УДК 343.007
DOI https://doi.org/10.32689/2617-9660-2024-4(32)-44-51

Флис Іван,
кандидат політичних наук, доцент кафедри права Львівського інституту ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Мазепи, 29, м. Львів, 79059; ivanFlys@qmail/com; https://orcid.org/0009-0005-9327-4098

ПРАВОВЕ РЕФОРМУВАННЯ КІБЕРЗАХИСТУ

Анотація. *Кібербезпека та боротьба з кіберзлочинністю в умовах інтеграційних процесів постійно потребують системних змін засобів і методів в регулюванні та впровадженні новітніх правових і високотехнологічних рішень. Закордонний досвід функціонування системи правового регулювання боротьби з кіберзлочинністю для нашої країни обумовлений загостренням ситуації зі збільшення обсягів злочинної діяльності в кібермережах і повільної на державному рівні передової розвиненості в даній сфері. Масштаби мережі Інтернет свідчать про відсутність локального функціонування окремих елементів кіберзлочинності в межах держави чи регіону, тому у будь-якому випадку національне законодавство повинно відповідати загальновизнаним, світовим стандартам у цій сфері для можливостей доцільної міжнародної співпраці. Окрім того, процес формування чи становлення системи правового регулювання протидії кіберзлочинності неможливий без урахування помилок і досягнень, допущених при формуванні концепції протистояння в окремо взятих країнах. Подальший розвиток системи захисту кіберпростору України від кібератак залежить від рівня взаємодії зацікавлених сторін: держави, громадян, науково-технічних систем, приватних господарств і полягає у розробленні новітніх інформаційно-комунікаційних технологій, законодавчої та нормативної бази, системи навчання населення безпечному використанню кіберпростору.*

Нині в обігу нове поняття – «кібервійна», що вказує на глобально-піратське використання мережі Інтернет, технічних та інформаційних засобів будь-якою країною-агресором, що за мету має заподіяння шкоди економічній, політичній, технічній, військовій та інформаційній безпеці та суверенітету будь-якої держави.

Оцінка нормативно-правових аспектів забезпечення інформаційної безпеки як складової національної безпеки України викликає застереження до рівня безпеки її національних інтересів в інформаційній сфері, та передбачає пріоритетні заходи у нормативно-правовому впорядкуванні правотворчого процесу у сфері протидії кіберзагрозам.

Ключові слова: *інформаційна безпека, інформаційний простір, інформаційні ре-сурси, інформаційна інфраструктура, національна безпека, кіберзлочинність, комп'ютерні системи, кібератаки, мережа Internet, правові механізми, декларації, правові акти.*

Flys Ivan,
Candidate of Political Sciences, Associate Professor at the Department of Law, The Lviv Institute of the Private Joint Stock Company «Higher education institution «The Interregional Academy of Personnel Management», 29, Mazepy Str., Lviv, 79059; ivanflys@qmail.com; https//orcid.org/0009-0005-9327-4098

LEGAL REFORM OF CYBER PROTECTION

Abstract. *Cybersecurity and the fight against cybercrime in the conditions of integration processes constantly require systemic changes in means and methods in regulation and implementation of the latest legal and high-tech solutions. The foreign experience of the functioning of the system of legal regulation of the fight against cybercrime for our country is due to the aggravation of the situation with the increase in the volume of criminal activity in cybernets and the slow state-level advanced development in this field. The scale of the Internet indicates the absence of local functioning of certain elements of cybercrime within the state or region, therefore, in any case, national legislation must meet the generally recognized global standards in this area for the possibility of appropriate international cooperation. In addition, the process of formation or establishment of a system of legal regulation of combating cybercrime is impossible without taking into account the mistakes and achievements made during the formation of the concept of confrontation in individual countries. The further development of the cyberspace protection system of Ukraine against cyber-*

attacks depends on the level of interaction of interested parties: the state, citizens, scientific and technical systems, private enterprises and consists in the development of the latest information and communication technologies, the legislative and regulatory framework, and the system of training the population in the safe use of cyberspace. Currently, a new relevant concept is used – «cyber war», which indicates the global pirate use of the Internet, technical and informational means by any aggressor country, which aims to harm the economic, political, technical, military and informational security and sovereignty of any – which country

The assessment of regulatory and legal aspects of ensuring information security as a component of Ukraine's national security raises concerns about the level of security of its national interests in the information sphere, and provides for priority measures in the regulatory and legal regulation of the law-making process in the field of countering cyber threats.

