ФП 2018-5
ISSN 1995-6134

УДК *341.48/.49*
DOI: http://doi.org/10.5281/zenodo.2009191

М.Ю. ЯЦИШИН,
старший викладач кафедри міжнародного права
Національного авіаційного університету, м. Київ, Україна;
e-mail: martayatsyshyn@nau.edu.ua;
ORSID: https://orcid.org/0000-0002-6013-7098

КРИМІНАЛІЗАЦІЯ КІБЕРЗЛОЧИНІВ У МІЖНАРОДНОМУ ПРАВІ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

M.Y. YATSYSHYN,
Assistant Professor, Chair of International Law,
National Aviation University, Kyiv, Ukraine; e-mail: martayatsyshyn@nau.edu.ua;
ORSID: https://orcid.org/0000-0002-6013-7098

CRIMINALIZATION OF CYBERCRIME IN INTERNATIONAL LAW: COMPARATIVE ANALYSIS

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEY WORDS)

Метою є визначення і аналіз окремих видів кібернетичних злочинів, криміналізованих за чинними міжнародними договорами. Аналізуються положення міжнародно-правових угод у сфері протидії кіберзлочинності, що були прийняті в рамках таких організацій, як Рада Європи, Ліга арабських держав, Співдружність незалежних держав, Шанхайська організація співробітництва та Африканський союз. Визначені спільні та відмінні риси положень вказаних договорів, зокрема, кваліфікаційні ознаки кожного з видів кіберзлочинів, що підлягають переслідуванню. Зроблено висновок про відмінність підходів до криміналізації та запропонована класифікація кібернетичних злочинів у міжнародному праві, яка може лягти в основу універсальної концепції кіберзлочинності – Конвенції ООН про кіберзлочинність.

Ключові слова: *кіберзлочинність; міжнародна злочинність; Будапештська конвенція; інформаційно-комунікаційні технології; міжнародне кримінальне право*

***

Information and communication technologies have widely spread around the world in the last decade. This made a significant influence on society, not only positive but also led to the criminalization of cyberspace. There is no universal treaty on cybercrime today. This sphere is very controversial and needs to be unified. International cooperation to combat cybercrime consists of material and procedural rules and principles of existing agreements. One of the main theoretical and practical problems is the absence of united terminology and classification of cybercrime. This article outlines issues of cybercrime classification under international law. The goal is to identify and analyze certain types of cybercrime criminalized under international agreements. The author compares provisions of international regional treaties adopted by the Council of Europe, League of Arab States, Commonwealth of Independent States, Shanghai Organization of Cooperation and African Union. The article established various types of cybercrime criminalized under these agreements. The author mentioned different qualifications of such cybercrimes as illicit access, illegal interception, data breaches, and others. We consider the criminalized list of cybercrimes to be not exhaustive. There are some crimes not mentioned in international agreements. The author points out common and different characteristics of compared provisions. In result, the author proposes a unified classification of cybercrimes in conclusion. This classification should be taken into account in the prose's of UN Convention on cybercrime creation. We suggest dividing all cybercrimes into three groups. First, cybercrimes that arise in the result of ICTs creation and damage members of the cyberspace by violating the confidentiality, integrity, and accessibility of ICTs. The second group includes traditional crimes committed with ICT, such as terrorism, fraud, offenses related to copyright etc. The last group provides cybercrimes related to illicit content. For example, produce, register, offer, manufacture, make available of child pornography or other illegal information. We believe that the only way to develop international cooperation in fight cybercrime is the adoption of the universal agreement by the United Nations. This process is difficult because of political and legal controversies. Unifying the main concepts of cybercrime law such as classification can solve this problem.

