УДК 343.91/.97:004.056 *DOI: https://doi.org/10.32631/vca.2025.1.66*

Петро Петрович ГАЛУШКО
(Харківський національний університет внутрішніх справ, м. Харків)

КІБЕРЗЛОЧИННІСТЬ: ПОНЯТТЯ ТА СОЦІАЛЬНО-ПРАВОВА ПРИРОДА

Стаття присвячена аналізу співвідношення поняття та правової природи кіберзлочинності у контексті національного законодавства та міжнародного права. Незважаючи на прийняття Закону України «Про основні засади забезпечення кібербезпеки України» у 2017 році, у якому вперше було дано визначення поняття «кіберзлочин», законодавче оформлення відповідальності за діяння у кіберпросторі досі викликає наукові дискусії. Досліджуються положення Будапештської конвенції та національного кримінального законодавства, аналізується питання про те, які правопорушення можна кваліфікувати саме як кіберзлочини. Увага приділяється як спеціальним нормам Кримінального кодексу України (розділ XVI), так і загальним складам, у яких використання комп'ютерних систем має факультативний характер. У статті аргументується теза про те, що кіберзлочинність є специфічною формою реалізації як традиційних злочинів у цифровому середовищі, так і самостійним кримінальним та соціальним феноменом.

Ключові слова: *кіберзлочинність, правова природа, кіберпростір, кіберзлочин, склад кримінального правопорушення, цифрове середовище, Будапештська конвенція, кримінальна відповідальність, комп'ютерні системи, інформаційна безпека, кваліфікація злочинів.*

Постановка проблеми. Проблема визначення правової природи кіберзлочинів, а також їх співвідношення із загальним поняттям кримінального правопорушення вже тривалий час є предметом наукової дискусії в межах кримінального права та кримінології.

У вітчизняній юридичній науці цій темі присвячено праці Р. В. Бараненка, О. М. Кравцової, О. В. Манжая, Д. В. Пашнєва, О. С. Передерія, В. В. Сокуренка, К. О. Черевка та низки інших дослідників, які аналізують понятійний апарат, ознаки кіберзлочинів та їх кримінально-правову кваліфікацію. Суттєвий внесок у формування теоретичних підходів також зробили дослідники інформаційної безпеки та фахівці у сфері міжнародного співробітництва з кіберзлочинністю. На міжнародному рівні ці питання досліджувалися у контексті прийняття Будапештської конвенції Ради Європи «Про кіберзлочинність» (2001 р.), яка заклала концептуальні основи протидії злочинам у цифровому середовищі. Актуальність подальшого аналізу обумовлена постійним зростанням кількості кіберзлочинів і розширенням сфер їх вчинення.

Мета статті – визначити поняття та встановити, описати соціально-

правову природу кіберзлочинності.

Виклад основного матеріалу. Вирішення питання законодавчого закріплення поняття в Україні було зроблене в 2017 році, коли прийняли Закон України «Про основні засади забезпечення кібербезпеки України»[1], у п. 8 ч. 1 ст. 1 якого з'явилося поняття кіберзлочину (комп'ютерного злочину). Під ним законодавцем запропоновано розуміти 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[2]. Втім, попри цілком логічну дефініцію, з неї не випливає жодної специфічної ознаки кіберзлочинів, (окрім, власне, використання для їх вчинення кіберпростору), які б вказували на особливості їх соціально-правової природи.

В нашій державі класичний підхід до визначення цього поняття зостається незмінним. За основу береться Будапештська конвенція[3], в якій немає поняття «кіберзлочину», але є чотири види діянь, які ми можемо вважати такими, що вчинені у сфері комп'ютерної інформації, а в нашому випадку – вважати кіберзлочинами. Так, Конвенція передбачає запровадження кримінальної відповідальності на національному рівні за такі групи злочинів:

– правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями);

– комп'ютерні правопорушення (підробка та шахрайство із застосуванням комп'ютерів);

– правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією);

– правопорушення віднесені до порушення авторських та суміжних прав;

– акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж[4].

Більшість діянь, передбачених у Конвенції, визнаються злочинами і в українському законодавстві. До таких, зокрема, належать: «нелегальне перехоплення» (ст.ст. 163, 361, 362 КК); «втручання в дані» (ст.ст. 361, 362 КК); «втручання в систему» (ст. 361 КК); злочини, пов'язані з дитячою порнографією (ст.ст. 301, 301-1, 301-2 КК); підробка, пов'язана з комп'ютерами (ст.ст. 358, 366 КК); шахрайство, пов'язане з комп'ютерами (ч. 4 ст. 190 КК). Діяння, передбачені Додатковим протоколом до Конвенції, охоплюються ст. 161 КК, яка встановлює відповідальність за порушення

[1] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[2] Там само.

