Державна наукова установа “Інститут інформації, безпеки і права
Національної академії правових наук України”

Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України

Відкритий міжнародний університет розвитку людини “Україна”

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 2(37)/2021

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 20117-9917ПР від 05.07.13 р.)

Згідно з Наказом МОН України від 02.07.20 р. № 886 (додаток 4) журнал включено до Переліку наукових фахових видань України, категорія “Б”, галузь науки - юридичні, спеціальність - 081. У журналі можуть публікуватися матеріали стосовно дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії – Ph.D.) і доктора наук у галузі юридичних наук. Друковане періодичне видання ІНФОРМАЦІЯ І ПРАВО внесене в міжнародну базу даних періодичних видань, згідно відповідного номеру ISSN, розміщується на інформаційній платформі “Наукова періодика України”, через яку здійснюється інтеграція з регіональним Реєстром DOI, Системою CrossRef, Міжнародним реєстром ORCID.

м. Київ

State Scientific Institution “Institute of Informatics, Security and Law of National Academy of Law Sciences of Ukraine”

Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND LAW

SCIENTIFIC PROFESSIONAL JOURNAL

№ 2(37)/2021

Registered by Ministry of Justice of Ukraine
(Certificate of state registration of printed communication media:
KV Series № 20117-9917PR dated 05.07.13)

Pursuant to Order of the Ministry of Education and Science of Ukraine dated 02.07.20 № 886 (Annex 4), the journal is included in the List of scientific professional publications of Ukraine, category “B”, branch of science - legal, specialty - 081.
The journal can publish materials related to thesis works aimed on the receipt of scientific degrees of Doctor of Philosophy – Ph.D. (candidate of sciences) and Doctor of Sciences in the area of Juridical Science.
The printed journal INFORMATION AND LAW is included in the international database of journal, in accordance with relevant ISSN number, is placed on the information platform “Scientific Periodicals of Ukraine”, through which integration with the regional DOI Register, CrossRef System, ORCID International Register is carried out.

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 17.5. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ "Видавничий дім "АртЕк".
04050, м. Київ, вул. Мельникова, буд. 63. Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою ДНУ ІБП НАПрН України, протокол № 2 від 23.06.21 р.

T A B L E O F C O N T E N T S

Informative Law

Legal Informatics

Informative and National Safety

Recommended for publication by the IISL of the NALS of Ukraine, protocol № 2 dated 23.06.21.

Інформаційне право

УДК 316(477)

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,* головний науковий співробітник Інституту інформації, безпеки і права НАПрН України.

ЦИФРОВА ЛЮДИНА ЯК ФІЛОСОФСЬКА ПРОБЛЕМА

Анотація. *Пропонується розглядати цифрову людину як новітній етап розвитку людини як основного об'єкта й суб'єкта інформаційних відносин в інформаційному суспільстві на останніх стадіях його розвитку; постмодерний вид людини розумної, здатної переробляти інформацію, створюючи нові інформаційні феномени, взаємозв'язки та структури. Обґрунтовується, що перехід до цифрової людини стався завдяки конвергенції технологій штучного інтелекту, машинного навчання і потужних баз даних, здатних використовувати необмежену кількість інформації з метою її обробки, класифікації та багаторазового використання. Акцентується увага на тому, що цифрова людина – це, перш за все, людина нових моральних цінностей, яка занурюється у віртуальну реальність симуляцій і усе більшою мірою сприймає світ як цифрове ігрове середовище, усвідомлюючи його умовність, керованість його параметрів і можливість виходу з нього.*

Ключові слова: *цифрова людина, інформаційний простір, цифровий простір, інформаційні процеси, віртуальна реальність.*

Summary. *It is proposed to consider a digital person as the latest stage of human development as a major object and subject of information relations in the information society at the latest stages of its development; as a postmodern type of a homo sapiens capable of processing information, creating new information phenomena, interconnections and structures. It is substantiated that the transition to a digital person occurred due to convergence of technologies of artificial intelligence, machine training and powerful databases capable of using an unlimited amount of information for its processing, classification and multiple use. The attention is drawn to the fact that a digital person is, first of all, a person of new moral values, which immerses in the virtual reality of simulations and increasingly perceives the world as a digital game environment, realizing its conventionality, controllability of its parameters and the possibility of exiting it.*

Keywords: *digital person, information space, digital space, information processes, virtual reality.*

Аннотация. *Предлагается рассматривать цифрового человека как новейший этап развития человека как основного объекта и субъекта информационных отношений в информационном обществе на последних стадиях его развития; постмодернистский вид человека разумного, способного перерабатывать информацию, создавая новые информационные феномены, взаимосвязи и структуры. Обосновывается, что переход к цифровому человеку произошел благодаря конвергенции технологий искусственного интеллекта, машинного обучения и мощных баз данных, способных использовать неограниченное количество информации с целью ее обработки, классификации и многоразового использования. Акцентируется внимание на том, что цифровой человек – это, прежде всего, человек новых моральных ценностей, который погружается в виртуальную реальность симуляций и все в большей степени воспринимает мир как цифровую игровую среду, осознавая ее условность, управляемость ее параметров и возможность выхода из нее.*

