СЕКЦІЯ 7
АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.9

ПОНЯТТЯ ТА ЗМІСТ КІБЕРЗЛОЧИННОСТІ

Діордіца І.В., к. ю. н., доцент,
доцент кафедри кримінального права і процесу
Національний авіаційний університет

У статті автором було проаналізовано низку дефініцій кіберзлочинності, акцентовано на відсутності уніфікованого. Визначено, що засобом для здійснення кіберзлочину є комп'ютер, а саме комп'ютерні мережі чи комп'ютерні системи. Зазначено, що суб'єктом є осудна фізична особа, яка і притягується до відповідальності. Підтверджено положення про те, що комп'ютер виступає як предмет злочину, а інформаційна безпека – об'єкта. Ці злочини вчиняються у віртуальному (кібернетичному) просторі або в межах комп'ютерних мереж. Аргументовано положення про те, що невідповідність чинного законодавства сучасним викликам та загрозам у кібернетичній сфері також створюють сприятливі умови для виникнення та розвитку кіберзлочинності.

Ключові слова: *кіберзлочин, кібербезпека, кіберпростір, кібернетична сфера, інформаційне суспільство, гібридна війна.*

В статье автором были проанализированы ряд дефиниций киберпреступности, акцент сделан на отсутствии унифицированного. Определено, что средством осуществления киберпреступления является компьютер, а именно компьютерные сети или компьютерные системы. Отмечено, что субъектом является вменяемое физическое лицо, которое и привлекается к ответственности. Подтверждено положение о том, что компьютер выступает в качестве предмета преступления, а информационная безопасность – объектом. Эти преступления совершаются в виртуальном пространстве или в пределах компьютерных сетей. Аргументировано положение о том, что несоответствие существующего законодательства современным вызовам и угрозам в кибернетической сфере также создают благоприятные условия для возникновения и развития киберпреступности.

Ключевые слова: *киберпреступление, кибербезопасность, киберпространство, кибернетическая сфера, информационное общество, гибридная война.*

Diorditsa I.V. THE CONCEPT AND CONTENT OF CYBERSECURITY

It was noted that the computer is used for committing of the computer cybercrime, namely computer networks or computer systems. From a criminal point of view, it is characterized by direct intention, almost eliminating the possibility of negligence. Also it was marked that a convicted individual, who is brought to justice is the subject of the cybercrime. It was stated that this type of crime is aimed at the violating of the activity of the information and computer systems, violation of copyright and related rights, illegal actions with documents transfer, payment cards and other means of access to bank accounts, equipment for their production, etc. It was noted that the consequences of this crime affect not only the interests of individual victims, but also companies, organizations, governments and society as a whole. Cybercrimes more often endanger the vital infrastructure, which in many countries is not controlled by the public sector, and such crimes can have a destabilizing effect on all segments of society. It was argument that the computer is the subject of a crime, and the information security is the object. These crimes are committed in a virtual space or within computer networks. Cybercrimes are committed by the usage of the computer systems or by using of the computer networks and other means of accessing the virtual space, as well as against computer systems, computer networks and computer data.

Key words: *cybercrime, cybersecurity, cyberspace, cybernetic sphere, information society, hybrid war.*

Постановка проблеми. Нині кіберзлочинність – актуальна проблема, з якою зіштовхнулись усі країни у XXI ст. і яка перманентно експоненційно збільшується як за своїми масштабами, так і за рівнем спричиненої шкоди. Незважаючи на комплекс заходів, які вживаються окремими фізичними та юридичними особами, а також державою, кіберзлочинці успішно продовжують свою діяльність у кіберпросторі. У зв'язку із цим нині особливо важливо переглянути усі наявні заходи та активно розробляти нові, що принесуть більшу користь та сформують надійну систему реалізації національних інтересів у кібернетичному просторі через формування надійного механізму профілактику та кіберзлочинності. Ці та інші фактори й зумовлюють актуальність теми наукової статті.

Ступінь розробленості проблеми. Під час написання статті були використані напрацювання різних науковців, зокрема: В.А. Ліпкан [1], О.О. Тихомирова [2], О.М. Пфо [3],

М.А. Погорецького, В.П Шеломенцева [4], Н.В. Міщука [5], С.І. Марківа [6], Ю. Бельського [7] тощо.

Мета статті – дослідити поняття та зміст кіберзлочинності. Заради досягнення мети були поставлені завдання: сформулювати авторське узагальнене розуміння терміна «кіберзлочинність», проаналізувати його ознаки та виокремити види та форми прояву даного явища на сучасному етапі, а також визначити основні суб'єкти та об'єкти.

