ПИТАННЯ КРИМІНАЛЬНОГО ПРАВА, КРИМІНОЛОГІЇ ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

ГРИЦУН О. О.,
здобувач кафедри міжнародного права
(Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка)

УДК 341:343.34:316.774

КРИМІНАЛЬНИЙ АСПЕКТ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті детально аналізується кримінальний аспект міжнародної інформаційної безпеки, а саме питання кіберзлочинності. Стаття присвячена огляду теоретичних концепцій щодо розуміння вищезазначеної проблематики та порівнянню різних підходів до визначення і класифікації кіберзлочинів. Крім цього у статті проаналізовано наукові підходи щодо розробки правової основи боротьби із кіберзлочинністю на глобальному рівні.

Ключові слова: *кіберзлочинність, комп'ютерна злочинність, інформаційна злочинність, високотехнологічні злочини, злочини, пов'язані з використанням мережі Інтернет.*

В статье подробно анализируется уголовный аспект международной информационной безопасности, а именно вопросы киберпреступности. Статья посвящена обзору теоретических концепций понимания вышеупомянутой проблематики, а также сравнению разных подходов к определению и классификации киберпреступлений. Кроме этого в статье проанализированы научные подходы к разработке правовой основы борьбы с киберпреступностью на глобальном уровне.

Ключевые слова: *киберпреступность, компьютерная преступность, информационная преступность, высокотехнологические преступления, преступления, связанные с использованием сети Интернет.*

This article analyzes in detail criminal aspect of international information security, namely issue of cybercrime. The article provides an overview of theoretical concepts in understanding above mentioned problems, comparing different approaches to definition and classification of cybercrime, as well as article analyzes scientific approaches to develop a legal framework on combating cybercrimes at the global level.

Key words: *cybercrime, computer crime, information crimes, high-tech crimes, Internet crimes.*

Вступ. Невпинні процеси глобалізації, поява нових видів технологій та масштаби впровадження і використання інформаційно-комунікаційних технологій по всьому світу сприяють не лише появі все нових різновидів кіберзлочинів, а й загострюють проблему боротьби із кіберзлочинністю. Актуальність досліджуваної теми не викликає сумнівів, оскільки кіберзлочинність визнано міжнародним співтовариством в якості загрози в сфері забезпечення міжнародної інформаційної безпеки. Проблему боротьби із кіберзлочинністю загострює і той факт, що єдиного визначення кіберзлочинності не існує, а тому під це визначення підпадає величезна кількість протиправних діянь, що ускладнює можливість їх класифікації та уніфікації.

Окремі теоретичні підходи до розуміння кіберзлочинності та класифікації кіберзлочинів розглядались у працях Т. Крона, К. Хейла,М. Гудмана, М. Форста, С. Гордона, Р. Форда,

Ш. Шольберга, С. Рассела, А. Щетилова, В. Номоконова, Т. Тропініної, С. Бренера, К. Вілсона та ряду інших науковців. Проте малодослідженим залишилось питання комплексного аналізу теоретичних підходів до розуміння кіберзлочинності та їх порівняльної характеристики.

Постановка завдання. Мета статті полягає у проведенні комплексного аналізу теоретичних та наукових підходів до визначення поняття кіберзлочинності, а також наукових підходів щодо розробки загального документа з питань боротьби із кіберзлочинністю.

Результати дослідження. Існує велика кількість термінів, що часто використовуються як синоніми для опису злочинів, скоєних з використанням комп'ютерів, серед них: комп'ютерні злочини; кіберзлочини; злочини, пов'язані з використанням комп'ютерів; віртуальні злочини; цифрові злочини; високотехнологічні злочини; злочини, пов'язані з використанням мережі Інтернет; злочини, пов'язані з використанням телекомунікаційних систем та електронні злочини.

