

УДК 343.985

DOI 10.36919/3041-1149(Print).3.2024.55-62

В. В. Удовенко,
аспірант кафедри права,
Європейський університет
email: law.kafedra@e-u.edu.ua
ORCID ID 0000-0003-3163-982X

ПОНЯТТЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЮЮТЬСЯ В СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ, ТА ЇХ КРИМІНАЛІСТИЧНА КЛАСИФІКАЦІЯ

У статті розглянуто, зіставлено та проаналізовано визначення основних понять, які застосовуються в чинних міжнародно-правових актах, національному законодавстві й наукових джерелах для позначення високотехнологічної злочинності. Обґрунтовано ефективність використання терміна «кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації». Надана класифікація та її мета, які можуть мати як криміналістичне, так і кримінологічне чи кримінально-правове значення.

Метою статті є висвітлення сучасних наукових і законодавчих підходів до визначення поняття кримінальних правопорушень, що вчинюються в сфері комп'ютерної інформації, та формування на підставі цього авторського бачення їх класифікації.

Ключові слова: кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації, кіберзлочин, кіберзлочинність, законодавство, класифікація, види, high-tech crime, cyber crime, network crime.

Постановка проблеми та її актуальність. Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства за будь-яких умов пов'язані з комп'ютерами, комп'ютерними мережами та комп'ютерною інформацією [1, с. 5].

Проте, коли існують нові можливості в суспільстві, вони завжди, безумовно, приносять багато позитивних аспектів, як-от підвищення комфорту, розвиток науки й економіки, поліпшення якості життя тощо. Водночас з цими благами й можливостями з'являються загрози, ризики та негативні наслідки. Зокрема, з'являється кримінальні правопорушення, що вчиняються в сфері комп'ютерної інформації.

Аналіз останніх досліджень і публікацій. Питання кримінальних правопорушень, що вчиняються в сфері комп'ютерної інформації, та їх розслідування розглядали такі вчені, як Дж. Арас, Г. П. Власова, О. Є. Користін, М. Ю. Літвінов, Р. В. Лук'янчук, В. В. Марков, М. А. Ожеван, Ю. М. Онищенко, О. В. Орлов, П. І. Пушкаренко, К. М. Рудой, Є. Д. Скулиш, В. Г. Хахановський та інші.

Метою статті є висвітлення сучасних наукових і законодавчих підходів до визначення поняття кримінальних правопорушень, що вчинюються в сфері комп'ютерної інформації, та формування на підставі цього авторського бачення їх класифікації.

Виклад основного матеріалу дослідження. На початку 60-х років минулого століття, коли були зареєстровані перші злочини, вчинені з використанням електронно-обчислювальних машин, в американській пресі з'явилося поняття «комп'ютерна злочинність». Цей термін використовували в засобах масової інформації, вчені, працівники правоохоронних органів, незважаючи на те, що для цього не було ні криміналістичних, ні правових підстав. Визначення поняття «комп'ютерний злочин» вперше було надане 1983 року в Парижі (Франція) групою експертів Організації економічного співробітництва та розвитку ООН: комп'ютерний злочин – це будь-яке незаконне, неетичне чи недозволене діяння, що стосується автоматизованої обробки чи передачі даних. Відтоді й застосовується поняття кіберзлочину, яке й сьогодні лишається дискусійним і одним із найбільш обговорюваних у правничих колах [2, с. 50].

На доктринальному рівні можна зустріти ряд аналогічних однорідних понять, зокрема: злочини, які вчиняються з використанням електронно-обчислювальної машин (ЕОМ), «комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «кіберзлочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин» тощо. Зарубіжними дослідниками частіше вживаються поняття *high-tech crime*, *cyber crime*, *network crime*, які, відповідно, перекладаються як «злочини у сфері високих технологій», «кіберзлочини», «злочини в комп'ютерних мережах» [3, с. 120].

Термін «комп'ютерний злочин», як вважає О. А. Самойленко, має розширене тлумачення. Ним позначають діяння, в яких комп'ютер є предметом, знаряддям або засобом учинення злочину. Терміносполучення «злочини у сфері комп'ютерної інформації» зумовлено важливістю та значенням об'єкта посягання – комп'ютерної інформації. Водночас, продовжує цей автор, сутність кіберзлочинів або ІТ-злочинів, полягає в тому, що це протиправні суспільно небезпечні діяння, тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача [4, с. 11].