[3] Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.

[4] Там само.

рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії, та загальними нормами Особливої частини КК України, що передбачають злочини проти свободи совісті (ст. ст. 178–181 КК); втручання в систему (ст. 361-1 КК); порушення авторських та суміжних прав (ст.ст. 176-177 КК); зловживання пристроями (ст.ст. 362, 363 КК); розповсюдження інформації з обмеженим доступом (ст. 361-2 КК); перешкоджання роботі ЕОМ, АС, КМ чи МЕ (ст. 363-1 КК), незаконний доступ (ст. 192 КК).

Треба погодитися з О. М. Кравцовою, яка наголосила, що в національному кримінальному законодавстві прямо не передбачено відповідальності за такі дії, як:

1) умисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна отримати доступ до всієї або частини КС з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5 Конвенції;

2) володіння пристроями, включаючи комп'ютерні програми, створені або адаптовані насамперед з метою вчинення будь-якого зі злочинів, перелічених у статтях 2–5 Конвенції, або комп'ютерними паролями, кодами доступу або подібними даними, за допомогою яких можна отримати доступ до всієї або частини КС з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5 Конвенції, з наміром використання зазначених предметів для вчинення будь-якого зі злочинів, перерахованих у статтях 2–5[1].

Попри це, вітчизняне законодавство вже є достатньо адаптованим для протидії кіберзлочинності, навіть якщо їх вчиняють кілька людей разом або якщо готуються до них. Наприклад, якщо хтось навмисно продає або передає іншим комп'ютерні паролі чи коди доступу, щоб останні могли вчинити злочин, це вже вважається пособництвом у вчиненні цього злочину. А якщо хтось здійснює розробку, придбання, збут шкідливого програмного забезпечення чи спеціалізованих пристроїв для його використання з метою вчинення злочину в майбутньому, то, будучи самостійним кримінальним правопорушенням, передбаченим ст. 361-1 КК України, фіксується ідеальна сукупність із готуванням до вчинення іншого злочину з використанням вказаних засобів, пристроїв. Адже, як випливає з міжнародних домовленостей, карати потрібно не просто за те, що людина має шкідливі програми чи коди, а лише тоді, коли доведено, що вона планувала використати їх для скоєння іншого злочину, тобто мала відповідну протиправну мету.

Хоча майже всі кримінальні правопорушення, про які йдеться в Будапештській конвенції про кіберзлочинність, є і в КК України, далеко не завжди відповідні норми КК дозволяють ідентифікувати відповідні склади

[1] Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : дис. ... канд. юрид. наук : 12.00.08 / Харківський національний університет внутрішніх справ. Х., 2015. С. 28.

злочинів з тими, вчинення яких пов'язане з комп'ютерами, комп'ютерними системами. Водночас ч. 4 ст. 190 та ст. 163 КК України вже містять пряму вказівку на комп'ютери, комп'ютерні мережі та інформацію, яка в них зберігається. Тому ці кримінальні правопорушення можна відразу назвати «кіберзлочинами». Але інші кримінальні правопорушення не мають таких прямих згадок і можуть вважатися «кіберзлочинами» лише тому, що про них згадує Конвенція, і лише в тому випадку, якщо вони були вчинені «за допомогою комп'ютерних систем».

Ми вважаємо, що кіберзлочини, насправді не створюють якусь абсолютно нову та окрему сферу відносин між людьми, яка б вимагала окремого розділу в Кримінальному кодексі для їхнього захисту. Самі по собі дії людей в мережі Інтернет не є чимось цінним самі по собі. Натомість, Інтернет – це просто інструмент, який допомагає людям спілкуватися та взаємодіяти в межах вже існуючих відносин, роблячи це простіше або навіть можливим. Тому відносини, які виникають в інтернеті, є скоріше допоміжними. Відповідно, самі кіберзлочини відбуваються, по-перше, в особливому (цифровому) техніко-комунікаційному середовищі Інтернет, а, по-друге, вони використовують технології та програми для впливу на віртуальні аспекти наших звичайних відносин, завдаючи шкоди, яка потім проявляється в реальному світі.

