Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 4 (44), 2024

УДК 343.97

Роман ШАК
Національний університет “Львівська політехніка”,
асистент кафедри міжнародного та кримінального права
Навчально-наукового інституту права,
психології та інноваційної освіти,
доктор філософії за спец. 081 Право
roman.i.shak@lpnu.ua
ORCID: 0000-0002-6658-4585

ПОНЯТТЯ ТА ВИДИ КІБЕРПРАВОПОРУШЕНЬ В КРИМІНАЛЬНОМУ ПРАВІ

http://doi.org/10.23939/law2024.44.325

Анотація. Стаття присвячена дослідженню поняття та класифікації кіберправопорушень у кримінальному праві. Автор аналізує різні підходи до визначення термінів “комп’ютерні правопорушення”, “кіберправопорушення”, “інтернет-злочинність” та інших, підкреслюючи різницю у їхньому застосуванні в юридичній науці. Особливу увагу приділено позиціям вчених щодо трактування кіберзлочинності та її місця у кримінально-правовому полі.

Автор констатує, що нині сформувалися два підходи до розуміння кіберправопорушень, вузький та широкий. Вузький підхід зосереджується на захисті інформаційної безпеки, тоді як широкий підхід охоплює всі види правопорушень, що здійснюються з використанням інформаційно-телекомунікаційних технологій. Відсутність єдиного підходу до визначення кіберправопорушень негативно впливає на практику протидії цим злочинним діям. Автором підкреслюється важливість уніфікації понятійного апарату та адаптації кримінального законодавства до нових викликів у сфері кібербезпеки.

У статті розглядаються міжнародні правові акти, зокрема Конвенція про кіберзлочинність, яка визначає п’ять груп злочинів, включаючи злочини проти конфіденційності, цілісності та доступності комп’ютерних даних, а також злочини, пов’язані з контентом та порушенням авторських прав, а також національне законодавство, зокрема Кримінальний кодекс України та Закон “Про основні засади забезпечення кібербезпеки України” Проводиться аналіз різних класифікацій кіберправопорушень, запропонованих науковцями, які охоплюють порушення конституційних прав, прав власності, суспільної моралі та державної безпеки.

У підсумку, автор наголошує на важливості адаптації національних правових систем до швидкозмінних умов цифрової епохи та розробки нових правових інструментів для захисту від кіберправопорушень. Основний висновок полягає в необхідності більш широкого визнання та визначення кіберправопорушень для ефективного розуміння та протидії цим злочинним діям на національному та міжнародному рівнях.

Ключові слова: кіберпростір; кіберправопорурення; комп'ютерні правопорушення кіберзлочинність; мережа Інтернет; кримінальна відповідальність.

Постановка проблеми. За останні десятиліття число кіберправопорушень у світі збільшилося у величезну кількість разів. Цьому свідчать величезні фінансові втрати юридичних осіб, осіб і державних структур, а також випадки кіберправопорушень, що почастішали, і проти фізичних осіб. Цю стрімко зростаючу за своїми масштабами проблему необхідно якнайшвидше почати ефективно вирішувати, тому що рівень кіберзлочинності та складності правопорушень зростає, а розкриття справ і ефективність роботи проти злочинців у кіберпростор падає.

Поряд із цим, правові системи стикаються із викликами, які пов'язані з міжнародним характером кіберправопорушень, коли дії, вчинені в одній країні, призводять до наслідків у іншій, що вимагає міждержавної кооперації та уніфікації правових норм. Транскордонність таких злочинних діянь ускладнює процес ідентифікації зловмисників і притягнення їх до відповідальності. Крім того, існує важливість адаптації кримінального законодавства до швидко змінюваних технологій, що вимагає постійного оновлення законодавчих актів і методів їх застосування. Це включає не тільки створення нових законодавчих норм, але й модифікацію існуючих, аби вони адекватно відображали реалії сучасного цифрового світу. Отже, питання пов'язані із кіберправопорушеннями у кримінальному праві вимагають всебічного аналізу та розробки комплексного підходу до їх визначення та класифікації.

Аналіз дослідження проблеми. Дослідження причин швидкого поширення кіберзлочинності та методи спільної боротьби з кіберправопорушеннями стають особливо важливими і відображаються у працях таких відомих українських науковців, як О. Амелін, Ю. А. Бельський, Б. М. Головкін, А. Голуб, М. Гуцалюк, О. П. Дзьобань, В. Б. Дзюндзюк, М. М. Дмитрук, Д. В. Дубов, С. Б. Жданенко, Ю. Б. Ірха, Н. В. Карчевський, Є. В. Коваленко, О. Копатін, М. С. Корнієнко, Є. М. Мануїлов, Г. Нагорняк, Я. Неділько, М. А. Погорецький, А. В. Савченко, М. Самбор, В. І. Тимошенко, С. Федонюк, О. І. Яременко. Також проаналізовано роботи зарубіжних дослідників, таких як Lessig L., Nottage L., Tropina T., Ivana dos Santos Teixeira, William M., Sheldon D., Katsh M. E., Post D. G., Ferzan K., Neil Boister, Vermeulen Gert, Wendy De Bondt, Charlotte Ryckman, Dupont B., Kshetri N.