Значного поширення набуває термін «кіберзлочини», коли було підписано державами – членами Ради Європи та іншими державами 2001 року Конвенцію про кіберзлочинність [5]. У наукових джерелах кіберзлочинність є видом транснаціональної злочинної діяльності, що базується на використанні як засобів вчинення злочинів кіберпростору [6, с. 68].

Кіберзлочинність можна вважати об'єднуючим поняттям, що характеризує пов'язані кримінальні дії: кіберзалежні та кіберутворюючі злочини. Кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм (поширення вірусів та інших шкідливих програм, хакерство, зламування серверів для захоплення мережевої інфраструктури або вебсторінок). Такі злочини спрямовані на пошкодження комп'ютерів і джерел мережі, мають наслідки як, наприклад, шахрайство. Кіберутворюючі злочини – це традиційні види злочинів, які стали кіберзлочинами через використання комп'ютерів, комп'ютерних мереж та інших видів комунікації. На відміну від кіберзалежних вони можуть учинятися й без застосування «комп'ютерного елемента» [7].

Водночас, як пише М. Ю Яцишин, у жодному універсальному міжнародно-правовому акті не закріплено визначення кіберзлочинності. До того ж експерти, які входять до групи Усестороннього дослідження проблеми кіберзлочинності та відповідних заходів зі сторони держав-членів міжнародного співтовариства й приватного сектору відповідно до Резолюцій 65/230 і 67/189 Генеральної Асамблеї ООН (UNODOC/CCPCJ/EG.4/2013/2 23.01.2013), наголошують на відсутності потреби у формуванні такого єдиного узагальнювального поняття [8, с. 5].

За таких умов важливим кроком стало укладання країнами регіональних договорів. Аналізуючи їх положення, варто зазначити, що в них використовується різний понятійно-категоріальний апарат, зокрема:

1. Конвенція Ради Європи про кіберзлочинність від 21 листопада 2001 року містить термін «кіберзлочинність» (*cybercrime*), однак його дефініція відсутня. Фактично в документі перелічені окремі види діянь, які логічно потрібно віднести до кіберзлочинності. Також у преамбулі визначається таке: «Ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами й даними...»; «...Конвенція має на меті доповнення цих конвенцій для підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами й даними, та для надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі» [5]. Отже, узагальнивши наведені положення, М. Ю Яцишин стверджує, що кіберзлочин – це кримінальне правопорушення в електронній формі, спрямоване проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами й даними [8, с. 8].

2. Угода про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 1 червня 2001 року визначає «злочин у сфері комп'ютерної інформації» як кримінально каране діяння, предметом посягання якого є комп'ютерна інформація, а саме така інформація, що міститься в пам'яті комп'ютера, на машинних чи інших носіях у формі, доступній сприйняттю ЕОМ (електронно-обчислювальна машина) чи передається каналами зв'язку [9].

3. Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16.06.2009 (набрала чинності з 5 січня 2012 року) містить термін «інформаційна злочинність», що тлумачиться як використання інформаційних ресурсів та/або вплив на них в інформаційному просторі в протиправних цілях [10].

4. Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21 грудня 2010 року застосовує термін «злочини у сфері інформаційних технологій» (information technology offences), визначення якого в тексті договору також відсутнє [11]. Водночас з огляду на контекст статті 2 М. Ю Яцишин вважає, що злочини у сфері інформаційних технологій – це злочини, пов'язані з будь-якими матеріальними чи віртуальними засобами або групами засобів, що використовуються для зберігання, сортування, організації, отримання, обробки, розробки й обміну інформацією відповідно до команд та інструкцій [8, с. 9].

Водночас у вітчизняних нормативно-правових актах, зокрема Законі України від 19 червня 2003 року «Про основи національної безпеки України», використовують терміни «комп'ютерна злочинність», «комп'ютерний тероризм» [12].

Натомість у Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року, вживають термін «кіберзлочини» [13]. У Законі України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність визначається як сукупність кіберзлочинів. А кіберзлочин – як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачено Законом України «Про кримінальну відповідальність» та/або визнано злочином міжнародними договорами України [14].