Ключевые слова: *цифровой человек, информационное пространство, цифровое пространство, информационные процессы, виртуальная реальность.*

Постановка проблеми. Інформаційне суспільство є надскладним і багатошаровим механізмом не лише з онтологічних позицій, але й у розрізі значної кількості суперечностей, з якими доводиться зіштовхуватися вперше. Такими є процеси розмивання меж віртуального й реального, внаслідок чого звичні і традиційні аспекти людської сутності переходять у площину цифровізації, проблематики контролю експонентного розширення комунікаційних зв'язків та збільшення швидкості потоків інформації.

У даний час активно формується нова глобальна соціальна реальність, яка діалектично поєднується з локальною соціальною реальністю. Світ на глобальному й на локальному рівнях стикається з ускладненням соціокультурної динаміки суспільства, небаченими раніше біфуркаціями. В умовах глобалізації конкретні культури, піддаючись змінам, починають не тільки активно протидіяти, але й рефлексувати, прагнучи підтримувати свою ідентичність. Зі свого боку місцеві, культурні особливості, представлені, в тому числі, у персональних, локальних мережах, впливають на характер рефлексії самої глобалізації, того соціуму, який продукує глобальні віртуальні мережі.

Нові соціокультурні реалії несуть екзистенційну невизначеність і ризики. Сучасній людині доводиться жити без стійких орієнтирів, довготривалих чинників порядку, загальновизнаних авторитетів. Зростає обізнаність про те, що нові культурні реалії перестають бути однозначно "хорошими" або "ворожими"; вони амбівалентні, оскільки несуть у собі не тільки очевидні блага, але й часом приховані небезпеки і навпаки [1, с. 14].

Основними технологічними трендами розвитку цифрового середовища є розширення телекомунікаційної інфраструктури, прогрес комп'ютерних, мережевих і мобільних технологій використання технологічних новацій у складних соціотехнічних системах. При цьому цифровий простір, що формується, відіграє вирішальну роль у новій інформаційній картині світу, коли інформація виступає як двигун суспільного й технічного прогресу і стає об'єктивною характеристикою матеріальних систем і їх взаємодії.

З позиції постмодернізму особистість, що загубилася в незліченних потоках інформації та комунікацій, не має певної системи цінностей і уявлень про права, обов'язки та відповідальність за вчинки, а тому втрачає будь-який сенс.

Сучасний постмодернізм є специфічним світоглядом інформаційного суспільства, відмінною рисою якого є плюралістичність, тобто допущення одночасного співіснування розмаїтих точок зору. У такій плюралістичності й полягає сама суть постмодерну, водночас вона ж є його найуразливішим місцем. Багато аспектів уразливості постмодернізму пов'язують з тим, що його світогляд не є універсальною системою відліку для суспільства в цілому і для окремої особистості. Ступінь його поширення обмежується наявністю доступу до інформаційних ресурсів. Тим не менше, сьогодні практично не залишається місць, неохоплених інформаційним полем.

Розвиток телебачення, Інтернету, мереж мобільного зв'язку стає фактором, що свідчить про входження інформаційної культури в життя основної маси населення і цифровізацію особистості під впливом технологічного прогресу. Якщо раніше для виходу за рамки сформованих моделей ідентифікації було необхідним докладання особливих зусиль, то використання сучасних електронних гаджетів гранично спрощує вибір рольової моделі [2, с. 132]. Зворотною стороною легкості й простоти досягнення нової моделі ідентифікації є відсутність культурного та екзистенційного досвіду використання засобів, що надають нові можливості комфортного існування в умовах глобальних мереж та інформаційних потоків.

Усе це спровокувало втрату суспільством вибудуваних раніше соціальних правил, представивши натомість необхідність індивідові здійснювати пошуки нових способів самореалізації у сформованому цифровому світі. Практично безмежні можливості у

виборі способів конструювання власної ідентичності надають нові цифрові технології, які проникають в усталені формати соціальних взаємовідносин. В інформаційному просторі спостерігаються тенденції до трансформації представлення особистості в її віртуальній формі, яка виконує завдання необхідної адаптації у мінливих інформаційних потоках глобального цифрового простору. В умовах сучасного розвитку суспільства цифровізація людини є важливою умовою соціальної адаптації до нових викликів постмодерного світу.

