КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343

Д. О. Ричка
аспірант юридичного факультету
Дніпровського національного університету імені Олеся Гончара

ТРАНСНАЦІОНАЛЬНА ЗЛОЧИННІСТЬ НОВІТНІХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Статтю присвячено аналізу кіберзлочинності як на території України, так і на міжнародному рівні. Розглянуто приналежність комп'ютерних злочинів до міжнародних злочинів та злочинів міжнародного характеру; найбільш розповсюджені види кіберзлочинів та їх категорії. Сформовано напрями вирішення існуючих прогалин у міжнародному законодавстві, що стосується новітніх комп'ютерних технологій.

Ключові слова: *кіберзлочини, кіберпростір, інтернет, кіберзлочини міжнародного характеру, транснаціональна злочинність, комп'ютерні технології.*

Постановка проблеми. Разом із розвитком інформаційних технологій із кожним днем вдосконалюється і комп'ютерна злочинність. Багатонаціональність електронних мереж дозволяє взаємодіяти користувачам різних країн світу. Даний аспект набув рис транснаціональної комп'ютерної злочинності, що набуває нових обертів, саме тому дослідження особливостей кіберзлочинів міжнародного характеру та злочинів, вчинених за допомогою комп'ютерної техніки, потребує поглибленого дослідження.

Міжнародна кіберзлочинність може завдати шкоду як громадянам певних країн, об'єднанням, установам, організаціям і т.д., так і державним інтересам у цілому. Інформаційна безпека є важливим компонентом захисту кожної держави, в якій інформація наділяється надзвичайною цінністю, виступаючи в певних випадках стратегічним ресурсом.

Аналіз останніх досліджень і публікацій. Дослідженням комп'ютерної злочинності міжнародного характеру займалися науковці: Батурин Ю.М., Біленчук П.Д., Волевоз А.Г., Демешко О.В., Європіна І.В., Мазоліна О.В., Манжул К.В., Машков В.М., Онищенко Ю.М., Орлов О.В., Музика А.А., Романюк В.С., Сорока Л.В., Цимбалюк В.С., Юртаєва К.В. та ін.

До останніх досліджень у даній тематиці можливо віднести працю Європіної І.В. «Види протиправних діянь у сфері новітніх інформаційних технологій», в якій автору вдається якісно проаналізувати Конвенцію про кіберзлочинність та прорахувати подальше розповсюдження міжнародної комп'ютерної злочинності.

Мета статті – ознайомитися з найбільш розповсюдженими видами міжнародної кіберзлочинності.

Виклад основного матеріалу. Під транснаціональною злочинністю новітніх комп'ютерних технологій у науковій праці розуміються види кіберправопорушень, які вчиняються в різних державах світу.

Міжнародні злочини – це злочини, що порушують міжнародні зобов'язання, які є основними для забезпечення життєво важливих інтересів міжнародного співтовариства, і розглядаються як злочини міжнародним співтовариством у цілому.

Міжнародні злочини:

1) здійснюються державами, посадовими особами держав, що використовують механізм держави в злочинних цілях, а також рядовими виконавцями;

2) здійснюються в безпосередньому зв'язку з державою;

3) зазіхають на міжнародний мир і безпеку;

4) загрожують основам міжнародного правопорядку;

5) спричиняють відповідальність держави як суб'єкта міжнародного права і персональну кримінальну відповідальності виконавців, що наступає в рамках міжнародної, а в деяких випадках – внутрішньодержавної (національної) юрисдикції.

Під злочинами міжнародного характеру розуміють діяння фізичної особи, що посягає на права й інтереси двох або декількох держав, міжнародних організацій, фізичних і юридичних осіб [1].

Злочини міжнародного характеру:

1) торкаються інтересів двох або декількох держав, юридичних осіб і/або громадян;

2) здійснюються окремими фізичними особами поза зв'язком із політикою держави;

3) спричиняють персональну відповідальність правопорушників у рамках національної юрисдикції.

На нашу думку, комп'ютерні злочини можна віднести як до міжнародних злочинів, так і до злочинів міжнародного характеру.