Key words: *information security, information space, information resources, information infrastructure, national security, cybercrime, computer systems, cyberattacks, the Internet, legal mechanisms, declarations, legal acts.*

З активним розвитком інформаційних технологій, глобалізації інформаційних процесів і появи глобальних комп'ютерних мереж, кінець XX – початок XXI ст. позначився появою нової специфічної інформаційної протиправної діяльності, що передбачає використання комп'ютерів, комп'ютерних мереж або мережевих пристроїв у посяганні на урегульовані законодавством суспільні відносини в інформаційному просторі, – кіберзлочинністю.

«Кіберзлочинність», як загальне поняття кримінальної діяльності, що появилася на інтернет-просторах, охоплює весь спектр злочинів у сфері інформаційних технологій, будь це використання комп'ютерних мереж для вчинення злочину, чи будь-який злочин, скоєний за допомогою комп'ютерів, комунікаційних мереж та інформаційних систем або злочини, предметом яких є інформація що зберігається в них. Як протидія кіберзлочинності, кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується учинення їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації [7].

У вітчизняній науці питання протидії кіберзлочинності досліджували провідні науковці О.М. Бандурка, М.О. Бутузов, М.М. Галамба, Р.А. Калюжний, В.В. Коваленко, Б.А. Кормич, О.В. Манжай, Ю.Є. Максименко, А.І. Марущак, Ю.Ю. Орлов, Г.В. Новицький та іноземні фахівці А. Роберт, К. Осакве, Т. Блентан, Д. Банісар та ін. Незважаючи на досягнення у сфері нормативного регулювання боротьби з кіберзлочинністю, слід констатувати, що багато проблем потребують вирішення.

Якщо оцінювати її як загрозливу проблему для країни, то кіберзлочинність, що у 2021 році завдала глобальних збитків на загальну суму 6 трильйонів доларів США, була б третьою за величиною економікою світу після США та Китаю. За даними Cybersecurity Ventures очікується що глобальні витрати на кіберзлочинність зростатимуть протягом наступних 5 років і досягнуть 10,5трильйонів дол. США на рік до 2025 року, порівняно з 3-ма трильйонами у 2015 р. Це приклад найбільшого перерозподілу коштів в історії, що ставить під загрозу стимули для інновацій та інвестицій. Крім того, це значно більше, ніж збитки що завдають стихійні лиха протягом року. І це буде більш прибутковим, ніж глобальна торгівля всіма наркотиками разом узятими [8].

Згідно аналізу, проведеного компанією «FireEye» у країнах Близького Сходу, Європи та Африки найбільше від кібератак нині страждають урядові сайти, сайти фінансових організацій та операторів зв'язку, що свідчить про зміщення вектору в бік міжнародної організованої злочинності у сфері економічних відносин в фінансових та банківських системах. Однак, не всі кіберзлочинці прагнуть грошей, деяким потрібна інформація. До прикладу – витік даних компанії Solarwinds, ексдержсекретар США Майк Помпео назвав «найгіршою в історії кібершпигунською атакою на американський уряд», та викриттям «найглибших таємниць» уряду США.

11 грудня 2020 р уряд США та компанія Solar Winds виявили порушення у програмному забезпеченні управління мережею Orion, яку використовують численні державні установи країни. Одразу ж з'явилося повідомлення, що деякі «найглибші таємниці» уряду США викрали в результаті скоординованої атаки хакерів. За даними Associated Press, щонайменше два урядові відомства та десятки інших «вартісних цілей державного та приватного сектору» були уражені. Тоді, понад 18 тисяч приватних та дер-

жавних користувачів змушені були оновити зіпсоване програмне забезпечення. Увійшовши в систему, хакери змогли відстежити внутрішні електронні листи службовців урядових органів США тощо і, як наслідок, постраждали урядові органи та компанії, які забезпечували життєдіяльність усієї країни. Певний час наймогутніша держава світу перебувала на межі катастрофи й навіть не підозрювала про це.