Термін "цифрова людина" вперше використаний у 2001 році американським письменником Марком Пренскі [3] для позначення людей, що народилися після цифрової революції, які живуть в оточенні комп'ютерів, відеоігор, плеєрів, відеокамер, мобільних телефонів (смартфонів), мереж тощо і які звикли отримувати інформацію через цифрові канали, і усе перераховане стає невід'ємною частиною їх життя. На думку Пренскі, люди, що народилися в кінці минулого століття, відрізняються від усіх інших. Такий висновок він зробив, спостерігаючи за школярами і студентами 2000-х років. Вони живуть в оточенні комп'ютерів, відеоігор, плеєрів, відеокамер, мобільних телефонів і Мережі – і все перераховане стає невід'ємною частиною їхнього життя. Таких людей Пренскі запропонував назвати "цифровими тубільцями" – носіями рідної для них цифрової мови комп'ютерів, відеоігор та Інтернету. У 2008 році Гері Смол і Гігі Ворган видали книгу "Мозок онлайн. Людина в епоху Інтернету" [4], у якій, висвітлюючи тему трансформації людського мозку під впливом зміни епох, також згадали "цифрових тубільців".

Людей, що народилися до цього періоду, Пренскі назвав "цифровими іммігрантами" (*Digital Immigrants*). Відповідно до теорії Пренскі, у "іммігрантів", як би вони не старалися, залишається щось на кшталт "акценту" – своєрідні "відлуння минулого", спроби поєднувати новітні можливості з колишніми (наприклад, коли людина по телефону підтверджує отримання електронного листа чи замість того, щоб редагувати текст на комп'ютері, роздруковує його і править від руки).

У 2007 році американські підприємці Джош Спір і Аарон Дігнан ввели в обіг поняття *Born Digital* ("цифрові від дня свого народження") [5], яке згодом трансформувалося у Digital Generation ("цифрове покоління"). У 2007 році компанія Gartner вже розробила комплекс технологій для цифрової людини і продемонструвала низку тенденцій розвитку цифрових технологій на Міжнародному науковому Симпозіумі "IT Expo (Emerging Trends) Symposium" у Барселоні.

У сучасних доробках вітчизняних дослідників проблема цифрової людини також піднімається неодноразово. Разом з тим, вказана проблема здебільшого розглядається "у контексті", у площині окремих наук. Так, наприклад О. Головко розглядає проблему цифрової людини у контексті цифрової та інформаційної культури [6].

К. Гончаренко акцентує свою увагу на питаннях стосовно того, яким чином можливо розглядати людину у цифровому світі та чим є її ідентичність за відповідних детермінант, які проявляються в умовах віртуалізації та цифровізації дійсності [7].

М. Кириченко концентрується на теоретичних і практичних аспектах розвитку інформаційно-технологічної сфери та на напрямках її впливу на формування цифрового світогляду та цифрової ідеології сучасної людини [8].

О. Овчарук виходить на проблему цифрової людини, розглядаючи проблеми розвитку цифрової компетентності людини та цифрового громадянства [9].

О. Радутний пропонує розглядати цифрову людину у контексті революційних винаходів у сфері біоінженерії, створення неорганічної форми життя та (або) живих істот, які поєднують органіку з неорганікою, а також у контексті впливу феноменів

штучного інтелекту та цифрової людини на мораль і право сучасного суспільства та майбутніх поколінь [10 – 11].

Таким чином, очевидна необхідність комплексного міждисциплінарного розуміння феномена людини цифрової і одночасно вузькоспеціалізована галузева спрямованість сучасних досліджень людини цифрової епохи зумовили філософський інтерес до означеної проблеми.

Мета статті – актуалізувати науковий міждисциплінарний дискурс стосовно осмислення нової фази еволюції людини – людини цифрової та її зв'язків з віртуальною реальністю, кіберпростором, новими формами культури, мережевими комунікаціями.

Виклад основного матеріалу. Перетворення "статистичного суспільства" XIX століття на "кібернетичне" суспільство XX століття докорінно змінило взаємозв'язок між інформацією та об'єктивною реальністю [2, с. 131].

Як зазначав ще чверть століття назад В. Розін, Інтернет і ЗМІ не просто інформують людину, але і створюють певні реальності, в які занурюють її. У рамках подібних – майже віртуальних реальностей усвідомлено, але частіше неусвідомлено програмуються не лише переживання людини, але і її думки, світовідчуття [12, с. 45].

Цілком слушною вважається точка зору К. Гарбузенка, який стверджує, що світ, у якому живе сучасна людина, можна представити у вигляді трьох сфер – світу речей, світу інформаційного і світу символічного. Між згаданими трьома світами – світом речей, інформаційним і символічним – існують фільтри, які ускладнюють перехід з одного світу в інший. У світі реальному відбуваються тисячі подій, але тільки одиниці з них перейдуть у світ інформаційний. У свою чергу, у світі інформаційному відбуваються сотні подій, але лише мала їх частка переходить у світ символічний. Подія, помітна у світі речей, може бути абсолютно незначною у світі інформаційному, і навпаки. А оскільки у світі інформаційному ми маємо справу швидше з індивідуальною пам'яттю людини, а у світі символічному – з соціальною, то світ символічний виступає як певне мірило для двох інших світів [13, с. 94].