На нашу думку, правильність використання термінології, зокрема, у науковому дослідженні залежить від контексту та специфіки дослідження. У цьому випадку використання терміна «кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації» є найбільш вдалим, оскільки він узагальнює різноманітні види злочинів, пов'язаних з використанням комп'ютерної технології та інформаційних систем. Термін «кримінальні правопорушення» зазначає суспільно небажану діяльність, яка порушує закони та призводить до кримінальної відповідальності. Додавши «у сфері комп'ютерної інформації», чітко вказує на те, що ці правопорушення відбуваються в контексті використання інформацією за допомогою комп'ютерів та інформаційних технологій. Такий підхід дозволяє охопити широкий спектр діяльності, яка може бути віднесена до кримінальних правопорушень у сфері комп'ютерної інформації, включаючи, але не обмежуючись, кіберзлочини, інциденти безпеки, обман і маніпуляції з інформацією в мережах тощо. Такий термін дозволяє більш точно описати сферу дослідження та зазначити його зв'язок із кримінальними аспектами.

Дослідники, які займаються цією проблемою, пропонують різні класифікації цього виду кримінальних правопорушень. Зокрема, поділяють на види залежно від об'єкта та предмета посягання. Найпоширенішим варіантом є це розподіл на комп'ютерні злочини й злочини, що здійснюються за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв доступу до кіберпростору. Цю класифікацію використовує Організація Об'єднаних Націй, поділяючи цей вид злочинної діяльності на кіберзлочини в «широкому» та «вузькому» розумінні. У цьому контексті комп'ютерні злочини – це злочини, основним об'єктом посягання яких є конфіденційність, цілісність, доступність і безпечне функціонування комп'ютерних даних і систем. Решта кіберзлочинів, крім комп'ютерних систем, зазіхають на інші об'єкти (як основні): безпека суспільства й людини (кібертероризм), майно та майнові права (крадіжки, шахрайства, скоєні за допомогою комп'ютерних систем або в кіберпросторі), авторські права (плагіат і піратство) [15, с. 215].

Класифікація «комп'ютерних злочинів», «злочинів у сфері комп'ютерної інформації» та «інформаційних злочинів» зазвичай здійснювалась за кримінально-правовими ознаками відповідної

групи злочинів. До таких відносять злочини, передбачені Розділом XVI КК України, а також частиною 3 статті 190 КК України (шахрайство, вчинене через незаконні операції з використанням електронно-обчислювальної техніки) та статтею 200 КК України (використання підроблених електронних засобів доступу до банківських рахунків) [4, с. 11].

Згідно з КК України поняття кіберзлочинності охоплює такі кримінальні правопорушення:

- 1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361);
- 2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361¹);
- 3) 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 361²);
- 4) 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);
- 5) 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);
- 6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку за допомогою масового розповсюдження повідомлень електрозв'язку (стаття 363¹) [16].

На відміну від кримінального права в криміналістиці вид кримінального правопорушення класифікують за видом злочинної діяльності, зокрема: 1) коли комп'ютер виступає *засобом* учинення злочину (дії, що кваліфікуються за статтями Розділу XVI КК України); 2) коли комп'ютер є *предметом* посягання (традиційно статті 185, 190, 191 КК України).

Водночас тенденції розвитку суспільних відносин в Україні впродовж останніх років демонструють такі найбільш поширені кіберзлочини: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини [3, с. 121].

Кіберзлочини мають широкий спектр прояву: від крадіжок даних і викрадення грошей до кібершпигунства та кібертероризму. Поряд з виникненням нових видів злочинів у сфері інформаційних технологій існують практично будь-які злочини, як-от привласнення, крадіжка, шахрайства, злочини в банківській сфері, комп'ютерне шпигунство, комп'ютерні диверсії (зокрема, руйнування операційних систем, сповіщень і використання комп'ютерних вірусів), комп'ютерний тероризм, крадіжка комп'ютерних послуг (зокрема, обчислювальних ресурсів), махінації та маніпулювання системою обробки даних, а також крадіжка фінансових засобів і підробка документів, порушення приватної або державної таємниці, протиправне копіювання програмних продуктів, яке порушує авторське та інші права [17, с. 59].

Відповідно до Конвенції про кіберзлочинність прийнято поділяти кіберзлочини на такі види:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем; нелегальне перехоплення інформації; втручання в дані та системи; виготовлення, розповсюдження та збут шкідливого програмного забезпечення й спеціальних пристроїв);
- правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство);
- правопорушення, пов'язані зі змістом (вироблення, володіння, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем);
- правопорушення, пов'язані з порушенням авторських і суміжних прав [5].