Виклад основного матеріалу. Перш за все, зауважу, що термін «кіберзлочинність» у національних офіційних нормативно-правових документах не визначений, незважаючи на те, що він вживаються в окремих нормативно-правових актах, що регулюють суспільні відносини в кіберпросторі. Разом із тим саме поняття закріпилося в лексиконі правоохоронних органів розвинених держав Європи і світу. Під ним зазвичай розуміється вид злочинності у сфері комп'ютерної інформації і телекомунікацій, незаконний обіг радіоелектронних і спеціальних технічних засобів, поширення неліцензійного програмного забезпечення для ЕОМ, а також деякі інші види злочинності.

Зазначу, що масштаби кіберзлочинності як транснаціонального явища зумовлюють чисельні проблеми практичного і наукового характеру, вирішення яких може забезпечити нівелювання негативного впливу та мінімізацію темпів та форм його розвитку.

Нині, в умовах ведення гібридної війни РФ проти нашої держави, кіберзлочинність становить для України серйознішу небезпеку, ніж 5 років тому. Однак у рамках наукових досліджень не спостерігається адекватної наукової рефлексії на зазначені питання. Незважаючи на окремі розрізнені зусилля правоохоронних органів, які спрямовані на боротьбу з окремими кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Одна з багатьох причин, на мій погляд, криється в тому, що проголошене завдання щодо створення національної системи кібербезпеки в реальному житті не реалізовано.

У 2008 р. у десятці найбільш небезпечних загроз, що зазначаються фахівцями, були мережі ботів – «цілеспрямовані» атаки на урядові сайти, приватні підприємства та кінцевих користувачів. А в 2013 р., згідно з прогнозом фахівців McAfee, на перший план вийшли загрози, пов'язані з використанням мобільного доступу в мережу.

Злочинність у кіберпросторі – одна з найгостріших проблем, з якою зіткнулося міжнародне співтовариство протягом останніх десятиліть у зв'язку з розвитком інформаційних технологій [8].

Сучасні інформаційно-комунікаційні технології запроваджуються і розвиваються набагато швидше, ніж законодавчі та правоохоронні органи можуть адекватно реагувати на їх збільшення.

Термін «кіберзлочинність» часто вживається поряд із терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) ширше за поняття «комп'ютерна злочинність» (computer crime), і точніше відображає природу такого явища, як злочинність в інформаційному просторі.

Так, Оксфордський тлумачний словник визначає приставку "cyber" як компонент складного слова. Її значення – те, що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке саме визначення дає Кембриджський словник. Таким чином, "cybercrime" – це злочинність, пов'язана як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. Водночас термін "computer crime" в основному стосується злочинів, які скоєні щодо комп'ютерів або комп'ютерних даних. Ідея поділу термінів «кіберзлочинність» і «комп'ютерна злочинність» і використанню першого терміна і закріплена в міжнародному праві. Рада Європи в листопаді 2001 р. прийняла Конвенцію про кіберзлочинність, вживши саме термін "cybercrime", а не "computer crime" [9]. Нині офіційне визначення кіберзлочинності на міжнародному рівні відсутнє.

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дає змогу стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 р. «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання ЕОМ, систем та комп'ютерних мереж» чинного Кримінального кодексу України. Але цього виявляється недостатньо для повного подолання кіберзлочинності в нашій країні.

Тому однією з проблем, на яких доцільно акцентувати, є проблема понятійно-категорійного апарату. Термін «кіберзлочин», яким нині у наукових колах прийнято позначати специфічні види злочинів, віднесених до так званої «кібернетичної сфери», набув на пострадянському просторі достатньо широкого вжитку, не маючи сформованого загальновизнаного юридичного наповнення. Залишається невирішеною проблема не тільки встановлення співвідношення «кіберзлочину» з такими правовими категоріями, як «комп'ютерний злочин», «злочин у сфері комп'ютерної інформації», «злочин у сфері використання комп'ютерів», «злочин у сфері використання інформаційних технологій», або із законодавчим в Україні поняттям «злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а й концептуального визначення місця «кіберзлочину» в системі протиправних діянь, передбачених національним законодавством: як окремого виду цих діянь, як специфічної форми їх скоєння, як того й іншого. Все це ставить під великий сумнів доцільність і можливість нормативного визначення кіберзлочину і впровадження його як окремого виду злочинів кримінальним правом [2, с. 189].

З метою формулювання авторського узагальненого розуміння терміна «*кіберзлочинність*» використано наявні доктринальні та законодавчі дефініції.

