МІЖНАРОДНЕ ПРАВО

УДК 341.4
DOI 10.36919/ELJ.1.2023.117

О. О. Семенюк,
кандидат юридичних наук, доцент,
доцент кафедри права
ПВНЗ «Європейський університет»
ORCID ID 0009-0007-9199-6657

ДО ПИТАННЯ ПРО МІЖНАРОДНО-ПРАВОВЕ РОЗУМІННЯ КІБЕРЗЛОЧИНУ

Стаття присвячена дослідженню питань щодо розуміння кіберзлочинів та їх класифікації за міжнародними нормативно-правовими актами. Визначено, що поняття кіберзлочин та його диференціація, за положеннями міжнародних нормативно-правових документів, представлено по-різному. Це ускладнює процеси в консолідації міжнародної спільноти в контексті захисту від кіберзлочинів і належного їм запобігання. Наголошено про потребу у виокремленні єдиних підходів до розуміння досліджуваних понять і їх класифікації, що забезпечить однозначну кваліфікацію та, як наслідок, підвищить ефективність протидії кіберзлочинності. Аналіз нормативної бази дозволив навести узагальнюючі дефініції та класифікації кіберзлочинів за об'єктивними ознаками: незаконний доступ; нелегальне перехоплення даних або їх підробка; втручання в дані або систему; кіберзлочини, пов'язані з порнографією, порушенням авторських і суміжних прав, шпигунством, саботажем, тероризмом, шантажем та маніпуляцією.

Ключові слова: *кіберзлочин, кібербезпека, кваліфікація, база даних, інформаційна система, підробка, тероризм.*

Постановка проблеми та її актуальність. У сучасному світі, де інформація і технології відіграють ключову роль, питання кібербезпеки набувають особливої актуальності та важливості. Щодня людство зіштовхується із загрозами в кіберпросторі, де потрібна інформація стає доступною за декілька кліків у процесі взаємодії із відповідними технічними засобами.

Безумовно, інтернет і цифрові технології дозволили досягти значної ефективності в повсякденному та професійному житті, але водночас з'явилася нова загроза – порушення кібербезпеки. Сьогодні кібератаки шкодять не лише фізичним та юридичним особам, але й державам загалом, зокрема й Україні. Саме тому кіберзлочинність і комп'ютерний тероризм визначені як одні із загроз національній безпеці України в інформаційній сфері. Відповідно до цього статтю присвячено порівняльно-правовому дослідженню розуміння поняття кіберзлочинів та їх класифікації.

Метою статті є дослідження національних і міжнародних нормативно-правових актів, присвячених захисту суспільних відносин у сфері кібербезпеки, а також визначення основного понятійного апарату в цьому контексті для правильної кваліфікації відповідних суспільно небезпечних діянь. Об'єктом дослідження є суспільні відносини, що виникають у кіберпросторі, а також використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Основною методологічною базою стали такі методи наукового пізнання: методи порівняння й аналогії застосовано для дослідження правового регулювання різних видів кіберзлочинів; метод спостереження було використано для ознайомлення із сутністю кіберзлочинів і загальною специфікою цього явища за міжнародним законодавством; метод узагальнення було використано для дослідження різних видів кіберзлочинів.

Виклад основного матеріалу дослідження. Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – сус-

пільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Кіберзлочинність законодавець визначає як сукупність кіберзлочинів.

Як бачимо, законодавче розуміння поняття кіберзлочин охоплює суспільно небезпечні діяння, які передбачені Кримінальним кодексом України (далі – КК України) та міжнародними нормативно-правовими актами, ратифікованими нашою державою.

Злочини, об'єктом яких є, зокрема, і кібербезпека, представлені в розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» стст. 361–363[1] КК України. Зі свого боку розуміння відповідних суспільно небезпечних діянь за міжнародними нормативно-правовими актами залишається дещо неоднозначним у своїй юридичній сутності.

