2 грудня 2008 року, № 64/25 від 2 грудня 2009 року, № 65/41 від 8 грудня 2010 року, № 66/24 від 13 грудня 2011 року); створення глобальної культури кібербезпеки та захист найважливіших інформаційних структур (Резолюція Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки та захист найважливіших інформаційних структур», № 57/239 від 20 грудня 2002 р., 23 грудня 2003 р. 58/ 199, 64/211 від 21 грудня 2009 р.). Крім того, Економічна і соціальна рада Організації Об'єднаних Націй прийняла кілька резолюцій щодо персональних даних (резолюція ECOSOR «Міжнародне співробітництво у запобіганні та розслідуванні шахрайства, злочинного використання та фальсифікації персональних даних і пов'язаних з цим 26, 2007/20 від 26 липня 2007 р.) [27].

Резолюція Генеральної Асамблеї A/RES/58/199 підкреслила необхідність захисту інформаційної інфраструктури, пропонуючи цикл компонентів для захисту найважливіших з них, зокрема: присутність мереж, які існують для негайного попередження про вразливі місця, небезпечних ситуацій, зон конфлікту; підвищення рівня обізнаності залучених сторін, щоб вони краще розуміли тип і розмір своїх первинних інформаційних інфраструктур і важливість, яку кожна з них повинна відігравати для їх захисту; відповідне матеріальне право та процесуальне право та присутність відомих осіб щоб держави мали можливість розслідувати спроби порушення захисту ключових інформаційних структур і притягувати причетних до відповідальності; формувати та забезпечувати функції комунікаційних концепцій і ключових умов, а також контролювати їх функціонування, щоб забезпечити їх нормальну роботу в критичні моменти; спільними зусиллями країн стежити за спробами проникнення у великі інформаційні будівлі тощо. Резолюцією A/RES/70/237 2015 Генеральна Асамблея закликала представників країн-учасниць сприяти багатостороннім обговоренням існуючих і потенційних небезпек у сфері інформаційної безпеки, а також можливих стратегій у цій сфері, виходячи з необхідності зберігати інформацію відкритою, продовжувати вивчати певну Ці міжнародні концепції зосереджені на посиленні безпеки масової інформації та телекомунікаційних концепцій [28].

У рамках ініціативи «Нове партнерство для розвитку Африки» (NEPAD) Організація Об’єднаних Націй співпрацює з Комісією Африканського Союзу над розробкою конвенції про кібербезпеку за зразком Африканської конвенції про кіберзлочинність. Обсяг положень про співпрацю, які містяться в багатосторонніх або двосторонніх документах, різниться в різних країнах світу, відсутність обмежених у часі зобов’язань реагування, відсутність домовленостей про надання прямого доступу до екстериторіальних даних, велика кількість неофіційних мереж правоохоронних органів та відмінності в гарантії співпраці серйозно проблематичні у справі забезпечення ефективної

міжнародного співробітництва в галузі електронних доказів по кримінальних справах [29].

У рамках дослідження міжнародно-правового регулювання інформаційного тероризму варто згадати проект Генеральної угоди з кібербезпеки та кіберзлочинності, запропонований професором Стайном Шолбергом, який головував на зустрічі високого рівня. Експертна група з кібербезпеки була створена в 2007 році для вивчення можливості створення загального документа про кіберзлочинність в рамках ООН і професора Соланж Гернуті-Елі. Автори проекту розглядають інфотероризм як різновид кібератак. Згідно з положеннями проекту угоди, до таких діянь належать: публічні заклики до вчинення терористичних злочинів, обшуки та заклики до вчинення терористичної діяльності, терористичні навчання. Угода також встановлює кримінальну відповідальність за такі діяння згідно з внутрішнім законодавством держав-членів [30].

У рамках ЮНЕСКО розроблено концепцію «Універсальності Інтернету», яка відображає позицію організації в рамках її мандату з питань, пов’язаних з Інтернетом, до 2021 року. Він також демонструє роль Інтернету в побудові суспільства знань і досягненні Цілей сталого розвитку ООН. Концепція базується на чотирьох ключових принципах, які наразі відомі як принципи R.O.A.M. – орієнтація на права людини, відкритість, доступність та багатостороння участь [31].

Концепція Міжнародної конвенції ООН про інформаційну безпеку була розроблена та представлена міжнародній спільноті на Конференції з кіберпростору в Лондоні в листопаді 2011 року, включаючи преамбулу, 23 статті, об’єднані в основні частини та заключні положення. Основна частина документа складається з п'яти частин, зміст яких становить єдину композиційну цілісність. Важливо, що в ст. Стаття 4 Конвенції визначає основні загрози міжнародному миру та безпеці в інформаційному просторі, виділяючи 11 основних і 4 додаткові загрози. Найбільш принциповими з них є, наприклад, використання інформаційних технологій і засобів для ведення бойових дій та

актів агресії, цілеспрямований і деструктивний вплив в інформаційному просторі на життєво важливі структури іншої держави, порушення принципів і норм міжнародного право, а також національним законодавствам держав.

Сьогодні міжнародні закони та правила боротьби з кіберзлочинністю є переважно регіональними. Таке співробітництво зазвичай здійснюється державами за підтримки міжнародних і регіональних організацій, до яких вони належать. За останні роки шляхом укладення регіональних угод, які мають вирішальне значення для цього питання, були створені не лише правові механізми боротьби з кіберзлочинністю, а й практичні механізми, втілені в роботі спеціалізованих установ, робочих дослідницьких груп, контакт-центрів тощо.

Організацією, яка ініціює регіональне міжнародно-правове співробітництво, є Рада Європи. Конвенція Ради Європи про кіберзлочинність, підписана на засіданні в Будапешті 23 листопада 2001 року, стала основою для боротьби з кіберзлочинністю, заклавши основу для співпраці, стандартів криміналізації кіберзлочинності та вимог процесуального законодавства не лише для держав-членів Ради Європи, а й для всього міжнародного співтовариства. Усі майбутні документи були розроблені відповідно до положень Конвенції, деякі з яких прямо посилалися на Конвенцію. Наприклад, Директива ЄС 2013/40 [32] щодо злому інформаційних систем. Відповідно до преамбули (15): «Нова стратегія повинна бути розроблена державами-членами та Комісією з урахуванням змісту Конвенції Ради Європи про кіберзлочинність 2001 року. Ця Конвенція є правовою основою для боротьби з кіберзлочинністю, включаючи атаки. щодо інформаційних систем Ця Директива складена відповідно до Конвенції».

За даними на 9 грудня 2018 року Конвенцію про кіберзлочинність підписали 62 країни (25 з них не є членами Ради Європи, а 4 країни підписали, але не ратифікували) [33]. Це є свідченням не лише якості самого договору, а й бажання країн долучитися до співпраці та впровадити норми у своє законодавство з метою ефективної боротьби та боротьби з кіберзлочинністю.

Як зазначалося раніше, Конвенція про кіберзлочинність є проривом у боротьбі з кіберзлочинністю. Саме вона вказує шлях для майбутнього узагальнення відповідних норм. Конвенція застосовує технологічно нейтральні правові методи, і, відповідно, положення застосовуються як до сучасних злочинів, так і до майбутніх злочинів, які можуть виникнути з розвитком технологій [34]. У 2003 році в Страсбурзі було прийнято додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації актів расистського та ксенофобського характеру, вчинених за допомогою комп'ютерних систем [35]. Він додав до переліку кіберзлочинів такі дії: поширення расистських і ксенофобських матеріалів через комп'ютерні системи, погрози з расистських і ксенофобських мотивів, образи з расистських і ксенофобських мотивів, заперечення, суттєве скорочення, схвалення або геноцид або загроза захисту злочинів проти людства. На сьогоднішній день 31 країна ратифікувала Додатковий протокол і 13 країн підписали Додатковий протокол.

Крім того, згідно зі статтею 46 Конвенції було створено Комітет з боротьби з кіберзлочинністю, метою якого є проведення консультацій щодо сприяння імплементації та ефективного застосування Конвенції для забезпечення обміну інформацією та подальшої реалізації. У 2017 році Комісія вирішила розробити проект Другого протоколу до Конвенції про кіберзлочинність, зокрема щодо таких категорій питань: заходи для ефективної взаємної співпраці; забезпечення прямої співпраці з провайдерами в інших юрисдикціях щодо запитів на інформацію користувачів, збереження інформації та термінових запитів. заходи, більш точне формулювання та суворіше застосування існуючої практики щодо транскордонного доступу до даних, заходи, спрямовані на забезпечення захисту даних [36]. Крім того, у Бухаресті (Румунія) Рада Європи має Проектний офіс з кіберзлочинності (C-PROC), місія якого полягає в тому, щоб допомогти державам зміцнити їхні правові механізми для протидії загрозам кіберзлочинності та виконувати роль електронних доказів відповідно до Конвенції про кіберзлочинність. Офіс бере

участь у реалізації проектів, які відрізняються залежно від регіональних особливостей, з метою більш ефективного визначення потреб правової системи та надання необхідних консультацій [37].