Значну роль тут відіграють комп'ютерні технології та перехід від моделі "знання" до моделі "інформації". Але звернення до числа (цифри) у системі масової культури носить вже імперативний характер. Вона не тільки вкорінена у науковій, виробничій діяльності, побуті, але стала повсякденністю. Звук, картина, книга, досвід, бажання – все може за подібною схемою опинитися в "цифрованому" вигляді. Велике відкриття сучасності – це універсальна схема конвертованості досвіду і знання в інформацію, а останньої – в цифру [13, с. 94].

Цифровий простір з його пріоритетом мобільності у сучасному суспільстві, може відображати не тільки нову соціальну свободу, але і всеосяжність механізмів контролю. Характерний для цифрових технологій зворотний зв'язок легко обертається функціональною тотальністю, що перевершує споконвічну ідею єдності людської спільноти, адже час великих діячів, грандіозних планів, проектів минув і натомість маємо суспільство "атомізованих" індивідів, які втягнуті у якийсь броунівський рух, де відсутні чітко визначені орієнтири [14].

У цифровому світі система цінностей значно трансформувалася: релігійні цінності поступилися місцем науковому світогляду, що поставив людину у центр світу і побачив її крізь призму числа. Змінилося і ставлення до природи та вирішення проблеми безсмертя. Якщо раніше людина прагнула пристосуватися до навколишнього середовища, жити відповідно до природних ритмів, то в даний час вона виступає як істота, яка пристосовує, перетворює навколишнє середовище відповідно до своїх потреб. Найважливішими стали інтереси і права особистості, що знайшло відображення в індивідуальній свободі вибору в

усіх сферах життя. Наприклад, в економічній сфері індивідуальна свобода вибору особистості означає можливість вибору професії і типу зайнятості, у політичній – політичну демократію і дотримання універсальних прав людини.

І взагалі, у житті суспільства зароджується більш складне, рефлексивне осмислення свободи – "парадоксальна свобода". Її сутнісними характеристиками є неминуче нав'язування і прийняття на себе відповідальності за явні та латентні наслідки ризиків: соціальний суб'єкт виявляється поставленим в такі умови життя, коли необхідно постійно вибирати, просто не можна не вибирати щось або когось з урахуванням фактора негайного або відкладеного, явного або латентного ризиків. Оцінки зробленого вибору активно варіюються у соціокультурному просторі і змінюються у часі. Вибір, який виявився функціональним, ефективним для одного культурного простору, не є універсальним для інших культур. Девіація в одному ціннісно-нормативному просторі стає інновацією в іншому [1, с. 14].

Будемо відстоювати позицію, згідно з якою цифрова людина – це новітній етап розвитку людини як основного об'єкта й суб'єкта інформаційних відносин в інформаційному суспільстві на останніх стадіях його розвитку; постмодерний вид людини розумної, здатної переробляти інформацію, створюючи нові інформаційні феномени, взаємозв'язки та структури.

В українській мові словосполучення "цифрова людина" є неологізмом, синонімами якого є поняття "інформаційна людина" (*homo informaticus*) та "мережева людина". Цифрова людина створює нові штучні взаємозв'язки в межах, які вона інформаційно може попередньо встановити, в результаті чого виникають відповідні інформаційні структури. Формування цифрової людини – це одна з базисних характеристик інформаційного суспільства, коли кожне з діалектично взаємопов'язаних начал людини: фізичне, психічне й соціальне, вимагає спеціального урахування, оскільки лише у цьому випадку нові можливості інформаційного суспільства можуть бути повною мірою використані для розвитку цифрової людини.

Перехід до цифрової людини стався завдяки конвергенції технологій штучного інтелекту, машинного навчання і потужних баз даних, здатних використовувати необмежену кількість інформації з метою її обробки, класифікації та багаторазового використання. Електронні пристрої, підключені до глобальної мережі, залишають цифрові сліди навіть якщо у них немає фактичного користувача. За допомогою пристроїв особистого, сімейного, виробничого, соціального та інших рівнів відбувається цифрова обробка не тільки людини як об'єкта, але й усієї світової інфраструктури для можливості її повної симуляції і відтворення.

На сучасному етапі тотального упровадження цифрових технологій змінюється не тільки те що робить людина, але й те, ким вона є і в кого перевтілюється. Цифрові трансформації у соціумі здійснюють багатоплановий вплив на людину і позначаються на всіх сферах її життєдіяльності: на недоторканності особистого життя і формах власності, на зміні характеру поведінки споживачів, на кількості часу, присвячуваного роботі, відпочинку й сім'ї, на принципах розвитку кар'єри та методах удосконалення навичок. Цифрова людина може змінювати свої корпоративні зв'язки, не будучи до них жорстко прив'язаною; вона може і здатна дуже гнучко вибудовувати стосунки з іншими людьми, долучатися до різних соціальних спільнот і різних культурних традицій. Цифрова людина менше обтяжена сформованими та історично обумовленими стереотипами, вона володіє більш мобільними реакціями і здатністю маніпулювати будь-якими пластами інформації, вона набуває нової абстрактної форми свого існування.