Key words: *cybercrime; international crimes; Budapest convention; information communication technologies; international criminal law*

ISSN 1995-6134

Постановка проблеми

Поширення інформаційно-комунікаційних технологій в усьому світі разом із багатьма позивними змінами призвело до значної криміналізації кіберпростору. За даними Інтерполу, кіберзлочинність є однією з найбільш швидко зростаючих сфер злочинності [1]. Це підтверджують звіти багатьох організацій, наприклад, Міжнародного союзу електрозв'язку, Конференції ООН з торгівлі та розвитку, Всесвітнього економічного форуму, асоціації ISACA, компаній Microsoft, IB-Group, McAfee, CISCO та ін. Зокрема, у звіті Європейського поліцейського управління (Європол) "Оцінка загрози організованої злочинності в Інтернеті" за 2018 рік зазначено, що за статистичними даними ряду держав-членів Європейського Союзу кількість зареєстрованих кіберзлочинів досягає або ж навіть перевищує кількість традиційних злочинів [2].

Необхідно зазначити, що в науці і практиці міжнародного права відсутня єдність у визначенні та застосуванні поняття "кіберзлочинність". У проведеному дослідженні кіберзлочин розглядається як протиправне суспільно небезпечне діяння, здійснене за допомогою інформаційно-комунікаційних технологій (далі – ІКТ) проти прав і законних інтересів учасників кіберпростору (фізичних, юридичних осіб, держав), що охороняються нормами кримінального та міжнародного права.

До основних властивостей високотехнологічної злочинності відноситься її транснаціональний характер, що означає взаємозв'язок з більш ніж одним правопорядком. А тому, ефективна протидія кіберзлочинності неможлива, якщо розслідування злочинів, видача правопорушників, їх обвинувачення в суді ускладнені або взагалі неможливі через значні відмінності у національних кримінальних законах, а також відповідних регіональних угодах. Фактично, така неузгодженість дозволяє злочинцям уникнути відповідальності, залишаючи їхні дії безкарними. Отже, чинні законодавчі акти, засновані на принципі nulla poena sine lege, повинні містити вичерпний перелік протиправних діянь з використанням ІКТ, а тому створення відповідних універсальних стандартів є об'єктивною необхідністю.

Проблематика кіберзлочинності, не дивлячись на її відносну новизну та актуальність, неодноразово визначалася як предмет наукових досліджень. Серед перших наукових розвідок тематики міжнародно-правового співробітництва держав у боротьбі із транскордонними злочинами з використанням ІКТ є робота І.М. Забари [3], в якій досліджені існуючі міжнародні механізми протидії кіберзлочинності, однак не проаналізовані питання криміналізації окремих видів правопорушень з використанням ІКТ. Важливий внесок у розробку проблематики міжнародно-правової протидії кіберзлочинності здійснив А.В. Пазюк, який у дисертації [4] та монографії "Міжнародне інформаційне право: теорія і практика" [5] щодо становлення і прогресивного розвитку нової галузі – міжнародного інформаційного права, розглядав окремі питання кібербезпеки та боротьби з кіберзлочинністю.

Слід відзначити також підрозділ "Злочинність у кіберпросторі: міжнародно-правовий дискурс" у підручнику "Теорія та практика міжнародного права" за редакцією Н.А. Зелінської [6], де розглядаються питання протидії кіберзлочинності в рамках сучасної концепції транснаціонального кримінального права.

Водночас, у вітчизняній доктрині міжнародного права не проводилось комплексного порівняльного дослідження міжнародної договірної практики щодо криміналізації кіберзлочинів. Експерт Ради Європи Захід Джаміл (Zahid Jamil, 2016) здійснив ґрунтовне порівняння положень Конвенції про кібербезпеку і захист персональних даних Африканського Союзу та Конвенції про кіберзлочинність Ради Європи. Автор слушно вказує на окремі відмінності кваліфікаційних ознак злочинів, криміналізованих названими угодами [7]. Однак, у сучасному міжнародному праві існує п'ять чинних регіональних угод у сфері боротьби з кіберзлочинністю, а тому представлена стаття логічно продовжує назване дослідження. Важливий внесок у розробку тематики здійснив також Штейн Штольберг (Stein Schjolberg, 2011) у працях "Всесвітній договір з кібербезпеки та кіберзлочинності" [8] та "Історія кіберзлочинності 1976–2016" (Stein Schjolberg, 2014) [9]. Підхід автора до класифікації кіберзлочинів має беззаперечну наукову цінність, проте не виключає існування й інших підходів. Тому дана стаття є доповненням і розвитком доробку вченого, а її метою є визначення та комплексний аналіз окремих видів кіберзлочинів, що криміналізуються відповідно до положень чинних міжнародно-правових договорів. Її новизна полягає в узагальненому підході до класифікації кіберзлочинів, який повинен бути врахованим при формуванні універсальної концепції кіберзлочинності та розробці Конвенції ООН у визначеній сфері. Завданнями статті є визначення чинних договірних джерел криміналізації кіберзлочинів у міжнародному праві,