Далі пропонуємо розглянути Лігу арабських держав. У грудні 2010 року в рамках цієї організації була прийнята Арабська конвенція про боротьбу з кіберзлочинністю [38], яка набула чинності в 2014 році. На сьогодні Конвенцію ратифікували вісім країн-учасниць LAD. Основною метою конвенції є створення зобов'язань для її учасників щодо забезпечення виконання положень їхніх національних законів, які криміналізують деякі кіберзлочини, а також запровадження процесуальних норм для спрощення процесу переслідування та збору електронних доказів кіберзлочинів. У конвенції також є розділ про налагодження співпраці між країнами-учасницями для боротьби з міжнародною кіберзлочинністю. Арабська конвенція проти кіберзлочинності не визначає механізмів забезпечення виконання чи процедур вирішення спорів. Конвенція містить багато суперечливих статей, особливо стаття 1. 21. Вимагати посилення покарання за традиційні злочини, якщо вони вчинені з використанням кіберпростору (на наш погляд, без об'єктивних причин). Крім того, стаття 21.1 передбачає покарання за розповсюдження порнографічних матеріалів, стаття 12.1 – поширення ідей і принципів терористичних груп, а стаття 15.4 – поширення релігійного фанатизму та інакомислення. Отже, можна зробити висновок, що К обмежує певні права людини, особливо права на свободу вираження поглядів і віросповідання.

Африканський Союз розпочав розробку Конвенції про кібербезпеку ще в 2011 році, яка спрямована на полегшення електронних транзакцій, захист особистих даних, заохочення впровадження заходів кібербезпеки, електронного уряду та боротьби з кіберзлочинністю. Однак Африканська конвенція про кібербезпеку та захист персональних даних була нарешті прийнята в 2014 році. Стаття 29 містить перелік злочинів, передбачених Конвенцією. Однак африканська конвенція не передбачає більшість процесуальних норм, які містяться в Конвенції про кіберзлочинність 2001 року. Крім того, Африканська

конвенція криміналізує не тільки закінчений злочин, але й замах на нього за певних обставин. Крім того, у жовтні 2018 року в рамках Африканської конвенції відбувся перший Африканський форум з боротьби з кіберзлочинністю. Розглянуті питання включали: політику боротьби з кіберзлочинністю, національне законодавство в рамках регіональних і міжнародних стандартів і практику їх впровадження; міжнародне співробітництво для боротьби з кіберзлочинністю та впровадження відповідних заходів для забезпечення транскордонного поширення електронної злочинності; відповідні програми були здійснюється для впровадження правоздатності для посилення роботи органів кримінальної юстиції [39].

Існують і інші форми міжнародно-правового співробітництва у боротьбі з кіберзлочинністю. Хоча ці інструменти не є юридично обов'язковими, вони забезпечують практичну співпрацю. Зокрема, у 2003 році Азіатсько-Тихоокеанське економічне співробітництво започаткувало Проект із сприяння розвитку законодавчої діяльності щодо кіберзлочинності та правоохоронної діяльності, який має на меті допомогти країнам регіону зміцнити їхню правову спроможність у боротьбі з кіберзлочинністю та сприяти розробці законодавства щодо правоохоронної діяльності та виявлення кіберзлочинності для ефективної боротьби з кіберзлочинністю. Крім того, АТЕС має групу телекомунікацій та інформаційної безпеки та розвитку (SPSG), яка відповідає за сприяння безпеці кіберпростору, особливо за справу запобігання кіберзлочинності [40].

Ще однією організацією, яка реалізує таку співпрацю, є Організація американських держав. У його межах було створено робочу групу та проект під назвою «Портал для міжамериканської співпраці проти кіберзлочинності». Метою порталу є сприяння співпраці та обміну інформацією між національними органами ОАД у сфері міжнародного співробітництва у боротьбі з кіберзлочинністю, розслідуванні та судовому переслідуванні. Тому регіональні механізми міжнародно-правового співробітництва між країнами у боротьбі з кіберзлочинністю мають дві форми: шляхом реалізації спільних заходів правового характеру відповідно до потреб конкретних регіонів та через

організацію спеціалізованої роботи з вивчення та координації національного законодавства. органів співробітництва, особливо на регіональному рівні. Основні аспекти забезпечення боротьби з кіберзлочинністю, особливо шляхом впровадження матеріальних і регіональних норм у національне законодавство держав, характерні не для всіх регіонів. Хоча така співпраця враховує специфіку правових систем держав-членів міжнародного співтовариства, вона не забезпечує універсалізацію норм на міжнародному рівні, яка є необхідною з огляду на те, що більшість проявів кіберзлочинності не поважають кордони та територію юрисдикції. обмеження. Крім того, узагальнення міжнародних законів і правил боротьби з кіберзлочинністю допоможе зменшити кількість випадків, коли країни впроваджують внутрішні правові норми, які обмежують основні права людини.

Крім того, створення єдиного міжнародно-правового механізму глобального співробітництва проти кіберзлочинності дасть можливість створити окремий спеціалізований орган з процесуальних аспектів запобігання та протидії кіберзлочинності, що дасть змогу вдосконалити існуючі форми співпраці та залучити більше учасників.

2.2. Правові механізми боротьби з кіберзлочинністю спеціалізованих установ ООН

Питання боротьби з кіберзлочинністю також було в центрі уваги органів і установ Організації Об’єднаних Націй, зокрема Генеральної Асамблеї (A/RES 63/195), Економічної та Соціальної Ради (резолюція 2009/22), Комісії з попередження злочинності і кримінального правосуддя (документ E/CN.15/2009/15), Конгрес ООН із запобігання злочинності та кримінального правосуддя, рішення якого вимагало розробки шляхів і засобів вирішення проблем [41, С. 109].

Такі інновації, як модуль електронних доказів, включений до переглянутого Протоколу запитів про взаємну правову допомогу Управління ООН з наркотиків і злочинності (UNODC), допомагають оптимізувати процес взаємної правової допомоги щодо електронних доказів. Однак у той же час

правоохоронним органам може дедалі більше знадобитися пошук інноваційних способів співпраці під час проведення розслідувань транснаціональних кіберзлочинів. Особливо важливим у цьому відношенні може бути участь у координації підтримки транснаціональних слідчих структур, таких як Глобальний інноваційний центр Інтерполу та Європейський центр по боротьбі з кіберзлочинністю (ЕЦК) та Європолу. Інші формати та ініціативи, такі як Глобальна конференція з кіберпростору, також надають державам можливість розглянути інноваційні підходи до міжнародного співробітництва у боротьбі з кіберзлочинністю [42].

Ще одним компонентом міждержавного інституційного механізму глобального інформаційного суспільства є ЮНЕСКО, яка, згідно з Женевським планом дій 2003 року, була визначена відповідальною за доступ до інформації та знань, електронне навчання, електронну науку, культурне різноманіття та ідентичність, лінгвістику. Різноманітність і місцевий контент, медіа та етичні виміри в інформаційному суспільстві. Комісія ООН з науки і техніки в цілях розвитку є допоміжним органом у структурі ECOSOR. З 2006 року проводить щорічну оцінку результатів реалізації досягнень ВСІС на міжнародному та регіональному рівнях і визначає їх відповідність цілям ВСІС. Комітет є міжурядовим органом і його рішення не мають обов'язкової сили.

З 2004 року в структурі Першого комітету Генеральної Асамблеї ООН чотири рази створювалися Групи урядових експертів для вивчення досягнень у сфері інформації та комунікації в контексті міжнародної безпеки. Влітку 2015 року Четверта група урядових експертів опублікувала звіт, у якому вперше висунула конкретні рекомендації щодо відповідальної поведінки держав у кіберпросторі. Генеральна Асамблея схвалила звіт і вирішила створити нову групу урядових експертів, яка повинна вперше зустрітися в серпні 2016 року в Нью-Йорку. У свою чергу ВОІВ контролює дотримання так званих Інтернет-договорів 1996 року — Договору про авторське право та Договору про виконання та фонограми. Отже, обидва договори зобов'язують держави-члени забезпечити належний рівень правового захисту та ефективні засоби правового

захисту, щоб неможливо було обійти технологічні обмеження, які використовуються для захисту об’єктів інтелектуальної власності. ВОІВ безуспішно намагалася встановити регулятивні положення для веб-трансляції та Інтернет-мовлення та розширення прав на трансляцію в кіберпросторі [43].

З метою координації виконання висновків Всесвітньої конференції на найвищому рівні за рішенням керівництва ООН Координаційний комітет створив Групу з вирішення та запобігання проблемам інформаційного суспільства (2006) як міжвідомчий інструмент. У проекті заходів на 2014-2015 роки група вирішила зосередити свою діяльність на координації просування інформаційно-комунікаційних технологій (пункт 42) у плані формування майбутньої сфери на 2015 рік. Генеральна Асамблея є важливим консультативним органом Організації Об’єднаних Націй, до повноважень якої входить обговорення важливих аспектів, що стосуються інтересів держав-членів та інших країн, особливо тих, що стосуються боротьби з кіберзлочинністю. Під її егідою встановлено цикл дій, що включає заяви про: регулювання інформаційного простору, захист інформаційної інфраструктури, забезпечення безпеки користувачів інтернет-сервісів, впровадження культури кібербезпеки, партнерство, в тому числі обмін даними, зустрічі представників правоохоронних органів на високому рівні, положення про конфіденційність, одноманітність та доступність інформації комп’ютерної системи від несанкціонованого втручання тощо. Вона є організатором компанії спеціалізованих спеціалістів з вивчення питань у сфері боротьби з кіберзлочинністю, координує роботу спеціалізованих установ ООН, які займаються боротьбою з кіберзлочинністю (Управління ООН з наркотиків і злочинності, Організація Об’єднаних Націй з питань освіти, науки і культури, Організація Об’єднаних Націй, Конференція з торгівлі та розвитку, робота Міжнародного союзу електрозв'язку тощо).