Україна не стала виключенням, і нині, в її безпековому полі в повному обсязі присутні всі ключові «класичні» кіберзлочини, а їх кількість щорічно зростає у 2,5 рази. За словами високих представників кіберполіції України, в червні 2016, у рік створення Національного координаційного центру кібербезпеки збитки від кіберзлочинів сягнули близько 39-40 млн гривень. Протягом 2022 року фахівці Держспецзв'язку зареєстрували в Україні понад 2 тисячі кіберінцидентів та ще більшу кількість кібератак. Втрати від шахрайства з використанням методів соціальної інженерії тільки у 2022 році становили більше 1 млрд грн. [9].

Для прикладу. У грудні 2015 року була проведена масштабна кібератака на урядові сайти Держказнечейства України, а також на внутрішні мережі державних органів, що привела до великої затримки бюджетних виплат. Відповідно, Кабінет міністрів змушений був на наступний день виділити 80 млн. гривень для захисту від кібератак, хакерів, зловмисників. У червні 2017 р відбулася наймасштабніша кібернетична атака, що зупинила роботу декількох тисяч українських компаній та держорганів. Лише протягом одного дня комп'ютерний шкідник «Ransom:Win33/Petya» здійснив атаку на державний та приватний сектор економіки країни. Атаки зазнали банки, держзалізниця, аеропорти, телекомпанії, гіганти-супермаркети, державні фіскальні служби, органи місцевого самоврядування тощо. Вірус-вимагач заморозив дані і вимагав внесення викупу у криптовалюті за відновлення доступу.

Безпекові структури виявились безсилими у протистоянні злочинним діям зловмисників. Загалом доводиться констатувати, що кількість реєстрованих! злочинів скоєних з використанням високих інформаційних технологій демонструє виразну тенденцію до зростання абсолютно за всіма основними статтями кримінального законодавства України. Держава, далеко не завжди реально обізнана з масштабами кіберзлочинності, більшість інцидентів залишаються незафіксованими або не публікуються в офіційних звітах державних органів. Наразі кіберпростір є ідеальним місцем для безкарного вчинення злочину. Як зазначає американський журнал «The Economist», «кібрепростір – це п'ятий регіон воєнних дій, після землі, моря, повітря та космосу» [10].

Досвід країн Євросоюзу, зокрема й країн Центрально-Східної Європи, показує, що належний захист від викликів інформаційної небезпеки, може бути реалізований лише за допомогою надійної системи інформаційної безпеки на основі ефективної стратегії кібербезпеки та відповідних механізмів управління, якими виступають державні інститути національної безпеки. Однак виявлення і припинення протиправних посягань на електронні інформаційні ресурси неможливе без тісної міжнародної співпраці. Відповідна взаємодія ґрунтується на двосторонніх та багатосторонніх міжнародних договорах про взаємну правову допомогу, взаємне визнання іноземних судових рішень. Спеціальні норми про кіберзлочинність в кримінальне законодавство, починаючи з 1985 р, були внесені Канадою, Німеччиною, Японією, Англією, Ірландією, Португалією, Туреччиною, Нідерландами, Ізраїлем, Бельгією та країнами Балтії. В другій половині 80-х Спеціальний комітет експертів Ради Європи з питань злочинності пов'язаної з комп'ютерами, виробив рекомендації з переліком правопорушень для єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Рекомендація містить перелік злочинів які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. У 1990 р VIII Конгрес ООН з попередження злочинності ухвалив резолюцію щодо посилення заходів боротьби з комп'ютерною злочинністю, сприяти розвитку структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області судового переслідування.

Продуктом багаторічних зусиль Ради Європи, базовим реально діючим багатостороннім міжнародним документом з інформаційної безпеки стала/є Конвенція про кіберзлочинність (Будапештська конвенція), прийнята Радою Європи в 2001 році [5]. Конвенція містить рекомендації органам законодавчої і виконавчої влади держав щодо боротьби з цими злочинами. Нині 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 інших країн затвердили національні стратегії кібербезпеки. До теперішнього часу Конвенція залишається найбільш актуальним міжнародним договором, та є «фундаментом для розробки відповідного законодавства європейських держав».

