Новицька О.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА СУЧАСНОМУ СУСПІЛЬСТВУ

Конституція України гарантує кожній особі право на таємницю листування та захист персональних даних [5]. Однак стрімка цифровізація суспільного життя створила принципово нове середовище для вчинення злочинів. Кіберзлочинність перетворилась на одну з найбільш динамічних загроз сучасності: за оцінками Cybersecurity Ventures, глобальні щорічні збитки від кіберзлочинів у 2024 році перевищили 9 трильйонів доларів США і продовжують зростати [1]. Транснаціональний характер цих загроз унеможливлює ефективну протидію силами однієї держави і вимагає скоординованих зусиль на міжнародному рівні.

Кіберзлочинність охоплює широке коло протиправних діянь: несанкціонований доступ до комп'ютерних систем, розповсюдження шкідливого програмного забезпечення, кібершахрайство, крадіжку персональних даних, кібербулінг та атаки на об'єкти критичної інфраструктури. Особливу небезпеку становлять атаки програм-вимагачів (ransomware), кількість яких у 2023 році зросла на 37% порівняно з попереднім роком, а також використання зловмисниками інструментів генеративного штучного інтелекту для автоматизації атак і створення переконливих фішингових повідомлень [1]. В умовах повномасштабного збройного вторгнення рф кіберпростір став для України повноцінним театром бойових дій. Агентство ЄС з кібербезпеки (ENISA) у щорічному звіті за 2024 рік зафіксувало масштабні атаки проти вітчизняної енергетичної інфраструктури, державних реєстрів і фінансового сектору та констатувало, що Україна залишається однією з найбільш атакованих країн світу [2].

Правові засади протидії кіберзлочинності в Україні закріплені в розділі XVI Кримінального кодексу («Злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку») і Законі «Про основні засади забезпечення кібербезпеки України» 2017 року. Водночас дослідники вказують на системні недоліки чинного регулювання: диспозиції статей КК не охоплюють низку нових форм кіберзлочинів, процедури збирання цифрових доказів потребують уніфікації, а санкції є недостатньо суворими для ефективного превентивного впливу. Зокрема, Чубань В. С. та Пасічник А. В. наголошують на необхідності гармонізації вітчизняного

кримінального законодавства з acquis ЄС у сфері кіберзлочинності як обов'язкової умови євроінтеграції [6].

На міжнародному рівні ключовим інструментом залишається Будапештська конвенція про кіберзлочинність 2001 року, ратифікована Україною у 2005 році. У 2023 році Генеральна Асамблея ООН ухвалила резолюцію про розробку нового глобального договору щодо кіберзлочинності, а в ЄС набула чинності Директива NIS2 із підвищеними вимогами до захисту критичної інфраструктури [2]. Разом з тим правова невизначеність щодо атак із застосуванням штучного інтелекту залишається невирішеною: технічна та правова неготовність більшості держав до ШІ-кіберзагроз становить системний ризик для інформаційного суверенітету [6].

Економіко-правові засади розвитку кіберзлочинності свідчать про те, що фінансова мотивація залишається головним рушієм зростання кількості кібератак, а недосконалість санкційної політики держави створює сприятливе середовище для розширення злочинного кіберринку [4, с. 27–28].

Окремої уваги заслуговує проблема відповідальності за кіберзлочини, вчинені організованими злочинними угрупованнями та державними акторами. Атрибуція кібератак — встановлення конкретного виконавця — залишається одним із найскладніших технічних і правових завдань. Зловмисники систематично використовують анонімізуючі мережі, підставні сервери та скомпрометовані пристрої третіх осіб для приховування слідів. У відповідь провідні держави розробляють доктрини кіберстримування та формують спеціалізовані підрозділи кіберрозвідки. США, Велика Британія та ЄС запровадили механізми публічної атрибуції кібератак і санкційні режими проти держав-спонсорів кіберзлочинності [2]. Міжнародний кримінальний суд у 2023 році підтвердив свою юрисдикцію щодо кіберзлочинів, що є важливим кроком до подолання безкарності на глобальному рівні.

Не менш актуальною є проблема захисту вразливих категорій населення в цифровому просторі. Кібербулінг, онлайн-шахрайство та сексуальні злочини проти неповнолітніх у мережі Інтернет набули масштабів, що вимагають спеціального правового регулювання. Згідно з офіційним звітом Департаменту кіберполіції, у 2023 році було виявлено понад 3,6 тисячі кіберзлочинів, повідомлено про підозру 1,7 тисячі осіб, а кількість звернень громадян сягнула 78,5 тисячі [3]. Це свідчить про необхідність не лише кримінально-правових, а й превентивних заходів: обов'язкового впровадження цифрової грамотності в освітні програми, посилення технічних стандартів безпеки для онлайн-платформ та розширення повноважень регуляторів у сфері захисту персональних даних.

Етико-правові аспекти впровадження систем штучного інтелекту у сфері кібербезпеки актуалізують проблему балансування між технологічним прогресом та фундаментальними правами людини,

зокрема правом на захист персональних даних і правом на приватність, що вимагає вироблення чітких правових меж застосування ШІ-інструментів як у злочинній діяльності, так і у протидії їй [7, с. 44–45].

Кіберзлочинність є однією з найгостріших загроз сучасному суспільству, що охоплює правову, технічну та соціальну сфери одночасно. В умовах цифровізації та геополітичної нестабільності ця проблема набуває для України особливого значення. Ефективна відповідь на неї потребує синхронного розвитку кримінального законодавства, міжнародної співпраці, технічних засобів захисту та цифрової освіти громадян. Лише комплексний підхід здатен забезпечити надійний захист прав особи і держави в цифрову епоху.

Список використаних джерел

1. Cybersecurity Ventures. Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. 2024. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
2. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
3. Звіт про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році. Департамент кіберполіції. 2024. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/
4. Колесніков А. П., Зяйлик М. Ф. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства*. 2017. №1. С. 26-29.
5. Конституція України від 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр
6. Чубань В. С., Пасічник А. В. Кримінальна відповідальність за кіберзлочини в Україні: проблеми та шляхи вдосконалення. Юридичний науковий електронний журнал. 2023. № 4. С. 312–316. URL: https://www.lsej.org.ua/4_2023/74.pdf
7. Чудик Н.О. Етико-правові аспекти впровадження систем штучного інтелекту: балансування технологічного прогресу та фундаментальних прав людини в умовах цифрової трансформації суспільства. *Актуальні проблеми правознавства*. 2024. № 3. С. 42-47