УДК 035.077

Таволжанський Олексій Володимирович –
кандидат юридичних наук,
асистент кафедри кримінології та кримінально-виконавчого права
Національного юридичного університету імені Ярослава Мудрого

Oleksii V. Tavolzhanskyi –
candidate of juridical sciences,
teaching assistant at criminology and penal law department,
Yaroslav Mudryi National Law University
(77, Pushkinskaya str., Kharkiv, Ukraine)

Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства

У статті визначено кримінологічні ознаки кіберзлочинності, в умовах розбудови інформаційного суспільства. Наведено деякі проблеми нормативного врегулювання кіберзлочинності. Проаналізовано актуальні питання супутні терміни, що дозволяють всебічно вивчити таке явище.

Ключові слова: *кіберзлочинність, комп'ютерна злочинність, кіберзлочин, кіберпростір, кібертероризм.*

В статье определены криминологические признаки киберпреступности, в условиях развития информационного общества. Приведены некоторые проблемы нормативного урегулирования киберпреступности. Проанализированы актуальные вопросы сопутствующие сроки, позволяющие всесторонне изучить такое явление.

Ключевые слова: *киберпреступность, компьютерная преступность, киберпреступления, киберпространство, кибертерроризм.*

O.V. Tavolzhanskyi Issues of Definition of Cybercrime in Conditions of Development of Information Society

Criminological signs of cybercrime are defined in the article, in the context of the development of an information society. Some problems of normative regulation of cybercrime are presented. The relevant issues are related terms that allow us to comprehensively explore such a phenomenon.

The latest technology has become an integral part of the development of social relations and interpersonal communication. The emergence of another plane of human activity, virtual reality, could not remain aside from the general patterns of movement and development of society. Undoubtedly, the unlawful behavior, and accordingly, the crime, accompanies the development of the information society, modifies, acquires additional tools.

Significant "penetration" of cybercrime into all spheres indicates the need to study this phenomenon on a qualitative side, outlining key features, understanding determinants that contribute to the emergence and accompany of this kind of crime, the definition of prevention measures. Quantitative indicators of crime reflect only the increase or decline of some or other unlawful acts at the same time, qualitative modifications to track much more difficult. But any phenomenon or process can not be understood without a clear definition of its content and volume, especially so relatively new phenomenon for our country, like cybercrime.

The problems outlined in the article after the legal definition of the concept of cybercrime in the context of the development of the information society becomes even more relevant and require additional, in-depth scientific analysis in order to formulate rational proposals and recommendations for improving the current legislation and cyber defense of society.

Keywords: *cybercrime, computer crime, cybercrime, cyberspace, cyberterrorism.*

Постановка проблеми. Новітні технології стали невід'ємною складовою розвитку суспільних відносин та міжособистісних комунікацій. Поява ще однієї площини життєдіяльності людини, віртуальної реальності, не могла залишитись осторонь загальних закономірностей руху та розвитку суспільства. Безперечно, протиправна поведінка, і відповідно злочинність, супроводжує розбудову інформаційного суспільства, видозмінюється, набуває додаткових інструментаріїв.

Значне "проникнення" кіберзлочинності в усі сфери вказує на необхідність вивчення цього явища з якісної сторони, окреслення ключових ознак, розуміння детермінант які сприяють появі та супроводжують такий вид злочинності, визначення заходів запобігання. Кількісні показники злочинності відображують лише приріст або спад тих чи інших протиправних діянь в той же час якісні видозміни відслідковувати значно складніше. Але будь-яке явище чи процес зрозуміти неможливе без чіткого окреслення його змісту і обсягу, тим паче такого відносно нового для нашої країни явища, як кіберзлочинність.

