Ткаченко К., здобувач
Науковий керівник: Ситніченко О.М.,
к.ю.н., доцент кафедри правового забезпечення безпеки бізнесу,
ЗВО "Державний торговельно-економічний університет",

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ ТА СУЧАСНІ ВИКЛИКИ

Сьогодні впровадження інформаційних технологій у всі сфери життя, розвиток електронного уряду, банківських систем стали буденністю. Але через швидкий темп їх розвитку, атаки на об'єкти критичної інфраструктури, витоки персональних даних, фішингові схеми та триваюча російська збройна агресія проти України спричинили значне зростання кількості кіберзлочинів, що становлять реальну загрозу національній безпеці України. Саме тому питання кримінальної відповідальності за такі діяння є надзвичайно актуальним [1,2].

Правовою основою кримінальної відповідальності за кіберзлочини в Україні є розділ XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». До нього входять такі статті: стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, стаття 362. Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах, стаття 363. Порушення правил експлуатації електронно-обчислювальних машин та стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин, систем та комп'ютерних мереж шляхом масового розповсюдження повідомлень електрозв'язку [3].

Важливе значення має правильне розмежування кіберзлочинів та інших кримінальних правопорушень, які вчиняються з використанням цифрових технологій. Не кожне правопорушення, пов'язане з Інтернетом, автоматично належить до складів кримінальних правопорушень, передбачених розділом XVI КК України. Наприклад, онлайн-шахрайство, незаконне збирання персональних даних, порушення авторських прав у цифровому середовищі або поширення певної інформації можуть потребувати правової оцінки за іншими положеннями кримінального законодавства залежно від фактичних обставин. Для правильної кваліфікації необхідно встановити об'єкт посягання, характер діяння, спосіб його вчинення, наслідки, форму вини та інші ознаки відповідного складу кримінального правопорушення. [3].

Також зазначимо, що кримінальне законодавство встановлює підвищену відповідальність за несанкціоноване втручання в роботу інформаційних систем, вчинене в умовах воєнного стану (ч. 5 ст. 361 ККУ), покарання у такому випадку - позбавлення волі на строк від 10 до 15 років [3].

Показовим прикладом небезпечності кіберзагроз стала масштабна кібератака на оператора мобільного зв'язку «Київстар» у грудні 2023 року. Унаслідок інциденту було порушено роботу мобільного зв'язку та окремих пов'язаних із ним сервісів, що продемонструвало залежність повсякденного життя громадян і функціонування підприємств від стабільності електронних комунікацій. 12 грудня 2023 року Служба безпеки України повідомила про відкриття кримінального провадження за вісьмома статтями КК України. Серед основних напрямів розслідування були несанкціоноване втручання в роботу інформаційних систем та перевірка можливої причетності російських спецслужб до організації атаки. Цей випадок засвідчив, що кіберінциденти можуть мати масштабні соціальні й економічні наслідки, а їх розслідування потребує комплексного аналізу технічних даних, цифрових слідів та обставин діяльності ймовірних причетних осіб [4].

Важливим міжнародно-правовим інструментом протидії кіберзлочинності є Конвенція Ради Європи про кіберзлочинність, відома як Будапештська конвенція 2001 року, яку Україна ратифікувала у 2005 році [5].

Цей документ визначив основні категорії кіберзлочинів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав. Саме на основі положень Конвенції було здійснено подальше впровадження й уточнення складів кримінальних правопорушень у чинному ККУ [3,5].

Окремої уваги потребують правові аспекти використання криптоактивів у кіберзлочинній діяльності. Цифрові активи можуть використовуватися для отримання неправомірних доходів, переміщення коштів між різними юрисдикціями та приховування фінансових потоків. Водночас саме по собі використання криптоактивів не є ознакою кримінального правопорушення. Визначальне значення мають походження активів, спосіб проведення операцій, мета відповідних дій та їхній зв'язок із конкретним протиправним діянням. Для ефективного розслідування таких випадків необхідні спеціальні знання з блокчейн-аналітики, фінансового моніторингу та міжнародного обміну інформацією.

Отже, кримінальна відповідальність за кіберзлочинність в Україні є важливим правовим механізмом захисту інформаційних систем, комп'ютерних даних та інформаційної безпеки держави. Щоб підвищити протидію таким кримінальним правопорушенням і зміцнити кібербезпеку в Україні, необхідно покращити адаптацію до технологічних змін, розширити співпрацю з міжнародними партнерами та збільшити рівень цифрової грамотності населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення 11.10.2026)
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. *Офіційний вісник Президента України*. 2021. № 21. Ст. 855. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 11.10.2026)
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws (дата звернення 11.10.2026)
4. СБУ відкрила справу за фактом кібератаки на «Київстар»: одна з версій – причетність РФ. *Інститут масової інформації*. 2023. 12 грудня. URL: https://imi.org.ua/news/sbu-vidkryla-spravu-za-faktom-kiberataky-na-kyyivstar (дата звернення 11.10.2026)
5. Конвенція про кіберзлочинність: Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 № ETS N 185. URL: https://zakon.rada.gov.ua/laws (дата звернення 11.10.2026)

Трубій Є.С., здобувач
Науковий керівник: Корнієнко О.О.,
к.ю.н., доцент кафедри права, публічного управління та адміністрування
Державний університет «Житомирська політехніка»

ПРАВОВА ПОЛІТИКА УКРАЇНИ У СФЕРІ ГРОМАДЯНСТВА: ІСТОРИЧНИЙ РОЗВИТОК, МНОЖИННЕ ГРОМАДЯНСТВО ТА СУЧАСНІ БЕЗПЕКОВІ ВИКЛИКИ

Громадянство є важливою складовою правового становища людини, оскільки визначає її правовий зв'язок із державою, взаємні права й обов'язки та право на державний захист. Тому політика у сфері громадянства має забезпечувати дотримання прав людини й національних інтересів України.

В умовах повномасштабної війни та міграції питання громадянства набуло особливої актуальності, адже багато українців перебувають за кордоном і набувають або планують набути громадянство інших держав. Це потребує дослідження принципу єдиного громадянства, закріпленого у статті 4 Конституції України [1, ст.4].