Петренчук Аліна Андріївна,
здобувач ступеня вищої освіти
бакалавра навчально-наукового
інституту поліцейської діяльності
Національної академії
внутрішніх справ
Науковий керівник:
Поштаренко Інна Валеріївна,
доцент кафедри кримінального права
Національної академії внутрішніх
справ, доктор філософії в галузі права

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

У сучасних умовах розвитку інформаційного суспільства та стрімкої цифровізації суспільних відносин особливої актуальності набуває проблема кіберзлочинності. Активне впровадження інформаційно-комунікаційних технологій у всі сфери життєдіяльності зумовлює не лише позитивні зміни, а й появу нових форм злочинної діяльності, що здійснюються у кіберпросторі або з використанням комп'ютерних систем [1]. Кіберзлочини можуть виявлятися як у формі традиційних злочинів, вчинених із використанням інформаційних технологій, так і у вигляді самостійних посягань на інформаційні системи та дані [2].

Особливої уваги в контексті кримінально-правової характеристики кіберзлочинності заслуговують норми Кримінального кодексу України, що передбачають відповідальність за відповідні правопорушення. Зокрема, значна частина кіберзлочинів на практиці кваліфікується за ст. 190 КК України (шахрайство), коли протиправне заволодіння майном здійснюється шляхом обману або зловживання довірою з використанням інформаційних технологій. Водночас спеціальною нормою, спрямованою на охорону інформаційної безпеки, є ст. 361 КК України, яка передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У сучасних умовах, зокрема в період воєнного стану, кіберпростір використовується як інструмент впливу на державні інституції, економіку та суспільну безпеку, що ще більше підвищує суспільну небезпечність таких правопорушень [4]. У зв'язку з цим постає необхідність комплексного дослідження кримінально-правової

характеристики кіберзлочинності, з урахуванням як загальних норм кримінального права, так і спеціальних складів злочинів у сфері використання комп'ютерних технологій. Актуальність теми зумовлена потребою вдосконалення кримінального законодавства, а також підвищення ефективності кваліфікації та протидії кіберзлочинам у правозастосовній практиці.

Кіберзлочини у власному розумінні – це ті, які неможливо вчинити без використання інформаційних (комп'ютерних) систем. Вони включають вияви кримінально протиправної поведінки, що спрямовані проти інформаційних (комп'ютерних) систем або проти об'єктів чи предметів, що існують, зберігаються, передаються, обробляються у цих системах. Прикладами можуть бути злом комп'ютерних мереж, викрадення даних, несанкціонований доступ до інформації та саботаж комп'ютерних систем. Кіберзлочини можна класифікувати за кількома основними категоріями: 1) крадіжка даних: незаконне отримання особистої, фінансової або іншої конфіденційної інформації; 2) фінансові махінації: шахрайські дії, що передбачають використання кібертехнологій для незаконного отримання коштів або майна; 3) хакерські атаки: несанкціонований доступ до інформаційних систем з метою їх пошкодження, зламу або викрадення даних; 4) поширення шкідливого програмного забезпечення: створення та поширення вірусів, троянських програм; 5) кібертероризм: використання кібертехнологій для здійснення терористичних актів або загроз.

Можна виокремити кілька основних інноваційних підходів до розслідування кіберзлочинів. По-перше, важливу роль відіграє використання штучного інтелекту та машинного навчання, що дозволяє автоматизувати аналіз великих обсягів даних і своєчасно виявляти підозрілу активність та аномалії в мережах. По-друге, ключовим елементом є цифрова криміналістика, яка охоплює методи збору, збереження та аналізу цифрових доказів, зокрема відновлення видалених даних і дослідження мобільних пристроїв. По-третє, ефективність розслідування залежить від рівня підготовки фахівців, що зумовлює необхідність спеціалізованого навчання та постійного підвищення кваліфікації. По-четверте, важливим є налагодження взаємодії між державними органами та приватним сектором, що сприяє об'єднанню ресурсів і технологій у протидії кіберзлочинності. По-п'яте, значення має міжнародна співпраця та уніфікація правових стандартів, що забезпечує ефективний обмін інформацією та координацію дій у розслідуванні кіберзлочинів [5].