ISSN 1995-6134

порівняння положень виділених угод, а також формування на основі проведеного аналізу узагальненого підходу до класифікації кіберзлочинів.

Договірні джерела криміналізації кіберзлочинів у міжнародному праві

Сучасний стан розвитку інституту міжнародно-правової протидії кіберзлочинності характеризується регіональним характером та інтенсифікацією уніфікації національних законодавств. За умов відсутності єдиного універсального міжнародного договору про кіберзлочинність, основними конвенційні засади містяться в положеннях чинних регіональних угод:

1) Конвенція про кіберзлочинність Ради Європи, прийнята 21.11.2001 року та Додатковий протокол від 28.01.2003 р. (далі – Будапештська конвенція) [10];

2) Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21.12.2010 р. (далі – Конвенція ЛАД) [11];

3) Угода про співробітництво держав – членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01.06.2001 р. (далі – Угода СНД) [12]. Нова редакція цієї Угоди була відкрита для підписання у 2018 р., однак поки ще не вступила в силу;

4) Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 р. (далі – Угода ШОС) [13];

5) Конвенція про кібербезпеку і захист персональних даних Африканського Союзу від 27.06.2014 р. (далі – Конвенція АС) [14].

Фактично, в текстах усіх зазначених актів містяться види протиправних діянь, що підлягають криміналізації в національних правових системах держав-учасниць. Варто відзначити, що важливим питанням є співвідношення сфер дії цих договорів та їх узгодження. Зокрема, враховуючи той факт, що Конвенція про кіберзлочинність Ради Європи отримала поширення за рамки європейського регіону (18 держав-учасниць не є членами Ради Європи), застосування перелічених міжнародно-правових актів може відбуватись паралельно.

Порівняльний аналіз окремих видів кіберзлочинів, криміналізованих у міжнародному праві

Ґрунтовний аналіз положень названих регіональних договорів дозволяє виділити такі види кіберзлочинів та їх кваліфікаційні ознаки відповідно.

Незаконний доступ – навмисний доступ до цілої комп'ютерної системи або її частини без права на це [10]. Цей вид протиправної поведінки у кіберпросторі передбачається усіма регіональними угодами. Однак, існують суттєві кваліфікаційні відмінності у складах передбачених злочинів, одна із основних з яких стосується об'єкту злочинних посягань. Будапештська конвенція, Конвенція ЛАД та Конвенція АС передбачають криміналізацію діянь проти комп'ютерної системи або її частини (а також у поєднанні з іншою комп'ютерною системою). В той час як Угода СНД забороняє незаконний доступ до комп'ютерної інформації, що охороняється законом, а Угода ШОС – до інформаційних систем (дефініція цього поняття відсутня).

Відрізняється й суб'єктивна сторона досліджуваного злочину. Виключно Будапештська конвенція встановлює наявність умислу як ознаки злочину незаконного доступу. Що стосується мети, то згідно положень Будапештської конвенції лише пропонується на розсуд держав-учасниць можливість додаткової кваліфікації: "з метою отримання комп'ютерних даних або з іншою недобросовісною метою". Конвенція ЛАД також пропонує додаткові кваліфікаційні ознаки щодо мети: "з метою стирання, зміни, спотворення, копіювання, переміщення чи знищення збережених даних, електронних засобів і систем, комунікаційних мереж, і нанесення шкоди користувачам і бенефіціарам", але в якості обтяжуючої обставини злочину незаконного доступу. В Угоді СНД мета проявляється в "знищенні, блокуванні, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ чи їх мереж". Конвенція АС пропонує криміналізацію незаконного доступу як з невизначеною метою (ст.29, a), так і "з метою вчинення або сприяння вчиненню іншого злочину" (ст.29, b). Угода ШОС визначає за мету: "порушення цілісності, доступності і конфіденційності інформації".