Цікавим є підхід до термінологічної бази, запропонований Т. Кроном. Зокрема, термін «комп'ютерний злочин» він розуміє як загальне визначення усіх злочинів, в яких комп'ютер є об'єктом злочину чи інструментом для його вчинення [1]. До поняття «інтернет-злочини» він відносить злочини, в яких використання Інтернету є ключовою особливістю, а також злочини, пов'язані з використанням контенту, такі як розповсюдження дитячої порнографії чи матеріалів расистського характеру. Відповідно до його категоризації «злочини, пов'язані з використанням комп'ютерів» – це злочини, в яких комп'ютер є невід'ємною частиною скоєння злочину. До таких злочинів він відносить комп'ютерну підробку даних та комп'ютерне шахрайство. «Електронними злочинами» Т. Крон називає злочини, вчинені з використанням електронних баз даних чи комунікаційних пристроїв. Що стосується визначення «кіберзлочинів», то Т. Крон підкреслює, що це поняття може вживатись у двох значеннях: як злочини проти комп'ютерних даних та систем, так і у більш широкому значенні, враховуючи міжнародний підхід, а саме Конвенцію Ради Європи про кіберзлочинність, в якій кіберзлочинність розуміється як узагальнюючий термін щодо правопорушень проти комп'ютерних даних та систем; правопорушень, пов'язаних з комп'ютерами; з порушенням авторських та суміжних прав, та зі змістом. Остання категорія злочинів, якій Т. Крон приділив увагу у своєму дослідженні, – це «високотехнологічні злочини». Існують різні підходи до їх розуміння. Зокрема суперечки точаться навколо питання: чи можна вважати інформаційно-комунікаційне обладнання, послуги та дані об'єктом правопорушення, чи інформаційно-комунікаційні технології є лише інструментом для здійснення злочину? Безсумнівним є лише той факт, що до високотехнологічних злочинів відносять злочини, в скоєнні яких основну роль відіграють інформаційно-комунікаційні технології [1].

Кріс Хейл визначає кіберзлочинність, як «діяльність, що здійснюється за допомогою комп'ютера, і яка є незаконною чи вважається такою окремою стороною, та яку можна здійснювати за допомогою глобальних електронних мереж» [2]. Відповідно до цього визначення автор розподіляє кіберзлочини на дві групи: кіберзлочини, в яких комп'ютер є об'єктом злочинної діяльності та кіберзлочини, в яких комп'ютер є інструментом у вчиненні злочину. До першої групи автор відносить такі злочини, як злом комп'ютерних мереж, промислове шпигунство та комп'ютерний саботаж, а до другої – кіберпереслідування, кібершахрайство, крадіжку програмного забезпечення, крадіжку особистих даних та дитячу порнографію [2].

На позиції більш широкого розуміння кіберзлочинності стоять і Марк Гудман та С'юзан Бренер. На їх думку до поняття кіберзлочинності відноситься надзвичайно широкий спектр злочинів від економічних, наприклад, шахрайство, крадіжка, промислове шпигунство, саботаж, вимагання та піратство, до посягань на недоторканність приватного життя, розповсюдження матеріалів, що пропагують жорстокість і проституцію, а також інші злочини проти суспільної моралі та інші види організованої злочинності. Вищезазначені науковці звертають увагу і на той факт, що часто кіберзлочини «граничать» із поняттям «кібертероризм», оскільки злочинні дій нерідко спрямовані проти об'єктів критично важливих інфраструктур, об'єктів підвищеної небезпеки та інших життєво необхідних об'єктів. Ці поняття часто переплітаються, оскільки в обох випадках компонент «кібер» означає скоєння якісно нових злочинів за допомогою інформаційних технологій, або ж інтеграції кіберпростору в більш традиційні види діяльності, наприклад, планування злочинів, розвідувальна діяльність, їх фінансування та інше. Проведення чіткої межі між цими поняттями є досить

умовним, а іноді неможливим, саме тому автори обмежились наданням умовної класифікації усіх діянь, що на їх думку можуть бути віднесені до поняття «кіберзлочин», оминувши пошук визначення самого поняття. До таких діянь було віднесено: незаконне втручання в роботу комп'ютерної системи, програм чи баз даних, та пов'язана із цим діяльність; розповсюдження вірусів та інших шкідливих програм; шахрайство та крадіжки; азартні ігри, розповсюдження порнографії та інші злочини проти моралі; дитяча порнографія та злочини проти неповнолітніх; переслідування, цькування та пропаганда ненависті; інші види злочинів проти особистості; кібертероризм [3].

