УДК 343.31.7:004.056.55
DOI https://doi.org/10.32782/2709-9261-2025-2-14-18

Габорець Ольга Андріївна,
доктор філософії в галузі освіти, доцент,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0001-7791-6795

Пекарський Сергій Петрович,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки факультету № 3
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0003-0538-0391

КІБЕРЗЛОЧИНИ ЯК ОБ'ЄКТ ПРАВОВОЇ КЛАСИФІКАЦІЇ

У статті проведено правовий аналіз кіберзлочинів як об'єкта класифікації в умовах цифровізації суспільства. Акцентовано на нормативній невизначеності, труднощах кваліфікації, особливостях використання електронних доказів і міжвідомчій координації. Запропоновано авторське бачення класифікації кіберзлочинів з урахуванням міжнародних стандартів та національного законодавства.
Ключові слова: *кіберзлочини, класифікація кіберзлочинів, електронні докази, цифрове середовище, кримінальне правопорушення, інформаційні технології, кримінальна відповідальність, кіберпростір, правове регулювання.*

Постановка проблеми. Цифровізація суспільства, глобальна інформатизація та повсюдне використання інформаційно-комунікаційних технологій зумовили трансформацію традиційних форм протиправної поведінки, спричинили виникнення нових видів кримінальних правопорушень, що вчиняються у віртуальному середовищі. Актуальність наукового осмислення феномену кіберзлочинів зумовлена необхідністю уніфікації підходів до їх визначення, систематизації, правової кваліфікації та ефективної протидії. Відсутність у чинному кримінальному законодавстві чіткого переліку кіберзлочинів, розбіжності в термінології, складнощі в доведенні складу злочину на підставі цифрових слідів, а також міжвідомча фрагментарність у боротьбі з кіберзлочинністю створюють суттєві бар'єри для забезпечення ефективного правосуддя. У цьому контексті особливої ваги набуває дослідження кіберзлочинів як об'єкта правової класифікації, що є основою для розроблення стратегії гарантування кібербезпеки та нормативного вдосконалення кримінально-правового регулювання.

Аналіз останніх досліджень та публікацій. Наукове пізнання кіберзлочинності було предметом дослідження таких вітчизняних науковців, як: Н. М. Ахтирська, В. Д. Гавловський, В. О. Голубєв, О. Ю. Довженко, М. В. Карчевський, О. В. Кузьменко, В. Г. Кундеус, М. Ю. Літвінов, О. В. Манжай, В. В. Попко, Є. В. Попко, О. А. Самойленко, В. Г. Хахановський, Д. М. Цехан та інші. Шановними науковцями дискутуються різні погляди, зокрема щодо класифікації кіберзлочинів, особливостей організації діяльності правоохоронних органів щодо протидії даним злочинам, міжнародного досвіду тощо. Однак, на нашу думку, в умовах правового режиму воєнного стану, у зв'язку з використанням новітніх інформаційних технологій і способів учинення кіберзлочинів представниками країни-агресорки, ці питання потребують подальшого дослідження та ретельного вивчення як наукової практично орієнтованої на діяльність різних правоохоронних органів України проблеми. Отже, зазначення кіберзлочинів як об'єкта правової класифікації становить предмет даного дослідження.

Метою статті є формування комплексного науково-правового уявлення про кіберзлочини як об'єкт правової класифікації шляхом аналізу наявних дефініцій, систематизації основних ознак кіберзлочинів, виявлення проблемних аспектів їх нормативного закріплення та обґрунтування авторського підходу до класифікації кримінальних правопорушень, учинених у кіберпросторі або з його використанням, з урахуванням сучасних викликів у сфері цифрової безпеки.

Виклад основного матеріалу. Сучасний етап розвитку людства характеризується глобалізацією інформаційних потоків і віртуалізацією способів комунікації між фізичними і юридичними особами. Водночас варто зауважити, що особи, які вчиняють кримінальні право-

порушення, не залишили поза увагою активне впровадження інформаційно-комунікаційних технологій у сферу суспільних відносин.