Метою статті є аналіз та класифікація кіберправопорушень в контексті чинного кримінального законодавства, визначення їх правових ознак та специфіки. Дослідження покликане виявити прогалини у нормативно-правовій базі, пов'язані з регулюванням цієї категорії правопорушень, та розробити пропозиції щодо вдосконалення законодавства для ефективнішої боротьби з кіберзлочинністю.

Виклад основного матеріалу. Поняття "кіберзлочинності" на сьогоднішній день набуло великого поширення у зв'язку з інформаційно-телекомунікаційним проривом, що стався у XXI ст. Кіберзлочинність – сукупність правопорушень, скоєних у "кіберпросторі" за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж та комп'ютерних даних.

У юридичній та іншій науковій літературі для позначення суспільно-небезпечних діянь, які здійснюються з використанням інформаційно-телекомунікаційних технологій, використовуються різні терміни та формулювання. Це "комп'ютерні правопорушення", "кіберправопорушення", "інтернет-правопорушення", "правопорушення, що скоюються з використанням інтернет-технологій", "правопорушення, що скоюються у віртуальному середовищі", "правопорушення, що скоюються в

Інтернеті", "правопорушення, що скоюються за допомогою інформаційно-телекомунікаційних технологій", "комп'ютерна злочинність", "кіберзлочинність", "інтернет-злочинність", "кібератаки", "кібервійни", "кіберконфлікти" та ін [1, с. 11]. Зміст кожної з вищезгаданих категорій піддається обговоренню та інтерпретації.

Аналіз наукових джерел, офіційних документів та нормативних правових актів, присвячених проблемі протидії діянням, що здійснюються з використанням інформаційно-телекомунікаційних технологій, показує, що одні правознавці схильні вузько трактувати зміст перерахованих вище дефініцій, зводячи їх до посягань на такий правоохоронний об'єкт, як інформаційна безпека.

В рамках "широкого" підходу вищезазначені терміни використовуються для позначення найрізноманітніших правопорушень, що скоюються у віртуальному (Інтернет) просторі з використанням комп'ютерної техніки та інформаційно-телекомунікаційних мереж, а також інших засобів доступу до кіберпростору.

Я. Неділько висловлює думку, що терміни "комп'ютерні правопорушення" та "кіберправопорушення" можна застосовувати для ефективної реалізації кримінологічних, кримінально-процесуальних та криміналістичних досліджень у загальноприйнятому сенсі. Однак у контексті національного кримінально-правового дискурсу рекомендується обмежити використання цих понять, віддаючи перевагу терміну "правопорушення у сфері використання інформаційних технологій" [2, с. 54].

У своєму аналізі вище згаданий вчений досліджує поняття "правопорушення у сфері інформаційних технологій" та "інформаційна безпека" та доходить висновку, що правопорушення у сфері інформаційних технологій належать до категорії кримінальних правопорушень, що стосуються інформаційної безпеки, визначаються Кримінальним кодексом України як суспільно небезпечні діяння, вчинені суб'єктом правопорушення, які завдають шкоди відносинам у сфері задоволення інформаційних потреб з використанням обчислювальної техніки. Вивчення діючих положень КК України дозволяє визначити, що до таких злочинів відносяться дії, які регламентуються статтями 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК [3].

Зазначене вище ствердження Я. Неділько про класифікацію певних дій як "кримінальні правопорушення у сфері інформаційних технологій" є не обґрунтованим. Якщо прийняти думку згаданого дослідника, виникає суперечність, адже порушення авторських прав через втручання в роботу ЕОМ, за його логікою, не вважається шкодою "відносинам у сфері задоволення інформаційних потреб" і не виконується з використанням "засобів обчислювальної техніки". Однак реальність показує прямо протилежне.

За словами О. Амелін, комп'ютерні кримінальні правопорушення та кіберправопорушення становлять окремі категорії кримінальних діянь у сфері передових інформаційних технологій. Вони класифікуються залежно від особливостей: комп'ютерні правопорушення визначаються через використання як знаряддя комп'ютерної техніки. Водночас, кіберправопорушення характеризуються особливістю середовища, де вони вчиняються – кіберпростором, який охоплює комп'ютерні системи та мережі. Автор також акцентує увагу на тому, що об'єктом нападу при таких злочинах діях є суспільні відносини, що регулюють автоматизовану обробку інформації. Звертаючись до норм Конвенції та її Додаткового протоколу, він стверджує, що лише дії, перелічені в цих документах, можуть бути класифіковані як кіберправопорушення [4, с. 5–6].

У свою чергу О. К. Копатін та Є. Д. Скулишин визначають кіберправопорушення як кримінальне правопорушення, що пов'язане з використанням кібернетичних комп'ютерних систем або вчиняється у кіберпросторі. Відмінність від комп'ютерного правопорушення, на їх думку, полягає в тому, що останнє поняття стосується використання будь-яких комп'ютерних технологій, тоді як кіберправопорушення має більш вузький характер і стосується лише функціонування кібернетичних комп'ютерних систем. [5, с. 85–86].

На думку М. О. Думчикова, під кіберзлочинністю розуміються правопорушення у сфері високих інформаційних технологій, скоєні зловмисниками, які використовують ці технології з протиправною метою. Інші автори визначають кіберзлочинність через поняття "кіберпростір". Кіберзлочинність, на їхню думку, – це злочинність у кіберпросторі [6, с. 66].