Міжнародна конференція, проведена в Дубаї Міжнародним союзом електрозв’язку (МСЕ), спеціалізованою установою ООН, не мала повного успіху, про що свідчить передача управління розподілом доменних імен та IP-

адрес до МСЕ, а через нього до національні органи зв'язку. Однак, незважаючи на суто консультативний характер рішення WCIT-2012, це серйозний результат для країн, які перебувають на шляху розвитку щодо впровадження інформаційного суверенітету. Рішення Дубайської конференції (WCIT-2012) на даному етапі розвитку є розумним і максимально можливим компромісом між інформаційними лідерами та країнами, що розвиваються, воно відкладає загрозу підриву єдності Всесвітньої мережі, хоча й не усуває повністю це свого роду загроза. Водночас досить ефективний підхід Китаю до побудови «національного Інтернету», що функціонує майже як «великий Інтернет», може спровокувати подібні спроби інших країн чи міждержавних об’єднань. Це питання може торкнутися й України, яка у віддаленому майбутньому повинна буде обрати власну позицію щодо цього глобального роз’єднання [44].

Робоча група КВУУ з кібербезпеки та кіберзлочинності провела зустріч у квітні та травні 2013 року під час прямого діалогу з усіма членами, щоб узагальнити отримані рекомендації та обговорити шляхи вдосконалення загальносистемної основи для кібербезпеки та кіберзлочинності [45].

ЮНОДК, як організація, що встановлює стандарти у сфері запобігання злочинності та кримінального правосуддя, слугуватиме платформою для багатосторонніх зв’язків, у яких країни, що розвиваються, повинні займати центральне місце. ЮНОДК продовжуватиме використовувати цілісний, заснований на партнерстві, міждисциплінарний підхід, поєднуючи свій перевірений досвід у сфері законодавства про боротьбу зі злочинністю, правоохоронної діяльності та технологій із конкретним, дуже глибоким досвідом ключових партнерів, які вже ведуть боротьбу з кіберзлочинністю. і навички. ЮНОДК шукатиме партнерства та мобілізуватиме наявні інструменти та досвід, у тому числі з приватного сектору, особливо постачальників послуг Інтернету, для вирішення проблем, характерних для країни. Пріоритетна увага приділятиметься наданню технічної допомоги державам-членам, які її потребують, щоб подолати брак можливостей та професійної підготовки та

надати боротьбі з комп'ютерною злочинністю стабільний і довгостроковий характер.

Перше засідання Міжурядової робочої групи ЮНОДК відбулося у Відні у січні 2011 року після рішення держав-членів про необхідність створення Міжурядової робочої групи ЮНОДК. До складу експертної групи входять представники держав-членів, міжурядових і міжнародних організацій, спеціалізованих установ, приватного сектору та наукових кіл. Під час зустрічі учасники експертної групи обговорили початкову структуру комплексного дослідження з аналізу кіберзлочинності та її правового регулювання. Що стосується законодавчого нагляду, деякі члени підкреслили переваги існуючих міжнародних правових інструментів, включаючи Конвенцію ООН проти транснаціональної організованої злочинності (UNTOC) [46] і Конвенцію Ради Європи про кіберзлочинність [47], а також створення окремі загальні правові документи для регулювання сфери кіберзлочинності. Рішення про розробку такого єдиного документа має бути прийнято після дослідження.

Міжнародний союз електрозв'язку (МСЕ), як спеціалізована установа в системі ООН, відіграє провідну роль у питаннях стандартизації та розвитку телекомунікацій, а також кібербезпеки. Серед інших заходів МСЕ є провідною організацією Всесвітнього саміту з питань інформаційного суспільства (WSIS), який проходив у два етапи: у Женеві, Швейцарія (2003) та в Тунісі (2005) за участю урядів, політиків з усього світу Експерти відбувся обмін думками та досвідом щодо того, як найкраще вирішити нові питання, пов'язані з розвитком глобального інформаційного суспільства, включаючи розробку сумісних стандартів і законів. Результати зустрічі на вищому рівні містяться в Женевській декларації принципів, Женевському плані дій, Туніському зобов'язанні та Туніській програмі інформаційного суспільства [47].

Таким чином, Організація Об'єднаних Націй та її спеціалізовані установи, як організація, метою якої є забезпечення мирної присутності та дипломатичних відносин замість відносин військового характеру, відіграють важливу роль у боротьбі з кіберзлочинністю. Було ухвалено низку правових

законопроектів для підтримки інформаційної безпеки та боротьби з кіберзлочинністю.

Правовий механізм регулювання протидії кіберзлочинності – це чітко визначена та організована система правових засобів, що забезпечує правовий вплив шляхом застосування нормативних положень щодо виникнення, зміни та припинення суспільних відносин у сфері протидії кіберзлочинності, що дозволяє впливати на учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

Характеристики загальних міжнародно-правових норм проти кіберзлочинності такі: 1) Відповідна діяльність зосереджена навколо Організації Об'єднаних Націй та інституцій або організацій, створених за її підтримки; 2) Наразі лише програмні документи та інші стратегічні документи можуть використовуватися як міжнародні правових норм у сфері відповідних відносин; 3) Основною сферою діяльності має стати розробка та розвиток організаційних та законодавчих заходів протидії кіберзлочинності, а також питання взаємодії у цій сфері діяльності; 4) Поліпшення взаємодії між різними національними органами; 5) Існує нагальна потреба у розробці та прийнятті універсальних конвенцій із суміжних питань для забезпечення участі більшості країн у відповідних заходи боротьби з кіберзлочинністю.

РОЗДІЛ 3.
ОПТИМІЗАЦІЯ МІЖНАРОДНО – ПРАВОВОГО СПІВРОБІТНИЦТВА ДЕРЖАВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

3.1. Специфіка міжнародно – правового співробітництва у боротьбі з кіберзлочинністю

Одним із пріоритетних напрямків удосконалення вітчизняної правової системи є впровадження міжнародних концепцій, принципів та ідей. В умовах євроінтеграційного процесу важливою є заміна застарілих способів і засобів регулювання суспільних відносин та задоволення конкретних вимог, які висуває Україна. Актуальність вивчення досвіду зарубіжних країн щодо організації та функціонування систем правового регулювання протидії кіберзлочинності зумовлена тим, що останнім часом ситуація погіршилася із збільшенням кількості кіберзлочинних дій та відсутністю значних успіхів у цій сфері в Україні. Наша країна. Розмір Інтернету свідчить про те, що певні елементи кіберзлочинності не можна обмежити територією однієї країни, і тому, у будь-якому випадку, національне законодавство має відповідати загальноприйнятим стандартам у цій сфері, щоб міжнародне співробітництво було можливим. Крім того, неможливо створити нормативно-правову систему боротьби з кіберзлочинністю без урахування досягнень і помилок зарубіжних країн у формуванні цього інституту.

Протягом останніх двох десятиліть в Україні ведеться активна розробка законів і нормативно-правових актів щодо боротьби з кіберзлочинністю. У багатьох зарубіжних країнах ця система діє вже тривалий час і має позитивні результати, хоча сучасний рівень розвитку кіберзлочинності все ще перевищує інструменти боротьби з нею. Тому, аналізуючи сучасні вітчизняні реалії, можна констатувати недосконаліть цього процесу в Україні та необхідність подальшої трансформації. У цьому контексті актуальним стає питання

позитивного та негативного досвіду інших країн, що є цілком підходящим інструментом для розвитку дослідницького інституту. Тому досвід інших країн у цій сфері корисний для нашої країни і є важливою темою для досліджень.

Обираючи країну, досвід якої є корисним для України, варто виходити з таких критеріїв: 1) стратегічним партнером України є Сполучені Штати, які протягом останніх років надають Україні велику юридичну та фінансову допомогу, тому вона підходить нарощувати свій досвід з огляду на рівень розвитку держави; 2) євроінтеграційні перспективи України безпосередньо залежать від ступеня імплементації європейських стандартів у вітчизняну правову систему; 3) важливо звертатися до досвіду деяких сусідніх країн, щоб порівняти рівень розвитку даного інституту та визначити, що наразі не реалізовано в Україні.

Почнемо з досвіду Сполучених Штатів Америки, як країни, яка страждає від серйозного негативного впливу кіберзлочинців і була однією з перших країн в історії, яка прийняла відповідні нормативно-правові законопроекти. Як слушно зазначає Н. В. Савчук, політика США у сфері кіберпростору мала значний вплив на країни Європейського співтовариства [48, С. 25], тому вивчення її досвіду є актуальним питанням у контексті нашого дослідження. тема. Серед специфікацій Стратегії національної внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес викликає розділ «Кіберзахист», в якому наголошується на необхідності захисту від кібератак у кіберпросторі.