Найбільш розповсюджені види кіберзлочинів відображені в Конвенції про кіберзлочинність [2], яка називає серед інших наступні склади:

1) незаконний доступ до комп'ютерної системи;

2) нелегальне перехоплення технічними засобами комп'ютерних даних;

3) втручання в комп'ютерні данні;

4) втручання у функціонування комп'ютерної системи;

5) підробку та шахрайство, пов'язані з комп'ютерами;

6) правопорушення, пов'язані з дитячою порнографією.

У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками зазначено, що існує дві категорії злочинів:

1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних;

2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або у зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [3, с. 338].

Кримінальну відповідальність за кіберзлочини як у вузькому, так і широкому розумінні врегульовує Конвенція про кіберзлочинність. Кримінальне законодавство окремо взятих країн світу визначає карну відповідальність за кіберзлочини лише у вузькому розумінні, що можна підтвердити на прикладі України [4, с. 129]. В Особливій частині Кримінального кодексу міститься Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», але жодна із 6-ти статей цього розділу не містить норми, згідно з якою можна було притягнути до відповідальності особу, що вчинила, наприклад, шахрайство шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК) або окремі суспільно-небезпечні дії, передбачені ст. 200 КК. Як зазначають науковці А.А. Музика та Д.С. Азаров, і варто із цим погодитись, застосування комп'ютерів для вчинення названих діянь є лише певним способом вчинення злочину, який зазвичай не включається до обов'язкових ознак об'єктивної сторони складу злочину. За наявності певних фактичних обставин ці злочини можуть кваліфікуватись за сукупністю зі злочинами, передбаченими Розділом XVI Особливої частини КК України [5]. Потрібно також зауважити, що завдяки застосуванню комп'ютерних технологій значна кількість «звичайних» злочинів перейшла сьогодні до категорії «кіберзлочинів». До того ж, способи їх вчинення істотно полегшились, а «географія» розширилась [4, с. 129].

До злочинів, що перейшли з реального, фізичного світу до кіберпростору, можна назвати тероризм, розповсюдження порнографічної інформації, відмивання грошей та ін. [8; 9, с. 130].

За характером їх умовно можна поділити на дві основні групи: воєнно-політичні і економічні.

До воєнно-політичної групи слід віднести кібервійни, зумовлені комп'ютеризацією ракетно-ядерного арсеналу кожної держави.

До економічних злочинів доцільно віднести «нелегальне інформаційне брокерство» (злам комп'ютерних систем з наступним продажем інформації як самим потерпілим, так і конкурентам); організоване промислове (комерційне, підприємницьке) шпигунство; організоване «комп'ютерне піратство».

Однією з підстав кіберзлочинності є відсутність належного законодавчого регулювання

в рамках міжнародного права, адже національним законодавством окремо взятої країни усіх проблем охорони комп'ютерних технологій не вирішити.

Європейський комітет із проблем злочинності Ради Європи у 1990 році підготував рекомендації з метою визначення в Європі правопорушень, пов'язаних з комп'ютерами і ввів їх до «Мінімального списку» та «Необов'язкового списку» комп'ютерних злочинів, які були рекомендовані для включення до законодавств європейських країн [7, с. 167].

До Мінімального списку входять такі види протиправних діянь:

1) комп'ютерне шахрайство, комп'ютерний підлог, знищення комп'ютерної інформації та комп'ютерних програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних мереж;

2) несанкціоноване копіювання захищених комп'ютерних програм;

3) незаконне виробництво типографічних копій.

Необов'язковий список включає в себе такі види протиправних діянь:

1) зміна інформації чи комп'ютерних програм;

2) комп'ютерне шпигунство;

3) протизаконне застосування комп'ютера;

4) несанкціоноване застосування захищених комп'ютерних программ [8, с. 265].

Кіберзлочини мають низку особливостей суб'єктів, завдяки яким вони посягають через комп'ютерні системи на сфери міжнародного правопорядку, і зокрема – на міжнародний обмін інформацією. Сьюзанн В. Бреннер виділяє такі ознаки «кіберзлочинів», що відрізняє їх від «звичайних» злочинних посягань та значно підвищує їх суспільну небезпечність.

По-перше, «кіберзлочин» не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого.

По-друге, «кіберзлочин» є «автоматизованим» злочином, це означає, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч.

По-третє, суб'єкт «кіберзлочину» не підвладний обмеженням, які існують у реальному, фізичному світі. Так, «кіберзлочини» можуть бути вчинені моментально, і тому потребують швидкої реакції у відповідь.