Ще одна важлива відмінність стосується визначення обсягу злочинних дій. Так, Будапештська конвенція та Угода СНД забороняють "незаконний доступ", в той час як Конвенція ЛАД додатково криміналізує перебування чи зв'язок з інформаційною технологією або її частиною, а також збереження (perpetuation) їх, а Конвенція АС – "неавторизований доступ" і "перевищення авторизованого доступу" (дефініція цих термінів відсутня). Слід відзначити також, що Конвенція ЛАД пропонує встановити додаткову обтяжуючу обставину і на випадок, коли визначені дії призведуть до заволодіння секретною урядовою інформацією.

ISSN 1995-6134

Нелегальне перехоплення – навмисне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування. Такий вид кіберзлочинів передбачений в Будапештській конвенції, Конвенції ЛАГ та Конвенції АС, а в Угодах СНД та ШОС – відсутній. Відповідно до Пояснювального звіту ETC-185, наданого Комітетом міністрів Ради Європи на 109 сесії 08.11.2001 року, стаття 3 Будапештської конвенції застосовується до всіх форм електронної передачі даних за допомогою телефону, факту, e-mail чи файлового обміну [15]. Для охоплення більш широкого кола протиправних діянь конвенція поширила обсяг поняття "нелегального перехоплення" на електромагнітні випромінювання комп'ютерних систем, що містять в собі комп'ютерні дані. Такі випромінювання можуть здійснюватися комп'ютером під час роботи і водночас не підпадають під визначення "даних" згідно Конвенції. Проте комп'ютерні дані можуть бути реконструйовані з електромагнітних випромінювань. Водночас, Конвенція ЛАГ та Конвенція АС такого підходу не передбачає.

Втручання в дані – навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерних даних без права на це [10]. Такий злочин передбачається Будапештською конвенцією, Конвенцією ЛАД, Угодою ШОС та Конвенцією АС. Водночас, існує певна неоднорідність підходів законодавців. Так, у Конвенції ЛАД відповідне діяння: "Навмисне протиправне знищення, стирання, перешкоджання, зміна, приховування даних інформаційних технологій" називається злочином проти цілісності даних. Згідно положень Конвенції АС такі дії визнаються як атаки на комп'ютерні системи: "Ст.29.1 f) Пошкодження або спроба пошкодження, знищення чи спроба знищення, погіршення чи спроба погіршення, переробка чи спроба переробки, зміна чи спроба змінити комп'ютерні дані за допомогою шахрайства", а також зломом комп'ютерних даних: "Ст.29.2 d) отримання за допомогою шахрайства для себе чи іншої особи, будь-якої вигоди шляхом введення, зміни, видалення чи знищення комп'ютерних даних чи будь-яким іншим способом втручання у функціонування комп'ютерної системи" [14]. Нарешті, відповідно до Угоди ШОС інформаційними злочинами слід визнати серед інших і "нанесення шкоди інформаційним ресурсам", де інформаційні ресурси – це інформаційна інфраструктура, а також інформація та її потоки. Таким чином, можна констатувати значні кваліфікаційні відмінності в наведених положеннях. Окремо слід відзначити, що Будапештська конвенція та Конвенція ЛАД передбачили можливість для держав-учасниць визначити ознакою злочину втручання у дані – нанесення серйозної шкоди.