Згідно з положеннями ст. 2 Кримінального процесуального кодексу України від 13 квітня 2012 р. № 4651-VI (далі – КПК України), завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод і законних інтересів учасників провадження, а також забезпечення швидкого, повного й неупередженого розслідування і судового розгляду для того, щоб кожна особа, яка вчинила кримінальне правопорушення, була притягнута до відповідальності відповідно до своєї вини, жодна невинувата особа не була обвинувачена чи засуджена, а також щоб не застосовувався необґрунтований процесуальний примус, до кожного учасника провадження було забезпечено належну правову процедуру [1].

У цьому контексті варто зазначити, що для досягнення цілей кримінального провадження, розпочатого за фактом учинення кіберзлочину, правоохоронні органи приділяють значну увагу пошуку, виявленню, фіксації та використанню доказів на стадіях досудового розслідування та судового розгляду. Відповідно до ст. 84 КПК України [1], доказами у кримінальному провадженні є фактичні дані, здобуті в установленому законом порядку, на підставі яких уповноважені суб'єкти (слідчий, прокурор, слідчий суддя, суд) установлюють наявність або відсутність фактів і обставин, що мають значення для провадження та підлягають доказуванню.

Згідно з положеннями Кримінального процесуального кодексу України, процесуальними джерелами доказів визнаються показання, речові докази, документи та висновки експертів. У контексті протидії кіберзлочинам правоохоронні органи приділяють особливу увагу виявленню та фіксації електронних доказів. Водночас у чинному КПК України відсутнє нормативне визначення поняття «електронний доказ». Для встановлення його змістовного наповнення, з урахуванням принципу аналогії права, доцільно звернутися до положень Цивільного процесуального кодексу України від 18 березня 2004 р. № 1618-IV (далі – ЦПК України) [2]. Згідно зі ст. 100 ЦПК України, електронними доказами визнається інформація в електронній (цифровій) формі, що містить відомості про обставини, які мають значення для розгляду справи. До таких доказів належать, зокрема, електронні документи (текстові файли, графічні зображення, плани, фотографії, аудіо- та відеозаписи), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в цифровому форматі.

Відповідно до цього ж положення електронні докази можуть зберігатися на різних носіях – портативних пристроях (зокрема, картах пам'яті, мобільних телефонах), серверах, у системах резервного копіювання та інших місцях збереження цифрової інформації, зокрема й в інтернеті.

Отже, застосування глобальної мережі «Інтернет», сучасних засобів комунікації та інших цифрових технологій стало одним із новітніх способів учинення кримінальних правопорушень. У таких злочинах зазвичай задіяні особи з різним правовим статусом – як ті, що вже мають судимість, так і учасники організованих злочинних угруповань, які за допомогою цифрових інструментів намагаються уникнути безпосереднього контакту з потерпілими та представниками правоохоронних органів. Це суттєво знижує ймовірність їх затримання безпосередньо під час учинення злочину. Такі особи, що є організаторами протиправної діяльності, активно залучають до її реалізації осіб із відповідними спеціальними знаннями у сфері ІТ – для створення вебсайтів, блогів, телеграм-ботів, технічного супроводу онлайн-ресурсів тощо. До цього процесу нерідко залучається й молодь, яка прагне гострих відчуттів або додаткових доходів і втягується у злочинну діяльність. Наприклад, шляхом спілкування з потенційними жертвами в інтернеті, виведення коштів із банківських карток і подальшої передачі цих коштів організаторам шахрайських схем.

Злочинці активно використовують сучасні засоби комунікації, шифровані інтернет-ресурси, псевдоніми, кодові слова та суворо дотримуються заходів конспірації. Вони координують свої дії та здійснюють обмін інформацією через різні телекомунікаційні мережі та мобільні застосунки. Останні, зокрема, забезпечують наскрізне шифрування повідомлень, що дає змогу прочитати їх лише учасникам листування (наприклад, WhatsApp), або містять функцію «секретного чату», у якому повідомлення автоматично видаляються після встановленого користувачем часу, без збереження на серверах (наприклад, Telegram). Такі технічні характеристики суттєво ускладнюють процеси виявлення, документування та розслідування відповідних кримінальних правопорушень.