Аналіз останніх досліджень та публікацій. Певний аналіз поняття кіберзлочинності, окремих її ознак та проявів проводили у своїх працях Азаров Д.С., Бельський Ю., Буров О., Голубев В.А., Дзюндзюк В.Б., Діордіца І.В., Демедюк С., Мисливий В.А., Марков В.В., Музика А.А., Іванченко О.Ю., Коваленко В.В., Кравцова М.О., Романюк Б.В., та інш. Деякі окремі питання, зокрема кіберзлочинності, кібербезпеки й кібертероризму тощо, було висвітлено в роботах дослідників: Ю.Р. Акчуріна, О.Г. Широкової-Мурараш, В.В. Топчія, Г.В. Форос, Є.А. Макаренко, М.А. Ожевана тощо. Усі перелічені та багато інших науковців достатньо ґрунтовно викладають матеріал у своїх дослідженнях, але виникає необхідність звернутись до змісту і легального розуміння кіберзлочинності за для аналізу та чіткого розуміння такого явища і можливого належного запобігання кіберзлочинності у майбутньому.

Невирішені проблеми. Безспірно, що масштаби кіберзлочинності, як транснаціонального явища, зумовлюють чисельні проблеми практичного і наукового характеру, вирішення яких може забезпечити нівелювання негативного впливу та мінімізацію темпів та форм його розвитку. Тому **метою цієї статті** є визначення основних кримінологічних ознак кіберзлочинності в сучасних реаліях її структури, надання критичне дослідження новел сучасного врегулюванню забезпечення кібербезпеки.

Виклад основного матеріалу. З наукової точки зору, надання поняття кіберзлочинності, як різновиду злочинності в цілому зобов'язує розкриваючи сутність спиратися на ознаки останньої. Все ж таки вважаємо за необхідне коротко описати загальновідомі авторські підходи до розуміння злочинності та виокремлення її сутнісних ознак, які можуть характеризувати і кіберзлочинність.

Передусім, при визначенні злочинності науковці наголошують на соціальному фундаменті її природи. Злочинності не буває поза суспільством, породжується умовами суспільного життя, навіть такої як кіберзлочинність. Статистичні дані з усією очевидністю доводять, що різкі зміни соціальних умов породжують зміни кількісних та якісних характеристик злочинності. Вона розглядається як: один з факторів суспільного здоров'я, нормальний і необхідний феномен суспільства; закономірне явище, що відображає стан суспільного організму (І. Н. Даньшин) [1, с. 13];

Криміногенну деформацію суспільної свідомості у виді антисоціальних поглядів, звичаїв, традицій, установок, що за певних умов закономірно породжують злочинність як свій наслідок вважає Головкін Б.М. причиною злочинності [2, с. 5]. Соціальні порушення містяться в основі і кіберзлочинності.

Наприкінці 2001 року в Будапешті з'явилась Конвенція Ради Європи про кіберзлочинність (далі – Конвенція). Основною метою Конвенції було визначено протидія комп'ютерним злочинам та встановлення співробітництва й координації діяльності правоохоронних органів різних держав. Україна ратифікувала Конвенцію 07 вересня 2005 року [3].

Понятійний апарат, що використовується в Конвенції та додатках до неї, а також національні легальні дефініції, що закріплені у вітчизняному законодавстві досі не приведений у відповідність. Хоча така потреба стає все нагальнішою.

У жовтні 2017 року прийнято та в подальшому підписано Президентом України Закон України «Про основні засади забезпечення кібербезпеки України». Закон набирає чинності через шість місяців з дня його опублікування, тобто 09 травня 2018. Вказаним Законом розкрито ряд термінів, що окреслюють та врегульовують кібервідносини зокрема: кіберзлочинність, кіберпростір, кіберзлочин, кібертероризм, кібершпигунство, тощо [4].

З кримінологічної точки зору кіберзлочинність як явище це не лише злочини визначені у глобальній мережі Інтернет, це і всі види злочинів вчинених в інформаційно-комунікаційній сфері, де відносини захисту інформації, інформаційні ресурси, обладнання, тощо можуть виступати об'єктом, предметом чи засобом злочинних посягань, реальністю, в якій відбуваються правопорушення і засобом або знаряддям злочину.

Важливою і обов'язковою ознакою кіберзлочинності є її кримінально-правовий характер, оскільки поза кримінально-правовою оцінкою немає як кіберзлочинів, так і кіберзлзлочинності взагалі. Вважаємо що безпосередньо легальне розуміння і тлумачення є першочерговим. Досить стисло законодавець визначив характерні ознаки кіберзлочинності вказавши лише, що вона (кіберзлочинність) – це сукупність кіберзлочинів.