Сполучені Штати Америки вважаються батьківщиною Інтернету та відповідають за забезпечення безпеки кіберпростору для всього онлайн-світу. Крім того, було проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав громадян [49, С. 12]. Тому Сполучені Штати є однією з країн, де надається перевага дослідницькому досвіду. У країні, де постійно проводяться активні кампанії по боротьбі з такими негативними явищами, як кіберзлочинність, безпека всіх громадян є пріоритетною. Сполучені Штати Америки є однією з головних цілей кіберзлочинців з усього світу, тому досвід держави стане в нагоді в розробці

правових інструментів, спрямованих на боротьбу з цим негативним явищем.

Тим не менш, концепція саморегулювання Інтернету є поширеною в Сполучених Штатах Америки, тому спеціальне законодавство в цій сфері представлено лише кількома нормативно-правовими актами. Серед них, наприклад, Закон про електронний підпис, прийнятий у 2000 році. Його основна мета – забезпечення правового режиму електронного підпису в господарських відносинах. У Сполучених Штатах Америки цьому нормативному акту прийнято приписувати ознаку того, що людство вступило в нову епоху — епоху електронної комерції. Сам закон досить лаконічний і встановлює невелику кількість понять і механізмів – в тому числі компетенцію державного органу, відповідального за функціонування всієї інфраструктури в цій сфері, взаємодію її елементів з органами державної влади тощо.

Найбільше нормативно-правових актів прийнято у сферах емісії цінних паперів, захисту інтелектуальної власності, захисту інформації від несанкціонованого доступу, авторського права тощо. Загалом і донедавна адвокати США підтримували точку зору, що для регулювання боротьби з кіберзлочинністю більш важливими є міждержавні, а не національні нормативні правові дії, оскільки введення певних обмежень одним суб’єктом може відповідати інтересам інших сторін. Проте внаслідок терористичних актів 11 вересня 2001 року боротьба з тероризмом, одним із яких є кібертероризм, значно посилилася. Того ж року уряд США прийняв Акт про об’єднану та зміцнену Америку, згідно з яким будь-які дії, що призводять до перерви в роботі або призводять до незаконного проникнення в комп’ютер, класифікуються як тероризм.

У свою чергу, провайдер зобов'язаний надати всю відому інформацію про користувача на першу вимогу ФБР [50]. Тому носій правових норм протидії кіберзлочинності сьогодні пов’язується з боротьбою з кібертероризмом, найбільш небезпечним проявом кіберзлочинності. Відповідно, 17 листопада 2014 року було оголошено, що система електронної пошти Державного департаменту США буде відремонтована після можливого збитку,

спричиненого ймовірною хакерською атакою [51]. Сьогодні Сполучені Штати Америки готові захистити своїх громадян від негативного впливу кіберзлочинців. Зважаючи на загальну кількість кібератак, важливе питання, яке стоїть перед Сполученими Штатами, – це впровадження ефективних слідчих заходів і покарання порушників. Одним із елементів такого процесу є підвищення рівня відповідальності за вчинення комп'ютерних злочинів та захист прав громадян у разі заподіяння шкоди.

Санкції США за деструктивну діяльність у кіберпросторі набагато суворіші, ніж у Європі. Так, у Сполучених Штатах кримінальна відповідальність визначається як неналежне зберігання та обробка особистої інформації або знищення особистої інформації способом, відмінним від передбаченого законом. Натомість у країнах ЄС кримінальне провадження може бути порушено лише у разі порушення національної безпеки та основних прав громадян [52]. Це свідчить про те, що соціальний вимір правового регулювання боротьби з кіберзлочинністю в Сполучених Штатах не був знехтуваний, оскільки захист не лише в інтересах країни, але й інтерес кожного окремого громадянина все ще є дуже важливим.

У контексті боротьби з кіберзлочинністю актуальним є аналіз нормативно-правових актів, які закріплюють повноваження національних органів влади та правоохоронних органів щодо боротьби з кіберзлочинністю.

У 2009 році в Сенаті США було зареєстровано Закон про кібербезпеку 2009 року (Cybersecurity Act of 2009) [53], прийнятий Національним розвідувальним управлінням США, який має на меті суттєво розширити повноваження федерального уряду у сфері кібербезпеки в інтересах національної безпеки..

Законопроект, у разі його ухвалення, може мати серйозний вплив на саму природу сучасного Інтернету, оскільки він допомагає планувати встановлення нових стандартів комп'ютерної безпеки, зокрема шляхом встановлення стандартів, які вимагатимуть обов'язкової ідентифікації користувачів і згоди урядів на перевірку електронної інформації. Юридичні причини вмісту

електронної пошти, переданих файлів, пошукових запитів користувачів кіберпростору тощо. Проте цей закон досі не прийнятий, що є позитивним моментом для захисту прав людини і громадянина. Прийняття такого нормативно-правового акту, який має суттєвий вплив на всі глобальні процеси, безсумнівно, матиме серйозний вплив на всю глобальну систему кібербезпеки, і цей досвід поступово буде використовуватися іншими країнами для довідки.

Крім того, привертає увагу система установ, які беруть участь у боротьбі з кіберзлочинністю: 1) Кіберкомандування США – підрозділ Збройних сил США, основним завданням якого є централізація операцій кібервійни, управління та захист військового комп'ютера США; 2) омп'ютерна команда екстреної готовності США, яка є частиною Національного відділу кіберзахисту Міністерства внутрішньої безпеки США, публікує інформацію про поточні проблеми безпеки, кібер-уразливі цілі та співпрацює з постачальниками програмного забезпечення. для створення спеціальних програмних додатків для усунення лазівок у системах безпеки; 3) Відділ комп'ютерних злочинів та інтелектуальної власності– кримінальний департамент при Міністерстві юстиції США, який розслідує комп'ютерні злочини та порушення прав інтелектуальної власності, а також відповідає за пошук і вилучення цифрових докази в комп'ютерах і мережах [54].

Натомість в Україні наразі існує лише одне подібне відомство – Департамент кіберполіції Національної поліції України, а це означає, що боротьба з кіберзлочинністю ведеться лише на рівні правоохоронних органів, чого в сучасних умовах недостатньо. У Сполучених Штатах є військовий, правоохоронний і судовий рівні, кожен з яких має особливі повноваження. Таким чином, з кіберзлочинністю можна боротися ефективніше. Звернемо увагу на військовий напрямок, який стосується країн, які ведуть неоголошені війни. О. В. Орлов та Ю. М. Онищенко використовують у цьому контексті термін «операції кібервійни». Транслюючи це визначення до реалій сучасної України, зазначимо, що сьогодні існують значні деструктивні впливи на мережу вітчизняних органів державної влади та інші стратегічні цілі країни. Крім того,

значних масштабів набули інформаційні атаки в Інтернеті, особливо в соціальних мережах. Тому цей американський досвід може бути корисним у сучасних умовах.

Тому США, як стратегічний партнер України та одна з найвпливовіших країн світу, продовжують привертати увагу вітчизняних юридичних кіл. Незважаючи на незначну кількість національного законодавства в цій сфері в США, всі правовідносини у сфері користування мережами врегульовані належним чином. Тому США є чудовим прикладом для залучення досвіду правового регулювання боротьби з кіберзлочинністю.

Крім Сполучених Штатів Америки, країни Європейського Союзу, які добре усвідомлюють загрози та небезпеки неконтрольованого використання можливостей кіберпростору в деструктивний спосіб, вже давно впроваджують правове регулювання Інтернету. У контексті просування України до євроінтеграційного процесу корисно будувати позитивний досвід усієї організації та окремих країн, що входять до неї.

Європейський Союз почав розглядати нормативно-правовий захист від кіберзлочинності ще на початку 20-го століття, зокрема в 2001 році з першим документом «Мережева та інформаційна безпека: європейський політичний підхід», у якому було запропоновано окреслити європейський підхід до інформаційної безпеки. Серед них поняття «мережева та інформаційна безпека» відноситься до здатності мережі або інформаційної системи протистояти нещасним випадкам або зловмисним діям, які загрожують доступності, автентичності, цілісності та конфіденційності збережених або переданих даних, а також послуг, що надаються через мережу [55].

Іншими словами, цей нормативно-правовий акт встановлює поняття та категорію порушень кібербезпеки. Прийняття цього документа пов’язане з розумінням Європейським співтовариством ролі кібербезпеки в суспільних відносинах. Позначення терміну «конфіденційність даних» свідчить про те, що розробники законопроекту допускають можливість атак на дані, що містять цінну інформацію з обмеженим доступом. Таким чином Євросоюз почав

готуватися до збою систем зв'язку та можливості запобігання витоку секретної інформації.