У сучасній правозастосовній практиці однією з ключових проблем є правильна кваліфікація кібершахрайства, зокрема розмежування застосування ст. 190 та ст. 361 КК України. Це зумовлено

тим, що значна частина кіберзлочинів має комплексний характер і поєднує ознаки як посягань на власність, так і втручання в роботу інформаційних систем. Одними з найбільш поширених способів вчинення кібершахрайства є фішинг та скімінг. Фішинг передбачає заволодіння конфіденційними даними користувачів (логінами, паролями, банківськими реквізитами) шляхом обману або створення фальшивих ресурсів, що імітують офіційні сервіси. За даними фахівців з кібербезпеки, саме фішинг залишається основним способом початкового доступу до даних і використовується приблизно у 60% кібератак. Скімінг, своєю чергою, полягає у незаконному зчитуванні інформації з платіжних карток за допомогою спеціальних технічних пристроїв або програмних засобів. Обидва способи спрямовані на подальше незаконне заволодіння грошовими коштами потерпілих [6].

Відповідно до положень кримінального законодавства, за ст. 190 КК України кваліфікуються дії, пов'язані із заволодінням чужим майном шляхом обману або зловживання довірою, у тому числі із використанням електронно-обчислювальної техніки. У свою чергу, ст. 361 КК України передбачає відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, мереж або електрозв'язку [7]. При кваліфікації кіберзлочинів вирішальним є визначення безпосереднього об'єкта посягання: якщо основною метою є заволодіння майном, застосовується ст. 190 КК України, натомість у випадку втручання в роботу інформаційних систем – ст. 361 КК України. Водночас у практиці можливе поєднання цих складів злочину, що зумовлює необхідність їх кваліфікації за сукупністю [6].

Водночас організаційними викликами є нестача кадрів, що виявляється у дефіциті кваліфікованих фахівців з кібербезпеки; необхідність ефективної координації між різними правоохоронними органами й організаціями; необхідність залучення значних фінансових ресурсів, що існує в умовах обмеженості бюджетів, що виділяються на розслідування кіберзлочинів [5]. Зрештою, критично важливо забезпечити захист приватності, що ґрунтується на балансі між повагою до прав людини та ефективним розслідуванням кіберзлочинів.

Отже, кіберзлочинність є складним і динамічним соціально-правовим явищем, яке вирізняється високим рівнем латентності, транснаціональністю та постійною еволюцією способів вчинення кримінальних правопорушень. В умовах стрімкої цифровізації суспільних відносин та активного використання інформаційно-комунікаційних технологій кіберзлочини становлять істотну загрозу як для приватних осіб, так і для функціонування держави загалом. Ефективна протидія кіберзлочинності потребує не лише належного

нормативно-правового регулювання, а й подальшого вдосконалення практики кваліфікації таких правопорушень, розвитку цифрової криміналістики та посилення міжвідомчої й міжнародної співпраці в цій сфері.

Список використаних джерел

1. Бабанін С. В. Кіберзлочинність: поняття та основні ознаки. *Вісник кримінального права.* 2019. URL: https://vakp.nlu.edu.ua/article/view/173523
2. Галушко О. М. Теоретико-правовий аналіз понять кіберзлочину та кіберзлочинності. *Підприємництво, господарство і право.* 2020. URL: https://pb.univd.edu.ua/index.php/PB/article/view/131
3. Русецький С. О. Кіберзлочинність: поняття та соціально-правова природа. 2025. URL: https://vca.univd.edu.ua/index.php/vca/uk/article/view/516
4. Аніщук Н. В. Історико-правові аспекти розвитку кіберзлочинності. 2023. URL: https://journal-app.uzhnu.edu.ua/article/view/277954
5. Ларченко М. В. Особливості розслідування кіберзлочинів. 2022. URL: https://journals.lvduvs.lviv.ua/index.php/law/article/view/910
6. Жевелєва І. С. Кримінально-правова кваліфікація правопорушень у сфері використання електронно-обчислювальних машин, автоматизованих систем та комп'ютерних мереж. 2025. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/343949
7. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III (зі змін. та доп.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

Шубін Дмитрій Сергійович,
тимчасово виконуючий обов'язки
помічника командира військової
частини з правової роботи
(військова частина 5287,
Збройні Сили України)

ІНФОРМАЦІЙНА СТІЙКІСТЬ ДЕРЖАВИ ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

У XXI столітті інформація перетворилася на ключовий стратегічний ресурс, що визначає рівень національної безпеки держави. В умовах гібридної війни кіберпростір стає повноцінним театром бойових дій, де поряд із традиційними загрозами виникають нові форми впливу – інформаційно-психологічні операції, кібератаки та маніпуляції суспільною свідомістю.