Отже, під «*кіберзлочинністю*» пропонується розуміти:

– незаконні дії, які здійснюються людьми, що використовують інформаційні технології зі злочинною метою [3, с. 33], це визначення є досить абстрактним та незрозумілим. Також використання терміна «людина» в юридичних науках є неприйнятним, і в цій дефініції зокрема. Людина – це, перш за все, жива істота, але не всі люди мають можливість використання інформаційних технологій. Крім того, кіборгізація суспільних відносин, подальше поширення ботів створює умови для вчинення ними тих чи інших протиправних дій;

– протиправне втручання в роботу кібернетичних систем, основною керівною ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання зі злочинною метою певної кібернетичної (комп'ютерної) системи, використання зі злочинною метою наявних кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо) [10, с. 85], зазначена дефініція може бути прийнята за приклад під час прийняття відповідних нормативно-правових актів;

– злочини, які вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, з яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [11];

– злочини у сфері комп'ютерної інформації [4, с. 89], тобто під час використання текстової, графічної чи будь-якої іншої інформації (даних), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись за допомогою АЕОМ;

– передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає у протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [12];

– сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, мереж і даних [13, с. 267];

– злочинність у кібернетичному (віртуальному) просторі – просторі комп'ютерно-телекомунікаційних мереж [1, с. 190].

Конвенція «Про кіберзлочинність» також не дає визначення поняття «кіберзлочинність». Водночас в її преамбулі зазначено, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [14].

Отже, в цьому контексті ***кіберзлочинність*** – це дії, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані або у систему; зловживання пристроям; шахрайство; правопорушення, пов'язані з дитячою порнографією; порушення авторських і суміжних прав; правопорушення, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, що тягнуть кримінальну відповідальність [9].

Резюмуючи вищезазначене, акцентую на тому, що, перш за все, засобом для здійснення кіберзлочину є комп'ютер, а саме комп'ютерні мережі чи комп'ютерні системи. З кримінально-правової точки зору, він характеризується прямим умислом, майже виключається можливість недбалості. Також суб'єктом виступає осудна фізична особа. Цей вид злочину спрямований на порушення діяльності інформаційних та комп'ютерних систем, порушення авторських і суміжних прав, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення тощо.

Наслідки кіберзлочинності зачіпають не лише інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство загалом. Кіберзлочини найчастіше ставлять під загрозу життєво важливу як інформаційну, так і взагалі критичну інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства. Таким чином стверджую: кіберзлочинність виступає загрозою національній безпеці в кібернетичній сфері.

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття «кіберзлочин», можна дійти висновку, що серед сучасних українських науковців немає єдиного підходу до визначення поняття «кіберзлочин». Причому підходи досить суттєво відрізняються, що може бути причиною неправильного трактування, а це, у свою чергу, може призвести до неправильної кваліфікації злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівнях.

Кіберзлочини поділяють на види залежно від об'єкта, від предмета посягання, залежно від способів скоєння і т. п.

Найбільш поширена класифікація кіберзлочинів нині ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність. Ця класифікація нині виступає «еталоном», оскільки наявні міжнародні та регіональні документи, а також наукова практика, використовують саме цей поділ.

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

• незаконний доступ – навмисний доступ до цілої комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою;

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

• втручання в систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

• зловживання пристроями, а саме їх виготовлення, продаж, придбання з метою використання, поширення або надання для використання іншим чином;

2) правопорушення, пов'язані з комп'ютерами;

3) правопорушення, пов'язані зі змістом;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [14];

5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [15].

Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злам паролів, крадіжку номерів кредитних карт і інших банківських реквізитів, а також поширення протиправної інформації через інтернет [3, с. 33].

За об'єктом посягання виділяються такі групи кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і комп'ютерних мереж, економічні комп'ютерні злочини, комп'ютерні злочини проти особистих прав і недоторканності приватної сфери, комп'ютерні злочини проти суспільних і державних інтересів. Проте варто відзначити, що багато кіберзлочинів зазіхають відразу на кілька об'єктів. Ще одна категорія злочинів, не включена окремо в Конвенцію Ради Європи (отримала поширення після прийняття Конвенції) – *identity theft*, крадіжка, передача і використання персональних даних із метою вчинення злочинів [5, с. 173].

Нині досить поширеною є така класифікація кіберзлочинів:

1) *агресивні* – кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кібersталкінг (протиправне сексуальне домагання та переслідування іншої особи через інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, поширення цих матеріалів, отримання доступу до них);

2) *неагресивні* – кіберкрадіжка, кібервандалізм, кібершахрайство, кібершпигунство, поширення спаму та вірусних програм [13, с. 156].