На необхідність розвитку міжнародного співробітництва в інформаційному просторі з метою запобігання кіберзлочинам вказують декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» прийнята на Всесвітній зустрічі з питань інформаційного суспільства у Женеві 2003 р., «Окінавська Хартія глобального інформаційного суспільства» ухвалена в 2000 р. лідерами країн «Великої вісімки», Туніська програма для інформаційного суспільства 2005 р., Програма «Інформація для всіх» (Information for All Programme), прийнята в 2001 р. ЮНЕСКО. Важливість інтернаціональних договорів в даній сфері, серед яких Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону, проект ООН з розроблення законодавства в галузі кіберзлочинності для країн Африки надзвичайно висока та необхідна.

Не менше важливими у забезпеченні кібербезпеки на міжнародному рівні стали директиви ЄС 2013 року щодо протидії кібератакам на інформаційні системи, Європарламенту про безпеку мереж та інформаційних систем 2016 р. та Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет за 2017 рік [11].

Спільне повідомлення, Єврокомісії та представництва ЄС із закордонних справ і політики безпеки для Європарламенту і Ради ЄС як технічні рекомендації, під назвою «Стійкість, стримування і захист: створення сильної кібербезпеки для ЄС» у вересні 2017 р, стало частиною пакету документів Євросоюзу спрямованих на забезпечення радикальнішого реагування на кіберзлочинність/кібератаки. Зокрема, Повідомлення передбачає цілеспрямовані заходи скеровані на створення більшої стійкості ЄС до кібератак, продуктивніше виявлення кібернападів і посилення міжнародної співпраці у сфері кібербезпеки. Викладені заходи, спрямовані на підвищення кіберстійкості ЄС, що наведені в наступних положеннях:

– прийняття нового Регламенту ЄС, який реформує Агентство ЄС з кібербезпеки;

– повна та ефективна імплементація Директиви ЄС про безпеку мережних та інформаційних систем усіма державами-членами ЄС;

– швидка реалізація «Концепції» для транскордонного реагування на великі інциденти;

– створення мережі центрів компетенції в області кібербезпеки з Європейським центром досліджень і компетенцій в області кібербезппеки;

– визнання пріоритетності кіберпросвіти в національних інформаційних кампаніях ЄС, включаючи кібербезпеку як частину національних навчальних програм з академічної та професійної підготовки ЄС;

– вироблення єдиного порталу (єдиного в масштабах ЄС) який буде надавати інформацію про останні кіберзагрози і об'єднувати практичні поради та інструменти кібербезпеки для допомоги жертвам кібератак.

Рада Європи останніми роками шляхом залучення якомога більшої кількості країн з різних частин світу до ратифікації Конвенції вживає зусиль щодо її перетворення на єдиний міжнародний механізм, на противагу позиції РФ, Китаю, Ірану, Південно-Африканської Республіки, які пропонують ухвалити свою, своєрідну, конвенцію щодо протидії інформаційним загрозам рішенням Ради Безпеки ООН.

Тим часом, у листопаді 2018 року в Євросоюзі набула чинності чергова Директива NIS4 щодо мережевої та інформаційної безпеки. Її мета – посилити кібербезпеку на європейських теренах. Вимоги Директиви у прийнятті національної стратегії безпеки мережевих та інформаційних систем та визначені державних інституцій, що відповідатимуть за кібербезпеку, єдину точку контакту та Групу реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT або CERT). Окрім того, у рамках ЮНЕСКО була розроблена концепція «Універсальності Інтернету». В її основу покладено чотири ключові принципи, відомі як R.O.A.M. – орієнтованість на права людини, відкритість, доступність та багатостороння участь. Таким чином, на рівні ЄС декларуються дії, спрямовані на створення ефективного кіберстримування та готовність держав-членів до сприйняття нового, передового в зазначеній галузі.