Цифрова людина стикається з декількома видами ідентичності, які піддаються позитивним і негативним змінам під впливом інформаційно-комунікаційних технологій. Головними з них є два типи ідентичності: *ipse*-ідентичність (відчуття власної особистості) та *idem*-ідентичність (більш формальна ідентичність, що залежить від контексту, оточення й ситуації). Комп'ютери накопичують інформацію, створюють профілі, здійснюючи внесок в *idem*-ідентичність користувача, який і не підозрює про ці профілі і про те, як вони впливають на його *ipse*-ідентичність, що суттєво впливає на позитивну свободу цифрової людини.

Отже, сучасні інформаційно-технологічні процеси призводять до зміни реальності, у якій перебуває людина, здебільшого переводять їх у цифрову площину. Врешті, ця реальність стає віртуальною: образно-особистісною та метафоричною, веде людину іншим витком спіралі розвитку, одночасно повертаючи її в царину архетипів і символів (цифри).

У віртуальній реальності поступово зникають просторові та часові розмежування, стираються міждержавні кордони, пропагуються нові цінності, моделі поведінки, світоглядні стереотипи. Феномен віртуалізації просторово-часового континууму, в якому існують людина та суспільство, характеризує принципово новий тип символічного існування людини, соціуму, культури [15, с. 123]. На слушну думку О. Сотнікової, соціальна віртуальна реальність – це особлива субкультура, з власними ідеалами, принципами, мовою і стилем спілкування [16]. Тобто створювані засобами комп'ютерних технологій "світи існування" набувають самостійного значення [13, с. 95].

Ще однією інфраструктурною технологією, яка охоплює практично всі сфери людського життя мережевого суспільства, стає кіберпростір. У кіберпросторі віртуальна реальність відрізняється яскраво вираженим інструментальним характером, інтерактивністю, модифікацією просторово-часових характеристик. Віртуальна реальність, сформована новими інформаційними технологіями, сприяла створенню мережевого суспільства, а існування кіберпростору є його основою, яка впливає на всі сфери суспільного життя і є однією з ключових детермінант формування цифрової людини [17, с. 20].

Віртуальний світ, створений новітніми інформаційними технологіями, включає людину у процес сприйняття цілком і відразу. Виникає багатоликість створюваного віртуального світу, нескінченне павутиння ходів користувача інформаційно-комунікаційних засобів. Залежно від ситуації один і той же контекст може бути розглянуто під різними кутами зору, і це вже накладає певний відбиток на створюваний віртуальний потік. Відповідно, нові ситуації й контексти, з якими стикається індивід, блукаючи у безкрайньому просторі мережі віртуального світу, вимагають від нього щоразу іншої поведінки.

Віртуальному простору притаманні зміщення реальності, наслідком чого постає зміщення полюсів того, що означується, і того, що означує. Останнє, у свою чергу, призводить до того, що весь зміст реальності переводиться у площину видовищного, а сама реальність втрачає основу, і в ній відбувається нейтралізація смислу. Актуалізація віртуального як форма трансгресії може сприяти збагаченню сфер свідомості та діяльності особистості, розширенню її життєвого світу і життєвих можливостей. Але актуалізація віртуальної складової життєвого простору й часу може бути й деструктивною для особистості, оскільки містить у собі загрозу нічим не обмеженої, демонічної творчості, яка може знищити як особистість, так і суще [18, с. 177].

Споживання у цифровому просторі супроводжується рутинізацією процесів обміну інформацією через публікацію, нагадування, визнання, посилання, коментування тощо.

Це змінює способи поведінки людини, її інформаційну культуру, природу сприйняття. Усе частіше замість пошуку релевантної інформації вона фактично споживає рекомендований членами її соціальної віртуальної спільноти (організованої за принципом соціального графа) так званий контент "швидкого сприйняття", переповнений інформаційним шумом [19, с. 141].

Принципово новий тип символічного існування цифрової людини характеризує віртуалізація життєвого простору й часу. Ведучи мову про віртуальний простір, насамперед, варто відзначити, що він тісно пов'язаний зі сприйняттям людиною зовнішнього світу і саме він є ключовим чинником формування людини цифрової. Новітні технології цілеспрямовано на рівні відчуттів прагнуть створити у користувача найбільш достовірну ілюзію реальності штучного світу. Органи почуттів якраз і є тим механізмом, за допомогою якого здобуваються знання про навколишнє середовище і створюються уявлення. Якщо їх піддати цілеспрямованому впливу певного роду штучних стимулів, то сукупність цих відчуттів також становитиме образ деякої віртуальної реальності. Таким чином, як справедливо стверджує О. Єлхова, віртуальний простір базується на перцептуальному типі простору, який є передумовою і найважливішою умовою для нього [20, с. 240]. Коли користувач виявляється зануреним у віртуальну реальність, то його свідомість живе інформацією, яка сприйнята органами почуттів, і ця інформація координує його положення у віртуальному просторі. Знаки, які сприймаються як відповідні елементи навколишнього світу, наділяються смислом, а також встановлюються смислові зв'язки між ними, зміна ж положення користувача задає новий потік інформації [21, с. 167].