Водночас, ***з урахуванням мотивації*** злочинців, кіберзлочини видається можливим умовно розділити на категорії:

• кібершахрайство з метою заволодіння коштами;

• кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу);

• втручання в роботу інформаційних систем із метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам);

• інші злочини [3, с. 34].

Кіберзлочинністю прийнято вважати кримінально карані дії, що передбачають несанкціоноване проникнення в роботу комп'ютерних мереж, комп'ютерних систем та програм, із метою видозміни комп'ютерних даних. При цьому комп'ютер виступає як предмет злочину, а інформаційна безпека – об'єктом [3, с. 33]. Варто зауважити, що *об'єктом кіберзлочинів* є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Найпоширенішими видами кіберзлочинів є також: кардинг, фішинг, вішинг, онлайн-шахрайство, пітратство, кард-шарінг, соціальна інженерія, молвер, протиправний контент, рефайлінг та ін. [6]

Акцентую увагу на таких ***ознаках кіберзлочинності***:

1. Ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Кіберпростір – це модульований за допомогою комп'ютера кібернетичний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться у процесі руху по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі.

2. Кіберзлочини вчиняються за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до кіберпростору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину [13, с. 126].

Цікавою і ґрунтовною є думка фахівця з інформаційної тематики В.М. Бутузова, який виділив свій вичерпний перелік *ознак кіберзлочинів*:

1) ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка. Причому об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації;

2) ознакою віднесення злочинів у сфері високих інформаційних технологій до кіберзлочинів є специфічне середовище вчи-

нення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). Причому об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що мають свій прояв у кіберпросторі. Дослідник посилається на перелік протиправних діянь, які передбачені в Конвенції та Додатковому протоколі до неї. На його думку, тільки діяння з цього переліку можуть бути віднесені до кіберзлочинів [16, с. 119].

Відсутність законодавчо закріплених визначень породжує на теоретичному рівні певні дискусії. Нині нормативно-правове регулювання кіберзлочинності не відповідає сучасному розвитку інформаційних технологій, що загострює проблему кіберзлочинності, перетворюючи її на реальну загрозу національній безпеці України. Щодо фізичних осіб, то кіберзлочинність пов'язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача. Піратство також створює надзвичайно сприятливі умови для виникнення та розвитку кіберзлочинності.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю [6].

Терміни, які вживаються в Конвенції та додатковому протоколі до неї, так і не знайшли свого визначення у вітчизняному законодавстві. Так, у Законі України «Про основи національної безпеки України» згадуються терміни «комп'ютерна злочинність» та «комп'ютерний тероризм», проте закон не дає визначення цим поняттям, також ці визначення відсутні в інших нормативних актах. Не визначено й поняття «комп'ютерний тероризм» (кібертероризм) у Законі України «Про боротьбу з тероризмом», а питання, які можуть охоплюватися цим поняттям, частково викладені як складова частина поняття «технологічний тероризм» [7, с. 414].

Варто зазначити, що в «Доктрині інформаційної безпеки України» згадувалися поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», а також питання захисту інформації від «кібернетичних атак». Проте в жодному з перелічених актів так і не було відображено визначення цих понять.

Відзначу, що частина цих деліктів передбачена як злочини в КК України у Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Поряд із цим суспільні відносини в даній сфері регулюються низкою підзаконних нормативно-правових актів.

В Указі Президента України Про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. «Про Концепцію розвитку сектору безпеки і оборони України» від 14 березня 2016 р. неодноразово вживаються поняття «кіберзлочин», «кіберзлочинність», «кіберзагроза», «кібербезпека», «кібершпигунство» та інші, однак не дається визначення жодному з цих понять.

4 червня 2013 р. був зареєстрований проект закону «Про кібернетичну безпеку України», однак в ньому також не міститься визначення поняття «кіберзлочинність» чи «кіберзлочин». Пізніше, у проекті закону «Про основні засади забезпечення кібербезпеки України» № 2126а, зареєстрованому 19.06.2015 р., під *кіберзлочином* визначають суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність, а під кіберзлочинністю – сукупність кіберзлочинів [9].

Нині питання кіберзлочинності є надзвичайно актуальним на державному рівні. Найчастіше кіберзлочини стосуються об'єктів критичної інфраструктури, зокрема інформаційної інфраструктури: енергетичні об'єкти, транспорт та банківський сектор.