У зв'язку із цим варто зазначити, що кіберпростір загалом, а також шахрайство як один із найпоширеніших його проявів, стали об'єктами пильної уваги з боку правової науки та правоохоронної практики. Особливої актуальності набуває їх вивчення в контексті гарантування кібербезпеки й ефективної протидії кіберзлочинності. У межах цього дослідження доцільним є аналіз поняття «кіберзлочин», визначення його сутності як окремого виду протиправної поведінки, а також обґрунтування авторського підходу до класифікації таких злочинів.

Практика діяльності правоохоронних органів засвідчує, що одним із найтиповіших кіберзлочинів натепер є шахрайство, учинене з використанням кіберпростору. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 17 серпня 2022 р. № 2163-VIII [3], кіберпростір визначається як середовище (віртуальний простір), що створює умови для комунікації та реалізації суспільних відносин, і формується через функціонування взаємопов'язаних комунікаційних систем і електронних комунікацій із застосуванням мережі «Інтернет» або інших глобальних мереж передачі даних. Поняття «кіберзлочин» («комп'ютерний злочин») охоплює суспільно небезпечне винне діяння, яке вчиняється в кіберпросторі чи за його допомогою і за яке передбачена відповідальність кримінальним законодавством України або міжнародними договорами.

Станом натепер відсутні чітко розроблені нормативні рекомендації чи методичні підходи щодо визначення кримінальних правопорушень, учинених у кіберпросторі, як таких, що мають характер кіберзлочинів. Серед науковців і практиків немає єдності щодо критеріїв віднесення тих чи інших діянь до цієї категорії, що ускладнює вироблення уніфікованої правозастосовної практики. Окрім того, відсутність усталеної класифікації переліку таких злочинів не дозволяє формувати об'єктивну статистику щодо рівня кіберзлочинності. У науковій літературі трапляються різні підходи до визначення поняття «кіберзлочин». Зокрема, одні автори розглядають його як кримінальне правопорушення, механізм підготовки, учинення або приховування якого передбачає використання електронно-обчислювальної техніки, телекомунікаційних систем, комп'ютерних мереж або засобів електрозв'язку. Інші трактують кіберзлочинність як сукупність злочинів, що скоюються в межах кібер-

простору з використанням комп'ютерних технологій або спрямовані безпосередньо проти них.

У науковій літературі існує декілька підходів до визначення понять «кіберзлочин» і «кіберзлочинність». Більшість дослідників пов'язують ці явища з особливим предметом посягання – комп'ютерною технікою, даними або зі способом учинення злочину, який реалізується шляхом використання інформаційно-комунікаційних технологій, або місцем – віртуальним кіберпростором. Отже, кіберзлочинність охоплює широкий спектр кримінальних правопорушень, що створює суттєві труднощі в систематизації та класифікації таких діянь. До них належать, зокрема, злочини з метою отримання незаконної фінансової вигоди, правопорушення, пов'язані з обробкою чи використанням інформації, що зберігається в комп'ютерних системах, а також діяння, які порушують конфіденційність, цілісність або доступність цифрових ресурсів [4].

В узагальненому вигляді кіберзлочинність може бути схарактеризована як сукупність кримінальних діянь, що здійснюються в кіберпросторі або з використанням цифрових технологій, включаючи комп'ютерні системи, мережі й інші засоби доступу до інформаційного середовища, а також злочини, які спрямовані безпосередньо проти цих систем або даних. Характерною рисою таких правопорушень є відсутність фізичного контакту з потерпілими особами (фізичними чи юридичними), а також високий рівень анонімності, швидкість реалізації злочинного задуму та низька вартість технічного забезпечення. Саме ці чинники сприяють підвищеному інтересу з боку злочинців до використання можливостей цифрових технологій.

З урахуванням вищевикладеного можна зробити висновок, що термін «кіберзлочинність» охоплює настільки різнопланові форми протиправної поведінки, що побудова універсальної та водночас ефективної системи їх класифікації є складним завданням. До основних категорій таких злочинів належать: діяння з метою особистого збагачення, неправомірний доступ або маніпулювання інформацією в комп'ютерних системах, а також правопорушення, які загрожують безпеці інформаційної інфраструктури.