Схожий підхід до розуміння «кіберзлочинності» використовується і в офіційних документах різних відомств. Наприклад, коли визначають, чим саме займається Департамент кіберполіції Національної поліції України, то в першу чергу беруться до уваги кримінальні правопорушення, які пов'язані з використанням комп'ютерів, комп'ютерних мереж та інтернету. Так, до задач кібеорполіції відноситься: реалізація державної політики в сфері протидії кіберзлочинності, завчасне інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів[1]. А вже потім до їхньої компетенції відносять інші кримінальні правопорушення, якщо для їх підготовки, вчинення або приховування використовувалися комп'ютери та Інтернет.

Варто зазначити, що в Будапештській Конвенції «Про кіберзлочинність» використовуються слова, які не завжди точно відповідають термінам в українських законах. Основні поняття, пов'язані з комп'ютерними технологіями та обробкою інформації, пояснюються в Законі України "Про захист інформації в інформаційно-комунікаційних системах"[2]. Згідно з цим законом, термін «комп'ютерна система», який використовується в міжнародній угоді, в Українському законодавстві замінюється на ширше поняття – «інформаційно-комунікаційна система».

[1] Кіберполіція. Офіційний сайт. URL: https://cyberpolice.gov.ua/normatyvno-pravovi-akty-yaki-rehlamentuiut-diialnist-politseiskoi-komisii/

[2] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

Це поняття об'єднує такі терміни, як «інформаційна (автоматизована) система», «комунікаційна система» та «інформаційно-комунікаційна система». Важливо розуміти, що інформаційно-комунікаційні системи складаються з програмного забезпечення та технічних пристроїв.

Так, Д. В. Пашнєв вказав, що термін «комп'ютерні дані» є аналогом терміну «комп'ютерна інформація» – інформація, технологія обробки та обміну якої реалізується в ІТС[1]. За нашим переконанням, комп'ютерна інформація також є елементом ІТС з огляду на такі міркування:

1. Відповідно до Закону, інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Слово «реалізується» використане в теперішньому часі, отже інформація повинна знаходитися в системі, щоб вона була інформаційною.

2. Сама назва «інформаційна (автоматизована) система» припускає, що система містить інформацію.

3. Предметом кіберзлочину вочевидь не може бути ІКС, в якій інформація ще не оброблюється чи не передається (не приймається). Як сукупність технічних засобів вона є предметом лише злочинів проти власності.

4. Одним із обов'язкових елементів ІКС є програмний засіб, тобто програма. Остання ж за положеннями Конвенції відноситься до комп'ютерних даних. Проте, слід погодитися із дослідниками, які відділяють комп'ютерні дані та комп'ютерні програми та вважають, що це складові елементи комп'ютерної інформації[2].

Хочеться наголосити і на тому що відповідно до Резолюції, яка ухвалена Генеральною Асамблеєю ООН 27 листопада 2024 року [за доповіддю Третього комітету (A/79/460, пункт 15)] 79/243, прийнято Звіт щодо протидії використанню інформаційно-комунікаційних технологій у злочинних цілях проти кіберзлочинності. Задачами цього звіту – є надання узагальної інформації для зміцнення міжнародного співробітництва в боротьбі з певними злочинами, вчинюваними з використанням інформаційно-комунікаційних систем, і в обміні доказами в електронній формі, що належать до серйозних злочинів[3]. Є певна схожість з Конвенцією про кіберзлочинність[4], затвердженою державами-членам Ради Європи та іншими державами, що підписали цю угоду. Так, у ст. 1 Резолюції ГА ООН вказано, що інформаційно-комунікаційна система – будь-який пристрій або група з'єднаних чи взаємопов'язаних пристроїв, один або декілька з яких за

[1] Пашнєв Д. В. Основні поняття комп'ютерних технологій у контексті комп'ютерної злочинності. *Кримський юридичний вісник*. 2007. Вип. 1 (1). С. 99.

[2] Пашнєв Д. В. Основні поняття комп'ютерних технологій у контексті комп'ютерної злочинності. *Кримський юридичний вісник*. 2007. Вип. 1 (1). С. 99–100.

[3] Countering the use of information and communications technologies for criminal purposes : Report of the Third Committee / Seventy-ninth session Agenda. Item 108 ; General Assembly 27 November 2024. URL: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

[4] Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.

командою програми здійснює збір, зберігання та автоматичну обробку електронних даних[1]. В Будапештській Конвенції в ст. 1 вказано: «Комп'ютерна система» означає будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних. Це вказую на певну послідовність ідей та напрямів боротьби з кіберзлочинністю. Теж саме продовжується і в інших термінах. Так, відповідно до Звіту щодо кіберзлочинності «електронні дані означають будь-яке представлення фактів, інформації або концепцій у формі, придатній для обробки в інформаційно-комунікаційній системі, включно з відповідною інформаційно-комунікаційній системі, включно з відповідною програму, в результаті дії якої інформаційно-комунікаційна система виконує ту чи іншу функцію система виконує ту чи іншу функцію»[2], що практично відповідає такому поняттю в Будапештській Конвенції: «Комп'ютерні дані означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, об спричинити виконання певної функції комп'ютерною системою»[3]. Так, є певні неточності в назві понять, але смисл залишається той самий.