І, по-четверте, «кіберзлочинність» і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це має місце зі злочинами, що вчиняються в реальному, фізичному світі [9].

Залишилися не врегульованими низка правових питань у даній сфері, зокрема,щодо визначення місця злочину, вчиненого за допомогою мережі Інтернет. Право якої держави потрібно застосувати, якщо правопорушник і об'єкт посягання знаходяться в різних країнах? Як має бути вирішено питання про межі можливого та необхідного застосування кримінального права країни до «кіберзлочинів», вчинених поза її територією [4, с. 130]?

Аллан Р. Стейн стверджує, що найбільш проблемною характеристикою мережі Інтернет з точки зору юрисдикційної політики є те, що він стирає межу між внутрішньодержавною і міжнародною передачею інформації [10]. Інтернет сформувався та являє собою позатериторіальний засіб комунікації та обміну інформацією, який не має централізованого управління. Кожнен індивідуум і його комп'ютер діють автономно та формують єдину транснаціональну мережу, яка виходить за межі географічної концепції державних кордонів. Інтернет-адреси, що підтримуються мережею, нематеріальні, і навіть адреси сайтів, які містять URL-індикатори країни походження, наприклад, «ua», «pl», не обов'язково мають бути точними. Інтернет-адреси є довільними та можуть залишатись незмінними, в той час як сервери переміщаються у фізичному просторі [11, с. 24]. Така особливість Інтернету ставить науку і практику перед необхідністю розроблення нових підходів до протидії злочинам міжнародного характеру з використанням комп'ютерних технологій та побудови юрисдикційної політики стосовно таких злочинних посягань [4, с. 130].

Існує декілька основних напрямів вирішення проблеми подальшого регулювання Інтернету та кримінальної відповідальності за злочини міжнародного характеру з використанням комп'ютерних технологій. Відповідно до першого з них рекомендується пристосувати до злочинів, які вчиняються з використанням новітніх інформаційних технологій, традиційні принципи кримі-нальної юрисдикції. Що стосується другого, пропонується розглядати Інтернет як самостійний «віртуальний» кіберпростір та розробляти нові правила застосування кримінальної

юрисдикції щодо злочинів, які в ньому вчиняються.

Кіберпростір є матерією зовні невідчуваємого поля інформаційних відносин, який слугує зменшеним прототипом Всесвіту, на тлі якого планети – електронно-обчислювальні машини (ЕОМ) та технічні засоби; осі – системи інформаційної передачі: автоматизована система, комп'ютерна мережа та телекомунікаційна мережа та ін. Це простір, на якому відбуваються інформаційні відносини в найширшому значенні [12, с. 54].

Конвенція про кіберзлочинність визначає традиційну схему кримінальної юрисдикції щодо регульованих злочинів, допускаючи територіальний та національний принципи кримінальної юрисдикції. Відповідно до частини 1 ст. 22 кожна із Сторін вживає таких законодавчих й інших заходів, які, на її думку, можуть бути необхідними для встановлення юрисдикції стосовно будь-якого злочину, криміналізованого Конвенцією, якщо він вчинений:

1) на її території;

2) на борту судна, яке плаває під прапором такої Сторони;

3) на борту літака, зареєстрованого відповідно до законодавства такої Сторони;

4) одним з її громадян, якщо таке правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої Держави.

Однак Конвенція не розтлумачує питання, за якими «кіберзлочини» слід вважати вчиненими на території даної країни, та поняття «місце вчинення злочину», і залишає це на розсуд національних судів. Міжнародна практика засвідчує, що єдиного підходу до вирішення цього питання на національному рівні досі не існує. Різне тлумачення місця вчинення злочинів, що пов'язано з комп'ютерними технологіями, а так само відсутність чіткого правового регулювання на міжнародному рівні можуть призвести, з одного боку, до позитивних конфліктів кримінальних юрисдикцій різних країн, коли дві і більше країни претендують на застосування закону про кримінальну відповідальність щодо одного злочинного діяння, а з іншого – до негативних конфліктів кримінальних юрисдикцій, коли жодна країна не вдається до переслідування вчиненого злочину.