Водночас кіберзлочини залежно від наслідків і масштабу можна поділити на дві категорії:

- кіберзлочини публічної дії, спрямовані на ураження комп'ютерних та інформаційно-телекомунікаційних систем державних органів, міжнародних організацій, великих підприємств, державних реєстрів, об'єктів критичної інфраструктури та ін.;

• кіберзлочини індивідуальної дії, спрямовані на заволодіння майном або інформацією певної особи, групи осіб або підприємства [18].

Отже, класифікація може бути здійснена за різними ознаками та підставами. На нашу думку, пропонуємо таку:

1. **За характером вчиненого злочину**, можна виділити такі види кримінальних правопорушень, що вчинюються в сфері комп'ютерної інформації:

- крадіжка даних;
- шахрайство в інтернеті;
- кібербулінг;
- кібертероризм;
- кібершантаж;
- хакерство та комп'ютерний злом [19, с. 98].

2. **За об'єктом посягання:**

- кримінальні правопорушення, пов'язані з комп'ютерами та інтернет-технологіями;
- кримінальні правопорушення, пов'язані з електронною інформацією та даними;
- кримінальні правопорушення, пов'язані з комунікаційними мережами та телекомунікаціями.

3. **За масштабом:**

- кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації масової дії (спрямовані на великі об'єкти, як-от державні системи або великі корпорації);
- індивідуальні кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації (спрямовані на окремих осіб або менші об'єкти).

4. **За метою:**

- кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації з фінансовою метою (наприклад, крадіжка грошей або кредитних карток);
- кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації з політичною або терористичною метою (наприклад, кібертероризм або кібершпигунство в інтересах держави);
- кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації з метою розважального характеру (наприклад, віруси або атаки на ігри та розважальні ресурси).

Висновки. Отже, з огляду на вищенаведене можна зробити висновок, що наданий нами для використання термін «кримінальні правопорушення, що вчинюються в сфері комп'ютерної інформації» є найбільш вдалим, а запропонована класифікація допоможе краще зрозуміти різноманітність кримінальних правопорушень, що вчинюються в цій сфері, та їх характеристики. Ця інформація може бути корисною для подальшого дослідження, а також для правоохоронних органів і законодавців під час удосконалення законодавства та боротьби з ними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Воронцов А. В. Лекція до теми «Кіберзлочинність: її детермінація та запобігання». URL : https://oduvs.edu.ua/wp-content/uploads/2016/09/lek-2016-d-z-3-4-kriminologia_ta_profilakt_zloginiv-10.pdf
2. Неділько Я. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60.
3. Шемчук В. В. Кваліфікаційно-дисциплінарна комісія прокурорів. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки* 2018. Том 29 (68), № 6. С. 119–124.
4. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник. Одеса, 2020. 112 с.
5. Конвенція Ради Європи про кіберзлочинність. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 09.03.2023).
6. Мищенко Д. В., Хомич О. Р. Основні засади протидії кіберзлочинності органами Національної поліції України. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнарод. наук.-практ. конф., м. Харків, 27 травня 2020 р. / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проєктів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 68–71.

7. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications. Home Office Research Report 75. University of Surrey, October, 2013. P. 29.
8. Яцишин М. Ю. Проблеми уніфікації поняття кіберзлочинності у міжнародному праві URL : <https://scholar.google.com/citations?user=C4QmGlcAAAAJ&hl=en>
9. Угода про співробітництво держав-членів Співдружності Незалежних Держав у боротьбі із злочинністю в сфері комп'ютерної інформації від 01 червня 2001 року. URL : http://zakon4.rada.gov.ua/laws/show/997_353
10. Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва 16.06.2009. URL : http://base.spinform.ru/show_doc.fwx?rgn=28340
11. Arab Convention on Combating Information Technology Offences. 21.12.2010. URL : <http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd>
12. Про основи національної безпеки України : Закон України від 19 червня 2003 року № 964-IV. URL : <https://zakon.rada.gov.ua/laws/show/964-15#Text>
13. Стратегія національної безпеки України : Указ Президента України від 26 травня 2015 року № 287/2015. URL : <https://www.president.gov.ua/documents/2872015-19070>
14. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19>
15. Орлов Р. Р., Оніщенко Ю. М. Боротьба з кіберзлочинністю на міжнародному рівні. *Протидія кіберзлочинності та торгівлі людьми* : зб. матеріалів Міжнарод. наук.-практ. конф., м. Харків, 27 травня 2020 р. / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 215–218.
16. Кримінальний кодекс України. URL : <http://zakon3.rada.gov.ua/laws/show/2341-14/page>
17. Ботвінкін О. В. Проблеми забезпечення національної безпеки в інформаційній сфері. *Юридичний журнал*. 2007. № 2 С. 59–60.
18. Кривенко К. Кіберзлочинність: актуальна судова практика. URL : https://biz.ligazakon.net/analitics/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 11.03.2023).
19. Удовенко В. В. Кіберзлочини: загроза для всіх і кожного. *Кібербезпека енергетики* : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, м. Київ, 31 травня 2023 р. Київ, 2023. С. 96–99.

REFERENCES

1. Vorontsov A. V. Lektsiia do temy «Kiberzlochynnist: yii determinatsiia ta zapobihannia». [lecture on the Topic Cybercrime: Its Determination and Prevention]. URL : https://oduvs.edu.ua/wp-content/uploads/2016/09/lek-2016-d-z-3-4-kriminologia_ta_profilakt_zloginiv-10.pdf [in Ukrainian] (2023, April 14).
2. Nedilko Ya. (2018). Poniattia kiberzlochyniv ta yikh vydy [The Concept of Cybercrimes and Their Types]. *Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy*. 2018. № 4. P. 49–60 [in Ukrainian].
3. Shemchuk V. V. (2018). Kvalifikatsiino-dystsyplinarna komisiia prokuroriv Kiberzlochynnist yak pereshkoda rozvytku informatsiinoho suspilstva v Ukraini [Qualification and Disciplinary Commission of Prosecutors: Cybercrime as an Obstacle to the Development of an Information Society in Ukraine]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: yurydychni nauky*. 2018. Tom 29 (68), № 6. P. 119–124 [in Ukrainian].
4. Samoilenko O. A. (2020). Vyiavlennia ta rozsliduvannia kiberzlochyniv [Detection and Investigation of Cybercrime] : navchalno-metodychnyi posibnyk. Odesa, 2020. 112 p. [in Ukrainian].
5. Konventsiiia Rady Yevropy pro kiberzlochynnist [The Council of Europe Convention on Cybercrime]. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian] (2023, April 3).