Смислова схема у внутрішньому просторі виникає шляхом отримання й обробки інформації в результаті досвіду постійної взаємодії людини з навколишнім світом. Поява і розвиток інформаційних технологій, специфічних засобів масової комунікації призвела до зміни світосприйняття людини, визначила формування нового типу простору – віртуального. М. Маклюен, одним із перших звертаючи увагу на роль впливу інформаційно-комунікаційних технологій на світосприйняття людини безвідносно змісту повідомлення, робить висновок: "засіб передачі повідомлення сам є повідомленням" [22, с. 11]. М. Маклюен вважає, що засіб масової інформації не є нейтральним. Він значно впливає на суспільство скоріше не своїм змістом, а характером передачі повідомлення. Так, наприклад, усе передане по телебаченню, стає "телегенним". Головною рисою "телегенності" є мозаїчність повідомлення, яка є обставиною порушення причинно-наслідкових зв'язків у свідомості людини і повернення її до структури донаукового міфологічного мислення [23].

Наприклад, при трансляції новин телебачення привертає увагу глядачів до минулого і тут же повідомляє про кінцевий результат. В результаті створюється ілюзія того, що демонстрація дії призводить до даного наслідку. Людина, що знаходиться перед екраном телевізора, з'єднує всю прогресивну телевізійну мозаїку через резонанс взаємних відображень її окремих елементів. У результаті у свідомості сучасної людини постійно формується і відтворюється "кулястий" космос миттєво виникаючих взаємозв'язків, що вбирає в себе все, що відбувається на телеекрані [24].

У таких умовах людина сприймає інформацію як потік, причому, сучасні телекомунікаційні засоби дозволяють людині самій конструювати складні інформаційні потоки. Яскравим прикладом тут може служити занурення людини у світ Інтернету, при якому вона починає сприймати гіпертекстову інформацію. М. Маклюен у зв'язку з цим називає нові засоби масової комунікації виведеною назовні нервовою системою людини.

Дійсно, нові інформаційні технології не підміняють реальність, а людина, використовуючи їх, створює нову віртуальну реальність зручним для себе способом.

Коли людина опиняється зануреною у віртуальну реальність, "у цифру", як особливе середовище, виявляються можливими два варіанти її сприйняття. У першому випадку користувач акцентується на чомусь логічному й абстрагованому, всезагальному й подібному. У другому ж випадку користувач занурюється у міфологічне сприйняття навколишнього середовища, акцентується вже на чомусь неповторному, конкретному, емоційно-образному. Таким чином, різні типи світосприйняття в результаті зумовлюють різні типи структурування, побудови віртуального простору, ніби дві проекції світу, що не перетинаються одна з одною. Причина ж такої множинності полягає в акцентах уваги, розставлених кожним користувачем по-своєму. У більшості випадків сприйняття й конструювання віртуальної реальності здійснюється за другим, емоційно-образним типом [21, с. 166].

Крім того, при частому спілкуванні з комп'ютерними системами трапляється інформаційне зараження особистості "числовим баченням світу": в активних Інтернет-користувачів формується звикання до цифрового зображення на рівні логіко-ментальних структур, що призводить до мозаїчності. Перемикаючись між різними інформаційними каналами людина конструює нову реальність. Сучасна людина підлаштовується під цю мозаїчність, адаптується до ситуації – це стає однією з її навичок. У зв'язку з цим виникають проблеми із засвоєнням, переробкою та аналізом більш глибинної інформації, що пов'язана з детермінантами аналізу зв'язків у природі та соціумі [13, с. 96].

Стосовно темпоральних вимірів віртуальної реальності варто зазначити, що час цієї реальності можна зупинити, за рахунок інверсії час віртуальної реальності втрачає свою безвихідну незворотність, його різні пласти перетинаються, зливаються. У віртуальній реальності допускається зворотний рух елементів, цифровій людині гарантується можливість у будь-який момент, починаючи з будь-якого елемента і з твердою впевненістю, що до нього можна буде повернутися, пограти у своє народження і смерть.

До якісних особливостей часу віртуальної реальності слід віднести також наявність певних часових циклів (ритмів). Фрактальний принцип, що лежить в основі віртуальної реальності, задає ритмічне повторення однієї структури, її безперервну зміну відповідно до заданого алгоритму. Віртуальна реальність постає як процес зі зворотним зв'язком, у якому знову і знову виконується одна і та ж операція, а результат однієї ітерації стає початковим значенням для наступного циклу [15, с. 121]

Віртуальний світ, створений новітніми інформаційними технологіями, включає людину у процес сприйняття цілком і відразу. Виникає багатоликість створюваного віртуального світу, нескінченна павутина ходів користувача. Залежно від ситуації один і той же контекст може бути розглянуто під різним кутом зору і це вже накладає певний відбиток на створюваний віртуальний потік. Відповідно, нові ситуації й контексти, з якими стикається користувач, блукаючи по безкрайньому простору мережі, вимагають від нього кожен раз іншої поведінки.