Застосовуючи ці терміни, якщо ми спробуємо визначити основні ознаки кіберзлочинів, пов'язаних з комп'ютерними технологіями, серед порушень, описаних у Конвенції та її Додатковому протоколі, ми можемо умовно поділити їх на такі категорії:

1. Правопорушення, предметом яких є ІТС чи її елементи:

1.1. Правопорушення, предметом яких є ІТС (незаконний доступ (ст. 2), втручання у систему (ст. 5), шахрайство, пов'язане з комп'ютерами (ст. 8)).

1.2. Правопорушення, предметом яких є комп'ютерна інформація:

1.2.1. Правопорушення, предметом яких є комп'ютерні дані незалежно від змісту (нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), зловживання пристроями (ст. 6), підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8)).

1.2.2. Правопорушення, предметом яких є комп'ютерні дані незаконного змісту (правопорушення, пов'язані з дитячою порнографією (ст. 9), правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10), поширення расистського та ксенофобного матеріалу через комп'ютерні системи (ст. 3 Протоколу), заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства (ст. 6 Протоколу)).

1.2.3. Правопорушення, предметом яких є комп'ютерна програма

[1] Там само.

[2] Countering the use of information and communications technologies for criminal purposes : Report of the Third Committee / Seventy-ninth session Agenda. Item 108 ; General Assembly 27 November 2024. URL: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

[3] Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.

(зловживання пристроями (ст. 6))[1].

2. Правопорушення, засобами яких є елементи ІТС (правопорушення, пов'язані з дитячою порнографією (ст. 9), правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10), погроза чи образа з расистських та ксенофобних мотивів (ст. ст. 4–5 Протоколу))[2].

Слід додати, що в Конвенції при описі деяких правопорушень вказано, що вони вчиняються за допомогою комп'ютерних систем, і за даною ознакою ми виділили тільки одну їх групу, але очевидно, що всі вони вчиняються з використанням комп'ютерної системи (ІКС відповідно до законодавства України) у якості засобу, знаряддя та/або предмету злочину.

Треба погодитися з Р. В. Бараненко, який вказує: «Дослідники розглядають поняття кіберзлочину у двох значеннях: 1) у вузькому сенсі (комп'ютерний злочин) – будь-яке протиправне діяння, вчинене за допомогою електронних операцій, об'єктом посягання якого є безпека комп'ютерних систем і оброблюваних ними даних; 2) у широкому розумінні (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж»[3]. Відповідно до такого підходу до кіберзлочинів слід віднести не тільки ті, ознаки складів яких передбачені статтями 361–363-1 КК України (Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а й ті, що передбачені ст.ст. 161, 176, 177, 178–181, 192, 301, 301-1, 301-2, 358, 366 КК України. Однак, виходячи з диспозицій цих статей КК, використання комп'ютерних систем при вчиненні відповідних кримінальних правопорушень є факультативною, а тому не суттєвою ознакою, яка не може бути покладена в основу визначення їх сутності саме як «кіберзлочинів». Те ж саме, на нашу думку, стосується й ч. 4 ст. 190 КК України – шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Останній є загальнокримінальним корисливим кримінальним правопорушенням. Способи його вчинення – вельми різнорідні (від гіпнозу до використання ЕОМ), але вони не впливають на природу та кримінологічну оцінку цього злочину.

До того ж не варто також мати на увазі і те, що російсько-українська війна вивела феномен кіберзлочинності з ординарного виміру та мілітарний, воєнно-контекстуальний. Кібернетичні атаки на цивільні об'єкти, об'єкти критичної інфраструктури, що за міжнародним гуманітарним правом не можуть бути визнані законною військовою ціллю,

[1] Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.

[2] Там само.

[3] Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2021. Вип. 1 (49). С. 85–90.

є, таким чином, воєнними кіберзлочинами та мають кваліфікуватись за ст. 438 КК України.