Суть документа полягає у визначенні таких напрямків європейської політики кібербезпеки: 1) освітній напрямок, включаючи підвищення обізнаності споживачів кіберпослуг про загрози; 2) створення надійної системи раннього попередження та сповіщення про нові загрози; 3) забезпечення відповідних технічне забезпечення; 4) стандартизація та сертифікація; 5) правове забезпечення; 6) посилення безпеки на національному рівні; 7) міжнародне співробітництво в галузі інформаційної безпеки [56]. Варто резюмувати, що більшість із цих напрямків і сьогодні є пріоритетними. Більше того, деякі з них є сучасними тенденціями розвитку законів і нормативних актів проти кіберзлочинності вже сьогодні. Особливу увагу приділимо напрямку юридичного супроводу.

До прийняття цього дослідницького документа існувало небагато міжнародних законодавчих актів у сфері кібербезпеки, але в подальшому для вирішення проблеми кіберзлочинності європейські країни прийняли низку нормативно-правових актів, серед яких Конвенція про кіберзлочинність, яка була створена Комітетом міністрів Ради Європи в листопаді 2001 р. та ратифікована Україною 7 вересня 2005 р. Тим не менш, наша держава зробила перші кроки до відповідності високим європейським стандартам. Водночас це не свідчить про те, що Україна набагато ближча до провідних європейських країн щодо правового регулювання боротьби з кіберзлочинністю. У цьому контексті важливо зазначити, що навіть у межах Європейського Союзу країни відрізняються своїми людськими та фінансовими можливостями, а отже, і потенціалом організації боротьби з кіберзлочинцями.

Щодо подальшого регулювання питання боротьби з кіберзлочинністю, у травні 2007 року Європейська комісія подала документ «Формулювання загальної політики боротьби з кіберзлочинністю», який вперше об'єднав термін «кіберзлочинність», щоб підкреслити важливість політики ЄС у сфері боротьби з кіберзлочинністю [57]. Кіберзлочинність визначається як злочини, вчинені з

використанням або проти електронних комунікаційних мереж та інформаційних систем. Це поняття включає три категорії злочинів: 1) традиційні форми злочинів (шахрайство та підробка в електронних комунікаційних мережах та інформаційних системах); 2) публікація незаконного контенту в електронних ЗМІ (дитяча порнографія, матеріали, що розпалюють расову ворожнечу тощо) ; 3) специфічні злочини в електронних мережах (атаки на інформаційні системи, хакерство тощо).

Вітчизняні дослідники відзначають роль Комп'ютерної групи швидкого реагування у Брюселі та Європейського центру боротьби з кіберзлочинністю в Гаазі, Європейського агентства з мережевої та інформаційної безпеки. Комп'ютерна група швидкого реагування у Брюселі спрямована на боротьбу з новітніми комп'ютерними вірусами та виявлення слабких місць у системах захисту інформації, розробку Інтернет-стратегії для Європейської комісії та організовує семінари з кібербезпеки з різними установами ЄС.

Тобто сфера діяльності цієї інституції досить широка, включає активну теоретичну, дипломатичну та практичну діяльність. У свою чергу, Європейський центр боротьби з кіберзлочинністю діє на базі Європолу та має на меті надавати інформаційну, оперативну та експертну підтримку розслідувань на міжнародному та регіональному рівнях. Що стосується місії організації, вони полягають у зборі та обробці даних про кіберзлочини, вчинені в Європі, у проведенні експертної оцінки інтернет-загроз, у сприянні обміну інформацією, у розробці передових методів запобігання та розслідування кіберзлочинів, у допомозі правоохоронним органамі судових органів, а також координувати відповідні спільні дії всіх сторін спрямовані на підвищення рівня безпеки в європейському кіберпросторі.

Отже, правові положення ЄС проти кіберзлочинності характеризуються: 1) наявністю національного та міжнародного законодавства проти кіберзлочинності; 2) одночасним здійсненням заходів проти кіберзлочинності національними та міжнародними організаціями, до складу яких входять найкращі експерти з країн-учасниць; 3) акцент з теоретичних питань, таких як

експертна оцінка кіберзлочинності, розробка передових методів запобігання та розслідування тощо 4) Впровадження проактивного обміну інформацією.

Тому виділимо такі шляхи використання позитивного досвіду ЄС в Україні:

1) Розробити національне законодавство на основі європейських стандартів.

2) Поширити діяльність європейських міжнародних організацій проти кіберзлочинності на територію України.

3) Рекомендовано уточнити поняття «кіберзлочин» у вітчизняному законодавстві за допомогою європейського законодавства.

Крім вивчення досвіду Європейського співтовариства в цілому, слід звернутися до аналізу практик основних країн Союзу. Почнемо з аналізу законів і нормативних актів Франції щодо боротьби з кіберзлочинністю, оскільки ця країна однією з перших у Європі вжила заходів для посилення ролі держави в поліцейському кіберпросторі. Отже, сьогодні в країні виявляються такі форми кіберзлочинності: 1) суспільно небезпечні діяння, пов’язані з незаконним копіюванням комп’ютерного програмного забезпечення, незаконним втручанням у роботу систем автоматичної обробки інформації, зломом веб-сайтів, створенням і розповсюдженням шкідливих програм тощо; 2) розповсюдження, продаж наркотиків, расистські, ксенофобські чи антисемітські тенденції, терористичні тенденції, втручання в приватне життя, інструкції щодо використання вибухівки, шахрайська реклама тощо [58, С. 241].

Враховуючи недосконале розуміння та формулювання сутності поняття «кіберзлочинність» у нашій державі, цей досвід має важливі наслідки для впровадження в Україні. Крім того, важливо чітко розподілити проступки за ступенем їх впливу на суспільні процеси в країні та негативними наслідками. Якщо перша форма кіберзлочинності, класифікована за Францією, адекватно врегульована в Україні відповідно до розділу XVI Кримінального кодексу України, то досвід регулювання другої форми кіберзлочинності придатний для

детального аналізу.

Також викликає занепокоєння французьке законодавство, яке встановлює обов'язкову реєстрацію для власників веб-сайтів у країні та кримінальну відповідальність для провайдерів, які пропонують послуги хостингу неідентифікованим користувачам. Ще одним цікавим аспектом нормативного законопроекту є вимога до провайдерів надавати третім особам інформацію про автора сайту, порушення якої тягне за собою кримінальну відповідальність. Крім того, така відповідальність поширюється на неповну або недостовірну інформацію, надану автором французького веб-сайту, а також на місця на серверах, надані постачальником неідентифікованим користувачам. Крім того, за всі сайти, авторство яких не встановлено, відповідальність несе провайдер із можливим покаранням у вигляді позбавлення волі на строк до шести місяців.

З точки зору активної боротьби з кіберзлочинністю, 14 лютого 2008 року у Франції була прийнята стратегія боротьби з кіберзлочинністю, метою якої є співпраця приватних компаній (провайдерів інформаційно-телекомунікаційних послуг) і правоохоронних органів для обміну інформацією та спільної боротьби з кіберзлочинністю. Цікавими аспектами стратегії є налагодження співпраці між провайдерами та поліцією та жандармерією, а також створення курсів для Національної комісії з професійної етики у зв'язках з громадськістю.

Таким чином, правове регулювання Франції щодо боротьби з кіберзлочинністю характеризується: 1) важливою роллю держави в регулюванні суспільних відносин в Інтернеті; 2) контролем користувачів шляхом встановлення вимог авторизації для авторів веб-сайтів; 3) партнерством для швидкого реагування на нові загрози; 4) вести двосторонній діалог з громадянами, надавати вказівки, належним чином роз'яснюючи їхні права та обов'язки як користувачів Інтернету; 5) вільно розвивати напрямки співпраці з іншими країнами, де відбуваються кіберзлочини у Франції, щоб забезпечити доступ до вашої власної мережі.

3.2. Тенденції та перспективи розвитку правового регулювання боротьби з кіберзлочинністю в Україні

Беручи до уваги стан боротьби з кіберзлочинністю в Україні, насамперед слід зазначити, що після укладення Угоди про асоціацію з ЄС почалися відносно серйозні кроки в цьому напрямку, при цьому Україна залишається важливим відкритим простором для кібератак та вчинення практично безперешкодно низки інших кіберзлочинів.

Важливою основою кіберзлочинності є поведінка, яка загрожує суспільству, передбачена Кримінальним законодавством, і це окремо передбачено в Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. З точки зору кримінального права до кіберзлочинності належать лише злочини, передбачені главою XVI Кримінального кодексу України, а в рамках кримінології до цього поняття доцільно віднести й інші злочини, в яких використовуються комп'ютери та Інтернет.

На сьогодні кіберзлочинність в Україні регулюється такими нормативно-правовими актами: Конвенцією про кіберзлочинність, Законом України про ратифікацію Конвенції про кіберзлочинність [59], Кримінальним кодексом України. Останнім часом рівень кіберзлочинності в Україні стрімко зріс.

Однак, на думку експертів, кіберзлочинність не є безпосередньою загрозою для України. Наша держава має унікальний особливий статус, оскільки є однією з найменш підключених до Інтернету країн Європи.

Раніше зазначалося, що Україна входить до трійки лідерів за DDoS-атаками. За даними «Лабораторії Касперського», 12 відсотків усіх атак сталося в Україні.