Не безспірною у науковому середовищі є така ознака злочинності, і кіберзлочинності зокрема, як «сукупність». Непоодинокими є випадки системного підходу до розуміння злочинності.

Системний підхід до визначення злочинності, згідно якого злочинність розглядається як: відносно самостійна, динамічна, імовірнісна система (І. Н. Даньшин) [1, с. 12]; складна соціальна, оптимально функціонуюча система тощо. Тобто серед останніх думки також не завжди збігаються. Одні науковці вважають що системою є унікальна сукупність елементів, зокрема, вони наголошують, що система – це цілісна сукупність елементів, в якій всі елементи настільки тісно пов'язані один з одним, що виступають стосовно навколишніх умов і інших систем як єдине ціле або за іншим підходом при визначенні системи враховують факт наявності зв'язків між елементами сукупності. Окремі фахівці при визначенні системи наголошують, що до вказаних двох ознак додається ще одна – мета існування. Вважаємо вдалою думку Оболєнцева В.Ф. щодо пояснення системного об'єкта, як унікальної реальності і специфічної сутності [5, 162]. Визначитись, з урахуванням новел законодавства, яка ознака сукупності або системності притаманна кіберзлочинності складна задача, що потребує окремого ґрунтовного дослідження та вирішення. Залишаємо це питання відкритим для подальших наукових досліджень.

Загальноприйнятим, з викресленням ідеологічно-класового забарвлення, є поняття злочинності, надане ще 1969 році Н. Ф. Кузнецовою в монографії «Злочин і злочинність» [6, с. 137]. Це обумовлено тим, що по- при всі термінологічні зміни наступних років концепція злочинності, розроблена вченою, є достатньо цілісною. Підхід до визначення злочинності, розроблений Н. Ф. Кузнецовою, називають фундаментальним, доктринальним або кримінально-правовим.

По цьому ж шляху пішов і законодавець при визначенні кіберзлочинності, яка розкривається через такий термін як кіберзлочин. Кіберзлочин у вказаному вище Законі прирівняного до комп'ютерного злочину. Сумнівною є абсолютне співпадіння обсягів вказаних понять, на нашу думку все ж таки кіберзлочин є більш ширшим поняттям бо його вчиненню не завжди передує, як варіант використання саме комп'ютеру. Можливо саме такий термін використано за для уніфікації термінології, що використовується в розділі 16 Кримінального Кодексу України, а саме злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [7]. Але це в свою чергу породжує додаткові незрозумілості і варіації у право застосовній діяльності.

Цим же Законом вказано, що кіберзлочин, це суспільно 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. Формально закріплена можливість притягнення до кримінальної відповідальності за діяння визнані

кіберзлочинами на міждержавному рівні та ратифіковані через підписані Україною угоди та договори, хоча процедурні механізми наштовхуються на ряд процедурних колізій, стосовно місця, події, складу злочину тощо.

Пояснюючи поняття кіберзлочин та кіберзлочинність використано наступний досить прогресивний для національного законодавства термін: «кіберпростір». Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Вказаний термін наголошує на системний характер відносин у кіберпросторі, що знову повертає нас до роздумів про ознаку системності.

За для всестороннього та повного розуміння явища кіберзлочинності необхідно класифікувати та структурувати це явище. Із всієї маси кіберзлочинів законодавцем виділено терористичну сферу. Раніше на законодавчому рівні цей термін неодноразова згадувався. Зокрема, у Законі України «Про основи національної безпеки України» опосередковано згадуються терміни «комп'ютерна злочинність» та «комп'ютерний тероризм» [8], але цим нормативним актом не розкриваються вказані терміни, а лише вказано, що серед інших «комп'ютерна злочинність» та «комп'ютерний тероризм» є основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві.

