УДК 343.97:343.9.01:343.3/.7
DOI https://doi.org/10.24144/2307-3322.2023.78.2.23

НОРМАТИВНО-ПРАВОВЕ ЗАКРІПЛЕННЯ ЗАСТОСУВАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ СУСПІЛЬСТВА

Бенескул А.В.,
аспірант Державного податкового університету
ORCID ID: https://orcid.org/0009-0004-5315-3374
e-mail: Beneskula@gmail.com

Бенескул А.В. Нормативно-правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства.

У статті досліджено напрями застосування цифрових технологій у різних сферах життєдіяльності громадянського суспільства та держави в межах забезпечення кримінологічної безпеки держави. Проаналізовано окремі нормативно-правові акти, які містять у собі норми, щодо необхідності використання різноманітних цифрових технологій та їх значення у розвитку правової держави. Автором відмічено необхідність не лише створення правової бази застосування цифрових технологій, а також значення розроблення системи дієвих заходів щодо ефективної протидії правопорушенням, що вчиняються з використанням цифрових технологій. Звернено увагу на проблематиці відсутності достатніх правових основ, пов'язаних з розумінням цифрової злочинності, що потребує детального вивчення та чіткої нормативної регламентації. Також, у статті проведено комплексне дослідження сфери використання цифрових технологій, а також окреслено напрями вирішення кримінологічних завдань, які передбачають визначення «кримінальних правопорушень, що вчиняються з використанням цифрових технологій» та пошуку нових форм і засобів боротьби з ними.

Досліджується взаємозв'язок використання цифрових технологій та забезпечення різних видів безпеки, а саме: інформаційної, економічної, національної, кримінологічної, кібербезпеки тощо. Крім цього, аналізується сучасний стан кримінальної ситуації, що складається у цій сфері та зазначаються соціально-економічні фактори, які пов'язані з розвитком цифрових технологій, що активно використовуються злочинцями як механізм у своїй злочинній діяльності. А саме, автором наголошується, що правопорушення, які вчиняються з використанням цифрових технологій, практично приховані від зовнішнього фактору, відбуваються дистанційно, що відповідно, дозволяє злочинцям бути (в іншому населеному пункті або навіть за кордоном) на значній відстані від об'єкта злочинного посягання, що досить утруднює процес їх виявлення, притягнення винних осіб до кримінальної відповідальності, що й актуалізує вказаний напрям наукового дослідження. Також, наведені конкретні пропозиції щодо вдосконалення кримінального законодавства у досліджуваній сфері.

Ключові слова: кримінологічна безпека, цифрові технології, цифровізація, кримінальні правопорушення, кіберправопорушення, кіберзлочинність, цифрова злочинність.

Beneskul A. Regulatory and legal consolidation of the application of digital technologies to ensure the criminology security of society.

The article examines the directions of application of digital technologies in various spheres of life of civil society and the state within the framework of ensuring criminological security of the state. Separate legal acts containing norms regarding the necessity of using various digital technologies and their significance in the development of the rule of law have been analyzed. The author noted the need not only to create a legal basis for the use of digital technologies, but also the importance of developing a system of effective measures to effectively combat crimes committed with the use of digital technologies. Attention is drawn to the problem of the lack of sufficient legal bases related to the understanding of digital crime, which requires detailed study and clear regulatory regulation. Also, the article carries out a comprehensive study of the field of use of digital technologies, as well as outlines directions for solving criminological tasks, which involve

the definition of «criminal offenses committed with the use of digital technologies» and the search for new forms and means of combating them.

The relationship between the use of digital technologies and the provision of various types of security, namely: informational, economic, national, criminological, cyber security, etc., is investigated. In addition, the current state of the criminal situation in this area is analyzed and socio-economic factors associated with the development of digital technologies, which are actively used by criminals as a mechanism in their criminal activities, are noted. Namely, the author emphasizes that crimes committed with the use of digital technologies are practically hidden from external factors, occur remotely, which, accordingly, allows criminals to be (in another locality or even abroad) at a considerable distance from the object of the criminal offense, which considerably complicates the process of their detection, bringing guilty persons to criminal responsibility, which actualizes the indicated direction of scientific research. Also, specific proposals for improving criminal legislation in the researched area are given.

Key words: criminological security, digital technologies, digitalization, criminal offenses, cybercrime, cybercrime, digital crime.