В той же час проблемно вважати, що задіювані заходи принципово змінюють в ЄС ситуацію щодо посилення кібербезпеки. «Гальмують» впровадження щодо досліджень та фінансування проєктів і пропозиції Єврkомісії для полегшення транскордонного доступу до електронних доказів по кримінальних справах, відсутність зобов'язання надавати відповідь на запити протягом певного, стислого терміну, відсутність домовленості про прямий доступ до екстериторіальних даних, швидке прийняття нової Директиви ЄС про боротьбу з шахрайством і підроб-

кою безготівкових платіжних засобів, технічне впровадження недавно прийнятої структури для спільного дипломатичного реагування ЄС на зловмисну кібердіяльність та інше.

Єврокомісія, у черговий раз, на розгляд євроспільноти, внесла пропозиції щодо покращення «Закону про кібербезпеку». А саме, пропозицію щодо змін в Положення про ENISA[1] та про діяльність Агентства ЄС з кібербезпеки, яке матиме оперативну роль для «протидії конкретним загрозам», як «центру експертизи» з сертифікації кібербезпеки та підтримки держав-членів у виконанні законодавства ЄС.

Упродовж останніх років Україною реалізовано низку заходів щодо вдосконалення законодавства в сфері кібербезпеки. Водночас, слід зазначити, що прогнози українських експертів щодо позитивного рівня та стану готовності кібербезпеки невтішні. Якщо узагальнено, то «уявлення України про кібербезпеку поки досить абстрактні, проте ведеться активна робота в цьому напрямку. Кожне з відомств вживає заходів щодо безпеки і веде статистику відповідних показників, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Цілісна політика поки відсутня, як і універсальні індикатори кібербезпеки, що могли б охарактеризувати її рівень»,– саме так проблему висвітлюють в Національному інституті стратегічних досліджень. Проблема полягає в тому, що українська правоохоронна система сконцентрована на майнових злочинах та злочинах проти життя і здоров'я. А законодавство у сфері інформаційних технологій, доступу до інформації та захисту персональних даних в Україні почало розвиватися лише у 2010-х роках, а сама система досі ігнорує це питання [12].

В Україні кібербезпека розглядається як складова національної безпеки та базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року, а також Стратегії кібербезпеки затвердженої Указом Президента України 15 березня 2016 року. Оновлені, з врахуваннями часу та вимог Стратегії приймалися також у 2015 та 2021 рр. [4].

Закон «Про основні засади забезпечення кібербезпеки України», радше, як заявляють фахівці, є дорожньою картою для розробки майбутніх нормативних актів, а не законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам і найкращим практикам. Відповідно, цей напрямок роботи все ще потребує значної уваги та відповідних зусиль [1]. Вищезгаданий Закон визначив основні завдання та компетенцію суб'єктів забезпечення кібербезпеки, до яких належить Національний координаційний центр кібербезпеки, МО, Генштаб ЗСУ, Державна служба спеціального зв'язку та захисту інформації, СБУ, Національна поліція, Національний банк, розвідувальні органи України тощо. Також передбачено створення умов для залучення до співпраці підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації, та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян. До основних досягнень зазначеного Закону також належить впровадження до правового поля однозначних правових визначень, що стосуються кібербезпеки, кібератак, кіберзахисту тощо. Відтак Закон України «Про основні засади забезпечення кібербезпеки України» із змінами і доповненнями, внесеними Законами України є важливим кроком держави у сфері регулювання кіберпростору [3]. Також «критичні інформаційні структури», як об'єкти зобов'язані проходити обов'язковий аудит з кібербезпеки і відповідати інфраструктурним вимогам Кабінету Міністрів України.

Нині, правову основу кібернетичної безпеки України забезпечують Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки», Доктрина інформаційної безпеки, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Фахівці галузі зазначають, що, в Україні існує необхідність привести національне законодавство у відповідність до сучасних міжнародних стандартів, на сьогодні галузі бракує як високих технологій, так і належних методологій з кібербезпеки. Фактично відсутня імплементація реальних заходів кіберзахисту в ІТ-інфраструктурах, має місце слабий процес навчання і підвищення обізнаності в питаннях кібербезпеки [13].