Як складова частина кіберзлочинності розглядається і таке явище, як «технологічний тероризм» (що мабуть на нашу думку включає і кібертероризм). Цей термін було введено до нормативного поля Законом України «Про боротьбу з тероризмом», безумовно, що питання, які охоплюватися цим поняттям, входять до обсягу поняття кіберзлочинність. Технологічний тероризм – злочини, що вчиняються з терорестичною метою, із застосуванням відповідної зброї або із застосуванням засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру.» [9].

У дослідників з проблем тероризму існує й інша точка зору щодо природи кібертероризму. Вони вважають, що кібертероризм проявляється у двох формах: по- перше, комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів- хакерів, серед яких: – махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання); – шпигунство (проникнення до конфіденційних каналів зв'язку державних органів для отримання інформації, шпигунство з метою отримання інформації щодо закритих технологій); – диверсія (завдання шкоди технічному та програмному забезпеченню вірусами, що порушують функціонування державних органів та інших установ); – незаконне користування комп'ютерними послугами (програмами, покупки за рахунок інших тощо); по-друге, розголошення таємниці – отримання комерційної та конфіденційної інформації (що нерозривно пов'язане з першим видом), серед чого: – несанкціоноване отримання інформації для нецільового її використання особами, які не мають на це відповідного доступу; – незаконний збір та переховування інформації; – порушення правил користування конфіденційною інформацією [10]. Досить дискусійним є питання меж та співвідношення вищенаведених термінів: кібертероризм та технологічний тероризм.

Термін кібертероризм у дещо ширшому розумінні розкрито у Законі України «Про основні засади забезпечення кібербезпеки України», так зокрема кібертероризм – це терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Інший підхід щодо класифікації надано у міжнародних документах. Відповідно до Конвенції нормативно визначена наступна класифікація кіберзлочинів: 1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями. 2. Правопорушення,

пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами. 3. Правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією.

Структуру кіберзлочинності можна розглядати під кутом об'єктів, що частіше потрапляють під кібератаку про які вже згадувалось в попередніх роботах [11, 83-84].

Ну і звісно не можна оминути кримінально-правову структуру кіберзлочинності за національним законодавством. Розділ XVI Кримінального кодексу України (далі - КК України)), зокрема визначена наступна система кіберзлочинів: • несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України); • створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 3611 КК України); • несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361 прим.2 КК України); • несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України); • порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 КК України); • перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363 прим. 1 КК України).

Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України - незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

На думку А.А. Музика та Д.С. Азаров, «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 [12, с. 234].

Згідно з рекомендаціями експертів ООН термін «кіберзлочинність» охоплює будь-який злочин, який може скоюватись за допомогою комп'ютерної системи чи мережі, в рамках комп'ютерної системи чи мереж [13]. Тобто різноманітність підходів до визначення кіберзлочинності наштовхує на подальші роздуми щодо визначення найбільш вдалих і повних ознак, що зможуть в повній мірі охарактеризувати кіберзлочинність.

Висновки: Таким чином, окреслені у статті проблеми після легального визначення поняття кіберзлочинності в умовах розбудови інформаційного суспільства стає ще більш актуальними та потребують додаткового, поглибленого наукового аналізу з метою формування раціональних пропозицій і рекомендацій із вдосконалення чинного законодавства та кіберзахисту суспільства.

Список використаних джерел:

1. Даньшин И. Н. Введение в криминологическую науку / И. Н. Даньшин. − Х. : Право, 1998. – 144 с.

2. Головкін Б. М. Причинність у системі детермінації злочинності / Б. М. Головкін // Теорія і практика правознавства. – 2014. – Вип. 1. – [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/j-pdf/tipp_2014_1_24.pdf.

3. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5. – С. 128. – Ст. 71.

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163-19.

5. Оболенцев В. Ф. Держава Україна як система: системний підхід до запобігання корупції [Електронний ресурс] / В. Ф. Оболенцев // Проблеми законності. – 2017. – Вип. 138. – С. 161–168. – Режим доступу : http://plaw.nlu.edu.ua/article/viewFile/110994/106114.

6. Кузнецова Н. Ф. Преступление и преступность / Н. Ф. Кузнецова. – М. : Издат-во Московского ун-та, 1969. – 232 с.