Особливістю шахрайських дій, що вчиняються в кіберпросторі, є їхній суто цифровий характер. Це створює нові виклики для правоохоронної діяльності, зокрема ускладнює процес ідентифікації цифрових слідів, їхнього взаємозв'язку та визначення суб'єктів злочинної активності. Відсутність територіальних обмежень у кіберпросторі дозволяє злочинцям діяти з будь-якої точки світу, використовувати інструменти для анонімізації трафіку та шифрування, що ускладнює процедуру досудового розслідування.

Натепер Кримінальний кодекс (далі – КК) України не містить вичерпного переліку складів злочинів, які можна було б однозначно віднести до категорії кіберзлочинів. Відсутній також уніфікований підхід до визначення чітких критеріїв, за якими можна кваліфікувати протиправне діяння як кіберзлочин як у вітчизняному, так і в міжнародному законодавстві.

Попри це, кримінальна відповідальність за кіберзлочини закріплена в низці положень Кримінального кодексу України, зокрема в таких статтях:

– ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин, комп'ютерних мереж, автоматизованих систем або мереж електрозв'язку;

– ст. 361-1 – створення та розповсюдження шкідливого програмного забезпечення чи технічних засобів;

– ст. 361-2 – незаконне розповсюдження інформації з обмеженим доступом, учинене особою, яка має право доступу до неї;

– ст. 363 – порушення правил експлуатації комп'ютерних систем або заходів захисту інформації;

– ст. 363-1 – перешкоджання функціонуванню комп'ютерних систем шляхом масового розповсюдження інформації електрозв'язку.

Окрім того, використання інформаційно-комунікаційних технологій виступає кваліфікуючою ознакою у складі низки інших кримінальних правопорушень. Наприклад, у злочинах, пов'язаних із доведенням особи до самогубства через загрозу розповсюдження інформації; правопорушеннях у сфері моральності; торгівлі людьми; виготовленні та розповсюдженні порнографічних матеріалів; незаконному обігу наркотичних засобів, зброї та боєприпасів тощо.

Окрім статей, безпосередньо спрямованих на протидію злочинам у сфері інформаційної безпеки, кримінальна відповідальність за діяння, що мають ознаки кіберзлочинів, передбачена й у низці інших положень Кримінального кодексу України. Зокрема, у ч. 3 ст. 190 передбачено відповідальність за шахрайство, учинене з використанням електронно-обчислювальної техніки. Аналогічно, у ст. 200 встановлено кримінальну відповідальність за незаконні дії з документами на переказ, платіжними картками, електронними грошима, а також пристроями, призначеними для їх виготовлення.

Окрім того, положення окремих статей КК України, зокрема ст. 163 («Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер») і ст. 176 («Порушення авторського права і суміжних прав»), також фіксують використання комп'ютерів, програмного забезпечення та інших цифрових засобів як інструментів учинення правопорушення.

У цьому контексті можна стверджувати, що ядром поняття «кіберзлочин» є правопорушення, учинені з використанням електронно-обчислювальних машин, комп'ютерних систем, мереж або мереж електрозв'язку. Сукупність таких діянь становить понятійний зміст кіберзлочинності у кримінально-правовій площині. В українській правозастосовній практиці найбільш поширеними залишаються правопорушення, передбачені ст. 361 КК України, що стосуються несанкціонованого втручання в роботу комп'ютерних систем і мереж.

Для побудови обґрунтованої системи класифікації кіберзлочинів як об'єкта правової кваліфікації доцільно враховувати міжнародні нормативні акти. Базовим у цій сфері є Конвенція Ради Європи про кіберзлочинність, ухвалена 23 листопада 2001 р. в м. Будапешті [5], яку Україна ратифікувала Законом від 7 вересня 2005 р. № 2824-IV. Цей документ виступає основоположним для гармонізації підходів до визначення складів кіберзлочинів на міждержавному рівні й у науковій доктрині [6].

Будапештська конвенція класифікує кіберзлочини на чотири основні категорії, до яких згодом Додатковим протоколом було додано ще одну. Ця класифікація є загальновизнаною в міжнародному праві:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних систем і даних (CIA-злочини): несанкціонований доступ до інформаційних систем; незаконне перехоплення даних; втручання в комп'ютерні дані (їх зміна, видалення, блокування); втручання в роботу систем (зокрема, DoS-атаки); обіг програмних засобів або пристроїв, призначених для вчинення таких дій.