Такий аналіз наукових підходів дозволяє стверджувати, що серед теоретиків немає однієї закріпленої позиції у визначенні кіберправопорушення, що обумовлено різним трактуванням способів використання комп'ютерних систем у вчиненні відповідних неправомірних дій.

Ми вважаємо, що широке тлумачення терміну "кіберзлочинність" є правомірним. Результати кримінологічних досліджень свідчать про наявність стійкої тенденції до появи у віртуальному просторі нових видів зазіхань на різні суспільні відносини, цінності, права та свободи, що охороняються законом. Об'єктами злочинних діянь стають життя, здоров'я, моральний, фізичний, статевий розвиток неповнолітніх. Злочинці посягають на власність, у тому числі інтелектуальну, на громадську безпеку, суспільний лад, суспільне здоров'я, суспільну моральність, основи конституційного ладу та державної влади, мир та безпеку людства. Для кіберправопорушень характерно те, що інформація, інформаційно-телекомунікаційні технології можуть виступати предметом, знаряддям або засобом скоєння суспільно-небезпечного діяння.

На міжнародному рівні тенденція до широкого тлумачення аналізованих понять виявила себе під час обговорення актуальних проблем протидії кіберзлочинам у рамках X Конгресу ООН, який відбувся 2000 р. [7, с. 110-111]. Експерти використовували поняття кіберзлочинності на цьому симпозіумі для позначення "комп'ютерних" правопорушень, де об'єктом є інформаційна безпека, а предметом – комп'ютер, а також зазіхань на будь-які суспільні відносини, що здійснюються з використанням комп'ютерів як знаряддя чи засіб.

Першим міжнародно-правовим актом, у якому було вжито заходів щодо уніфікації переліку та ознак кіберправопорушень, стала Конвенція про кіберзлочинність, ухвалена Комітетом міністрів Ради Європи 8 листопада 2001 р. у Будапешт [8].

Конвенцією РЄ та Протоколом № 1 (прийнятий у 2002 р.) до Конвенції про кіберзлочинність передбачено п'ять груп злочинів:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.
2. Злочини, пов'язані з використанням комп'ютерних засобів.
3. Злочини, пов'язані із змістом даних.
4. Злочини, пов'язані з порушенням авторських та суміжних прав.
5. Акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Перша категорія злочинів, зазначених у Конвенції Ради Європи, охоплює діяння, які загрожують конфіденційності, цілісності та доступності комп'ютерних систем та даних. Ці злочини включають незаконний доступ (навмисний протиправний доступ до комп'ютерної системи або її частини, стаття 2 Конвенції), незаконне перехоплення (навмисне протиправне перехоплення не призначених для загального доступу передач даних до, з або всередині комп'ютерної системи, стаття 3 Конвенції), втручання в дані (протиправне втручання у вигляді пошкодження, видалення, зміни або припинення комп'ютерних даних, стаття 4 Конвенції), втручання у функціонування системи (стаття 5 Конвенції), та незаконне використання пристроїв (стаття 6 Конвенції).

Друга категорія злочинів, зазначена в Конвенції Ради Європи, включає діяння, які безпосередньо здійснюються за допомогою комп'ютерних засобів. Вона охоплює злочини, такі як фальсифікація, яка полягає у введенні, зміні, стиранні або блокуванні комп'ютерних даних з метою порушення їхньої автентичності, щоб такі дані вважались законними для юридичного використання, незалежно від того, чи можуть вони бути прямо прочитані чи зрозумілі (стаття 7 Конвенції). Також до цієї групи відноситься комп'ютерне шахрайство, що здійснюється через введення, зміну, видалення або блокування даних, або через втручання в роботу комп'ютерних систем з метою

шахрайського чи нечесного заволодіння майном іншої особи, спрямоване на неправомірне отримання економічної вигоди для себе або третіх осіб (стаття 8 Конвенції).

Третя категорія порушень, описаних у Конвенції Ради Європи, стосується злочинів, пов'язаних з контентом. Вона охоплює дії, такі як виробництво дитячої порнографії з метою її поширення через комп'ютерні системи, а також пропонування, доступність, розповсюдження, купівля або володіння такими матеріалами у комп'ютерній системі чи на носіях. Дитяча порнографія за Конвенцією визначається як порнографічні матеріали, що містять зображення неповнолітніх у сексуальних актах, особи, що виглядають як неповнолітні, або реалістичні зображення неповнолітніх, залучених до сексуальних дій. Під "неповнолітнім" розуміється особа, яка не досягла віку 18 років, хоча Конвенція дозволяє країнам-учасницям самостійно встановлювати віковий ценз не нижче 16 років (ст. 9 Конвенції РЄ).

Четверта група включає злочини, які стосуються порушень авторських і суміжних прав. Ці порушення не виділені окремо в Конвенції про кіберзлочинність, а відповідність актів до таких злочинів визначається національними законодавствами згідно зі статтею 10 Конвенції РЄ. Вчинення таких актів має бути умисним, у комерційних масштабах і з використанням комп'ютерної системи, за винятком порушень моральних прав.