У доповіді міжурядової групи експертів, заснованої Комісією з попередження злочинності і кримінальному правосуддю ООН для проведення дослідження проблеми кіберзлочинності і відповідних заходів щодо боротьби з нею, вказано, що «...комп'ютерна злочинність і, більш конкретно, кіберзлочинність – терміни, що використовуються для позначення конкретної категорії злочинних діянь. Пов'язані з цією категорією злочинних діянь виклики включають не тільки широке коло правопорушень, що вже підпадають під цю категорію, але й нові методи вчинення злочинів, що швидко формуються» [3]. Водночас дослідження нормативних документів ООН свідчить, що поняття кіберзлочин може охоплювати будь-який злочин, який може здійснюватися за допомогою комп'ютерної системи чи мережі, в рамках комп'ютерної системи чи мережі або проти комп'ютерної системи чи мережі [9, с. 276; 8, с. 440]. Тобто до кіберзлочинів може бути віднесено будь-який злочин, вчинений в електронному середовищі [4; 5].

Базовим документом у протидії кіберзлочинності для європейських держав є Конвенція про кіберзлочинність Ради Європи [6] від 23 листопада 2001 р. та Додатковий протокол до неї від 28 січня 2003 р. (далі – Конвенція) [7]. Вони є «фундаментом для розробки відповідного законодавства європейських держав» [8, с. 140].

Відповідно до змісту Конвенції кіберзлочин – це злочин, який вчиняється шляхом використання інформаційних систем, включаючи комп'ютерні системи та інші пристрої, які від них працюють або з ними взаємодіють, а також інтернет-мережі таких систем.

Конвенція розрізняє два види протиправних дій, пов'язаних із кіберзлочинністю: злочини та правопорушення. Частина І Другого розділу Конвенції («Матеріальне кримінальне право») побудована у такий спосіб, що всі склади злочинів розподілені підрозділами (групами) за родовим об'єктом, а підрозділи зі свого боку об'єднують злочини за видовими ознаками об'єкта посягання. У Конвенції виділено чотири види комп'ютерних злочинів: 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з використанням комп'ютерних засобів; 3) правопорушення, пов'язані із змістом даних; 4) правопорушення, пов'язані з порушенням авторського права і сумісних прав, а також додаткові види відповідальності та санкції (замах, співучасть). Протокол до Конвенції розширює це коло злочинів і містить зобов'язання стосовно криміналізації таких діянь: поширення расистських і ксенофобських матеріалів через комп'ютерні системи (ст. 3); мотивована загроза расизму і ксенофобії через комп'ютерну систему здійснення серйозного кримінального злочину, як визначено її внутрішнім правом стосовно осіб із причини того, що вони належать до групи, відмінної за расою, кольором шкіри, національним чи етнічним походженням, а також релігією, чи групи осіб з урахуванням цих факторів (ст. 4); публічну расистську і ксенофобську образу через комп'ютерну систему (ст. 5); поширення чи забезпечення доступу для громадськості через комп'ютерну систему матеріалу, який повністю заперечує чи надзвичайно применшує негативні наслідки, схвалює чи виправдовує дії, що є геноцидом чи злочинами проти людяності, як визначено міжнародним правом та як це визнано остаточними й обов'язковими рішеннями Міжнародного воєнного трибуналу, утвореного, відповідно до Лондонської угоди, від 8 серпня 1945 року, чи будь-якого іншого міжнародного суду, утвореного згідно із відповідним міжнародним документом і юрисдикція яких визнана стороною Протоколу (ст. 6) [11, с. 281].

Робоча група, яка займалася розробкою проєкту Конвенції щодо боротьби із кіберзлочинністю, обговорювала на рівні пропозицій можливість включення до наведеного переліку інших правопорушень, пов'язаних із використанням глобальних мереж, зокрема таких як пропаганда расизму в інтернеті. Однак через дискусійних характер цього аспекту між учасниками групи криміналізація такого діяння не відбулася.

Крім вказаної вище Конвенції щодо боротьби із кіберзлочинністю, окремі моменти розуміння поняття кіберзлочину (кіберзлочинність) представлені також у положеннях таких регіональних угод: Конвенція про кібербезпеку і захист персональних даних Африканського Союзу від 27 червня 2014 р. [3]; Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21 грудня 2010 р. [1]; Угода про співробітництво у сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16 червня 2009 р. [10].

Фактично в текстах усіх зазначених актів містяться види протиправних діянь, що підлягають криміналізації в національних правових системах держав-учасниць. Варто зазначити, 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 відбуватися паралельно [12, с. 94].