Зокрема, частка положень інформаційного законодавства є застарілою, недостатньо розроблені юридичні механізми реалізації і захисту, спостерігається термінологічна невпорядкованість, мають місце суперечності у регулюванні

[1] Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Функціонує з 1 вересня 2005 року. Розміщене в Іракліон, Крит.

певних відомчих відносин різними законами, що призводить до неоднозначного тлумачення їх норм та створює труднощі для їх застосування, не наведені визначення і не регулюються «термінове збереження та часткове розкриття даних про рух інформації», що заважає ефективному виконанню положень Будапештської конвенції та обмежує можливості взаємодопомоги з іншими країнами у сфері попередження кіберзлочинності та протидії кіберзлочинам. Крім того, експерти відзначають наступні проблемні моменти правового забезпечення кібербезпеки в України:

– невизначеність в розумінні критичної інфраструктури, внаслідок чого наразі відсутня єдина національна система захисту критичної інфраструктури, а регуляторні правила щодо її захисту – недостатні та непослідовні;

– відсутність правил щодо проведення аудитів інформаційної безпеки об'єктів критичної інфраструктури, які мають ґрунтуватись на стандартах Європейського Союзу і НАТО;

– існує правова невизначеність щодо повноважень, завдань та обов'язків державних агенцій, відповідальних за захист критичної інфраструктури. Закон України «Про основні засади забезпечення кібербезпеки України» передбачає повноваження СБУ щодо кіберінцидентів, однак це не відображено належним чином в інших нормативно-правових актах. Правоохоронні повноваження не є чітко визначеними в українському кримінально-процесуальному законодавстві, дублюються, і це негативно впливає на співробітництво між надавачами правоохоронних послуг на права конфіденційності, а іноді й на верховенство права;

– має місце відсутність вимог щодо дотримання протоколу безпеки та інформування загроз для операторів об'єктів критичної інфраструктури та провайдерів цифрових послуг. Директива Європарламенту і Ради ЄС NIS 4 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу вимагає, щоб країни встановили відповідні вимоги щодо безпеки та інформування для операторів суттєвих послуг і для провайдерів цифрових послуг. Закон «Про основні засади забезпечення кібербезпеки України» вимагає від операторів об'єктів критичної інфраструктури інформувати CERT-UA[2] про кіберінциденти, однак, ця норма залишається декларативною;

– відсутність довгострокового стратегічного планування з чітко визначеними проміжними результатами, часовими рамками та відповідальністю за їх досягнення;

– бюджетні обмеження здатності фінансувати інтелектуальні та технічні ресурси з питань кібербезпеки.

Висновки. Однією з найбільших проблем боротьби з кіберзлочинністю є ефективність процедур правової допомоги країн-підписантів Конвенції, імплементація досвіду та кращих практик країн ЄС і стандартів НАТО.

Зокрема, Україна повинна беззаперечно виконувати вимоги для операторів об'єктів критичної інфраструктури щодо інформування із зазначенням обставин, за яких вони повинні інформувати про інциденти, а також категоризацію кіберінцидентів, встановити процедуру інформування інших держав про кіберінциденти, які можуть на них вплинути, з урахуванням вимог конфіденційності та комерційної таємниці, здійснити аудит чинного законодавства на предмет виявлення норм, які суперечать Директиві NIS4, а також неузгодженостей термінологічного характеру, а також на законодавчому рівні розмежувати й конкретизувати повноваження та сферу відповідальності суб'єктів забезпечення кібербезпеки. Також слід зазначити, що з метою попередження кіберзлочинів необхідно продовжити проведення досліджень соціального та кримінологічного напряму щодо вивчення психофізіологічних властивостей кіберзлочинців. Доцільне вдосконалення вітчизняного законодавства у сфері охорони державної таємниці та службової інформації, міжнародної взаємодії у сфері поліпшення змісту вищої освіти фахівців з інформаційної безпеки [14].