7. Кримінальний кодекс України : Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25-26. – Ст. 131.

8. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

9. Про боротьбу з тероризмом : Закон України від 20.03.2003 № 638-IV. [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/638-15.

10. Тероризм: сучасний стан та міжнародний досвід боротьби / В. П. Журавльов, Б. В. Романюк, В. В. Коваленко. – Національна академія внутрішніх справ України, 2003. – 403 с.

11. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах / О. В. Тавожанський // Журнал східноєвропейського права. Електронне науково-практичне фахове видання. – 2016. – № 31. – С. 80-86.

12. Музика А. А. Законодавство України про кримінальну відповідальність за комп'ютерні злочини : науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. – К. : Вид-во Паливода А. В., 2005. – 345 с.

13. Рекомендації експертів ООН [Електронний ресурс]. – Режим доступу : // http://www.un.org/ru.

References:

1. I. N. Danshin, Vvedenie v kriminologicheskuyu nauku / I. N. Danshin. – Kh. : Pravo, 1998. – 144 p.

2. B. M. Holovkin, Prychynnist u systemi determinatsii zlochynnosti / B. M. Holovkin // Teoriia i praktyka pravoznavstva. – 2014. – Vyp. 1. – [Elektronnyi resurs]. – Rezhym dostupu : http://nbuv.gov.ua/j-pdf/tipp_2014_1_24.pdf.

3. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist : Zakon Ukrainy vid 7 veresnia 2005 r. No. 2824-IV // Vidomosti Verkhovnoi Rady Ukrainy. – 2006. – No. 5. – S. 128. – St. 71.

4. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05 zhovtnia 2017 r. [Elektronnyi resurs]. – Rezhym dostupu : http://zakon3.rada.gov.ua/laws/show/2163-19.

5. V. F. Obolentsev, Derzhava Ukraina yak systema: systemnyi pidkhid do zapobihannia koruptsii [Elektronnyi resurs] / V. F. Obolentsev // Problemy zakonnosti. – 2017. – Vyp. 138. – Pp. 161–168. – Rezhym dostupu : http://plaw.nlu.edu.ua/article/viewFile/110994/106114.

6. N. F. Kuznetsova, Prestuplenie i prestupnost / N. F. Kuznetsova. – M. : Izdat-vo Moskovskogo un-ta, 1969. – 232 p.

7. Kryminalnyi kodeks Ukrainy : Kodeks Ukrainy, Kodeks, Zakon vid 05.04.2001 No. 2341-III // Vidomosti Verkhovnoi Rady Ukrainy (VVR). – 2001. – No. 25-26. – St. 131.

8. Pro osnovy natsionalnoi bezpeky Ukrainy : Zakon Ukrainy vid 19 chervnia 2003 roku No. 964-IV // Vidomosti Verkhovnoi Rady Ukrainy. – 2003. – No. 39. – St. 351.

9. Pro borotbu z teroryzmom : Zakon Ukrainy vid 20.03.2003 No. 638-IV. [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/638-15.

10. Teroryzm: suchasnyi stan ta mizhnarodnyi dosvid borotby / V. P. Zhuravlov, B. V. Romaniuk, V. V. Kovalenko. – Natsionalna akademiia vnutrishnikh sprav Ukrainy, 2003. – 403 p.

11. O. V. Tavolzhanskyi, Kryminolohichni aspekty kiberzlochynnosti u suchasnykh umovakh / O. V. Tavozhanskyi // Zhurnal skhidnoievropeiskoho prava. Elektronne naukovo-praktychne fakhove vydannia. – 2016. – No. 31. – Pp. 80-86.

12. A. A. Muzyka, Zakonodavstvo Ukrainy pro kryminalnu vidpovidalnist za komp'iuterni zlochyny : naukovo-praktychnyi komentar i shliakhy vdoskonalennia / A. A. Muzyka, D. S. Azarov. – K. : Vyd-vo Palyvoda A. V., 2005. – 345 p.

13. Rekomendatsii ekspertiv OON [Elektronnyi resurs]. – Rezhym dostupu : // http://www.un.org/ru.