З узагальнення вказаних нормативно-правових актів можна виокремити такі види кіберзлочинів: незаконний доступ – навмисний доступ до усієї комп'ютерної системи або її частини без права на це; нелегальне перехоплення – навмисне перехоплення технічними засобами без права на це передач комп'ютерних даних, які не є призначеними для публічного користування; втручання в дані – навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерних даних без права на це; втручання в систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи; зловживання пристроями – навмисне виготовлення, продаж, володіння чи розповсюдження пристроїв і засобів для вчинення кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних систем і мереж; 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; 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; правопорушення, пов'язані з порушенням авторських і суміжних прав, – розглядаються як порушення авторських і суміжних прав відповідно до чинних міжнародних угод [12, с. 94–96].

Така класифікація досліджуваних суспільно небезпечних діянь, безумовно, кореспондується з відповідними правопорушеннями, вказаними у Конвенції, що дозволяє дійти висновку про схожий підхід міжнародної спільноти до визначення їх змісту.

Досить цікавим у контексті нашого дослідження є позиція Організації Північноатлантичного договору (НАТО). Нова Стратегічна концепція оборони та безпеки країн-членів НАТО, що була прийнята главами держав й урядів під час Лісабонського саміту країн-членів НАТО 19 листопада 2010 р., фактично прирівняла загрози кібератак до військових загроз, що зі свого боку передбачає можливість відповіді на масовані кібератаки із застосуванням національних збройних сил. Кібератаки стали одним із найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення кібернетичної безпеки було зазначено як другий за значимістю пріоритет НАТО [11].

Аналіз доктринальної нормативної бази вказує, що основні категорії кіберзлочинів, які розглядаються в рамках НАТО, включають: кібершпигунство (Cyber Espionage) – отримання конфіденційної інформації через несанкціонований доступ до комп'ютерних систем. Ця діяльність може бути спрямована на критичні галузі, включаючи військові, економічні, технологічні та політичні сфери; кіберсаботаж (Cyber Sabotage) – це атаки, спрямовані на нанесення шкоди комп'ютерним системам, мережам або інформаційним ресурсам. Вони можуть призвести до втрати даних, збоїв у роботі систем і критичних інфраструктур; кібертероризм (Cyber Terrorism) – використання кіберзлочинів для залякування населення, дестабілізації суспільства або завдання серйозної шкоди значному масштабу; кібершантаж (Cyber Extortion) – вимагання викупу або інші форми тиску через загрозу витоку конфіденційної інформації, блокування доступу до даних або систем, використовуючи кібератаки; кіберманіпуляція (Cyber Manipulation) – маніпулювання інформацією або вплив на системи з метою зміни вирішальних рішень або перекручення фактів.

Зважаючи на доктрини НАТО, кіберзлочини за їх об'єктивною стороною можна умовно класифікувати як шпигунство, саботаж, тероризм, шантаж і маніпуляцію. Ці категорії відображають різноманітні аспекти атак на кібербезпеку. Кожен такий тип кібезлочину має свої

наслідки – від втрати даних до дестабілізації суспільства. Саме тому важливою є співпраця між країнами-членами Альянсу та потенційними кандидатами для розробки стратегій протидії цим загрозам і встановлення стандартів кібербезпеки на міжнародному рівні.

Висновки. Викладене вище дозволяє зробити таке узагальнення:

– розуміння поняття кіберзлочин та його класифікації за міжнародними нормативно-правовими актами залишається дещо неоднозначним у своїй юридичній сутності. Така ситуація ускладнює процеси в консолідації міжнародної спільноти в контексті захисту від кіберзлочинів і належного їм запобігання;

– аналіз існуючої нормативної бази щодо розуміння досліджуваних суспільно небезпечних діянь дозволяє виокремити такі види кіберзлочинів за їх об'єктивними ознаками: незаконний доступ; нелегальне перехоплення даних або їх підробка; втручання в дані або систему; кіберзлочини, пов'язані із порнографією, порушенням авторських і суміжних прав, шпигунством, саботажем, тероризмом, шантажем та маніпуляцією.

– варто зазначити, що без однозначного розуміння поняття кіберзлочину та чіткої його диференціації неможлива ефективна йому протидія. Міжнародна правоохоронна діяльність у цій сфері вимагає єдиної кваліфікації відповідних діянь і визначення диференційованої системи покарань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arab Convention on Combating Technology Offences of 21.12.2010. URL : https://cms.unov.org/DocumentRepositoryIndexer/ GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a4af0-95ce-a8bbd1ecd6dd

2. African Union Convention on Cyber Security and Personal Data Protection. June 27, 2014. URL : https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_ data_protection_e.pdf

3. Док. ООН. E/CN.15/2011/19. П. 10.