Постановка проблеми. У сучасних умовах інтеграція цифровізації у всі сфери життєдіяльності як держави так і громадянського суспільства не завжди дозволяє своєчасно реагувати на трансформацію цифрових технологій і їх вплив на всі сфери, що забезпечують діяльність громадян, суспільства і в цілому самої держави. Це, у свою чергу впливає і на якість дієвих механізмів створення та формування правового регулювання сфери використання цифрових технологій, що загалом знижує рівень економічної взаємодії між суб'єктами різного рівня і як наслідок призводить до криміналізації цифрової сфери. Враховуючи не лише стрімкий розвиток сфери цифрових технологій, але й її криміналізацію, то очевидно є необхідність вжиття заходів щодо запобігання глобалізації криміналізації даної сфери. Адже, широкий, швидкий та інтенсивний розвиток платформ цифрових послуг, а також розповсюдження новітніх цифрових технологій, таких як зокрема штучний інтелект, впливають на всі сфери нашого громадянського суспільства. Багато нових способів спілкування та доступу до інформації в Інтернеті увійшли в наше повсякденне життя і постійно розвиваються.

Аналіз останніх досліджень і публікацій. Окремі аспекти цього наукового напряму розглядали у своїх фундаментальних працях такі науковці, як: П.Д. Біленчук, В.М. Бутузов, С.В. Демедюк, В.В. Марков, О.В. Орлов, В.С. Цимбалюк та інші. Проте, враховуючи, стрімкий розвиток інформатизації та цифровізації різноманітних сфер громадянського суспільства, значне їх поширення у правову сферу, а також значне використання у кримінально-правовій і кримінологічній політиці, то їх дослідження є актуальним, необхідним та перспективним.

Метою статті є аналіз нормативно-правових актів щодо законодавчого закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та пропозиції на основі цього, змін до кримінального законодавства України щодо належного та чіткого урегулювання кримінальної відповідальності за правопорушення у сфері використання цифрових технологій.

Виклад основного матеріалу. На сучасному етапі життя громадян суспільства та держави загалом неможливо уявити без комп'ютерної інформації, що забезпечує функціонування в галузі управління фінансами, медицини, освіти (дистанційне навчання), а також політики, безпеки держави тощо. Повномасштабне вторгнення росії на територію України, попередні умови пандемії COVID тільки посилили інтеграцію криміналізації цифрової сфери, що забезпечує життєдіяльність громадян, суспільства і держави в цілому, в тому числі негативно позначилися на організаційній, економічній, культурно-моральній, морально-психологічній, інформаційно-телекомунікаційній сфері, що вимагає від держави пошуку економічно необхідної, точно вивіреної моделі ресурсного (правового, організаційного, соціально-економічного, культурного, морального тощо) та іншого забезпечення реалізації кримінологічної політики у сучасних реаліях.

Вирішення такої проблеми стає пріоритетним для нашої держави, у тому числі шляхом пошуку та вирішення кримінологічних завдань, які передбачають визначення «кримінальних правопорушень, що вчиняються з використанням цифрових технологій» та нових форм і засобів боротьби з ними. Потрібно звернути окрему увагу, на необхідності не лише створення правової бази цифрових технологій, а також розробити систему дієвих заходів щодо ефективної протидії правопорушенням, що вчиняються з використанням цифрових технологій. Проблема відсутності достатніх правових основ, пов'язаних з розумінням цифрової злочинності потребує детального вивчення та нормативної регламентації.

Розслідування майже всіх видів кримінальних правопорушень має цифрову складову. За оцінками, існує близько 700 мільйонів нових зразків злочинного програмного забезпечення – найчастішого засобів сприяння кібератакам. Річні витрати світової економіки від кіберзлочинності в 2020 році оцінюються в 5,5 трильйона євро, що вдвічі більше, ніж у 2015 році. Для прикладу, в результаті одного великого злочинного інциденту, кібератаки програм-вимагачів WannaCry у 2017 році, світова економіка втратила понад 6,5 мільярдів євро [2].