Миттєве подолання відстані за допомогою наднових телекомунікацій і надшвидкісних транспортних засобів дає можливість цифровій людині проводити час і комунікувати без безпосереднього просторового зближення, що переходить у діючі й постійно оновлювані мережі взаємодії. Час багато в чому знищується миттєвим зв'язком між комп'ютерами. Зміни часових меж, поява позачасових понять в інформаційну епоху пов'язані також з новітніми репродуктивними технологіями людського організму, в тому числі й шляхом клонування.

Отже, віртуалізація простору й часу створюють так званий “дигітал-континуум” мережевої комунікації [25], визначальними характеристиками якого є поверхневість та площинність. Це призводять до того, що цінність інформаційної діяльності визначається фактом присутності інформації, інформаційного продукту у полі зору цифрової людини (на поверхні її інформаційного поля) – ризомність мережевих комунікацій поглинає глибину. “Тому, – як справедливо зазначає І. Сілютіна, – у щільному сплетінні ризомних з’єднань для інформаційного продукту надзвичайно важливим є модус “теперішнього”. Минуле й майбутнє для інформації й інформаційного продукту у соціальних мережах існують тільки як потенція. Постійний потік нової інформації зносить з поверхні інформаційної атенції старий. Після нього можуть залишитися гіпертекстові сліди: посилання, теги, мітки, за якими може рухатися індивід, як за ниткою Аріадни. Але в наш час для пересічного індивіда це може бути свого роду подвигом, оскільки потребує докладання вольових зусиль” [26, с. 172].

У результаті маємо той факт, що “дигітал-континуум” мережевого суспільства має всі ознаки гіперреальності. Ж. Бодрійяр, який ввів у обіг це поняття, у своїх роботах вказував, що реальність у процесі розвитку суспільства споживання замінюється гіперреальністю у процесі симуляції дійсності й супроводжується заміною реальності симулякрами – знаками реальності й утратою почуття реальності [27], що яскраво свідчить про поступове еволюціонування людини інформаційної до людини цифрової.

Важливим атрибутом цифрової людини є біометрія – система розпізнавання людей за індивідуальними фізичними і поведінковими рисами, такими, як ДНК, відбитки пальців, тривимірна фотографія обличчя або тіла, голос, фото рогівки ока. Біометричними передавачами даних про особу є вживлені датчики й чіпи, біометричні паспорти, банківські картки, фітнес-браслети, розумні годинники, смартфони, комп’ютерна техніка, домашня електроніка, камери відеоспостереження та фіксації звуку. Основною сферою використання біометричних даних є ідентифікація громадян з метою контролю доступу та виявлення порушень.

Соціокультурний портрет цифрової людини визначається наступними технологічними та процесуальними характерними рисами [7; 10; 28 – 30]:

- цифрова людина формується як інформаційно-знаннєвий носій та інтерпретатор величезної кількості інформації. Інформація відповідно до мети наділяється певним суб’єктивним змістом, перетворюючись на знання – основу розвитку. Інформація є ресурсом для реалізації інтелектуальних здібностей людини;
- у когнітивній сфері повсюдно спостерігається підвищення цінності швидкості сприйняття й переробки інформації, причому, часто на шкоду глибині сприйняття;
- зниженням потреби у тренуванні оперативної пам’яті, яку можна передати пристроям;
- мобільні засоби зв’язку набувають рис “психічного органу”, винесеного назовні: опинившись без гаджета або мобільного телефону, людина відчуває себе безпорадною, позбавленою пам’яті й комунікативної функції у цілому;
- втратою інтересу до фундаментального знання основ, задовольняючись поверхневим знанням проблем, ігноруючи перевірку досвідом і критичність мислення; формуванням особливого типу наочно-образного “кліпового” мислення, де яскравість і доступність змісту цінується вище його глибини;
- можливістю отримання практично необмеженої кількості інформації за відносно короткий проміжок часу;
- віртуалізацією міжособистісних контактів, що, з одного боку, полегшує комунікацію, а з іншого – породжує ілюзію доступності й легкості відносин;

- перетворенням гаджетів на елемент підсвідомості, індивідуальний зовнішній носій колективного несвідомого;
- перенесенням різноманітних видів і способів комунікації в онлайн сферу;
- збільшенням кількості патологій внаслідок заздрості через чітко виражене майнове розшарування;
- ідентифікація цифрової людини відбувається через причетність людини до тієї чи іншої сфери інформації, віртуального та соціального просторів;
- самопрезентація індивіда в Інтернеті здійснюються через нік, аватар, сторінку у соціальній мережі, завдяки свободі їх конструювання та привабливості для користувачів.

Висновки.