2. Злочини, пов'язані з використанням комп'ютерів як інструменту (наприклад, шахрайство чи підробка).

3. Злочини, пов'язані зі змістом інформації, що розповсюджується в кіберпросторі (наприклад, дитяча порнографія).

4. Порушення авторських прав, включаючи незаконне копіювання та поширення цифрових об'єктів.

5. Злочини расистського та ксенофобного характеру, учинені з використанням інформаційних технологій (передбачені Додатковим протоколом до Конвенції).

Окрім цього, дослідники пропонують класифікувати кіберзлочини за функціональною роллю інформаційних технологій у структурі правопорушення:

– злочини, де ІТ-системи є об'єктом посягання (наприклад, знищення, зміна чи блокування інформації);

– злочини, де ІТ-засоби є інструментом досягнення мети (наприклад, шахрайство чи викрадення інформації);

– злочини, де ІТ лише опосередковують протиправну діяльність (наприклад, підроблення документів);

– злочини, у яких ІТ-технології забезпечують організацію злочинної діяльності (наприклад, ведення баз даних незаконного характеру).

Отже, ефективна правова кваліфікація кіберзлочинів потребує не лише глибокого розуміння кримінально-правових норм, а й урахування міжнародних підходів, технічних аспектів учинення діянь і функціонального навантаження інформаційних технологій у структурі правопорушення.

Попри відсутність натепер єдиного загальноприйнятого визначення терміна «кіберзлочин», у середовищі науковців і практиків, а також фахівців у сфері кібербезпеки сформовано досить змістовне розуміння його правової природи, механізмів учинення, а також пов'язаних із ним загроз і ризиків. Це, у свою чергу, створює концептуальне підґрунтя для формування національної системи запобігання та протидії кіберзлочинності як суспільно небезпечному явищу.

З урахуванням практичного досвіду протидії злочинам, учиненим у кіберпросторі або з його використанням, варто зазначити, що до процесів виявлення, документування, розкриття та розслідування кіберзлочинів залучаються представники різних правоохоронних органів України. У зв'язку із цим доцільним видається формування класифікації кіберзлочинів із позиції функціональної відомчої належності, що враховує компетенцію конкретного суб'єкта у сфері розкриття та розслідування таких правопорушень.

Так, у межах покладених на неї повноважень, Служба безпеки України (далі – СБУ) забезпечує реалізацію заходів із контррозвідувального захисту у сфері інформаційної та кібернетичної безпеки держави. До пріоритетних напрямів діяльності СБУ в цьому контексті відносять [7]:

– запобігання, виявлення, припинення та розслідування кримінальних правопорушень, учинених у кіберпросторі, які посягають на мир і безпеку людства;

– здійснення контррозвідувальних і оперативно-розшукових заходів із протидії кібертероризму та кібершпигунству, під якими в чинному законодавстві відповідно розуміються терористична діяльність або шпигунство, що здійснюються в кіберпросторі або з його використанням. Наприклад, залучення спецслужбами РФ української молоді до підривної діяльності через мережу каналів у соцмережах і месенджерах, які закликають до вчинення диверсій і терористичних актів;

– протидія кіберзлочинності, наслідки якої можуть створювати загрозу життєво важливим інтересам держави;

– розслідування інцидентів, пов'язаних із кібератаками на державні електронні інформаційні ресурси й об'єкти критичної інформаційної інфраструктури;

– запобігання, нейтралізація спеціальних інформаційних операцій, спрямованих проти України, зокрема тих, що мають на меті дестабілізацію конституційного ладу, порушення суверенітету, територіальної цілісності або загострення суспільно-політичної та соціально-економічної ситуації в державі.

На тлі повномасштабної збройної агресії Російської Федерації проти України загрози національній безпеці охоплюють не лише фізичний вимір (обстріли, ракетно-дронові атаки на об'єкти критичної інфраструктури), але й цифровий простір. Україна систематично зазнає масштабних кіберзагроз і кібератак, спрямованих на дестабілізацію роботи державних інституцій, об'єктів критичної інфраструктури, банківського сектору, телекомунікацій тощо.