Крім того, на сучасному етапі, значно зросла активність користувачів ресурсами мережі «Інтернет», кількість здійснення транзакцій за допомогою цифрових технологій, що не залишилося і поза увагою й злочинців. Останнім часом, все більше уваги приділяється питанням, що стосуються правопорушень, вчинених з використанням цифрових технологій, а також цифрових активів, виробляються різноманітні форми, засоби боротьби з цим явищем. Інтеграція цифрових технологій у кожну із сфер юридичної діяльності: правотворчу, правозастосовну, правоохоронну, окрім цього у діяльність щодо тлумачення права однозначно має свої переваги, адже відкриває широкі можливості. Проте, з швидким розвитком інформаційних технологій в Україні, який активно відбувається останнім часом, набуває динаміки і злочинність у цій сфері, що свідчить про те, що кожен прогрес чи розвиток, який несе для суспільства певні новітні можливості, цивілізаційні блага, досить часто супроводжується і протиправними, негативними явищами. Так само, це стосується і стрімкого розвитку цифрових технологій, масової комп'ютеризації, цифровізації, які однозначно спростили життя, адже полегшили досить велику кількість процесів, які раніше відбувалися з використанням робочої сили, але й понесли за собою виникнення протиправних діянь та зловживань. Враховуючи особливість та складність сфери цифрових технологій, діяльність правоохоронних органів вимагає особливої уваги та підходу до виконання завдань із захисту прав та свобод особи, суспільства і держави від посягань у цифровій сфері, зокрема від кримінальних правопорушень, які вчиняються з використанням цифрових технологій.

Цифрові технології та їх застосування і використання в громадянському суспільстві і державі набувають широкого розповсюдження, зокрема й ту правозастосовній практиці, що обумовлює актуальність досліджуваної теми та проблематики, особливо з погляду забезпечення належного рівня кримінологічної безпеки у суспільстві. Так, зокрема, необхідно дослідити дефініції понять «кримінальні правопорушення у сфері цифрових технологій», «злочинність у сфері цифрових технологій» та загалом поняття «кіберзлочинність» і «цифрова злочинність». Дослідивши та проаналізувавши окремі національні нормативно-правові акти, необхідно зазначити, що в основному у нас використовують наступні поняття: «інформаційні технології», «інформаційно-комунікаційні технології», «інформаційно-комп'ютерні технології», «електронно-обчислювальні машини» (комп'ютери), «інформаційні системи та комп'ютерні мережі», проте зміст термінів потребує чіткого розмежування для їх правильного використання та застосування.

Так, поняття «цифрова технологія» має нормативно закріплене визначення на законодавчому рівні. Відповідно до п. 24 і п. 25 ч. 1 ст. 1 Національної програми інформатизації, «цифрова технологія – це сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій», а «цифровізація – процес впровадження цифрових технологій у всі сфери суспільного життя» [9].

Як бачимо, цифрові технології є широким збірним поняттям, які в свою чергу включають і комп'ютерні, і електронні, і інформаційно-комунікаційні та інші засоби та технології. Тому, доцільно, цей термін використовувати і кримінально-правових і кримінальних процесуальних нормативних актах, адже сфера його застосування доволі широка.

Так, Закон України «Про авторське право і суміжні права» фактично ототожнює поняття «цифрової» та «електронної» інформації і надає наступне визначення: цифровий контент (електронна (цифрова) інформація) – будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет [8]. Тобто, можна визначити, що під «цифровою технологією» мається на увазі електронний спосіб передачі, зберігання, обробки та здійснення інших дій з інформацією.

Окрім цього, Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки передбачає теж використання цифрових технологій. Зокрема: підтримку процесів

цифрової трансформації діяльності інститутів громадянського суспільства з метою сприяння підвищенню ефективності їх діяльності; навчання та надання консультаційної підтримки інститутам громадянського суспільства щодо впровадження та використання в їх діяльності цифрових технологій та інструментів електронної демократії [6].

Стратегія кібербезпеки України конкретно вказує на необхідності того, що країна повинна мати змогу забезпечити свій соціально-економічний розвиток у цифровому світі, і це в свою чергу вимагає досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі і набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі [11]. Проаналізувавши норми Концепції розвитку електронного урядування в Україні, які передбачають, що повсякденне життя громадян стає дедалі все більш «цифровим». Так вона містить положення щодо розвитку сучасних електронних форм взаємодії, прозорості та відкритості діяльності, залучення громадян до прийняття управлінських рішень. Окрім цього, відмічається, що реалізація вказаної Концепції здійснюється за одним із основних принципів, який має назву «цифровий за замовчуванням» [4].