Служба безпеки України та МВС в особі Управління по боротьбі з кіберзлочинністю опинилися в критичній ситуації. На жаль, їхніх зусиль виявилося недостатньо. Особливо, враховуючи реалії нашої України. Якщо раніше українські розробники програмного забезпечення – хакери –

створювали віруси для злому та крадіжки інформації з багатих західних країн, то відтепер, коли північноамериканські та європейські уряди посилили опір комп'ютерній злочинності, їхні інтереси перемістилися й на Україну.

Низька поінформованість нашої держави про шкідливість використання комп'ютера, низька інформаційна безпека перетворюється на їхній справжній клондайк. Крадіжка коштів в онлайн-банкінгу, даних кредитних карток, DDoS-атаки сайтів, шахрайство в інформаційних мережах і втрата внутрішніх даних стають звичним явищем.

Так, за останні кілька місяців тільки відділ боротьби з кіберзлочинністю Києва, згідно з аналізом експертів, виявив аж 20 випадків розкрадання коштів за допомогою клієнтів банків. Щодо суми втрат, то вона коливалася від 20 до 40 мільйонів. Проте ці дані не є загальнодоступними та майже не висвітлюються в ЗМІ. Шум навколо подібних злочинів не цікавить жертв, а також банки та органи внутрішніх справ. У багатьох випадках це стосується випадків, коли подібними шахрайськими схемами керують сформовані групи, зокрема представники банків та правоохоронних органів.

Проблема в Україні полягає в тому, що національних експертів у сфері комп'ютерної та промислової спеціалізації не вистачає, тому результати досліджень експертів комерційних інституцій складно ввести в правове поле. Через велике завантаження національних спеціалізованих установ типовий термін виконання експертизи комп'ютерної галузі становить шість місяців або більше. Протягом цього терміну підсудний може перебувати під вартою в СІЗО відповідно до закону [60].

Нормативне регулювання даної галузі в Україні не встигає за технологічним розвитком, що загострює проблему кіберзлочинності. На особистому рівні кіберзлочинність пов'язана з використанням піратського програмного забезпечення: злочинці отримують доступ до особистої інформації користувача. В Україні до кіберзлочинності відносяться порушення авторського права та суміжних прав, шахрайство, протиправні дії з використанням документів на переказ грошей, платіжних карток та інших

засобів доступу до банківських рахунків, обладнання, що використовується для виготовлення цих документів, ухилення від сплати податків, зборів (власних платежів) , імпорт, виробництво, продаж і реклама аморальних товарів, підготовка до використання даних, що становлять комерційну або банківську таємницю [61].

Статистика показує, що тільки в період 2015-2021 рр. багато країн світу створили системи кіберкомандування та безпеки як органи державного управління. Їх типова структура складається з підрозділів:

а) мережеві операції;

б) інформаційні операції та інформаційна безпека;

с) підтримка та забезпечення операцій у кіберпросторі;

г) радіоелектронна боротьба;

д) Оперативні (командні) центри (центри управління в кризових ситуаціях) тощо.

Для забезпечення кібербезпеки перш за все необхідно забезпечити захист від руйнівних впливів у цій сфері та протидіяти їм. Тому основними складовими кібербезпеки мають бути кіберрозвідка, кіберзахист і пов'язаний з ними кібервплив [62].

Слід зазначити, що українське законодавство досі не визначає термінів, пов'язаних із правопорушеннями у сфері ІТ. Водночас, як базовий термін у цій сфері кіберзлочинність фігурує в законодавстві деяких країн, особливо США (як базова країна в цій галузі, вона навіть визначає види кіберзлочинності), Нової Зеландії (кіберзлочинність (або комп'ютерний злочин) – будь-який злочин, у якому інформаційно-комунікаційні технології використовуються як засіб злочину; об'єкт злочину; пристрій зберігання даних у злочині), Франція (кіберзлочин означає націлювання на мережу чи інформаційну систему з порушенням міжнародних договорів і національних законів) тощо.

Водночас, з огляду на те, що в нашій країні досі немає легалізованого поняття «кіберзлочин», правоохоронцям доводиться шукати можливості «притягнути» до відповідальності. Насправді мова йде якщо не про зміну чи

створення нового актуального і справедливого нормативно-правового акту, то про додавання статей до кримінального закону, щоб вони не суперечили міжнародним нормам [63].

Європейський напрям розвитку України спонукає до адаптації та імплементації окремих директив ЄС щодо захисту прав інтелектуальної власності у вітчизняну законодавчу систему. Меморандум між урядом України та Всесвітньою організацією інтелектуальної власності (Женева) безпосередньо враховує підготовку висококваліфікованих кадрів з питань управління інтелектуальною власністю та її захисту. У цьому контексті розробка навчального курсу для професійних правоохоронців з питань захисту прав інтелектуальної власності на базі Державної академії внутрішніх справ стане платформою для вивчення нових освітніх проектів, за якими нове покоління юридичних радників має бути навчене захищати українські інноваційні можливості.

На даному етапі вже виявили бажання долучитися до навчання українських експертів міжнародні експерти з державних та суспільних інституцій, які безпосередньо протидіють кіберзлочинності та піратству. Навчальні курси розраховані на правоохоронців МВС, СБУ, фінансових і митних органів, Держспецзв'язку, до безпосередніх обов'язків яких входить захист прав інтелектуальної власності та боротьба з кіберзлочинністю та піратством [64].

На рівні фінансової, правоохоронної та судової систем України існують великі прогалини в статистиці шахрайства, а також відмінності в принципах інтерпретації онлайн-порушень. Це значно знижує ефективність боротьби з кіберзлочинністю.

Наразі в судовій системі відсутній єдиний підхід до судових процедур з питань кіберзлочинності. При прийнятті рішень на власний розсуд судді продовжують керуватися окремими та відмінними правовими нормами.

Тому за вчинення онлайн-злочинів стаття 200 Кримінального кодексу передбачає відносно легкі покарання. Фактично, зараз можна обібрати

банкомат за 500 тис. грн, потім заплатити 85 тис. грн штрафу і залишитися вільним. Потрібно внесені зміни в дану статтю та замінити звичайні штрафи на більш серйозніше покарання [65].

Боротьба з кіберзлочинністю на національному та міжнародному рівнях за допомогою нормативно-правової, організаційної та технічної підтримки. Для виконання умов Угоди про асоціацію, ратифікованої Конвенції Ради Європи про кіберзлочинність, Стратегії національної безпеки (2015) [66], Стратегії кібербезпеки України (2016) [67], Планів дій 2016 щодо виконання Стратегія кібербезпеки України (2016), Доктрина інформаційної безпеки (2017), Рішення РНБО «Про загрози національній кібербезпеці та надзвичайні заходи їх нейтралізація» (2017) [68], Створено Національний координаційний центр з кібербезпеки (2016).

Угода про асоціацію між Україною та Європейським Союзом, ратифікована Законом України від 16 вересня 2014 року № 1678-VII, передбачає, що сторони Угоди співпрацюють у запобіганні та боротьбі зі злочинністю та незаконною організованою чи іншою діяльністю, і спрямовані на вирішення низки ключових проблем, серед яких одна з них – кіберзлочинність. Пріоритетами забезпечення кібербезпеки та безпеки інформаційних ресурсів у Стратегії національної безпеки України визначено: розвиток національної інформаційної інфраструктури, створення систем кібербезпеки, розвиток комп'ютерної мережі реагування на надзвичайні ситуації (CERT), моніторинг кіберпростору з метою своєчасного виявлення запобігання кіберзагрозам та їх усунення; розвиток можливостей правоохоронних органів з розслідування кіберзлочинів; забезпечення захисту об'єктів критичної інфраструктури, національних інформаційних ресурсів від кібератак; відмова від програмного забезпечення, розробленого Російською Федерацією, особливо антивірусного програмного забезпечення; врахування практики держав-членів НАТО та ЄС щодо реформування системи захисту державної таємниці та іншої інформації з обмеженим доступом, захисту

національних інформаційних ресурсів, систем електронного урядування, технічного та криптографічного захисту інформації тощо.

Важливим питанням оперативної та ефективної протидії кіберзлочинності є розробка проекту закону та внесення його до Верховної Ради України в установленому порядку на виконання положень Конвенції про кіберзлочинність, ратифікованої законодавством України від 7 вересня 2005 р. Положення № 2824-ІУ, серед іншого:

● уповноважує правоохоронні органи видавати обов'язкові для виконання приписи власникам комп'ютерних даних (операторам і постачальникам телекомунікацій, іншим юридичним і фізичним особам) терміново записувати та зберігати комп'ютерні дані, необхідні для розкриття злочинів, на термін до 90 днів, а також можливість продовжити цей термін. терміном до 3 років та унормувати порядок розроблення рецептів;

● забезпечувати надання операторам та постачальникам телекомунікацій на запити правоохоронних органів інформації, необхідної для ідентифікації надавачів послуг та шляхів передачі інформації;

● блокування (обмеження) операторами та провайдерами телекомунікацій визначених (ідентифікованих) інформаційних ресурсів (інформаційних послуг) за рішеннями судів;

● запровадити ефективні механізми використання у кримінальному провадженні доказів, зібраних в електронному вигляді під час проведення оперативно-розшукових заходів.