Досліджуючи поняття кіберзлочинності, Мартін Форст зазначає, що це поняття стосується «усіх видів незаконної діяльності, що вчинені шляхом використання або за допомогою комп'ютерів чи інформаційних технологій, або в яких комп'ютери є об'єктом злочинної діяльності» [4].

Сара Гордон та Річард Форд у своєму дослідженні щодо кіберзлочинності пропонують визначати кіберзлочин, як «будь-який злочин, якому посприяло, або який було вчинено з використанням комп'ютера, мережі або електронного пристрою» [5]. Крім цього, усі кіберзлочини автори умовно розділили на дві категорії. До першої категорії увійшли кіберзлочини, що в переважній більшості мають технологічний характер, а до другої – кіберзлочини, що мають більш виражений людський фактор. На їх думку, перша категорія злочинів відрізняється такими характеристиками: 1) з точки зору жертви − це, зазвичай, одноразова дискретна подія; 2) такі злочини вчиняються за допомогою проникнення в комп'ютерну систему користувача різних видів вірусів, руткітів, троянів та інших шпигунів; 3) як правило, сприяти такому проникненню можуть вразливі місця в захисті комп'ютерної системи жертви. До другої категорії злочинів автори відносять таку діяльність, як віртуальне переслідування та цькування, наруга над дітьми, вимагання, шантаж, маніпуляції на фондових ринках та інші [5].

Аналізуючи проблему кіберзлочинності, Кларк Вілсон звертає увагу на те, що єдиного погодженого визначення кіберзлочинності не існує, оскільки кіберпростір – це лише новий інструмент, що використовується для вчинення вже відомих злочинів. До кіберзлочинів, на його думку, можна віднести крадіжку інтелектуальної власності, порушення патентів, крадіжку комерційної таємниці, порушення авторських та суміжних прав, а також атаки проти комп'ютерів, навмисне порушення обробки даних, електронне шпигунство з метою несанкціонованого отримання інформації та секретних даних. Він визначає кіберзлочин, як злочин, що вчинено за допомогою комп'ютера, або ціллю якого є комп'ютери. Його підхід викликає цікавість ще й тому, що він наполягає на тому, що якщо терористична група вчинила кібератаки з метою заподіяння шкоди, то таке діяння цілком вписується в розуміння кіберзлочинності, оскільки основна різниця між кібератаками, спрямованими на заподіяння шкоди, та кібератаками, спрямованими на досягнення терористичних цілей, полягає лише в намірах зловмисника [6].

Неможливо оминути увагою дослідження, проведене Смітом Расселом та його співавторами. Детально дослідивши питання кіберзлочинності, вони зосередились на так званій теорії «3-елементної профілактики злочинності», під якою розуміється система кримінального правосуддя, яка могла б стримувати правопорушників, обмежувати їх дії та поновлювати правопорушників в їхніх правах. Автори дійшли висновку, що «кіберзлочинність – це будь-яка заборонена поведінка, що здійснюється шляхом використання чи проти цифрових технологій [7].

Відповідно до свого розуміння автори розподілили усі діяння, які можна розглядати як кіберзлочини, на 3 групи: 1) діяння, в яких цифрові технології використовуються для вчинення правопорушення, наприклад, поширення заборонених матеріалів в електронному вигляді, онлайн-шахрайства та фінансові злочини, електронні маніпуляції на фондових ринках, а також поширення неправдивої рекламної інформації; 2) діяння, спрямовані проти комп'ютерних та комунікаційних технологій, зокрема, несанкціонований доступ до комп'ютерів та комп'ютерних мереж, злочини, пов'язані з актами вандалізму та вторгненням в особистий простір, наприклад, кіберпереслідування, атаки, спрямовані на відмову в обслуговуванні, а також крадіжка телекомунікаційних та інтернет-послуг; 3) супутні діяння, пов'язані з вчиненням злочину, наприклад, кодування, записи на прихованих носіях інформації з метою приховування інформації, або криптографія, тобто вбудовування інформації

в інші дані, наприклад, у фотографії, використання електронних баз даних для зберігання інформації про майбутні чи вчинені злочини.