У Стратегії розвитку інформаційного суспільства в Україні було зазначено, що цифрові технології давно стали потужною рушійною силою соціального та економічного розвитку. Окрім цього, Стратегія передбачала, що для прискореного впровадження інформаційних і комунікаційних технологій, створення на їх основі нових методів, ресурсів, інструментів, технологій необхідно прискорити розвиток національної системи цифрової науково-технічної інформації, забезпечивши при цьому створення цифрових ресурсів та електронних баз даних наукової та науково-технічної інформації та забезпечити доступ до іноземних цифрових ресурсів і електронних світових баз даних наукової та науково-технічної інформації [12].

Стратегія інформаційної безпеки визначає стратегічні цілі та завдання, спрямовані на протидію загрозам національній безпеці України в інформаційній сфері, захист прав осіб на інформацію та захист персональних даних, а також передбачає, що в умовах стрімкого розвитку цифрових технологій, але недостатнього рівня медіаграмотності (медіакультури), відбувається значне розширення джерел доступу до інформації, проте воно супроводжується зменшенням критичності сприйняття інформації, що сприяє зростанню впливу дезінформації та деструктивної пропаганди та створює підґрунтя для можливих маніпуляцій громадською думкою [13].Саме тому, Стратегія й вказує основні напрямами, стратегічні цілі і завдання для забезпечення інформаційної безпеки України, серед яких в першу чергу відмічені стійкість та взаємодія.

Для їх втілення та реалізації був затверджений План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, відповідно до якого передбачені стратегічні цілі, завдання і строки їх виконання. Так, зокрема однією із стратегічних цілей, поряд з іншими, є саме розвиток інформаційного суспільства та запобігання інформаційним загрозам в цифровому полі [7].

Таким чином, як бачимо досить широке законодавче застосування сфери цифрових технологій у сучасному громадянському суспільстві. Так, ЄС також приділяє увагу навчанню громадян щодо використання цифрових технологій.

План дій із цифрової освіти (2021–2027) – це оновлена політична ініціатива ЄС, спрямована на підтримку стійкої та ефективної адаптації освітніх і навчальних систем держав-членів ЄС до епохи цифрових технологій. Для досягнення цих цілей план дій визначає два пріоритетні напрямки: сприяння розвитку високоефективної екосистеми цифрової освіти та підвищення цифрових навичок і компетенцій для цифрової трансформації [1]. Як бачимо, сфера цифрових технологій досить активно поширюється та трансформується в громадянське суспільство, тому однозначно необхідно на це звертати увагу та своєчасно реагувати в нормативно-правовому та законодавчому полі.

Тобто, цифрові технології – це електронні інструменти, пристрої та ресурси , які обробляють генерують або зберігають дані. Відомі приклади: соціальні мережі, ігри, мультимедіа, планшети та мобільні телефони тощо [3].

Таким чином, до кримінальних правопорушень, вчинених з використанням цифрових технологій, можна віднести, протиправні дії, що здійснюються в цифровій сфері за допомогою різноманітних технічних засобів, телефонних пристроїв (смартфонів, айфонів, цифрових телевізорів, планшетів та іншої гаджетоподібної техніки). У зв'язку з цим очевидно, що роль цифрових технологій зростає, а механізм їх проникнення у всі галузі життєдіяльності громадян, суспільства, держави загалом продовжує удосконалюватись та видозмінюватися.

Проаналізувавши, норми КК України, жодна із статей не містить саме поняття цифрових технологій, хоча в реальності вони вчиняються з їх використанням, що однозначно потребує внесення змін до

КК України [5]. Самі поняття, такі як: «кіберправопорушення», «кіберпростір» та «кіберзлочинність» наведені у Законі України «Про основні засади забезпечення кібербезпеки України» [10].

Незважаючи на суспільну небезпеку вказаних злочинних дій, в теорії та практиці відсутнє єдине їх визначення, що відображає відсутність нормативних визначень таких термінологічних понять, як: «цифрова злочинність», «злочини, вчинені з використанням цифрових технологій» або «злочини, вчинені у цифровій сфері». Небезпека кримінальних правопорушень у цій сфері, вчинених за допомогою цифрових технологій у телекомунікаційних мережах, обумовлена не тільки кількістю вчинених протиправних дій, а й правопорушеннями, пов'язаними з результатами зазіхань на об'єкти, такі як інформація, майно (шляхом розкрадання), зокрема державні важливі об'єкти (економіку, оборону, безпеку тощо).