П'ята група злочинів, описаних в межах кіберзлочинності, включає дії расизму та ксенофобії, реалізовані через комп'ютерні мережі. Ці злочини характеризуються розповсюдженням матеріалів, які викликають агресію, спонукають до дискримінації або виражають ненависть до осіб або груп, заснованих на расовій, національній, релігійній, або етнічній ідентифічності. Такі правопорушення можуть містити текст, зображення або інші форми, які пропагують чи заохочують до ненависті та насильства проти окремих осіб або груп, зафіксовані на основі їхньої раси, шкірного кольору, етнічного чи національного походження, а також віросповідання.

Станом на 2023 року цей нормативний акт ратифікували 67 держав, у тому числі Австралія, Канада, Сполучені Штати, Ізраїль, Японія, Аргентина, Гана, Домініканська Республіка, Кабо-Верде, Колумбія, Коста-Ріка, Маврикій, Марокко, Нігерія, Панама, Парагвай, Перу, Сенегал, Філіппіни, Чилі, Шрі-Ланка, Тонга.

У цьому документі державам-учасницям пропонується криміналізувати посягання на такі об'єкти, як інформаційна (комп'ютерна) безпека, власність, інтелектуальна власність, а також дії, пов'язані з поширенням незаконного контенту інформаційних мережах (дитяча порнографія; інформація екстремістського характеру). Подібне трактування кіберзлочинності простежується і в інших директивах країн – учасниць Конвенції, присвячених проблемам протидії атакам на інформаційні мережі, а також збереження безпеки мереж та інформаційних систем [9, с. 20].

Таким чином, у вищезгаданих документах ООН та Євросоюзу до кіберзлочинності зараховуються не лише "комп'ютерні" правопорушення, які посягають на інформаційну безпеку, а й інші злочинні дії, що використовують комп'ютер як зброю (computer-facilitated) чи засіб правопорушення (computer-related). Здається, ця позиція є загалом правильною, оскільки використання інформаційно-телекомунікаційних технологій як знаряддя або засобу злочинного посягання на будь-які об'єкти підвищує ефективність злочинної діяльності, надаючи їй якісно нову форму, роблячи її транскордонною, масштабною та важко досліджуваною.

На жаль, у зазначених вище документах ООН та Євросоюзу нічого не йдеться про протидію використанню інформаційно-телекомунікаційних технологій як зброї у військово-політичних конфліктах, для втручання у внутрішні справи держав, для здійснення підривної, терористичної, шпигунської та диверсійної діяльності.

Крім того, в аналізованих офіційних актах ООН та Євросоюзу не враховуються можливості "мобільного" доступу до Інтернету для вчинення кіберправопорушень. Це не дозволяє відносити до кіберправопорушень зазіхання, під час яких використовуються не комп'ютерні, інші пристрої, які забезпечують доступ до мережі, зокрема, "портативні" мобільні телефони. Тому правильніше було б вважати, що кіберзлочинність є сукупністю правопорушень, що скоюються з використанням

інформаційно-телекомунікаційних технологій, які посягають на інформаційну безпеку та (або) використовують комп'ютер, а також інші пристрої, що забезпечують доступ до мережі, як знаряддя або засоби скоєння злочину [10, с. 313].

В контексті національного законодавства, Закон України "Про основні засади забезпечення кібербезпеки України" визначає "кіберзлочин" (комп'ютерний злочин) як діяння, яке є суспільно небезпечним та винним, вчинене у кіберпросторі чи за допомогою нього, відповідальність за яке передбачена українським кримінальним законодавством або яке визнано злочином відповідно до міжнародних договорів, які Україна ратифікувала [11]. Тобто "кіберзлочинність" – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій та глобальних мереж. Водночас ми вважаємо, що термін "комп'ютерна злочинність" відноситься лише до правопорушень, що скоєні проти комп'ютера або комп'ютерних даних.

Отож наведені нами вище дефініції підкреслюють ключові особливості кіберзлочинності, найбільше розкривають його природу, оскільки;

– по-перше, відбивають ставлення кіберпростору до інформаційного простору як приватного до спільного;

– по-друге, спеціально звертають увагу на той факт, що інформаційно-телекомунікаційні мережі (зокрема і мережа Інтернет) є матеріальними складовими кіберпростору.

Беручи до уваги поняття "кіберпростір", можна охарактеризувати кіберзлочинність як комплекс діянь, які здійснюються у кіберпросторі за допомогою комп'ютерних систем чи мереж, а також інших інструментів для доступу до цього простору, здійснюваних всередині комп'ютерних систем чи мереж або спрямованих проти цих систем, мереж та їхніх даних [12, с. 92].

Натомість, М.М. Дмитрук також використовує термін "кіберпростір", але вже для розкриття змісту поняття "кіберправопорушення". Під кіберправопорушенням він розуміє правопорушення, що завдає шкоди різнорідним суспільним відносинам, скоєне дистанційно, шляхом використання засобів комп'ютерної техніки та інформаційно-телекомунікаційних мереж та освіченого ними кіберпростору [13, с. 17]. У наведеному визначенні кіберпростір виступає як безпосередній засіб скоєння правопорушення

На нашу думку, визначення сутності понять "кіберзлочинність" і, відповідно, "кіберправопорушення" через поняття "кіберпростір" є розумним, оскільки його використання дозволяє не тільки найповніше розкрити особливості явищ, що відбуваються в різних інформаційних мережах, але й охопити набагато більше коло суспільних відносин: так, конкретне правопорушення не обмежуватиметься окремо взятими об'єктом зазіхання та інформаційно-телекомунікаційної мережею, що опосередковує можливість віднесення до кіберправопорушень як неправомірного доступу до комп'ютерної інформації, і, наприклад, шахрайства у мережі Інтернет.