Крім того, в контексті нових загроз національній та міжнародній безпеці, кількість та сила кібератак на країни та фінансові установи зростає щодня на користь окремих країн, груп та окремих осіб, необхідно затвердити суб'єкти кібербезпеки, усі Протоколи спільних дій ключових об'єктів інформаційної інфраструктури (адміністраторів) під час виявлення, запобігання, припинення кібератак та кіберінцидентів та ліквідації їх наслідків.

В Україні на базі НЦБ Інтерполу створено Національний центральний консультативний пункт з питань комп'ютерної злочинності. Це дало змогу

накопичити матеріали щодо національного законодавства та організаційного досвіду протидії кіберзлочинності, підготувати аналітичні огляди та публікації з цих питань, ознайомити працівників МВС, прокуратури з новим видом злочинності та внести конкретні пропозиції, удосконалити кримінальне законодавство України. Міністерство спеціальних телекомунікацій та захисту інформації входить до складу Служби безпеки України. У 2001 році в структурі СБУ МВС України було створено підрозділ по боротьбі зі злочинами у сфері інтелектуальної власності та високих технологій, одним із завдань якого було протидія злочинам у сфері комп'ютерної техніки, інформації, електронних рахунків та телекомунікації.

5 листопада 2015 року була створена нова Кіберполіція як структурний підрозділ Національної поліції. Основною метою створення Кіберполіції є реформування та розвиток підрозділів МВС України, які забезпечуватимуть підготовку та роботу висококваліфікованих спеціалістів поліції, оперативно-розшукових підрозділів, у боротьбі з кіберзлочинність, здатна інтегрувати новітні технології на високому професійному рівні Застосовується до операційної та сервісної діяльності.

15 березня 2016 року Президент видав указ «Про введення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У складі РНБО створено робочий орган – Національний координаційний центр з кібербезпеки. Поява цього органу є виправданою, оскільки в умовах домінування інформаційних технологій вони активно використовуються «для здійснення терористичних актів, у тому числі порушень штатного режиму роботи автоматизованих систем управління технічними процесами в інфраструктурі [69].

Але, на жаль, практика показала, що правоохоронні органи та суди у питаннях кримінального провадження щодо кіберзлочинності часто дотримуються старих усталених практик, які в даному випадку не сприяють ні збору доказової бази, ні вирішенню справи. об'єктивне рішення.

Враховуючи проблеми, які існують у діяльності судових та правоохоронних органів у сфері протидії кіберзлочинності, вирішення або подолання цих проблем має бути спрямоване насамперед на:

• по-перше, гармонізація міжнародного та національного законодавства у сфері протидії кіберзлочинності та внесення відповідних змін до кримінально-процесуального законодавства України, особливо з урахуванням особливостей оцінюваних судами електронних доказів, які найчастіше зустрічаються у кримінальних провадженнях щодо кіберзлочинів;

• по-друге, подальший розвиток окремих криміналістичних методик розслідування кіберзлочинів з урахуванням останніх тенденцій типових способів вчинення таких злочинів;

• по-третє, забезпечити належну професійну підготовку працівників правоохоронних органів та суддів, до обов'язків яких входить розслідування кіберзлочинів та розгляд пов'язаних із ними судових справ [70].

Україна є членом Конвенції про кіберзлочинність (Будапештська конвенція) та бере участь у проекті CyberCrime@EAP з кіберзлочинності в рамках Програми Східного партнерства. У контексті співпраці України з Європейською комісією влада визначила певні стратегічні пріоритети щодо кіберзлочинності та оцінила заходи, вжиті в цьому напрямку. Крім того, Рада Європи надала Україні інструменти боротьби з кіберзлочинністю, зокрема міжнародні заходи, спрямовані на боротьбу з кіберзлочинністю. Тому, аналізуючи поточний стан боротьби з кіберзлочинністю в Україні, варто відзначити певні позитивні зрушення, а саме: рівень співпраці з Європейським Союзом та іншими міжнародними організаціями, створення кіберполіції. Тому, хоча більшість заходів є результатом підписання Угоди про асоціацію з ЄС та вимог Європейського співтовариства, ми також можемо продемонструвати зростання рівня відповідності єдиним міжнародним стандартам боротьби з кіберзлочинністю. Є ще деякі проблеми в Україні сьогодні, які необхідно уважно вивчити, вирішити якнайшвидше та знайти механізм запобігання.

ВИСНОВКИ

У роботі представлені теоретичні узагальнення та нові розв'язання наукових завдань, у тому числі виявлення теоретико-правових основ міжнародно-правових норм боротьби з кіберзлочинністю. Основними результатами роботи є наступні висновки та рекомендації:

1. Кіберзлочин – це найнебезпечніший кіберправопорушення, вчинення якого на всіх стадіях безпосередньо пов'язане з використанням комп'ютерної техніки через або з використанням комп'ютерних систем, за яке чинним законодавством передбачена кримінальна відповідальність.

2. Правовий механізм регулювання протидії кіберзлочинності – це чітко визначена та організована система правових засобів, що забезпечує правовий вплив злочинності шляхом застосування нормативних положень до суспільних відносин, що виникають, змінюються та припиняються у сфері протидії кіберзлочинності, що дозволяє вплинути на бажану поведінку учасників цих відносин для досягнення належної та ефективної боротьби з кіберзлочинністю.

3.Загальні міжнародно-правові норми боротьби з кіберзлочинністю характеризуються наступним чином: 1) відповідна діяльність зосереджена навколо Організації Об'єднаних Націй та створених під її егідою інституцій чи організацій; 3) основною сферою діяльності має бути розробка та розвиток організаційних і законодавчих заходів протидії кіберзлочинності, а також питання співробітництва у цій сфері діяльності; 4) необхідність створення міжнародних спільних органів для здійснення оперативно-розшукової діяльності з метою забезпечення документування вчинених злочинів; 5) покращення взаємодії між різними національними органами; 6) існує нагальна потреба в розробці та прийнятті універсальних конвенцій із відповідних питань, щоб забезпечити участь більшості країн у відповідних заходах по боротьбі з кіберзлочинністю.

Характерними рисами регіональних міжнародних законів і нормативних

актів щодо боротьби з кіберзлочинністю є: 1) регіональні міжнародні організації надають великого значення боротьбі з кіберзлочинністю; 2) було сформульовано низку регіональних угод про співпрацю у сфері боротьби з інформаційною злочинністю; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. - на початку 2000-х рр.; 4) ця діяльність є невід'ємною частиною міжнародних інформаційних відносин і кримінального правосуддя.

4. 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.

Правові положення ЄС проти кіберзлочинності характеризуються наступним: 1) наявність національного та міжнародного законодавства проти кіберзлочинності; 2) одночасне здійснення заходів проти кіберзлочинності національними та міжнародними організаціями, до складу яких входять найкращі експерти з країн-учасниць; 3) наголос на теоретичних питаннях, таких як експертна оцінка кіберзлочинності, розробка передових методів запобігання та розслідування тощо; 4) запровадити проактивний обмін інформацією.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіберзлочинність: проблеми боротьби і прогнози URL: http://anticyber.com. иа/а1Лс1е_бе1аИ.рЬр?ЫI=140 (дата звернення 15.05.2023)

2. Поняття та сутність кібернетичної злочинності UPL :http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425 %3A09121607&са1ЫI=170%3А51216&ИетЫI=211&^=еп. (дата звернення 15.05.2023)

3. Тихомиров О.О. Кіберзлочин: теоретико–правові проблеми. *М*атеріалів наук.–практ. конф. «Інформаційна безпека: виклики і загрози сучасності» (5 квітня 2013 р. м. Київ), 2013. С. 179–182.

4. Пфо О.М. Основні поняття і класифікація кіберзлочинності. *М*атеріали всеукр. наук.–практ. конф.(23–25 листоп. 2016 р. м. Кропивницький), 2016. С. 33–34.

5. Словник термінів із кібербезпеки / За заг. ред. О.В. Копана, Є.Д. Скулиша. – Київ: ВБ «Аванпост–Прим», 2012. 214 с.

6. Проблеми чинної вітчизняної нормативно–правової бази *у* сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка URL: http://www.niss.gov.ua/articles/454 (дата звернення 15.05.2023)

7. Стратегічні комунікації : [словник] *І* Т.В. Попова, В.А. Ліпкан ; за заг. ред. доктора юридичних наук В.А. Ліпка– на. – К. : ФОП Ліпкан О.С., 2016. – 416 с.

8. Конвенція про кіберзлочинність від 23.11.2001 р. Офіційний вісник України. 2007. №65, Ст. 2535

9. Поняття та сутність кібернетичної злочинності URL :http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425 %3A09121607&са1ЫI=170%3А51216&ИетЫI=211&^=еп. (дата звернення 15.05.2023)

10. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру,

вчинених через комп'ютерні системи, від 28.01.2003 р. URL: http://zakon2.rada.gov.ua/laws/show/994_687(дата звернення 15.05.2023) – Назва з екрана.

11. Міщук Н.В. Кіберзлочинність як загроза інформаційному суспільству. Вісник Львівського університету. Серія економічна. 2014. Випуск 51. С. 173–179.

12. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини :навч. посіб. Харків: Право,2014. 513 с.

13. Марків С.І. Кіберзлочинність. Нова кримінальна загроза. URL: http://gurt.org.ua/articles/34602(дата звернення 15.05.2023)

14. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно–структурний аналіз) : монографія. – Київ: КИТ, 2010. 148 с.

15. Бельський Ю. Щодо визначення поняття кіберзлочину. Юридичний вісник. 2014. №6. С. 414–418.

16. Яцишина М. Ю. Проблеми уніфікації поняття кіберзлочинність у міжнародному праві. Науковий вісник Ужгородського національного університету. Ужгород, 2013. Вип. 23. Ч. 1. Т. 3. С. 235–240.

17. Римарчук Г. С. Юридична природа кіберзлочинів. Науковий вісник Ужгородського національного університету: Серія: Право. Ужгород : Видавничий дім «Гельветика», 2014. Вип. 24. Т. 4. С. 50–53.

18. Стратегічні комунікації : словник. Київ : ФОП Ліпкан О.С., 2016. 416 с.

19. Акімов В. Кіберзлочинність URL: http://n–auditor.com.ua/uk/component/na_archive/695?view=material (дата звернення 15.05.2023)

20. Гвоздецька М. О. Кримінологічна характеристика кіберзлочинності : сучасний стан, структура та специфіка вчинення. Актуальні задачі та досягнення у галузі кібербезпеки : матеріали всеукр. наук.–практ. конф.(23–25 листоп. 2016 р. м. Кропивницький), 2016. С. 52–53.

21. Кримінальний Кодекс України : від 05.04.2001 № 2341-III // Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.

22. Омельченко В. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби URL: https://www.gurt.org.ua/articles/34602/ (дата звернення 15.05.2023)

23. Діордіца І. В. Поняття та зміст кіберзлочинності/ URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti/ (дата звернення 15.05.2023) - Назва з екрана.

24. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і Безпека. 2011. № 4. С. 107-112.

25. Кіберзлочинність : проблеми боротьби і прогнози URL: http://anticyber.com.ua/article_detail.php?id=140 (дата звернення 15.05.2023)

26. Надання допомоги країнам у боротьбі з кіберзлочинністю URL: https://www.unodc.org/unodc/ru/frontpage/2015/May/assisting-states-in-their-efforts-against-cybercrime.html (дата звернення 15.05.2023)

27. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. Часопис Академії адвокатури України. 2012. № 17. С. 1-6.

28. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності URL: http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1445%3A31-0117-16&catid=173%3A2-0217&Itemid=216&lang=en (дата звернення 15.05.2023)

29. Орлов О. В. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління. 2013. Вип. 4 (43). С. 1-6

30. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму . Часопис Київського університету права. 2014. № 4. С. 312-317.

31. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Актуальні проблеми міжнародних відносин. 2015. Випуск 126 (частина ІІ). С. 77-90.

32. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN (дата звернення 15.05.2023)

33. Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=j5hEAdZ2(дата звернення 15.05.2023)

34. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva URL: http://cybercrimelaw.net/documents/cybercrime_history.pdf (дата звернення 15.05.2023)

35. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer URL: https://rm.coe.int/168008160f(дата звернення 15.05.2023)

36. Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime URL: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additionalproto/168072362b(дата звернення 15.05.2023)

37. Cybercrime Programme Office (C-PROC) URL: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc31 (дата звернення 15.05.2023)

38. Arab Treaty on Combating Cybercrime URL: http://www.riyadh.om/2015/arabtreaty-on-combating-cybercrime(дата звернення 15.05.2023)

39. The First African Forum on Cybercrime URL: https://au.int/en/newsevents/20181016/first-african-forum-cybercrime(дата звернення 15.05.2023)

40. Security and Prosperity Steering Group URL:https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-andTechnical-Cooperation/Working-Groups/Telecommunications-andInformation/Security-and-Prosperity-Steering-Group. (дата звернення 15.05.2023)

41. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності Право і Безпека. 2015. № 2. С. 107 -113.

42. Тринадцятий Конгрес Організації Об'єднаних Націй щодо попередження злочинності та кримінального правосуддя: Довідковий документ. Доха, 12-19 квітня 2015 року. 25 с.

43. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Актуальні проблеми міжнародних відносин. 2015. Випуск 126 (частина ІІ). С. 77-90.

44. Ожеван М. А. «Спроби впровадження міжнародного контролю за діяльністю в Інтернеті під егідою ООН: нові можливості реалізації Україною інформаційного суверенітету». Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1093/ (дата звернення 15.05.2023)

45. Доповідь Генерального секретаря Генеральна асамблея Двадцята сесія Вікторія-Фоллс, Замбія/Зімбабве, 24-29.08.2013 URL: http://cf.cdn.unwto.org/sites/all/files/pdf/a20_05_i_d _unwto_in_the_united_nations_system_ru_0.pdf(дата звернення 15.05.2023)

46. Конвенція Організації Об’єднаних Націй проти транснаціональної організованої злочинності URL : http://zakon3.rada.gov.ua/laws/show /995_789 (дата звернення 15.05.2023)

47. Конвенція про Кіберзлочинність URL : http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення 15.05.2023)

48. Савчук Н. В. Світовий досвід державного регулювання ринку інтернет- послуг. Формування ринкових відносин в Україні. 2012. № 4. С. 24-28

49. 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 15.05.2023)

50. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism : USA PATRIOT ACT (Act of 2001). Public Law 107-56—OCT. 26, 2001 URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата звернення 15.05.2023)

51. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. Юридичний вісник. Повітряне і космічне право. 2014. № 4. С. 70-75.

52. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. Наукові записки Інституту законодавства Верховної Ради України. 2013. № 3. С. 123-126.

53. Cybersecurity Act of 2010. S. 773 (111th). April 1, 2009. URL: https://www.congress.gov/bill/111th-congress/senate-bill/773 (дата звернення 15.05.2023)

54. Орлов О. В. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам у мережі інтернет. Теорія та практика державного управління. 2014. Вип. 2. С. 212-219.

55. Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM (2001) 298 (June 6, 2001). URL: http://ec.europa.eu/information society/eeurope/2002/news library/pdf files/netse c en.pdf (дата звернення 15.05.2023)

56. Communication from the Commission: Towards a general policy on the fight against cyber crime. Brussels, 22.5.2007. COM(2007) 267 final. URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007 0267en01.pdf (дата звернення 15.05.2023)

57. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин : зб. наук. пр. Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. К., 2009. Вип.87, ч.2. С.36-45.

58. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2008. Вип. 19. С. 240-246

59. Закон України «Про ратифікацію Конвенції про кіберзлочинність» : від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71.

60. Довбиш Н. Кіберзлочинність в Україні. URL: https://www.science-community.org/uk/node/16132 (дата звернення 15.05.2023)

61. Голуб А. Кіберзлочинність у всіх її проявах. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення 15.05.2023)

62. Мельников О. Ф. Реформування державних механізмів боротьби з кіберзлочинністю . Теорія та практика державного управління. 2015. Вип. 3. С. 18-24.

63. Волощук Я. О. Кіберполіція як запорука боротьби з порушеннями права людини на інформацію : міжнародний досвід та проблеми національного законодавства. Національні та міжнародні механізми захисту прав людини : тези доп. Всеукр. круглого столу (20 квітня 2016 р. м. Харків), 2016, Харків. С. 164-166

64. В Україні на базі Національної Академії Внутрішніх Справ готуватимуть спеціалістів по боротьбі з кіберзлочинністю та піратством URL: http://mvs.gov.ua/ua/news/6544_V_Ukraini_na_bazi_Nacionalnoi_akademii_vnutris

hnih_sprav_gotuvatimut_specialistiv_po_borotbi_z_kiberzlochinnistyu_ta_piratstvom.htm (дата звернення 15.05.2023)

65. Савенко С. Кіберзлочинність не спить – як не потрапити у тенета аферистів URL: https://news.finance.ua/ua/news/-/395023/kiberzlochynnist-ne-spyt-yak-ne-potrapyty-v-siti-aferystiv (дата звернення 15.05.2023)

66. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : від 26.05.2015 № 287/2015 URL: http://zakon3.rada.gov.ua/laws/show/287/2015 (дата звернення 15.05.2023)

67. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : від 15 березня 2016 року №96/2016 URL: http://www.president.gov.ua/documents/962016-19836 (дата звернення 15.05.2023)

68. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32» : від 30.08.2017 № 254/2017 URL: http://zakon5.rada.gov.ua/laws/show/254/2017 (дата звернення 15.05.2023)

69. Грибок В. С. Боротьба з кіберзлочинністю в Україні. Проблеми українського суспільства : кіберзлочинність : мат. VII регіонал. міжвузівської студент. наук.-практ. конф. (27 квітня 2017 року, м. Рівне). 2017. С. 70-73.

70. Карачевська Г. Р. Кіберзлочинність – правовий аспект URL: http://ukrainepravo.com/legal_publications/essay-onitlaw/it_law_karachevska_cybercrime/ (дата звернення 15.05.2023)