Європейська практика засвідчує, що не другорядною складовою діяльності правоохоронних органів у сфері боротьби із кіберзлочинністю є державно-приватне партнерство. У цьому контексті доцільне посилення співпраці шляхом удосконалення і відпрацювання Меморандуму про взаєморозуміння між Інтернет-провайдерами та правоохоронними органами України.

Останніми роками особливої уваги держави-члени ЄС приділяють дезінформуванням спільноти, визначаючи його як «будь-які форми неправдивої, неточної або такої, що вводить в оману інформації, розробленої, презентованої і поширюваної умисно для нанесення шкоди суспільству або для отримання прибутку». Зазначимо, що означений вид діяльності в Україні визначений як вид правопорушення в інфор-

[2] Команда реагування на комп'ютерні надзвичайні події України — спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України

маційній сфері Законом Про доступ до публічної інформації.[2] Однак, протидія дезінформаційним кампаніям з міркувань національної безпеки, формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки здійснюються недостатньо продуктивно. Президент України указом № 187/2021затвердив Положення «Про створення Центру протидії дезінформації», яким встановив його сфери впливу: воєнний напрям, боротьбу зі злочинністю та корупцією, зовнішню та внутрішню політику, економіку, інфраструктуру, екологію, охорону здоров'я, соціальну сферу та науково-технологічний напрям. Але основна увага зосереджена на протидії поширенню неправдивої інформації в Інтернеті та фейків у медіа. Центр не має каральних функцій за дезінформацію і не зможе застосовувати санкції, але може вносити подання до РНБО щодо певних порушень [6]. Зважаючи на суспільно негативні наслідки, які спричиняє дезінформування, доцільно законодавчо цей вид інформаційного правопорушення внести в кримінальне та адміністративне законодавства у вигляді окремого складу правопорушення за умисне поширення неправдивої, неточної або такої, що вводить в оману інформації [15].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. Про доступ до публічної інформації : Закон України. *Відомості Верховної Ради України (ВВР)*, 2011, № 32, ст. 314.
3. Про основні засади забезпечення кібербезпеки України: Закон України із змінами і доповненнями. *Відомості Верховної Ради (ВВР)*, 2017, № 45 ст. 403.
4. Стратегія національної безпеки України: Указ Президента України № 287 від 26.05.2015. Стратегія кібербезпеки України : Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 ІНФОРМАЦІЯ І ПРАВО. № 1 (40). 2022.
5. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. Верховна Рада України. URL: http://zakon0.rada.gov.ua
6. Положення про Центр протидії дезінформації: Указ Президента України від 07.05.21 р. № 187/2021. *Офіційний вісник Президента України*. 2021. № 15. Ст. 774.
7. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2. (42).
8. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html
9. Національний інститут стратегічних досліджень, Департамент кіберполіції Нац. поліції України URL: https://t.me/stoprussiachannel
10. Войнович В. С. Гринок Р. О. Проблеми та перспективи розвитку системи життєдіяльності. Дослідження проблематики кібербезпеки України. Львівський ДУБЖ.
11. Як в Україні розслідуються кіберзлочини? АЛЬТЕРНАТИВНИЙ ЗВІТ (проєкт) з оцінки ефективності впровадження державної антикорупційної політики. Сайт Центру політико-правових реформ. URL: www.pravo.org.ua [Архівовано 20 жовтня 2014 у Wayback Machine.]
12. Directive on security of network and information systems (NIS Directive). URL: https://www.enisa.europa.eu/topics/nis-directive
13. Дубов Д. В. Стратегічні аспекти кібербезпеки України. Стратегічні пріоритети. Н І С Д 4 (2013).
14. Войцехівський А. В. Кібербезпека як напрям євроатлантичної інтеграції України. *Право і безпека у контексті європейської та євроатлантичної інтеграції* : зб. ст. та тез наук. доп. За матеріалами дискус панелі Ш Харків. Міжнар. юрид. форум (м. Харків, 28 вересня 2018 р.). Нац. юрид. ун-т ім. Ярослава Мудрого, НАПН України, Фонд Конрада Аденауера. Харків : Право, 2018. С. 42–48.
15. Марущак А. І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми (ст. 82–88). *Інформація і право*. 1 (40). 2022. URL: https://doi.org/10.37750/2616-6798.2022.1(40).254345