Відповідно до Закону України «Про критичну інфраструктуру» від 16 листопада 2021 р. № 1882-IX, охорона об'єктів критичної інфраструктури включає комплекс режимних, інженерних, інженерно-технічних та інших заходів (за винятком заходів інформаційного та кіберзахисту), які здійснюються суб'єктами національної системи захисту критичної інфраструктури з метою запобігання, недопущення або припинення актів несанкціонованого втручання в діяльність таких об'єктів [8].

У межах функціонального розмежування повноважень, визначення відомчої належності у процесі розкриття та розслідування злочинів дозволяє стверджувати, що підрозділи кримінальної поліції України, здійснюючи оперативно-розшукову діяльність, зокрема шляхом використання відкритих джерел інформації (OSINT), у взаємодії з органами досудового розслідування Національної поліції України (далі – НПУ) забезпечують протидію широкому спектру кримінальних правопорушень, які мають ознаки кіберзлочинів [9].

Зокрема, підрозділи Департаменту карного розшуку НПУ фокусують свою діяльність на виявленні та припиненні злочинів проти життя і здоров'я особи, майнових злочинів, а також кримінальних правопорушень у сфері моральності, які вчиняються із використанням кіберпростору як засобу або середовища реалізації злочинного умислу [10].

Водночас Департамент міграційної поліції НПУ спеціалізується на протидії злочинам, пов'язаним із торгівлею людьми, незаконною міграцією, сексуальною експлуатацією неповнолітніх, що все частіше реалізуються через цифрові платформи, зокрема месенджери, вебресурси та соціальні мережі. Особливої актуальності набули питання функціонування нелегальних схем працевлаштування за кордоном, діяльності фіктивних шлюбних агентств, незаконної трансплантології, секс-бізнесу та розповсюдження порнографічного контенту. Наприклад, у взаємодії з Державною прикордонною службою та Службою безпеки України поліція регулярно викриває канали незаконного переміщення чоловіків через державний кордон [9].

Підрозділи Департаменту боротьби з наркозлочинністю НПУ здійснюють виявлення механізмів незаконного обігу наркотичних засобів, зокрема тих, що реалізуються з використанням сучасних інформаційно-комунікаційних технологій. У своїй діяльності підрозділи дедалі частіше стикаються з випадками поширення наркотиків через анонімні онлайн-майданчики, месенджери, соціальні мережі, спеціалізовані мобільні застосунки та DarkNet-платформи.

Особливу увагу в контексті протидії кіберзлочинності варто приділити діяльності Департаменту кіберполіції НПУ, який виконує функції спеціалізованого органу з виявлення, запобігання, розкриття та розслідування злочинів у сфері використання комп'ютерних технологій. Основні напрями його діяльності включають: реалізацію державної політики у сфері протидії

кіберзлочинності; інформування населення про нові загрози та типові кіберзлочинні схеми; розроблення та впровадження програмних засобів для обліку та систематизації кіберінцидентів; забезпечення міжнародної взаємодії через канали Національної цілодобової мережі контактних пунктів [11].

Отже, функціональна відомча належність у сфері виявлення та розслідування кіберзлочинів засвідчує, що протидія таким є сферою спільної відповідальності низки правоохоронних органів. Окрім традиційних слідів злочинної діяльності, слідчі, оперативні працівники й експерти мають працювати з так званими віртуальними (або цифровими) слідами, що значно ускладнює фіксацію обставин підготовки та вчинення злочину.

Злочини, зокрема шахрайства, які реалізуються суто в цифровому середовищі, не передбачають фізичного контакту між потерпілим і зловмисником, що унеможливлює отримання показань про зовнішність чи інші індивідуальні ознаки злочинців. Використання правопорушниками телекомунікаційних і комп'ютерно-технічних засобів, цифрових платформ і мережі «Інтернет» вимагає від працівників правоохоронних органів володіння сучасними компетентностями, зокрема: навичками роботи з комп'ютерною технікою та спеціалізованим програмним забезпеченням; умінням виявляти, фіксувати, копіювати й аналізувати інформацію з комп'ютерів, смартфонів, цифрових носіїв та інтернет-ресурсів; здатністю працювати з електронними документами, створеними, переданими, збереженими та представленими у візуальній формі; знаннями про процедури автентифікації – електронного процесу підтвердження ідентифікації особи чи інформаційної системи; застосуванням електронної ідентифікації – використання унікальних електронних ідентифікаційних даних для встановлення особи або уповноваженого представника юридичної особи [12].

