УДК 004.056

Н.В. Соловйов
Л.О. Майданевич

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ: СУТНІСТЬ ТА ОСОБЛИВОСТІ

Вінницький національний технічний університет

Анотація.
У дослідженні розкрито сутність кримінальної відповідальності за кіберзлочини з урахуванням міжнародних та національних правових підходів. Проаналізовано класифікацію кіберзлочинів, визначену в Конвенції про кіберзлочинність. Розглянуто законодавче визначення кіберзлочину в національному законодавстві. Визначено особливості предмету доказування у справах щодо розслідування кіберзлочинів. Обґрунтовано, що кримінально-правові механізми є ключовим елементом державної політики в боротьбі з кіберзлочинністю.
Ключові слова: кіберпростір, кібербезпека, кіберзлочинність, кримінальна відповідальність, цифрові докази.

Abstract.
The study reveals the essence of criminal liability for cybercrimes, taking into account international and national legal approaches. The classification of cybercrimes defined in the Convention on Cybercrime is analyzed. The legislative definition of cybercrime in national legislation is considered. The features of the subject of evidence in cases of investigation of cybercrimes are determined. It is substantiated that criminal legal mechanisms are a key element of state policy in the fight against cybercrime.
Keywords: cyberspace, cybersecurity, cybercrime, criminal liability, digital evidence.

Вступ

Стрімка цифровізація суспільства, розвиток інформаційно-комунікаційних технологій та зростання залежності держави, бізнесу й громадян від цифрової інфраструктури зумовили появу нових форм протиправної діяльності в кіберпросторі. Насамперед, зазнають втручання комп'ютерні дані. Відповідно до Конвенції про кіберзлочинність: комп'ютерні дані – це 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, щоб забезпечити виконання певної функції комп'ютерною системою [1].

Відтак, кіберзлочини стали одним з найбільш динамічних та суспільно небезпечних видів правопорушень, оскільки посягають на конфіденційність, цілісність та доступність інформації, стабільність функціонування інформаційних систем та безпеку цифрових сервісів. У таких умовах особливої уваги набуває формування ефективного механізму кримінально-правового реагування на кіберзагрози.

Для фахівців спеціальності 125 «Кібербезпека та захист інформації» розуміння кримінально-правових механізмів протидії кіберзлочинності є необхідною складовою професійної підготовки (насамперед, це сприяє поєднання технічних аспектів захисту інформації з правовими інструментами забезпечення кібербезпеки).

Результати дослідження

В Конвенції про кіберзлочинність [1] обумовлено такі групи кіберзлочинів: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4) втручання у систему (ст. 5), зловживання пристроями (ст. 6)); 2) правопорушення пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами (статті 7, 8)); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією (ст. 9) тощо); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10).

Згідно пункту 8 частини першої статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» «кіберзлочин (комп'ютерний злочин) – 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].

Коло обставин, що підлягають доказуванню за комп'ютерними злочинами, залежить від виду вчиненого кіберзлочину. Суттєвою особливістю предмета доказування є відмінність складових його елементів не лише в межах категорії злочинів, але й за кожною конкретною кримінальною справою. Загальне коло обставин, що належать до предмета доказування, міститься в законі. Встановити в законодавчому порядку точний і вичерпний перелік обставин, які підлягають доказуванню, абсолютно неможливо. Він обумовлений багатьма особливостями в межах кожного конкретного діяння. Нині в Кримінальному кодексі України [3] передбачено ряд злочинів, які вчиняються в кіберпросторі (відомості про найпоширеніші із них наведено в Розділі XVI).

Кримінальна відповідальність за кіберзлочини є ключовим інструментом державної політики у сфері забезпечення кібербезпеки. Тут можна говорити про поєднання правових, організаційних та технічних заходів протидії кіберзлочинності. Її сутність полягає у встановленні кримінально-правових заборон на суспільно небезпечні діяння у кіберпросторі та застосуванні санкцій до осіб, винних у їх вчиненні.

Водночас, варто зауважити, що специфіка кіберзлочинів має транснаціональний характер (що ускладнює їх розслідування через унікальність кіберпростору та особливостей збирання цифрових доказів).

Висновки

Кіберзлочинність є складним багатовимірним явищем сучасного цифрового суспільства. Їх правове визначення сформовано на національному та міжнародному рівнях. Міжнародні стандарти класифікації закріплено в Конвенції про кіберзлочинність. Вона визначає основні групи протиправних дінь в кіберпросторі. Українське законодавство узгоджується з цими підходами. Поняття кіберзлочину офіційно закріплено в профільному законі. Кримінальний кодекс України встановлює відповідальність за найбільш поширені кіберзлочини. Предмет доказування у таких справах має специфічний характер. Він залежить від виду правопорушення та конкретних обставин. Універсального переліку доказових обставин не існує. Кожне провадження потребує індивідуального підходу. Особливу роль відіграють цифрові докази. Кримінальна відповідальність є ключовим інструментом протидії кіберзлочинності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конвенція про кіберзлочинність : від 23.11.2001р. / Верховна Рада України. Офіційний вісник України від 10.09.2007. №65, стор.107. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 02.03.2026).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII . Відомості ВРУ від 10.11.2017. 2017 р. № 45, стор. 42, стаття 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 02.03.2026)
3. Кримінальний кодекс України : Закон України, 05.04.2001. № 2341-III. Голос України від 19.06.2001. №107. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 02.03.2026).

Соловйов Назарій Валерійович – студент 3 курсу групи 2БС-23б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: nazarsoloviоff@gmail.com.

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Soloviov Nazarii – student of group 2BS-23b, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vdemcenko234@gmail.com

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com