У міжнародній правозастосовчій практиці питання кримінальної юрисдикції поставлене в залежність від існуючого поділу кіберзлочинів за колом об'єктів:

– злочини, що націлені та спричинюють шкоду конкретним об'єктам (наприклад, установі банку, електронній скринці приватної особи тощо);

– злочини, що націлені та посягають на невизначене коло об'єктів (наприклад, у разі розповсюдження комп'ютерних вірусів або порнографічної продукції) [4, с. 131].

Об'єктом кіберзлочинності, відповідно до Конвенції, є широкий спектр суспільних відносин, які охороняються нормами права. Ці відносини виникають під час здійснення інформаційних процесів із приводу виробництва, збору, обробки, накопичення, збереження, пошуку, передачі, розповсюдження і споживання комп'ютерної інформації, а так само в інших областях, де використовуються комп'ютери, комп'ютерні системи і мережі. Серед них, з огляду на підвищену суспільну значимість, відокремлюються правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності комп'ютерних даних і систем, законного використання комп'ютерів і комп'ютерної інформації (даних), авторського і суміжного прав [8, с. 267].

Питання застосування закону держави про кримінальну відповідальність до «кіберзлочинів», які посягають на конкретні об'єкти, найчастіше вирішується за правилами об'єктивної територіальності. Знаходячись в одній країні, особа спрямовує злочинне діяння на територію інших юрисдикцій, застосовуючи сучасні комп'ютерні мережі. Правоохоронні органи країни фізичного місця знаходження правопорушника можуть навіть не здогадуватися про вчинені ним кримінальні діяння, а виявляти їх вже за наслідками, які настають в іншій країні. У таких випадках кримінальне переслідування злочинця стає неможливим без міждержавного співробітництва.

Правопорушник притягується до відповідальності на території країни перебування або ж видається «потерпілій» країні за умов наявності відповідних міжнародних договорів та задоволення інших правових вимог, які супроводжують процедуру екстрадиції. Однак процедура екстрадиції є досить складною і скоріше винятком, ніж правилом розв'язання подібних питань.

Міжнародний досвід також демонструє виняткові випадки, коли «потерпіла» країна вирішує питання про притягнення злочинця до кримінальної відповідальності без звер-

нення до країни його місця знаходження [4, с. 131].

Дещо по-іншому вирішуються питання застосування кримінальної юрисдикції країни до «кіберзлочинів», які посягають на невизначене коло об'єктів та відповідно порушують правопорядок у невизначеній кількості країн. У таких випадках притягнення особи до кримінальної відповідальності можливе за правилами екстериторіальності, проте із застереженням: за умови наявності в ній кримінальної заборони щодо «кіберзлочинів».

На підставі викладеного можна дійти висновку, що сьогодні країнами світу до «кіберзлочинів» застосовуються традиційні принципи кримінальної юрисдикції, засновані на ідеології географічної територіальності. Оскільки технологія сучасних комп'ютерних мереж функціонує поза межами територіального суверенітету та є позатериторіальною за своєю природою, існуючі принципи кримінальної юрисдикції стають неефективними та породжують низку юридичних питань.

Між тим право на існування має й інший підхід до регулювання правових відносин у мережі Інтернет, який може стати альтернативою традиційному, оскільки, на нашу думку, краще підходить до реалій сьогодення. Його прихильники пропонують вважати місцем вчинення «кіберзлочину» не територію певної країни або будь-яку іншу географічну територію, а безпосередньо кіберпростір [4, с. 132].

Верховний Суд США дав таке визначення кіберпростору: «Унікальний носій, який не знаходиться на певній території, але доступний кожному в будь-якій точці світу через Інтернет» [13, с. 152]. Інституціональним втіленням кіберпростору є Інтернет, що являє собою глобальну інформаційну систему, яка складається з інших інформаційних систем і дозволяє користувачам обмінюватися інформацією з будь-яким комп'ютером у цій системі [14].

Цілком логічно, з урахуванням вищезазначеного, надати правовому режиму Інтернету статус, аналогічний територіям спільного користування. Це дозволить запровадити відповідальність за протиправні діяння в кіберпросторі згідно з принципом кримінальної юрисдикції, який діє в інших територіях загального користування. Тобто особа, яка вчинила злочин у кіберпросторі, буде нести відповідальність перед країною свого громадянства. Це правило може набути чинності лише за умови прийняття універсального зводу правил користування Інтернетом та запровадження принципу обов'язкового співробітництва між країнами в розслідуванні злочинів, що вчиняються в кіберпросторі [13, с. 152].