Втручання в систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи. Відповідні положення знаходимо в Будапештській конвенції та Конвенції АС, які також містять кваліфікаційні відмінності у складі цього злочину. На відміну від положень Будапештської конвенції, в Конвенції АС передбачена криміналізація "перешкоджання, спотворення чи спроба перешкоди або спотворення функціонування комп'ютерної системи" (ст.29.1. d), а також "введення або спроба введення даних за допомогою шахрайства в комп'ютерну систему" (ст.29.1. e). Таким чином, встановлено два окремих самостійних склади злочинів в рамках атак на комп'ютерні системи. У Конвенції ЛАД, Угодах СНД і ШОС відсутня криміналізація описаних злочинних діянь.

Зловживання пристроями – навмисне виготовлення, продаж, володіння чи розповсюдження пристроїв і засобів для вчинення кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних систем та мереж. Описане злочинне діяння криміналізовано в положеннях усіх регіональних актів, окрім Конвенції АС. Будапештська конвенція забороняє злочинне використання пристроїв, включаючи комп'ютерні програми, комп'ютерних паролів, кодів доступу або подібних даних. Відповідно до Угоди СНД держави-учасниці погодились встановити кримінальну відповідальність лише за "створення, використання чи розповсюдження шкідливих програм" (ст.3.1.б), а згідно з Угодою ШОС за "умисне виготовлення і розповсюдження комп'ютерних вірусів та інших шкідливих програм" (визначення поняття "комп'ютерні віруси" в Угоді відсутнє), що є набагато вужчим, аніж положення закріплене Будапештською конвенцією. Положення ст.9 "Зловживання технічними засобами" Конвенції ЛАД охоплює додатково імпорт перерахованих вище засобів. Обидві Конвенції передбачають відповідальність у випадку, коли протиправні дії здійснюються з метою вчинення інших злочинів, які сформульовані за допомогою відсилочного способу. Так, Будапештська конвенція забороняє зловживання пристроями для вчинення незаконного доступу, нелегального перехоплення, втручання у дані та втручання в систему. Натомість, Конвенція ЛАД передбачає криміналізацію зловживання технічними

Forum Prava, 2018. 53(5). 92–99
(Research Article)

ISSN 1995-6134

засобами з метою здійснення незаконного доступу, незаконного перехоплення та злочинів проти цілісності даних. Таким чином, обсяг проаналізованих положень також не співпадає.

Підробка, пов'язана з комп'ютером - навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти (ст.7) [10]. Конвенція ЛАД закріпила також криміналізацію підробки у ст. 10, відповідно до якої забороняється: "використання засобів інформаційних технологій для зміни правдивості даних способом, що наносить шкоду, з метою використання їх як правдивих даних" [11]. Відповідно ст.29.2.b, Конвенція АС криміналізує зазначені протиправні діяння в контексті зламу комп'ютерних даних.

Шахрайство, пов'язане з комп'ютерами – навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: а) будь-якого введення, зміни, знищення чи приховування комп'ютерних даних; б) будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи (ст.8) [10]. Шахрайство з використанням ІКТ криміналізується відповідно до усіх регіональних актів, крім Угоди СНД. Положення Конвенції ЛАГ встановлюють додаткову кваліфікуючу обставину, що полягає в третьому способі здійснення шахрайства, а саме: "оспорювання електронних засобів, програм і сайтів" [11]. В Угоді ШОС та Конвенції АС шахрайство, пов'язане з комп'ютерами розглядається не як окремий кіберзлочин, а як спосіб здійснення уже існуючого в кримінальному законодавстві держав-членів злочину шахрайства, нарівні з іншими протиправними діяннями, такими як: крадіжка, викрадення, вимагання, шантаж, відмивання грошей, контрабанда, незаконна торгівля наркотиками тощо. В Конвенції АС шахрайство розглядається у ст.30 "Адаптація деяких правопорушень до ІКТ", а саме п.1 "Злочини проти власності" [14]. В доктрині дослідження злочинності у сфері шахрайства за допомогою ІКТ здобули широкого поширення. Таке явище у науці отримало назву "фрауд" чи "фрод" (від англійського fraud).