Отже, станом натепер кіберпростір розглядається не лише як сфера правопорушень, але і як окремий «театр» сучасних гібридних воєн, у якому реалізуються як кіберзлочини, так і державні чи квазідержавні інформаційні операції. Зростає технологічна складність реалізації кіберзагроз, удосконалюються інструменти атак на об'єкти критичної інфраструктури, упроваджуються нові форми цифрового шахрайства, що часто супроводжуються інформаційно-психологічним впливом на потерпілих з метою введення їх в оману або маніпуляції свідомістю.

У цьому контексті Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021, визначає: «Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі» [13].

Висновки. Отже, кіберзлочини виступають об'єктом правової класифікації, а протидія кіберзлочинності є ключовим елементом національної системи забезпечення кіберстійкості, що має стратегічне значення для збереження державного суверенітету, стабільності інформаційного простору та цифрового добробуту громадян.

Список використаних джерел

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 р. № 4651–VI. Дата оновлення: 21 листопада 2024 р. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

2. Цивільний процесуальний кодекс України від 18 березня 2004 р. № 1618-IV. Дата оновлення: 19 жовтня 2024 р. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 17 серпня 2022 р. № 2163-VIII. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України.* 2018. № 2 (19). С. 155–166.

5. Конвенція про кіберзлочинність : міжнародний документ Ради Європи від 23 листопада 2001 р., ETS № 185. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

6. Про ратифікацію Конвенції Ради Європи про кіберзлочинність : Закон України від 7 вересня 2005 р. № 2824-IV. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

7. Захист інформаційного та кіберпростору : вебсайт. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky.

8. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882–IX. Дата оновлення: 21 вересня 2024 р. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

9. Структура та функції органів (підрозділів) Національної поліції України. *Сайт Національної поліції України*. URL: https://www.npu.gov.ua/pro-policiyu/struktura-nacionalnoyi-policiyi.

10. Кіберполіція України. *Офіційний сайт кіберполіції Національної поліції України*. URL: https://cyberpolice.gov.ua/.

11. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-IV. Дата оновлення: 31 грудня 2023 р. *Вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

12. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII. Дата оновлення: 15 листопада 2024 р. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2155-19#n3.

13. Стратегія кібербезпеки України, затв. Указом Президента України від 26 серпня 2021 р. № 447/2021. *Вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

References

1. Kryminalnyi protsesualnyi kodeks Ukrainy: vid 13 kvitnia 2012 r. № 4651–VI [Criminal Procedure Code of Ukraine from April 13, 2012, № 4651-VI]. (2024, November 21). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

2. Tsyvilnyi protsesualnyi kodeks Ukrainy: vid 18 bereznia 2004 r. № 1618–IV [Civil Procedure Code of Ukraine from March 18, 2004, № 1618-IV]. (2024, October 19). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/1618-15#Text [in Ukrainian].

3. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vid 17 serpnia 2022 r. № 2163-VIII [Law of Ukraine "On Basic Principles of Ensuring Cybersecurity of Ukraine" from August 17, 2022, № 2163–VIII]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

4. Kravtsova, M. O. (2018). Suchasnyi stan i napriamy protydii kiberzlochynnosti v Ukraini [Current state and directions of combating cybercrime in Ukraine]. *Visnyk kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine*, 2 (19), 155–166 [in Ukrainian].

5. Konventsiia pro kiberzlochynnist: mizhnarodnyi dokument Rady Yevropy vid 23 lystopada 2001 r., ETS № 185 [Convention on Cybercrime: Council of Europe International Document of November 23, 2001, ETS № 185]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

6. Zakon Ukrainy "Pro ratyfikatsiiu Konventsii Rady Yevropy pro kiberzlochynnist" vid 7 veresnia 2005 r. № 2824-IV [Law of Ukraine "On Ratification of the Council of Europe Convention on Cybercrime" from September 7, 2005, № 2824–IV]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2824-15#Text [in Ukrainian].