Вищезазначена класифікація кіберзлочинів Сміта Рассела ґрунтується не лише на законодавчих нормах, а й враховує судову практику [7].

Деякі автори справедливо зауважують, що поняття «кіберзлочини» та «комп'ютерні злочини» часто ототожнюють, проте не всі з цим погоджуються. Існує ще один погляд на розмежування цих понять: до комп'ютерних злочинів відносять злочини, для вчинення яких зловмисники використовують комп'ютер чи комп'ютери, а до кіберзлочинів – злочини, в яких зловмисниками використовуються комп'ютерні мережі. Проте, зазвичай, в наукових цілях використовують широкий підхід до розуміння кіберзлочинів. Такий підхід поєднує у собі елементи обох вищезазначених визначень та відповідно до якого кіберзлочинність розглядається як «злочини, в яких комп'ютери використовуються, як інструменти для вчинення злочину, або як об'єкт правопорушення, або ж злочини, які було скоєно за допомогою засобів зв'язку в мережі» [8].

Існує ще одна точка зору щодо розмежування понять «кіберзлочинність» та «комп'ютерна злочинність». Оскільки комп'ютерними злочинами вважаються злочини, які зазіхають на безпечне функціонування комп'ютерів та комп'ютерних мереж, а також на дані, які вони обробляють, а кіберзлочинами – усі злочини в сфері інформаційних технологій, включаючи злочини, здійснені за допомогою комп'ютерів, та злочини, предметом яких є комп'ютери, комп'ютерні мережі та інформація, що зберігається на цих носіях, то, відповідно до цієї теорії комп'ютерні злочини є різновидом кіберзлочинів [9].

На такій же позиції розуміння кіберзлочинів стоїть А. Щетилов, оскількивважає за недоцільне обмежувати поняття кіберзлочинів лише мережею Інтернет. Він наполягає на тому, що поняття кіберзлочинності поширюється на усі види злочинів, що здійснюються в інформаційно-комунікаційній сфері, де інформація, інформаційні ресурси, техніка можуть бути предметом або ціллю злочинних дій, середовищем їх вчинення чи засобом злочину [10; 187].

Продовжуючи тему термінологічних розбіжностей, варто звернутись до спеціального глосарію у сфері міжнародної інформаційної безпеки з перекладом ключових термінів на дві мови – англійську та російську «Російсько-американського базового переліку критичних понять у сфері кібербезпеки». Обидві редакції глосарію містять лише визначення поняття «кіберзлочин», під яким розуміється «використання кіберпростору в злочинних цілях, що визначаються такими національним чи міжнародним законодавством» [11]. На відміну від згаданого глосарію словник-довідник з інформаційної безпеки для Парламентської Асамблеї Організації Договору про колективну безпеку 2014 року містить визначення «інформаційної злочинності» та «міжнародної інформаційної злочинності». Відповідно до словника ОДКБ міжнародна інформаційна злочинність – це «використання телекомунікаційних, інформаційних систем та ресурсів і вплив на такі системи та ресурси в міжнародному інформаційному просторі в протиправних цілях», а інформаційна злочинність – це «використання інформаційних ресурсів та (чи) вплив на них в інформаційному просторі в протиправних цілях» [12].