Правопорушення, пов'язані з дитячою порнографією – охоплює виробництво, розповсюдження, пропонування, передачу, надання доступу, а також володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації. Названа група злочинів є визнаною у всіх чинних міжнародно-правових угодах. Слід відзначити, що положення Конвенції ЛАД є найбільшими широкими за сферою охоплення протиправних дій, оскільки включають дві статті щодо злочинів, пов'язаних з порнографією. При чому, забороняється: "виробництво, демонстрація, розповсюдження, постачання, публікація, придбання, продаж, імпорт порнографічних матеріалів в цілому, а також матеріалів, що порушують пристойність за допомогою інформаційних технологій". Здійснення такого роду протиправних діянь проти дітей та неповнолітніх визнається обтяжуючою обставиною. У ст.13 передбачено криміналізацію "Інших злочинів, пов'язаних з порнографією", що включають: азартні ігри та сексуальну експлуатацію, однак Конвенція не надає визначень цим поняттям.

Правопорушення, пов'язані з порушенням авторських та суміжних прав – розглядаються як порушення авторських та суміжних прав відповідно до чинних міжнародних угод (наприклад, Бернської Конвенції про захист літературних та художніх творів) у випадку, коли такі дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем [10].

Порушення в сфері права інтелектуальної власності криміналізуються у всіх досліджуваних міжнародно-правових актах, окрім Конвенції АС. Конвенція ЛАГ надає право державам-учасницям визначати порушення авторського і суміжних прав відповідно до внутрішнього законодавства. Встановлюються лише дві кваліфікаційні ознаки щодо умислу та не особистого використання. Угода ШОС розглядає цю категорію кіберзлочинів в контексті більш широкої групи протиправних діянь: "порушення законних прав і свобод громадян в інформаційній сфері". Угода СНД передбачає дещо звужений підхід, криміналізуючи лише "незаконне використання програм для ЕОМ і баз даних, що є об'єктами авторського права".

В досліджуваних регіональних міжнародно-правових актах передбачено криміналізацію й інших злочинних діянь, які не отримали такого загального визнання, але закріплені в окремих угодах. Серед них доцільно виділити наступні: правопорушення, пов'язані з расизмом та ксенофобією; правопорушення, пов'язані з геноцидом та злочинів проти людства; злочини, пов'язані з тероризмом; злочини проти приватності; незаконне використання електронних платіжних

ISSN 1995-6134

засобів; порушення правил експлуатації ЕОМ, системи ЕОМ чи їх мережі; здійснення DOS-атак.

Важливо відзначити, що використання таких кваліфікаційних ознак, як "неавторизований доступ" та "перевищення авторизованого доступу" в положеннях Конвенції АС засуджується експертом Ради Європи Західом Джамілем (Zahid Jamil) [7]. Натомість технічно більш коректним визначається термінологія Будапетської конвенції, а саме конструкція "без права на це", що надає змогу правильно охопити весь обсяг кіберзлочинів. Порівняльний аналіз також звертає увагу на використання в Конвенції АС в якості кваліфікаційної ознаки способу здійснення злочину: "за допомогою шахрайства". Експерти вважають таке застосування не доцільним та таким, що зменшує ефективність відповідних норм, створюючи прогалини. Однак, в доктрині кримінального права існують погляди, зокрема у працях А.А. Комарова, про необхідність розширити розуміння обману, поширивши його на вплив не лише на людину, а й на автоматизовані комп'ютерні системи [10].

Висновки

Можна зазначити, що Інститут міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю – це комплекс матеріальних і процесуальних норм та принципів, що регулюють співробітництво держав щодо визначення, розслідування та попередження кіберзлочинів. Означений інститут перебуває на стадії формування, характеризується фрагментарністю і неоднорідністю та потребує узгодження і подальшої гармонізації.

Основними джерелами регулювання міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю є чинні регіональні договори, порівняльний аналіз положень яких було здійснено. Встановлено, що досліджувані угоди криміналізують різні види кіберзлочинів. Їх кваліфікаційні ознаки в більшості випадків не співпадають, на основі чого розслідування передбачених злочинних діянь значно ускладнюється або унеможливлюється. З іншої сторони, перелік визнаних кібернетичних злочинів не можна вважати вичерпним.