Отже, поняття «кіберзлочинність» репрезентоване трьома блоками кримінальних практик:

1) ***ординарні кримінальні правопорушення у сфері використання комп'ютерів систем та комп'ютерних мереж і мереж електрозв'язку*** – передбачені ст. ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України, сконцентровані у Розділі XVI Особливої частини КК «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»;

2) ***ординарні кримінальні правопорушення, що вчиняються з використанням комп'ютерів*** – ст. ст. 161, 176, 177, 178–181, ч. 4 ст. 190, 192, 301, 301-1, 301-2, 358, 366 КК України. І хоча в законах використовується термін «сфера» для опису використання комп'ютерів та інтернету при вчиненні кримінальних правопорушень, для розуміння «кіберзлочинності» важливо усвідомлювати, що суть цих кримінальних правопорушень полягає не просто в якійсь окремій галузі суспільства, а в їхній віртуальній частині, яка перемістилася в кіберпростір. А кіберпростір існує та функціонує лише завдяки цим самим комп'ютерам та мережам;

3) ***воєнно-контекстуальні кіберзлочини***, які представлені двома групами діянь: а) воєнні кіберзлочини (ст. 438 КК України); б) пов'язані з війною кіберзлочини, що посягають на основи національної, громадської безпеки (ст. ст. 114-1, 114-2, 258 КК України).

Висновки. У результаті проведеного дослідження встановлено, що поняття кіберзлочину не є самостійною кримінально-правовою категорією, відокремленою від загального розуміння злочину. Законодавчі визначення, зокрема норма п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», а також положення Будапештської конвенції, окреслюють лише сферу вчинення злочинів – кіберпростір або з використанням комп'ютерних технологій.

У національному законодавстві України відсутнє чітке та вичерпне нормативне розмежування між традиційними злочинами та кіберзлочинами. Частина кримінальних правопорушень, що підпадають під визначення «кіберзлочин», передбачена розділом XVI КК України, тоді як інші охоплюються загальними нормами Особливої частини Кримінального кодексу.

Враховуючи вищевикладене, вважаємо за можливе запропонувати під кіберзлочинністю розуміти соціально-правовий феномен, що проявляється у стійких кримінальних практиках правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, форми прояву яких передбачені законом про кримінальну відповідальність. Цей феномен репрезентований трьома групами кримінальних правопорушень 1) ординарні кримінальні правопорушення у сфері використання комп'ютерів систем та комп'ютерних мереж і мереж електрозв'язку; 2) ординарні

кримінальні правопорушення, що вчиняються з використанням комп'ютерів; 2) воєнно-контекстуальні кіберзлочини. Детальний їх кримінологічний аналіз є перспективним напрямом подальших кримінологічних досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2021. Вип. 1 (49). С. 85–90

2. Кіберполіція. Офіційний сайт. URL: https://cyberpolice.gov.ua/normatyvno-pravovi-akty-yaki-rehlamentuiut-diialnist-politseiskoi-komisii/

3. Конвенція про кіберзлочинність : Міжнародний документ. Конвенція Ради Європи від 23.11.2001 р. URL: http://zakon1.rada.gov.ua/laws/show/994_575.

4. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : дис. ... канд. юрид. наук : 12.00.08 / Харківський національний університет внутрішніх справ. Х., 2015. 216 с.

5. Пашнєв Д. В. Основні поняття комп'ютерних технологій у контексті комп'ютерної злочинності. *Кримський юридичний вісник*. 2007. Вип. 1 (1). С. 98–103.

6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

8. Countering the use of information and communications technologies for criminal purposes : Report of the Third Committee / Seventy-ninth session Agenda. Item 108 ; General Assembly 27 November 2024. URL: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

Стаття надійшла до редакції 10.04.2025

Petro P. HALUSHKO,
Postgraduate Student
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

CYBERCRIME: CONCEPT AND SOCIO-LEGAL NATURE

The article is devoted to the analysis of the content of the concept and the legal nature of cybercrime in the context of national legislation and international law. to stop the adoption of the Law of Ukraine "On Basic Measures to Ensure Cybersecurity of Ukraine" in 2017, which first defined the concept of

"cybercrime", the legislative formulation of liability for actions in cyberspace is still the subject of scientific discussions. The provisions of the Budapest Convention and national criminal legislation are studied, the questions of which offenses can be classified as cybercrimes are analyzed. Attention is paid to both the special norms of the Criminal Code of Ukraine (Chapter XVI) and the general provisions in which the use of computer systems is optional. The article argues that cybercrime is a special form of implementation of both traditional crimes in the digital environment and an independent criminal and social phenomenon.

Keywords: *cybercrime, legal nature, cyberspace, cybercrime, elements of a criminal offense, digital environment, Budapest Convention, criminal liability, computer systems, information security, qualification of criminals.*