4. Док. ООН. A/CONF. 187/10.

5. Док. ООН. A/CONF. 203/14.

6. Конвенція про кіберзлочинність від 23.11.2001 / Верховна Рада України. URL : http://zakon0.rada.gov.ua

7. Конвенція про кіберзлочинність від 23.11.2001. URL : http://zakon.rada.gov.ua/laws/show/994_575

8. Міжнародне кримінальне право (співробітництво держав у протидії злочинності) : підручник / Грінчак В. А., Земан І. В., Когутич І. І., Марін О. К. Харків : Право, 2019. 440 с.

9. Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2021. № 66. С. 276–283.

10. 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

11. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору від 19.11.2010 / Організація Північноатлантичного договору : офіційний вебсайт. URL : https://www.nato.int/cps/uk/natohq/official_texts_68580.htm

12. Яцишин М. Ю. Криміналізація кіберзлочинів у міжнародному праві: порівняльний аналіз. Форум права. 2018. № 5. С. 92–99. URL : http://nbuv.gov.ua/UJRN/FP_index.htm_2018_5_12

REFERENCES

1. Arab Convention on Combating Technology Offences 2010. URL : https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a4af0-95ce-a8bbd1ecd6dd [in English]. (2010, Dec, 21).

2. African Union Convention on Cyber Security and Personal Data Protection 2014. URL : https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_ protection_e.pdf [in English]. (2014, June, 27).

3. United Nations Organization. (2011). E/CN.15/2011/19. Chapter 10.

4. United Nations Organization. (No date). A/CONF. 187/10.

5. United Nations Organization. (No date). A/CONF. 203/14.

6. Convention on Cybercrime as of 23.11.2001 / Verkhovna Rada of Ukraine [Онлайн]. URL : http://zakon0.rada.gov.ua

7. Convention on Cybercrime of 2001 [Online]. URL : http://zakon.rada.gov.ua/laws/show/994_575 [in English]. (2001, Nov, 23).

8. International Criminal Law (State Cooperation in Combating Crime) : handbook / Hrynchak, V. A., Zeman, I. V., Kohutych, I. I., & Marin, O. K. Kharkiv : Pravo, 2019.

9. Popko, V. V., & Popko, Ye. V. (2021). International Legal Regulation of Transnational Cybercrime in Cyberspace. Scientific Bulletin of Uzhhorod National University. Series: Law. 66, 276–283.

10. Agreement Among the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in Ensuring International Information Security dated 2009. [Online]. URL : https://ccdcoe.org/sites/ default/files/documents/SCO-090616-IISAgreementRussian.pdf [in English]. (2009, Jun, 16).

11. Official Website of the North Atlantic Treaty Organization / NATO 2010. Strategic Concept for Defense and Security of the Members of the North Atlantic Treaty Organization. URL : https:// www.nato.int/cps/uk/natohq/ official_texts_68580.htm [in English]. (2010, Now, 19).

12. Yatsyshyn, M. Yu. (2018). Criminalization of Cybercrimes in International Law: Comparative Analysis. Forum of Law, 5, 92–99. URL : http://nbuv.gov.ua/UJRN/FP_index.htm_2018_5_12

O. O. Semenuk. REGARDING THE ISSUE OF INTERNATIONAL LEGAL UNDERSTANDING OF CYBERCRIME

The article is dedicated to exploring the understanding of cybercrimes and their classification according to international normative legal acts. It is identified that the concept of cybercrime and its differentiation according to the provisions of international normative legal documents varies. This complicates the processes of consolidating the international community in the context of protection against cybercrimes and their prevention.

Emphasis is placed on the necessity of establishing unified approaches to understanding the researched concepts and their classification, which will ensure clear qualification and consequently enhance the effectiveness of combating cybercriminality.

An analysis of the normative base has allowed for general definitions and classifications of cybercrimes based on objective criteria: unauthorized access; illegal interception or falsification of data; interference with data or systems; cybercrimes associated with pornography, infringement of copyrights and related rights, espionage, sabotage, terrorism, extortion, and manipulation.

Key words: *cybercrime, cybersecurity, qualification, database, information system, falsification, terrorism.*