Таким чином, протидія та попередження кіберзлочинності та рівень кібербезпеки нині є одним із найпріоритетніших напрямів у політиці нашої держави. Але заради комплексної боротьби з цією проблемою необхідні спільні зусилля держави, громадян та міжнародної спільноти загалом.

Проблема профілактики кіберзлочинності в Україні – це комплексна проблема. Нині закони мають відповідати сучасним реаліям, а не рівню розвитку чи то науки, чи то розуміння правлячої групи щодо пріоритетності тих чи інших національних інтересів. Розвиток технологій, кіборгізація та подальше впровадження штучного інтелекту в наше життя – це вже не майбутнє, а сьогодення. Тому будь-які подальші рефлексії з цього питання лишень затягуватимуть час тоді, коли відносини у кіберпросторі розвиваються швидкоплинно і нелінійно.

Пріоритетним напрямом є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх не лише найсучаснішою матеріально-технічною базою, а й розвиток акмеологічних засад кібербезпекової освіти, підготовка відповідних фахівців. Жодна держава нині не в змозі самотужки протистояти кіберзлочинності. Нагальною необхідністю є активізація участі України в інтересах національної безпеки в різноманітних системах міжнародної та глобальної інформаційної безпеки, посилення співпраці з всесвітніми інформаційними гігантами: Facebook, Apple, Google із залученням широкого кола аналітичних центрів, зокрема недержавних та інститутів громадянського суспільства.

Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, безпосередню шкоду вони завдають у реальному світі. Яскравим прикладом стала масштабна атака вірусу Petya на українські ресурси, виведення з ладу чисельних інформаційних систем органів державної влади України.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно.

Висновки. Відсутність уніфікованого визначення терміна «кіберзлочинність» створює сприятливі умови для виникнення та неможливості вирішення низки проблем. Невідповідність чинного законодавства сучасним загрозам та небезпекам у кібернетичній сфері також сприяють виникненню та розвитку кіберзлочинності. Суб'єктом даного виду злочинів є фізична осудна людина, об'єктом є, перш за все, кібербезпека. Кіберзлочини найчастіше ставлять під загрозу життєво важливу інфраструктуру. Кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

ЛІТЕРАТУРА:

1. Стратегічні комунікації : [словник] / Т.В. Попова, В.А. Ліпкан ; за заг. ред. доктора юридичних наук В.А. Ліпкана. – К. : ФОП Ліпкан О.С., 2016. – 416 с.
2. Тихомиров О.О. Кіберзлочин: теоретико-правові проблеми / О.О. Тихомиров // Зб. матеріалів наук.-практ. конф. «Інформаційна безпека: виклики і загрози сучасності»; 5 квітня 2013 р. – К. : Наук.-вид. центр НА СБ України. – 2013. – С. 179–182.
3. Пфо О.М. Основні поняття і класифікація кіберзлочинності / О.М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 33–34.
4. Погорецький М.А. Кіберзлочини: до визначення поняття / М.А. Погорецький, В.П. Шеломенцев // Вісник прокуратури. – 2012. – № 8. – С. 89–96.
5. Міщук Н.В. Кіберзлочинність як загроза інформаційному суспільству / Н.В. Міщук // Вісник Львівського університету. Серія економічна. – 2014. – Випуск 51. – С. 173–179.
6. Марків С.І. Кіберзлочинність. Нова кримінальна загроза / С.І. Марків [Електронний ресурс]. – Режим доступу : http://gurt.org.ua/articles/34602.
7. Бельський Ю. Щодо визначення поняття кіберзлочину / Ю. Бельський // Юридичний вісник. – 2014. – № 6. – С. 414–418.
8. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. – Режим доступу : http://anticyber.com.ua/article_detail.php?id=140.
9. Поняття та сутність кібернетичної злочинності [Електронний ресурс]. – Режим доступу : http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en.
10. Словник термінів із кібербезпеки / За заг. ред. О.В. Копана, Є.Д. Скулиша. – К. : ВБ «Аванпост-Прим», 2012. – 214 с.
11. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/454.
12. Стратегія забезпечення кібернетичної безпеки України (Проект) [Електронний ресурс]. – Режим доступу : www.niss.gov.ua/public/File/2013_nauk.../kiberstrateg.pdf.
13. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини [Навчальний посібник] / В.В. Голіна, Б.М. Головкін. – Х.: Право, 2014. – 513 с.
14. Конвенція про кіберзлочинність від 23.11.2001 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.
15. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_687.
16. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В.М. Бутузов. – К. : КИТ, 2010. – 148 с.