А. Осипенко виділяє такі характерні особливості для більшості злочинів, які здійснюються в комп'ютерних мережах: 1) підвищена секретність здійснення злочинів; 2) транскордонний характер мережевих злочинів; 3) інтелектуальний характер злочинної діяльності; 4) своєрідність, складність та різноманіття способів здійснення злочинів та застосування спеціальних засобів; 5) можливість здійснення злочину в різних місцях одночасно; 6) дистанційний характер злочинних діянь, оскільки фізичний контакт між злочинцем та потерпілим відсутній; 7) необізнаність потерпілих про те, що вони стали жертвами злочинів; 8) багаторазовий характер злочинних дій і велика кількість потерпілих; 9) неможливість попередження та запобігання кіберзлочинам звичайними засобами [13, с. 109−110].

Було здійснено кілька наукових спроб щодо розробки правової основи для вирішення проблеми кіберзлочинності на глобальному рівні. Однією із таких спроб є проект Стенфордської міжнародної конвенції щодо посилення захисту від загроз кіберзлочинності та тероризму. У проекті під кіберзлочинністю розуміються «дії щодо кібернетичних систем, за які відповідно до положень проекту конвенції передбачено відповідальність» [14]. Зупинимось детальніше на вищезгаданих злочинах. Згідно з положеннями проекту конвенції злочинами визнаються такі діяння, вчинені особою незаконно та навмисно без дозволу чи згоди упов-

новаженого органу: 1) створення, зберігання, зміна, знищення, переміщення, переадресація, підробка чи втручання в дані чи програми кіберсистем із метою спричинення, знаючи, що така діяльність може спричинити зупинення функціонування кіберсистем; 2) створення, зберігання, зміна, знищення, переміщення, переадресація, підробка чи втручання в дані кіберсистем із метою надання неправдивої інформації, що може спричинити істотну шкоду особам чи майну; 3) втручання у кіберсистеми, доступ до яких явно обмежено; 4) втручання в особливо-чутливі чи аутентичні механізми; 5) створення, продаж, використання, пересилка чи розповсюдження іншим чином будь-яких пристроїв чи програм, спрямованих на вчинення забороненої конвенцією діяльності; 6) використання кіберсистем в якості матеріальної передумови для вчинення дій, що визнані незаконними чи забороненими наданим переліком міжнародних конвенції; 7) участь у вчиненні будь-яких дій, заборонених відповідно до положень проекту з метою нанесення шкоди критичній інфраструктурі будь-якої із договірних сторін. Також проектом конвенції злочинами визнаються незаконні та навмисні спроби вчинення будь-якого із вищеперерахованих злочинів, фінансування чи підбурення інших осіб до вчинення чи намагання вчинити зазначені злочини та змова з метою їх вчинення [14].

Загалом, проект Стенфордської конвенції охоплює як питання матеріального права, так і процесуального, а також питання міжнародного співробітництва. Проект містить статті щодо вдосконалення національного законодавства договірних сторін, юрисдикції, взаємної правової допомоги, екстрадиції, кримінального переслідування, заходів щодо забезпечення позовів, питання щодо розширення прав обвинувачених осіб, співпраці правоохоронних органів, захисту права на приватність та інших прав людини [15]. Цікавим є підхід, закріплений у проекті конвенції щодо створення спеціалізованої установи з питань захисту інформаційної інфраструктури з відповідним колом повноважень та процедури щорічних доповідей договірних сторін. Проект отримав низку схвальних відповідей, але й немало зауважень, та залишився лише одним із наукових підходів до вирішення проблеми кіберзлочинності на міжнародному рівні.

Ще однією спробою науковців щодо розробки загального документа з питань кіберзлочинності став проект Загального договору з питань кібербезпеки та кіберзлочинності, запропонований професором Штайном Шольбергом та професором Соланж Гернуті-Елі. Цей документ складається із 25 статей та регулює питання матеріального кримінального права, процесуального права, питання обміну інформацією та міжнародного співробітництва, а також заходи щодо заборони використання мережі Інтернет в терористичних цілях та ряд інших питань [16].

Висновки. Проаналізувавши різні наукові підходи до розуміння природи та визначення такого складного поняття як кіберзлочинність, ми дійшли висновку, що термінологічні та концептуальні розбіжності в розумінні цього поняття та відсутність узгодженого критерію щодо класифікації діянь, які можна розглядати як кіберзлочинність, унеможливлюють визначення єдиного терміну для розуміння кіберзлочинності.