Проте зазначимо, що низка авторитетних учених дотримується думки про те, що використання поняття "кіберпростір" у вітчизняній юридичній науці поки що перебуває під питанням [14, с. 13]. Більше того, з метою запобігання надмірному використанню англіцизмів у наші дні доцільно звертатися до іншої термінології [15, с. 122].

В даний час поряд з терміном "кіберзлочинність" у міжнародній та вітчизняній юридичній науці найчастіше використовуються такі поняття, як "злочинні діяння у сфері комп'ютерної інформації" та "злочини, скоєні з використанням інформаційних технологій".

У науковій літературі можна зустріти різні підходи до їхнього розуміння та використання. Позиція одних учених у тому, що є різниця між цими термінами. Прихильники другої точки зору вважають, що оскільки дані поняття використовуються для назви тих самих суспільно-небезпечних діянь, то їх можна вважати рівнозначними [16, с. 415]. Звісно ж, що другу позицію не можна визнати вірною. Цілком очевидно, що термін "кіберзлочинність" трактується набагато ширше оскільки за змістом включає себе обидва поняття.

Крім того, якщо звернувшись до першоджерела – іноземної термінології – можна помітити, що за кордоном поняття "computercrime" і "cybercrime" мають змістовні відмінності.

Першим терміном охоплюються лише злочинні дії, що посягають на комп'ютерні дані, тоді як другий включає у собі злочинні діяння з використанням як глобальних мереж, інформаційних технологій, так і комп'ютерів. [17, с. 13-14], що також доводить ширше значення поняття "кіберзлочинність".

Наукові праці зарубіжних дослідників, серед яких Morrison P., Colin B., Parker Donn Ст, Brenner S.W., Shelley, Louise I., Williams P., Sieber U. та ін., присвячені аналізу кіберзлочинності, містять уявлення про це явище. Проте дані дослідження практично не мають відношення до українського простору і не охоплюють національне законодавство. Незважаючи на це, вони дають стійкі теоретичні основи з метою вивчення кіберзлочинності у глобальному напрямку [18].

Зазначимо, що сьогодні немає єдиної думки щодо переліку кіберправопорушень. Так, за інформацією Управління ООН з наркотиків та злочинності великий діапазон кіберправопорушень умовно можна поділити на три групи:

– які здійснюються з метою отримання матеріальної вигоди;

– пов'язані з використанням інформації, що зберігається у комп'ютерах;

– спрямовані проти цілісності, конфіденційності та доступності комп'ютерних систем;

– злочини пов'язані з порушенням авторських та суміжних прав [8].

Опираючись на це визначення, кіберзправопорушення (комп'ютерні правопорушення) слід класифікувати як суспільно небезпечні винні діяння, вчинені в кіберпросторі та/або за допомогою його ресурсів, за які передбачена відповідальність згідно з Кримінальним кодексом України.

Кіберправопорушення можна поділити на такі категорії:

1. Правопорушення, вчинені в кіберпросторі або з його використанням, за які передбачена відповідальність за різними розділами Кримінального кодексу України. Ці правопорушення зачіпають різні сфери кримінально-правової охорони: національну безпеку, громадську безпеку, захист права на інтелектуальну власність, власність, господарські відносини, а також права і свободи особистості. Характерним є використання новітніх інформаційних технологій та комп'ютерної техніки у їх вчиненні. Наприклад, крадіжки реквізитів платіжних карт (фішинг, вішинг, шиммінг, скіммінг); незаконні фінансові операції з використанням платіжних карток без згоди власника (кардінг); заволодіння коштами через неіснуючі інтернет-магазини, інтернет-аукціони або інші онлайн-платформи (інтернет-шахрайство); порушення авторських прав та суміжних прав через незаконне розповсюдження програмного забезпечення через мережі (піратство).

2. Правопорушення у сфері використання комп'ютерів, їх систем та мереж, які регулюються Розділом XVI КК України. Ці діяння впливають на відносини, які виникають у процесі використання електронно-обчислювальних машин, їх систем і мереж, а також мереж електрозв'язку [19, с. 60-61].

Необхідно підкреслити, що перелік правопорушень у сфері комп'ютерної інформації, відображений у Кримінальному кодексі України, не охоплює всі можливі злочинні дії, що відбуваються в кіберпросторі. Існує кілька наукових класифікацій кіберправопорушень. Наприклад, А. Голуб пропонує розділити кіберправопорушення на такі категорії:

– кримінальні правопорушення у сфері комп'ютерної інформації, спрямовані проти інформаційних комп'ютерних відносин;

– кримінальні правопорушення у інформаційному комп'ютерному просторі, які впливають на відносини з реалізації прав на інформаційні ресурси;

– інші кримінальні правопорушення, характерні за умовами використання комп'ютерної інформації або її складових частин [20].