Висновки і пропозиції. За компетентними прогнозами в недалекому майбутньому можливе стрімке зростання кількості «кіберзлочинів», і передусім таких особливо небезпечних, як «кібервійни», «кібертероризм», «кібершпигунство» тощо [4, с. 135]. Кіберпростір набув величезних масштабів, що стало підґрунтям до розвитку злочинності. Законодавче регулювання кіберпростору в одній окремо взятій країні не забезпечує дотримання законності в іншій. Необхідний комплексний підхід, чого можливо досягти шляхом розширення міжнародної співпраці в боротьбі з кіберзлочинністю та підписання міжнародних договорів про співпрацю.

Список використаної літератури:

1. Відповідальність у міжнародному праві та мирні засоби розв'язання міжнародних спорів / Національна Академія Внутрішній Справ. URL: http://www.naiau.kiev.ua/books/mg/lectures/lecture_8.html.
2. Конвенція про кіберзлочинність від 23.11.2001 р. (у редакції від від 07.09.2005). URL: ttp://zakon2.rada.gov.ua/laws/show/994_575.
3. Волевоз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. С. 338.
4. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. Число 3. С. 129. URL: http://nbuv.gov.ua/UJRN/vaau_2010_3_19.
5. Музика А.А. Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практичний коментар і шляхи вдосконалення. К.: Вид-во Паливода А.В., 2005.
6. Юртаєва К.В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. URL: http://www.nbum.gov.ua.
7. Комп'ютерна злочинність: Навчальний посібник. К.: Атіка, 2002. С. 167.
8. Сорока Л.В. Види правопорушень у сфері комп'ютерних та інформаційних технологій // Наукові записки КДПУ. Серія: Історичні науки / ред. В.М. Філоретов [та ін.]. Кіровоград: КДПУ ім. В. Винниченка, 2005. Вип. 9. С. 262. URL: http://dspace.kspu.kr.ua/jspui/bitstream/123456789/1222/1/Види%20правопорушень%20у%20сфері%20комп%27ютерних%20та%20інформаційних%20технологій%20.pdf.

9. Brenner S.W. Toward a Criminal Law for Cyberspace A New Model of Law Enforcement 30 Rutgers Computer & Tech. L.J.1 (2004).
10. Stein A.R. Simposium: Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulator Precision. 98 Nw. U.L.Rev. 411 (2004).
11. Ансельмо Э. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве? Экономические стратегии. 2006. № 2. С. 24.
12. Rychka D.O. Types of crime in information and telecommunication systems. Cybersquatting (cybercrime)/ Z 40 Zbiór artykułów naukowych z Konferencji Miedzynarodowej Naukowo-Praktycznej (on-line) zorganizowanej dla pracowników naukowych uczelni, jednostek naukowo-badawczych oraz badawczych z państw obszaru byłego Związku Radzieckiego oraz byłej Jugosławii. Warszawa, 2017. 116 str. Str. 54.
13. Мазолина О.В. Вопросы международно-правового регулирования Интернета. Московский журнал международного права. 2004. № 4. С. 152.
14. ASLU v.Reno,929 F. Supp 824 (E.D.Pa.1996).

Ричка Д. О. Транснациональная преступностью новейших компьютерных технологий

Статья посвящена анализу киберпреступности, как на территории Украины, так и на международном уровне Рассмотрены принадлежность компьютерных преступлений в международных преступлений и преступлений международного характера; наиболее распространенные виды киберпреступлений и их категории. Сформировано направление решения существующих пробелов в международном законодательстве, касающемся новейших компьютерных технологий.

Ключевые слова: *киберпреступления, киберпространство, интернет, киберпреступления международного характера, транснациональная преступность, компьютерные технологии.*

Rychka D. O. Transnational crime of the latest computer technology

The article is devoted to the analysis of cybercrime, both on the territory of Ukraine and internationally. The affiliation of computer crimes to international crimes and crimes of an international character is considered; the most widespread types of cybercrime and their categories. Directions of resolving existing gaps in the international legislation concerning the latest computer technologies have been formed.

Key words: *cybercrime, cyber space, internet, cybercrime of international character, transnational crime, computer technology.*