Проте усі вищезгадані наукові підходи свідчать про те, що, зазвичай, кіберзлочинність розглядають у вузькому на широкому сенсі. У вузькому сенсі її часто ототожнюють із комп'ютерною злочинністю, розуміючи як протизаконну поведінку в формі електронних операцій, спрямовану проти безпеки комп'ютерних систем та даних, а в широкому сенсі – як протизаконну поведінку, що здійснюється шляхом використання чи по відношенню до комп'ютерної системи, чи мережі.

Не дивлячись на те, що єдиного уніфікованого визначення кіберзлочинності наразі не існує, міжнародні організації та законодавці більшості країн використовують типологію різних видів кіберзлочинів для врегулювання питань, пов'язаних із попередженням та боротьбою з кіберзлочинністю.

Список використаних джерел:

1. Krone T. High tech crime brief Australian Institute of Criminology [Електронний ресурс] / T. Krone. – // Режим доступу: http://aic.gov.au/publications/current%20series/htcb/1-20/htcb001.html.

2. Hale C. Cybercrime: Facts and Figures Concerning this Global Dilemma [Електронний ресурс] / C. Hale. – // Режим доступу: http://www.cjimagazine.com/archives/cji4411.html?id=37.

3. Goodman M. D., Brenner S. W. The Emerging Consensus on Criminal Conduct in Cyberspace [Електронний ресурс] / M. D. Goodman, S. W. Brenner. – // Режим доступу: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php.

4. Forst M. L. Cybercrime: Appellate Court Interpretations [Електронний ресурс] / M. L. Forst.– // Режим доступу:https://www.ncjrs.gov/App/publications/abstract.aspx?ID=181163.

5. Gordon S., Ford R. On the definition and classification of cybercrime [Електронний ресурс] / S. Gordon, R. Ford. – // Режим доступу: http://link.springer.com/article/10.1007%2Fs11416-006-0015-z.

6. Wilson C. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy [Електронний ресурс] / C. Wilson. – // Режим доступу: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

7. Smith R. G., Grabosky P., Urbas G. Cyber Criminals on Trial [Електронний ресурс] / R. G. Smith, P. Grabosky, G. Urbas. – // Режим доступу: http://assets.cambridge.org/97805218/40477/frontmatter/9780521840477_frontmatter.pdf.

8. Masadeh A. M. S. Combating Cyber Crimes – Legislative Approach – Comparative Study (Qatar, UAE, UK) [Електронний ресурс] / A. M. S. Masadeh. – // Режим доступу: http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en.

9. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза [Электронный ресурс] / В.А. Номоконов, Т.Л. Тропина. – // Режим доступа: http://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza.

10. Щетилов А.А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. – М., 2002. – С. 187.

11. Rauscher K.F., Yaschenko V. Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations [Електронний ресурс] / K.F. Rauscher, V. Yaschenko. – // Режим доступу: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=130080.

12. Словарь-справочник по информационной безопасности для Парламентской Ассамблеи ОДКБ / Под общ. ред. М.А. Вуса и М.М. Кучерявого. – СПб.: СПИИРАН. Из-во «Анатолия». «Полиграфические технологии», 2014. – 96 с.

13. Осипенко А.Л. Сетевая компьютерная преступность. – Омск, 2009. – С. 109−110.

14. Sofaer A.D., Grove G.D., Wilson G.D. Draft International Convention to Enhance Protection from Cyber Crime and Terrorism [Електронний ресурс] / A.D. Sofaer, G.D. Grove, G.D. Wilson. – // Режим доступу: http://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf.

15. Sofaer A.D. Toward an International Convention on Cyber Security [Електронний ресурс] / A.D. Sofaer. – // Режим доступу: http://media.hoover.org/sites/default/files/documents/0817999825_221.pdf.

16. A Global Treaty on Cybersecurity and Cybercrime [Електронний ресурс].// Режим доступу: http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.