Професор Савченко А.В. вважає, що до кіберправопорушень можуть також належати інші злочинні дії, зазначені в Кримінальному кодексі України, якщо інструментом вчинення обираються інформаційні мережеві технології, а наслідки таких дій виявляються у кіберпросторі [21, с. 154]. Автор відносить до категорії кримінальних правопорушень, які вчинені в кіберпросторі, такі

злочинні дії як державна зрада, шпигунство, диверсія, порушення таємниці голосування, незаконне розкриття медичної таємниці, а також розкриття таємниці у комерційній та банківській сферах, сутенерство та інші. Можна стверджувати, що практично у кожному розділі спеціальної частини Кримінального кодексу України є кримінальні правопорушення, які можуть бути вчинені в кіберпросторі за допомогою комп'ютерів та програмного забезпечення.

Також варто відзначити класифікацію кіберправопорушень, запропоновану В. Б. Дзюндзюком:

1. Правопорушення проти конституційних прав та свобод людини та громадянина, які включають порушення недоторканності приватного життя, таємниці листування та інших повідомлень, а також порушення авторських прав;

2. Правопорушення проти життя та здоров'я, до яких відносяться рецепти виготовлення наркотичних речовин домашнім способом і їх поширення;

3. Правопорушення проти честі та гідності, включаючи розповсюдження компрометуючої інформації та наклепи;

4. Правопорушення проти власності, зокрема кримінальні дії в сфері платіжних і банківських систем;

5. Правопорушення у сфері комп'ютерної інформації, які включають неправомірний доступ до інформації, створення та розповсюдження вірусів;

6. Правопорушення проти суспільної моралі;

7. Правопорушення проти безпеки держави, такі як незаконний доступ до державних секретів, що стає можливим через використання Інтернету у державних структурах [56].

Така велика кількість видів кіберправопорушень свідчить про те, що масштаби кіберзлочинності збільшуються. Тим самим зростає необхідність взаємодії держави із суспільством і міжнародною спільнотою з метою подолання цього негативного явища.

Висновки. Отже поняття "кіберправопорушення" відображає широкий спектр суспільно небезпечних діянь, що здійснюються в кіберпросторі за допомогою комп'ютерних систем та мереж. Сучасне розуміння кіберзлочинності включає не лише традиційні правопорушення, адаптовані до цифрового середовища, але й злочинні дії, які стали можливими завдяки новітнім технологіям. Ці правопорушення мають різноманітний характер і об'єкт впливу, охоплюючи від порушень інформаційної безпеки до шахрайств та кібератак. Науковці та правозахисники вживають різні терміни для опису цих правопорушень, зокрема "комп'ютерні правопорушення", "кіберправопорушення", та інші, кожен з яких має свою специфіку та значення залежно від контексту. Відмінності у трактуванні цих понять негативно впливають на законодавчі та практичні аспекти протидії кіберправопорушенням.

Важливо зазначити, що визначення кіберправопорушення не є статичним і продовжує розвиватися з огляду на швидкий розвиток технологій та зміни в соціальному контексті. Це підтверджується різними підходами до класифікації та інтерпретації кіберзлочинності у науковій літературі. Дискусії стосуються не тільки специфіки правопорушення, але й методів їх розслідування та запобігання.

З урахуванням цих факторів, вважаємо що нині кіберправопорушення може бути визначено як комплекс правопорушень, що включають зловживання комп'ютерною технікою або кіберпростором для здійснення актів, які шкодять фізичним особам, організаціям чи державі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіберзлочинність та електронні докази = Cybercrime and digital evidence (2022): навч. посібник / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан]; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів: ЛНУ ім. Івана Франка, 298 с.

2. Неділько Я. (2018). Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України* № 4. С. 49–60.

3. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України (ВВР)*. 2001. № 25–26. ст.131.

4. Амелін О. (2016). Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. № 3. С.1–6.

5. Копатін О. (2012). Словник термінів з кібербезпеки /О. Копатін, Є. Скулишин. Київ: ВБ "Аванпост-Прим", 214 с.

6. Думчиков М. О. (2022). Кримінально-правова характеристика поняття та видів кіберзлочинів. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. № 55. С. 65–68.

7. Тимошенко В.І. (2019). Десятий Конгрес ООН з попередження злочинності і поводження з правопорушниками. Велика українська юридична енциклопедія: у 20 т. Т. 18: Кримінологія. Кримінально-виконавче право / редкол.: В. І. Шакун (голова), В. І. Тимошенко (заст. голови) та ін.; Нац. акад. прав. наук України; Нац. акад. внутр. справ. С. 110–111.

8. Конвенція про злочинність у сфері комп'ютерної інформації ETS No. 185 (Будапешт, 23 листопада 2001 р.). URL: https://rm.coe.int/1680081580 (Дата звернення: 11.09.2024)

9. Гуцалюк М. (2002). Європейська конвенція з кіберзлочинів / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: *науково-технічний збірник*. Вип. 4. С. 19–23.

10. Грицун О. О. (2014). Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. № 4. С. 312–317.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст. 403.

12. Погорецький М. А. (2012). Кіберзлочини: до визначення поняття. *Вісник прокуратури*. № 8. С. 89–96.

13. Дмитрук М.М. (2017). Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав) Кібербезпека в Україні: правові та організаційні питання: *матеріали Всеукраїнської науково-практичної конференції* (м. Одеса, 17 листопада 2017 р.). Одеса: Одеський державний університет внутрішніх справ, С. 16–18.