Так, КК України, оперує поняттям інформації, яка міститься в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних системах, електронних комунікаційних мережах.

Комп'ютерна інформація, будучи елементом, що відноситься до механізму цифрової сфери, одночасно виступає системою, що акумулює в собі та наповнюється змістом постійних процесів виникнення, формування, видозміни різних баз даних, інформаційних банків та інших сховищ, у яких поряд з іншими відомостями даних концентрується необхідна інформація.

«Цифрове середовище» та «цифрові технології» широко увійшли у життєдіяльність суспільства та держави загалом, стали основою багатьох процесів та застосовуються не тільки в електротехнічній галузі або комп'ютерних гаджетах, але також при розробці, виробництві робототехніки, телекомунікаційних та інформаційних мереж, штучного інтелекту тощо. Усе це стає одним з найважливіших елементів цифрового середовища, компонентами якого є не тільки «телекомунікаційні та інтернет-лінії (оптоволоконні кабелі тощо), але й комп'ютерна інформація; обчислювальні комплекси різної розмірності від потужних комп'ютерів до смартфонів та планшетів чи телефонів.

На сучасному етапі розвитку цифрової сфери розширюються можливості телекомунікаційного зв'язку через мережу «Інтернет» та комп'ютеризації, спрямованої на забезпечення комунікаційного механізму різних форм взаємодії людей, організацій та установ, у тому числі з органами державної влади. У мережі «Інтернет» та межах інформаційного простору відбувається як отримання важливої, необхідної інформації, так і обмін нею між користувачами. Дані потоки утворюють обробку величезного обсягу комп'ютерної інформації у вигляді телекомунікаційного зв'язку. Згодом необхідна інформація формується до баз різного призначення (особиста, що належить окремим користувачам, організаціям, юридичним та фізичним особам), що, безумовно, необхідно як для соціально-економічного забезпечення, а також забезпечення безпеки держави.

Враховуючи кримінальну ситуацію, пов'язану з поширенням цифровізації злочинних дій з боку осіб, які мають спеціальні знання у сфері цифрових технологій, необхідно відзначити той факт, що на сучасному етапі немає загальновизнаної типології таких кримінальних правопорушень, не розроблено детально понятійний апарат цих усіх визначень, тобто не визначено багато термінів, які пов'язані з кримінальними правопорушеннями, вчиненими з використанням цифрових технологій та цифровою злочинністю загалом.

Кримінальна ситуація, що склалася у цій сфері, обумовлена соціально-економічними факторами, у тому числі випереджаючим розвитком цифрових технологій, що активно використовуються злочинцями як механізм у своїй злочинній діяльності. Правопорушення, що вчиняються з використанням цифрових технологій, практично приховані від зовнішнього фактору, відбуваються дистанційно, що відповідно, дозволяє злочинцям бути (в іншому населеному пункті або навіть за кордоном) на значній відстані від об'єкта злочинного посягання, що досить утруднює процес їх виявлення, притягнення винних осіб до кримінальної відповідальності. Кримінальний закон охороняє суспільні відносини у зазначеній сфері від протиправних діянь, що здійснюються дистанційно, за допомогою інформаційно-телекомунікаційних зв'язків та цифрових технологій з метою заволодіння інформацією, що знаходиться в індивідуальних комп'ютерах, планшетах, смартфонах та інших гаджетах, тощо. Тобто, як бачимо сфера цифрових технологій в тому складна і неоднозначна, що з одного боку за її допомогою особа злочинця вчиняє протиправні кримінальні правопорушення, а з іншого боку, саме вони й допомагають правоохоронним органам вчасно виявити та запобігти їх вчиненню. Тут лише питання в оперативності, своєчасності і головне обізнаності у цій сфері, що інколи викликає труднощі.