Виділені критерії дозволяють узагальнити основні кваліфікаційні ознаки кібернетичних злочинів як основи їх класифікації:

1. Кіберзлочини, що виникли в результаті створення і поширення ІКТ, та завдають шкоду учасникам кіберпростору шляхом порушення конфіденційності, цілісності та доступності ІКТ. До цього виду злочинних діянь відносяться: незаконний доступ; нелегальне перехоплення; втручання в дані; втручання в систему; зловживання пристроями.

2. Традиційні злочини, вчинені з використанням ІКТ: тероризм; підробка; шахрайство; переслідування, вимагання, порушення права інтелектуальної власності та ін.

3. Кіберзлочини, що пов'язані зі створенням та розповсюдженням нелегального контенту за допомогою ІКТ. До цієї групи злочинних діянь відносимо будь-які цифрові операції із забороненою інформацією, яку становить дитяча порнографія, расистський та ксенофобний матеріал тощо.

Запропонований підхід є узагальненням існуючої міжнародно-правової практики в сфері боротьби з кіберзлочинністю, відображає регіональні уніфікації та може бути використаний при формуванні універсальної концепції кіберзлочинності і створенні Конвенції ООН про кіберзлочинність.

Конфлікт інтересів

Автор підтверджує відсутність будь-якого конфлікту інтересів.

Вираз вдячності

Щодо дослідження не було отримано фінансової або фактичної підтримки з боку юридичних або фізичних осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Interpol: Cybercrime is entering a new dimension. URL: https://money.cnn.com/video/technology/2018/01/24/davos-interpol-cybersecurity.cnnmoney/index.html
2. Internet organized crime threat assessment 2018. URL: https://www.europol.europa.eu/iocta/2018.
3. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. URL: http://e-pub.aau.edu.ua/index.php/chasopys/article/view/212 .
4. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти): дис. … докт. юрид. наук : 12.00.11. К., 2015. 467 с.
5. Пазюк А. В. Міжнародне інформаційне право: теорія і практика: монографія. Дніпропетровськ, 2015. 447 с.
6. Теорія та практика міжнародного кримінального права : підручник / Зелінська Н. А., Андрейченко С. С., Дрьоміна-Волок Н. В., Коваль Д. О.; за ред. проф. Зелінської Н. А., Одеса : Фенікс, 2017. 582 с.

ISSN 1995-6134

7. Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime. URL: https://rm.coe.int/16806bf0f8.
8. Stein Schjolberg, Solange Ghernaouti-Helie. A Global Treaty on Cybersecurity and Cybercrime. URL: http://pircenter.org/media/content/files/9/13480907190.pdf.
9. Stein Schjolberg. The History of Cybercrime: 1976-2014. URL: https://www.bod.de/buchshop/the-history-of-cybercrime-stein-schjolberg-9783734732942.
10. Конвенція про кіберзлочинність від 23.11.2001 р. URL: http://zakon.rada.gov.ua/laws/show/994_575.
11. Arab Convention on Combating Technology Offences of 21.12.2010. URL: https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd.
12. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001. URL: http://base.garant.ru/12123778.
13. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf.
14. African Union Convention on Cyber Security and Personal Data Protection of 27.06.2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_ protection_e.pdf.
15. Explanatory Report to the Convention on Cybercrime, Budapest, 23.XI.2001. URL: https://rm.coe.int/16800cce5b.
16. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. … канд. юрид. наук: 12.00.08. Пятигорск, 2010. 262 с.