14. Карчевский Н.В. (2016). Киберпреступление или преступление в сфере использование информационных технологий? Кібербезпека в Україні: правові та організаційні питання: *матеріали всеукр. наук.-практ. конф*., м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, С. 10–15.

15. Шемчук В. В. (2018). Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки.* Том 29 (68) № 6. С. 119–124.

16. Бельський Ю. А. (2014) Щодо визначення поняття кіберзлочину. *Юридичний вісник*. Вип. № 6. С. 414–418.

17. Privacy and legal issues in cloud computing. Elgar law, technology and society (2015) /ed. by R. H. Weber, A. Cheng. London: Edward Elgar Pub, XIV, 290, 14 p.

18. Schriver R. (2002). You cheated, you lied: the safe harbor agreement and its enforcement by the Federal Trade Commission. *Fordham Law Review*. Vol. 70, iss. 6. P. 2777–2818.

19. Коваленко Є. В. (2019). Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання. Актуальні проблеми управління інформаційною безпекою України: *зб. тез наук. доповідей X Всеукраїнська наук.-практ. конф*., Київ, 4 квітня 2019 року / Нац. акад. СБУ. Київ, С. 57–61.

20. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL:http://www.gurt.org.ua/articles/34602**.** (Дата звернення: 13.09.2024)

21. Савченко А. В. (2012) Кваліфікація кіберзлочинів. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. Київ: Видавничий дім "Скіф", С. 140–210.

22. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (Дата звернення: 13.09.2024)

REFERENCES

1. ***Kiberzlochynnist ta elektronni dokazy*** [Cybercrime and electronic evidence] = Cybercrime and digital evidence (2022): navch. posibnyk /B. M. Holovkin, O. I. Denkovych, V. V. Lutsyk, D. M. Tsekhan]; za red. kand.

yuryd. nauk, dots. Olhy Denkovych, d-r prava, prof. Habriele Shmeltser. Elektron. vyd. Lviv: LNU im. Ivana Franka, 298 p. [In Ukrainian].

2. Nedilko Ya. (2018). ***Poniattia kiberzlochyniv ta yikh vydy*** [The concept of cybercrimes and their types]. Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy No. 4. P. 49–60. [In Ukrainian].

3. ***Kryminalnyi kodeks Ukrainy*** [Criminal Code of Ukraine]. Zakon Ukrainy vid 05.04.2001 No 2341-III. Vidomosti Verkhovnoi Rady Ukrainy (VVR). 2001. No. 25–26. st.131. [In Ukrainian].

4. Amelin O. (2016). ***Vyznachennia kiberzlochyniv u natsionalnomu zakonodavstvi*** [Definition of cybercrime in national legislation]. Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy. No 3. P.1–6. [In Ukrainian].

5. Kopatin O. (2012). ***Slovnyk terminiv z kiberbezpeky*** [Glossary of cyber security terms] / O. Kopatin, Ye. Skulyshyn. Kyiv: VB "Avanpost-Prym", 214 p. [In Ukrainian].

6. Dumchykov M. O. (2022) ***Kryminalno-pravova kharakterystyka poniattia ta vydiv kiberzlochyniv*** [Criminal law characteristics of the concept and types of cybercrimes]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Ser.: Yurysprudentsiia. No. 55. P. 65–68. [In Ukrainian].

7. Tymoshenko V. I. (2019). ***Desiatyi Konhres OON z poperedzhennia zlochynnosti i povodzhennia z pravoporushnykamy*** [Tenth UN Congress on Crime Prevention and Treatment of Offenders]. Velyka ukrainska yurydychna entsyklopediia: u 20 t. T. 18: Kryminolohiia. Kryminalno-vykonavche pravo / redkol.: V. I. Shakun (holova), V. I. Tymoshenko (zast. holovy) ta in.; Nats. akad. prav. nauk Ukrainy; Nats. akad. vnutr. sprav. P. 110–111. [In Ukrainian].

8. ***Konventsiia pro zlochynnist u sferi kompiuternoi informatsii ETS No 185*** [Computer Information Crime Convention ETS No. 185] (Budapesht, 23 lystopada 2001 r.). URL: https://rm.coe.int/1680081580 (Accessed: 11.09.2024) [In Ukrainian].

9. Hutsaliuk M. (2002) ***Yevropeiska konventsiia z kiberzlochyniv /Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini: naukovo-tekhnichnyi zbirnyk*** [European Convention on Cybercrimes / Legal, regulatory and metrological support of the information protection system in Ukraine: scientific and technical collection.]. Vyp. 4. P. 19–23. [In Ukrainian].

10. Hrytsun O. O. (2014). ***Pytannia mizhnarodno-pravovoho rehuliuvannia informatsiinoho teroryzmu. Chasopys Kyivskoho universytetu prava*** [The issue of international legal regulation of information terrorism]. No 4. P. 312-317. [In Ukrainian].

11. ***Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*** [About the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy vid 05.10.2017 No 2163-VIII. Vidomosti Verkhovnoi Rady (VVR), 2017, No 45, st.403. [In Ukrainian].

12. Pohoretskyi M. A. (2012). ***Kiberzlochyny: do vyznachennia poniattia*** [Cybercrime: to the definition of the concept]. Visnyk prokuratury. No. 8. P. 89–96. [In Ukrainian].