Звертаючи увагу на постійне створення нових та вдосконалення існуючих інформаційно-телекомунікаційних та цифрових технологій, відбуваються зміни і в структурі злочинної діяльності. Адже

вчиняються порушення різноманітних електронних систем, які забезпечують безпеку інформації, що знаходиться на зберіганні власника, у тому числі щодо конфіденційних даних, а також особистих та фінансових операцій, щодо яких й здійснюються протиправні діяння, вчинені задля досягнення своєї протиправної мети шляхом заволодіння ними необхідною інформацією. Наслідком цього виступає створення та вдосконалення інформаційно-телекомунікаційних та цифрових технологій для підготовки злочинної діяльності в сучасних умовах, метою якої може виступати порушення систем, які забезпечують безпеку інформації, що знаходиться на зберіганні власника, у тому числі незаконне отримання конфіденційних особистих даних, різноманітної інформації щодо фінансових операцій тощо. Тому, поширення злочинного досвіду у цій сфері, з однієї сторони, зумовлює збільшення вчинення кримінальних правопорушень з допомогою сучасних цифрових технологій, а з іншої – створює перешкоди правоохоронним органам з метою ухилення від кримінальної відповідальності за діяльність протиправного характеру у цифровій сфері.

Стратегія кібербезпеки ЄС на цифрове десятиліття передбачає, що Європейська Комісія продовжить працювати над забезпеченням відповідних каналів і роз'ясненням правил отримання транскордонного доступу до електронних доказів для кримінальних розслідувань (потрібно у 85% розслідувань, при цьому 65% загальних запитів надходять до постачальників, що знаходяться в іншій юрисдикції), шляхом сприяння прийняттю та подальшій реалізації «пакету електронних доказів» і практичних заходів. Електронні докази повинні мати чітке зчитування, тому Комісія й надалі працюватиме над підтримкою потенціалу правоохоронних органів у сфері цифрових розслідувань, зокрема щодо шифрування під час кримінальних розслідувань, повністю зберігаючи свою функцію захисту основних прав і забезпечення кібербезпеки [2].

Саме тому, дотримання та забезпечення кримінологічної безпеки у сфері цифрових технологій є вагомим пріоритетом у системі державної, економічної, національної безпеки України загалом та кібербезпеки зокрема. Щоб належним чином реалізовувати зазначений пріоритет, потрібно в першу чергу посилювати спроможності національної системи кібербезпеки з метою протидії кіберзагрозам, кібератакам та кібершахрайствам у сучасному безпековому середовищі.

Висновки. Проаналізувавши зазначені вище нормативно-правові акти, можна сформулювати визначення «злочинності у сфері використання цифрових технологій», а саме як сукупність кримінальних правопорушень, що вчиняються із використанням систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій.

Окрім цього, для вдосконалення нормативно-правового регулювання у сфері телекомунікаційних та цифрових технологій в сучасних умовах їх розвитку, необхідно сформулювати та закріпити чіткі норми, що визначають напрями боротьби зі злочинністю у цифровій сфері. Також, для боротьби зі злочинними діяннями, що вчиняються з використанням цифрових технологій, пропонуємо внести до КК України зміни, а саме: змінити назву Розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Кримінальні правопорушення у сфері використанням цифрових технологій» та розширити його, шляхом перенесення статей, склади яких передбачають застосування чи використання будь-яких цифрових технологій, що дозволить систематизувати ці види кримінальних правопорушень, враховуючи їх значне поширення на сучасному етапі розвитку громадянського суспільства та його цифровізації.

Список використаних джерел:

1. Digital Agenda for Europe. Fact Sheets on the European Union. European Parliament. URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe (дата звернення: 13.06.2023).
2. The EU's Cybersecurity Strategy for the Digital Decade. Joint communication to the European parliament and the council. Brussels, 16.12.2020 JOIN(2020) 18 final URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата звернення: 23.06.2023).
3. Категорія: Цифрові технології. Вільна енциклопедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D1%96%D1%8F:%D0

%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97 (дата звернення: 19.06.2023).
4. Концепція розвитку електронного урядування в Україні. Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (дата звернення: 13.06.2023).
5. Кримінальний кодекс України. Закон України від 5 квітня 2001 року. № 2341-III (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 13.06.2023).
6. Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки. Указ Президента України від 27 вересня 2021 року № 487/2021. URL: https://zakon.rada.gov.ua/laws/show/487/2021#Text (дата звернення: 13.06.2023).
7. План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text (дата звернення: 13.06.2023).
8. Про авторське право і суміжні права. Закон України від 1 грудня 2022 року № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 13.06.2023).
9. Про Національну програму інформатизації. Закон України від 1 грудня 2022 року № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 13.06.2023).
10. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 13.06.2023).
11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.06.2023).
12. Стратегія інформаційної безпеки. Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення: 13.06.2023).
13. Стратегія розвитку інформаційного суспільства в Україні. Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (дата звернення: 13.06.2023).