REFERENCES

1. Interpol: Cybercrime is entering a new dimension. Retrieved from: https://money.cnn.com/video/technology/2018/01/24/davos-interpol-cybersecurity.cnnmoney/index.html.
2. Internet organized crime threat assessment 2018. Retrieved from: https://www.europol.europa.eu/iocta/2018.
3. Zabara, I. M. *Mizhnarodno-pravove rehulyuvannya spivrobitnytstva derzhav u borot'bi z informatsiynoyu zlochynnistyu* [nternational legal regulation of cooperation of states in the fight against information crime]. Retrieved from: http://e-pub.aau.edu.ua/index.php/chasopys/article/view/212 (in Ukr.).
4. Pazyuk, A. V. (2015). *Mizhnarodno-pravove rehulyuvannya informatsiynoyi sfery (teoretychni i praktychni aspekty)* [International legal regulation of the information sphere (theoretical and practical aspects)]. Doctor's thesis (12.00.11). Kyiv (in Ukr.).
5. Pazyuk, A. V. (2015). *Mizhnarodne informatsiyne pravo: teoriya i praktyka: monohrafiya* [International Information Law: Theory and Practice: Monograph]. Dnipropetrovs'k (in Ukr.).
6. Zelins'ka, N. A., Andreychenko, S. S., Dr'omina-Volok, N. V., & Koval', D. O.; Zelins'ka, N. A. (Red.). (2017). *Teoriya ta praktyka mizhnarodnoho kryminal'noho prava: pidruchnyk* [The theory and practice of international criminal law: a textbook]. Odesa: Feniks (in Ukr.).
7. Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime. Retrieved from: https://rm.coe.int/16806bf0f8.
8. Stein Schjolberg, Solange Ghernaouti-Helie. A Global Treaty on Cybersecurity and Cybercrime. Retrieved from: http://pircenter.org/media/content/files/9/13480907190.pdf
9. Stein Schjolberg. The History of Cybercrime: 1976-2014. Retrieved from: https://www.bod.de/buchshop/the-history-of-cybercrime-stein-schjolberg-9783734732942
10. *Konventsiya pro kiberzlochynnist'* [Convention on Cybercrime]. (23.11.2001). Retrieved from: http://zakon.rada.gov.ua/laws/show/994_575 (in Ukr.).
11. Arab Convention on Combating Technology Offences of 21.12.2010. Retrieved from: https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd.
12. *Soglasheniye o sotrudnichestve gosudarstv-uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v bor'be s prestupleniyami v sfere komp'yuternoy informatsii* [Agreement on Cooperation of the States Parties of the Commonwealth of Independent States in the Fight against Computer Crime]. (01.06.2001). Retrieved from: http://base.garant.ru/12123778 (in Russ.).
13. *Soglasheniye mezhdu pravitel'stvami gosudarstv-chlenov Shankhayskoy organizatsii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informatsionnoy bezopasnosti* [Agreement

between the governments of the Shanghai Cooperation Organization member states on cooperation in the field of ensuring international information security]. (16.06.2009). Retrieved from: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (in Russ.).
14. African Union Convention on Cyber Security and Personal Data Protection of 27.06.2014. Retrieved from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_ protection_e.pdf.
15. Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001. Retrieved from: https://rm.coe.int/16800cce5b.
16. Komarov, A. A. (2010). *Kriminologicheskiye aspekty moshennichestva v global'noy seti Internet* [Criminological aspects of fraud in the global Internet].Candidate's thesis (12.00.08). Pyatigorsk (in Ukr.).

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права: 53 pp. 92–99.

Related identifiers:

10.5281/zenodo.2009191

http://forumprava.pp.ua/files/092-099-2018-5-FP-Yatsyshyn_12.pdf

http://nbuv.gov.ua/UJRN/FP_index.htm_2018_5_12.pdf

Received: 19.10.2018
Accepted: 15.11.2018
Published: 27.11.2018

Cite as:

Яцишин, М. Ю. (2018). Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. *Форум Права,* 53(5). 92–99. DOI: http://doi.org/10.5281/zenodo.2009191.

Yatsyshyn, M. Y. (2018). Kryminalizatsiya kiberzlochyniv u mizhnarodnomu pravi: porivnyal'nyy analiz [Criminalization of Cybercrime in International Law: Comparative Analyses]. *Forum Prava,* 53(5). 92–99. DOI: http://doi.org/10.5281/zenodo.2009191.