13. Dmytruk M.M. (2017). ***Pytannia terminolohii u vyznachenni systemy zlochyniv v sferi IT (dosvid inshykh derzhav) Kiberbezpeka v Ukraini*** [Issues of terminology in defining the system of IT crimes (experience of other countries) Cybersecurity in Ukraine]: pravovi ta orhanizatsiini pytannia: materialy Vseukrainskoi naukovo-praktychnoi konferentsii (m. Odesa, 17 lystopada 2017 r.). Odesa: Odeskyi derzhavnyi universytet vnutrishnikh sprav, P. 16-18. [In Ukrainian].

14. Karchevskyi N.V. (2016) ***Kyberprestuplenye yly prestuplenye v sfere yspolzovanye ynformatsyonnыkh tekhnolohyi*** [Cybersecurity in Ukraine: legal and organizational issues]? Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: materialy vseukr. nauk.-prakt. konf., m. Odesa, 21 zhovtnia 2016 r. Odesa: ODUVS, P. 10–15. [In Ukrainian].

15. Shemchuk V.V. (2018) ***Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini*** [Cybercrime as an obstacle to the development of the information society in Ukraine]. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: yurydychni nauky. Tom 29 (68) No. 6. P. 119–124. [In Ukrainian].

16. Belskyi Yu. A. (2014) ***Shchodo vyznachennia poniattia kiberzlochynu*** [Regarding the definition of cybercrime]. Yurydychnyi visnyk. Vyp. No. 6. P. 414–418. [In Ukrainian].

17. ***Privacy and legal issues in cloud computing***. Elgar law, technology and society (2015) /ed. by R. H. Weber, A. Cheng. London: Edward Elgar Pub, XIV, 290, 14 p. [In English].

18. Schriver R. (2002) ***You cheated, you lied: the safe harbor agreement and its enforcement by the Federal Trade Commission***. *Fordham Law Review*. Vol. 70, iss. 6. P. 2777–2818. [In English].

19. Kovalenko Ye. V. (2019). ***Peredumovy zahroz u sferi informatsiinoi bezpeky ta perspektyvy yikh podolannia*** [Prerequisites of threats in the field of information security and prospects for overcoming them]. Aktualni

problemy upravlinnia informatsiinoiu bezpekoiu Ukrainy: zb. tez nauk. dopovidei Kh Vseukrainska nauk.-prakt. konf., Kyiv, 4 kvitnia 2019 roku / Nats. akad. SBU. Kyiv, P. 57–61. [In Ukrainian].

20. Holub A. ***Kiberzlochynnist u vsikh yii proiavakh: vydy, naslidky ta sposoby borotby*** [Cybercrime in all its manifestations: types, consequences and methods of combat]. Retrieved from: http://www.gurt.org.ua/articles/34602. (Accessed: 13.09.2024) [In Ukrainian].

21. Savchenko A. V. (2012). ***Kvalifikatsiia kiberzlochyniv*** [Qualification of cybercrimes]. Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady: navch. posib. Kyiv: Vydavnychyi dim "Skif", P. 140–210. [In Ukrainian].

22. Dziundziuk V. B. ***Poiava i rozvytok kiberzlochynnosti*** [Emergence and development of cybercrime]. Derzhavne budivnytstvo. 2013. No. 1. Retrieved from: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (Accessed: 13.09.2024) [In Ukrainian].

Дата надходження: 23.09.2024 р.

Roman SHAK
Lviv Polytechnic National University,
Educatinoal and Rasearch Institute of Law,
Psychology and Innovative Education,
Assistant Professor of the International
and Criminal Law Department,
Ph.D. in Law
roman.i.shak@lpnu.ua
ORCID: 0000-0002-6658-4585

CONCEPTS AND TYPES OF CYBER OFFENSES IN CRIMINAL LAW

Abstract. The article is devoted to the study of the concept and classification of cyber offenses in criminal law. The author analyzes different approaches to defining the terms "computer crimes", "cyber crimes", "Internet crime" and others, emphasizing the difference in their application in legal science. Special attention is paid to the positions of scientists regarding the interpretation of cybercrime and its place in the field of criminal law.

The author states that two approaches to understanding cybercrimes have been formed today, narrow and broad. The narrow approach focuses on the protection of information security, while the broad approach covers all types of offenses committed using information and telecommunication technologies. The lack of a unified approach to the definition of cybercrimes has a negative impact on the practice of countering these criminal acts. The author emphasizes the importance of unifying the conceptual apparatus and adapting criminal legislation to new challenges in the field of cyber security.

The article examines international legal acts, in particular the Convention on Cybercrime, which defines five groups of crimes, including crimes against the confidentiality, integrity and availability of computer data, as well as crimes related to content and copyright infringement, as well as national legislation, in particular the Criminal Code of Ukraine and the Law "On Basic Principles of Ensuring Cybersecurity of Ukraine" The analysis of various classifications of cybercrimes proposed by scientists, which cover violations of constitutional rights, property rights, public morality and state security, is carried out.

In conclusion, the author emphasizes the importance of adapting national legal systems to the rapidly changing conditions of the digital age and developing new legal tools to protect against cybercrimes. The main conclusion is the need for a wider recognition and definition of cybercrime in order to effectively understand and counter these criminal acts at the national and international levels.

Key words: cyberspace; cybercrime; computer crimes; cybercrime; the Internet; criminal responsibility.