6. Myshchenko D. V., Khomych O. R. (2020). Osnovni zasady protydyi kiberzlochynnosti orhanamy Natsionalnoi politsii Ukrainy [The Basic Principles of Combating Cybercrime by the National Police of Ukraine]. *Protydiia kiberzlochynnosti ta torhivli liudmy* : zb. materialiv Mizhnarod. nauk.-prakt. konf., m. Kharkiv, 27.05.2020 r. / MVS Ukrainy, Kharkiv. nats. un-t vnutr. sprav ; Koordynator proektiv OBSIe v Ukraini. Kharkiv : KhNUVS, 2020. P. 68–71 [in Ukrainian].
7. Dr. Mike McGuire and Samantha Dowling Cybercrime: a review of the evidence Summary of key findings and implications. Home Office Research Report 75. University of Surrey, October, 2013. 29.
8. Yatsyshyn M. Yu. Problemy unifikatsii poniattia kiberzlochynnist u mizhnarodnomu pravi [The Challenges of Standardizing the Concept of Cybercrime in International Law]. URL : <https://scholar.google.com/citations?user=C4QmGlcAAAAJ&hl=en> [in Ukrainian] (2023, April 3).
9. Uhoda pro spivrobitnytstvo derzhav-chleniv Spivdruzhnosti Nezalezhykh Derzhav u borotbi iz zlochynnistiu v sferi kompiuternoï informatsii [Agreement on Cooperation of Member States of the Commonwealth of Independent States in Combating Computer Information Crime] vid 01.06.2001. URL : http://zakon4.rada.gov.ua/laws/show/997_353 [in Ukrainian] (2023, April 23).
10. Uhoda pro spivrobitnytstvo v sferi zabezpechennia mizhnarodnoi informatsiinoï bezpeky Shankhaiskoi orhanizatsii spivrobitnytstva [Agreement on Cooperation in the Sphere of Ensuring International Information Security of the Shanghai Cooperation Organization] 16.06.2009. URL : http://base.spinform.ru/show_doc.fwx?rgn=28340 [in Ukrainian] (2023, April 23).
11. Arab Convention on Combating Information Technology Offences 21.12.2010. URL : <http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drxx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd> (2023, April 13).
12. Pro osnovy natsionalnoi bezpeky Ukrainy [Basic Principles of National Security of Ukraine] : Zakon Ukrainy vid 19.06.2003 № 964-IV. URL : <https://zakon.rada.gov.ua/laws/show/964-15#Text> [in Ukrainian] (2023, April 3).
13. Stratehiia natsionalnoi bezpeky Ukrainy [National Security Strategy of Ukraine] : Ukaz Prezydenta Ukrainy vid 26.05.2015 № 287/2015. URL : <https://www.president.gov.ua/documents/2872015-19070> [in Ukrainian] (2023, April 3).
14. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Fundamental Principles of Ensuring Cybersecurity in Ukraine] : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2163-19> [in Ukrainian] (2023, April 3).
15. Orlov R. R., Onishchenko Yu. M. (2020). Borotba z eiberzlochynnistiu na mizhnarodnomu rivnii [Combatting Cybercrime at the International Level]. *Protydiia kiberzlochynnosti ta torhivli liudmy* : zb. materialiv Mizhnarod. nauk.-prakt. konf., m. Kharkiv, 27 travnia 2020 r. / MVS Ukrainy, Kharkiv. nats. un-t vnutr. sprav ; Koordynator proektiv OBSIe v Ukraini. Kharkiv : KhNUVS, 2020. P. 215–218 [in Ukrainian].
16. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]. URL : <http://zakon3.rada.gov.ua/laws/show/2341-14/page> [in Ukrainian] (2023, April 3).
17. Botvinkin O. V. (2007). Problemy zabezpechennia natsionalnoi bezpeky v informatsiinii sferi [Issues of Ensuring National Security in the Information Sphere]. *Yurydychnyi zhurnal*. 2007. № 2. P. 59–60 [in Ukrainian].
18. Kryvenko K. (2023). Kiberzlochynnist: aktualna sudova praktyka [Cybercrime: Current Judicial Practices]. URL : https://biz.ligazakon.net/analytics/209283_kberzlochinnst-aktualna-sudova-praktika [in Ukrainian] (2023, April 13).
19. Udovenko V. V. (2023). Kiberzlochyny: zahroza dlia vsikh i kozhnoho [Cybercrimes: a Threat to Everyone]. *Kiberbezpeka enerhetyky* : materialy naukovo-praktychna konferentsiia Instytutu problem modeliuvannia v enerhetytsi im. H. Ie. Pukhova Natsionalnoi akademii nauk Ukrainy, m. Kyiv, 31.05.2023. Kyiv, 2023. P. 96–99 [in Ukrainian].

V. V. Udovenko. THE CONCEPT OF CRIMINAL OFFENSES COMMITTED IN THE FIELD OF COMPUTER INFORMATION AND THEIR CRIMINALISTIC CLASSIFICATION

New opportunities in society invariably bring both positive and negative consequences. While technological advancements enhance our lives, they also give rise to new threats and risks, such as cybercrime.

This article examines, compares, and analyzes the definitions of key terms used in international legal instruments, national legislation, and academic sources to describe high-tech crime. It justifies the effectiveness of using the term «criminal offenses committed in the field of computer information». The article provides a classification and its purpose, which may have both criminalistic and criminological or criminal law significance. Classification can be carried out according to various criteria and grounds, such as the nature of the crime, the object of the encroachment, the scale, and the purpose.

The aim of this article is to highlight modern scientific and legislative approaches to defining the concept of criminal offenses committed in the field of computer information and to form, on this basis, the author's vision of their classification.

The term «criminal offenses committed in the field of computer information» proposed by the author is the most successful, and the proposed classification will help to better understand the variety of criminal offenses committed in this area and their characteristics.

Keywords: *criminal offenses committed in the field of computer information, cybercrimes, cybercrime, legislation, classification, types.*

Стаття надійшла до редакції 20 серпня 2024 року