REFERENCES:

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy vid 5.10.2017. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19
2. Pro dostup do publichnoi informatsii [On access to public information: Law of Ukraine]: Zakon Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2011, № 32, st. 314.
3. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy iz zminamy i dopovnenniamy. Vidomosti Verkhovnoi Rady (VVR), 2017, № 45 st. 403.
4. Stratehiia natsionalnoi bezpeky Ukrainy [National security strategy of Ukraine]: Ukaz Prezydenta Ukrainy № 287 vid 26.05.2015. Stratehiia kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 26.08.21 r. № 447/2021. Retrieved from: https://www.president.gov.ua/documents/4472021-40013 *INFORMATsIIa I PRAVO*. № 1 (40). 2022.
5. Konventsiia Rady Yevropy pro kiberzlochynnist vid 21.11.2001 r. [Council of Europe Convention on Cybercrime dated November 21, 2001] Verkhovna Rada Ukrainy. Retrieved from: http://zakon0.rada.gov.ua
6. Polozhennia pro Tsentr protydii dezinformatsii [Regulations on the Center for Combating Disinfor-

mation]: Ukaz Prezydenta Ukrainy vid 07.05.21 r. № 187/2021. *Ofitsiinyi visnyk Prezydenta Ukrainy*. 2021. № 15. St. 774.
7. Baranov, O. A. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka» [On the interpretation and definition of the concept of "cyber security"]. *Pravova informatyka*. № 2. (42).
8. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. Retrieved from: www.iso.org/standard/44375.html
9. Natsionalnyi instytut stratehichnykh doslidzhen [National Institute of Strategic Studies], Departament kiberpolitsii Nats. politsii Ukrainy. Retrieved from: https://t.me/stoprussiachannel
10. Voinovych, V. S., Hrynok, R. O. Problemy ta perspektyvy rozvytku systemy zhyttiediialnosti. Doslidzhennia problematyky kiberbezpeky Ukrainy [Problems and prospects of the development of the vital activity system. Study of the problems of cyber security of Ukraine]. Lvivskyi DUBZh.
11. Iak v Ukraini rozsliduiutsia kiberzlochyny? ALTERNATYVNYI ZVIT (proiekt) z otsinky efektyvnosti vprovadzhennia derzhavnoi antykoruptsiinoi polityky [How are cybercrimes investigated in Ukraine? ALTERNATIVE REPORT (project) on the evaluation of the effectiveness of the implementation of the state anti-corruption policy]. Sait Tsentru polityko-pravovykh reform. Retrieved from: www.pravo.org.ua [Arkhivovano 20 zhovtnia 2014 u Wayback Machine.]
12. Directive on security of network and information systems (NIS Directive). Retrieved from: https://www.enisa.europa.eu/topics/nis-directive
13. Dubov, D. V. (2013). Stratehichni aspekty kiberbezpeky Ukrainy [Strategic aspects of cyber security of Ukraine]. Stratehichni priorytety. N I S D 4.
14. Voitsekhivskyi, A. V. (2018). Kiberbezpeka yak napriam yevroatlantychnoi intehratsii Ukrainy [Cyber security as a direction of Euro-Atlantic integration of Ukraine]. Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zb. st. ta tez nauk. dop. Za materialamy dyskus paneli Sh Kharkiv. Mizhnar. yuryd.forum (m. Kharkiv, 28 veresnia 2018 r.). Nats. yuryd. un-t im.Iaroslava Mudroho, NAPN Ukrainy, Fond Konrada Adenauera. Kharkiv: Pravo, S.42–48.
15. Marushchak, A. I. (2022). Peredumovy dlia formuvannia pravovykh mekhanizmiv protydii dezinformatsii v sotsialnykh media u konteksti natsionalnoi bezpeky [Prerequisites for the formation of legal mechanisms for combating disinformation in social media in the context of national security]: postanovka problemy (st. 82–88). *Informatsiia i pravo*. 1 (40). Retrieved from: https://doi.org/10.37750/2616-6798.2022.1(40).254345