7. Zakhyst informatsiinoho ta kiberprostoru [Information and cyberspace protection] [website]. Retrieved from https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky [in Ukrainian].

8. Zakon Ukrainy "Pro krytychnu infrastrukturu" vid 16 lystopada 2021 r. № 1882-IX [Law of Ukraine "On Critical Infrastructure" from November 16, 2021, № 1882-IX]. (2024, September 21). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/1882-20#Text [in Ukrainian].

9. Struktura ta funktsii orhaniv (pidrozdiliv) Natsionalnoi politsii Ukrainy [Structure and functions of the National Police of Ukraine divisions] [website]. (n.d.). National Police of Ukraine. Retrieved from https://www.npu.gov.ua/pro-policiyu/struktura-nacionalnoyi-policiyi [in Ukrainian].

10. Kiberpolitsiia Ukrainy [Cyberpolice of Ukraine] [website]. (n.d.). Cyberpolice.gov.ua. Retrieved from https://cyberpolice.gov.ua/ [in Ukrainian].

11. Zakon Ukrainy "Pro elektronni dokumenty ta elektronnyi dokumentoobih" vid 22 travnia 2003 r. № 851-IV [Law of Ukraine "On Electronic Documents and Electronic Document Flow" from May 22, 2003, № 851-IV]. (2023, December 31). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/851-15#Text [in Ukrainian].

12. Zakon Ukrainy "Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy" vid 5 zhovtnia 2017 r. № 2155–VIII [Law of Ukraine "On Electronic Identification and Electronic Trust Services" from October 5, 2017, № 2155–VIII]. (2024, November 15). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19#n3 [in Ukrainian].

13. Stratehiia kiberbezpeky Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021 [Cybersecurity Strategy of Ukraine, approved by Presidential Decree of August 26, 2021, № 447/2021]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

Haborets Olha,
PhD in Educational and Pedagogical Sciences, Associate Professor,
Associate Professor at the Department of Operational and Investigative Activities and Information Security,
Faculty No. 3
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0001-7791-6795

Pekarskyi Serhii,
Candidate of Law, Associate Professor,
Associate Professor at the Department of Operational and Investigative Activities and Information Security,
Faculty No. 3
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0001-7791-6795

CYBERCRIMES AS AN OBJECT OF LEGAL CLASSIFICATION

The article provides a comprehensive analysis of cybercrimes as an object of legal classification in the context of the transformation of legal relations driven by global digitalization and the growing level of criminal activity in cyberspace. The study examines key theoretical and legal approaches to the definition of "cybercrime" and "cybercriminality" and highlights the lack of a unified classification in national legislation, along with inconsistencies in academic discourse. Particular attention is paid to the normative uncertainty regarding the legal qualification of offenses committed using information and communication technologies. The article explores the procedural peculiarities of handling electronic evidence during pre-trial investigation and the challenges associated with its admissibility and reliability. Based on the provisions of the Budapest Convention on Cybercrime and Ukrainian criminal law, the author proposes a systematization of cybercrimes according to the nature of harm, method of commission, technological complexity, and subject composition. The study emphasizes the importance of delineating the functional jurisdiction of law enforcement agencies engaged in combating cybercrime, including the Security Service of Ukraine and various structural units of the National Police, in particular the Cyber Police Department. The author argues for the need to establish an integrated interagency mechanism for information sharing and cooperation. The paper underlines that the digital nature of modern crimes, their high level of anonymity, cross-border character, and use of encrypted communication channels create significant challenges for criminal justice systems. This necessitates the advancement of digital forensic tools and the training of qualified professionals. The article concludes by substantiating the necessity of a coherent conceptual framework for the legal classification of cybercrimes as a prerequisite for effective criminal-legal response to threats in the digital environment.

Key words: *cybercrimes, classification of cybercrimes, electronic evidence, digital environment, criminal offense, information technology, criminal liability, cyberspace, legal regulation, functional jurisdiction.*