Віртуалізація життєвого часу у просторово-часовому континуумі характеризує принципово новий тип символічного існування соціуму, культури, людини. Цифрова людина – це, перш за все, людина нових моральних цінностей, яка занурюється у віртуальну реальність симуляцій і усе більшою мірою сприймає світ як цифрове ігрове середовище, усвідомлюючи його умовність, керованість його параметрів і можливість виходу з нього.

Миттєве подолання відстані за допомогою наднових телекомунікацій і надшвидкісних транспортних засобів дає можливість організаціям і індивідам спільно проводити час без безпосереднього просторового зближення, що включає їх у пластичні багатопростірні структури, які плавно переходять у діючі й постійно оновлювані мережі взаємодії.

Суперечливі реалії формування цифрового простору знаходять відображення у всіх сферах життєдіяльності соціуму, індивідів і зумовлюють тенденції формування цифрової людини. Глобальність цих процесів загострює не тільки технічні та комунікаційні аспекти розвитку інформаційного суспільства, а й актуалізує широкий спектр складних світоглядних питань, соціокультурних проблем, породжуваних самим фактом формування цифрової людини.

Використана література

1. Danilyan O., Dzoban A. Existence-network dimension of information security in modern society. *Схід*. – (Аналітично-інформаційний журнал). 2021. Т. 1 (1). С. 11-17.

2. Мозговий А.А. Конфлікти в цифрову добу: проблема суб'єктності та ідентичності. *Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Серія: "Релігієзнавство. Культурологія. Філософія"*. 2019. Вип. 41. С. 129-136.

3. Prensky M. Digital Natives, Digital Immigrants. *On the Horizon MCB University Press*. 2001. Vol. 9. № 5. URL: https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (дата звернення: 22.03.2021).

4. Small G., Vorgan G. IBrain: Surviving the Technological Alternation of the Modern Mind. New-York: Harper Collins, 2008. 256 с.

5. Digital natives are those. URL: https://cbo.org.ua/digital-natives-are-those-pereklad-na-rosijsku-prikladi-anglijska (дата звернення: 22.03.2021).

6. Головко О.М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. *Інформація і право*. № 4(31)/2019. С. 37-44.

7. Гончаренко К.С. Цифрова людина: фантазм втрати ідентичності. *Філософські обрії.* 2019. № 42. С. 137-140.

8. Кириченко М.О. Розвиток інформаційно-технологічної сфери та її вплив на формування цифрового світогляду та цифрової ідеології сучасної людини. *Гуманітарний вісник ЗДІА*. 2019. Вип. 77. С. 35-46.

9. Овчарук О.В. Сучасні підходи до розвитку цифрової компетентності людини та цифрового громадянства в європейських країнах. *Інформаційні технології і засоби навчання*. 2020. Т. 76. № 2. С. 1-13.

10. Радутний О.Е. Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект. *Інформація і право.* № 2(25)/2018. С. 158-170.

11. Радутний О.Е. Мораль і право для штучного інтелекту та цифрової людини: закони робототехніки та "проблема вагонетки". *Інформація і право*. № 3(30)/2019. С. 78-95.

12. Розин В.М. Мистические и эзотерические учения и практики в средствах массовой информации. *Общественные науки и современность*. 1997. № 3. С. 44-54.

13. Гарбузенко К.А. Від інтелектуальності "числа" до соціуму "цифри": числова магія Піфагора як складова сучасної квазірелігійності в Інтернет-просторі. *Наука. Релігія. Суспільство*. 2012. № 4. С. 93-98.

14. Соціокультурні та теоретичні засади філософії постмодерну / В.В. Лях, О.М. Йосипенко, Я.В. Любивий, В.С. Пазенок, К.Ю. Райда, Л.А. Ситніченко. Київ, 2017. 312 с.

15. Дзьобань О.П. Темпоральна складова у просторово-часовому континуумі віртуальної реальності. *Стратегічні пріоритети*. 2018. № 2 (47). С. 118-126.

16. Сотникова О.О. Соціальність віртуальної реальності. Філософські перипетії. *Вісник Харківського національного університету ім. В.Н. Каразіна*. 2002. № 547. С. 138-141.

17. Данильян О.Г., Дзьобань О.П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. *Інформація і право*. № 4(35)/2020. С. 9-21.

18. Ігнатко В. Ціннісні пріоритети життєвого простору людини індустріальної та постіндустріальної епохи. *Гілея: науковий вісник*: зб. наукових праць. 2016. Вип. 111 (8). С. 175-179.

19. Марьина Е.Ю. Особенности потребления информации в цифровом пространстве. *Молодий вчений*. 2017. № 12. С. 139-142.

20. Елхова О.И. Онтологическое содержание виртуальной реальности: дис. ...д-ра филос. наук. Уфа, 2011. 330 с.

21. Дзьобань О.П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. *Стратегічні пріоритети*. *Серія: "Філософія"*. 2017. № 3. С. 163-170.

22. Маклюэн М. Понимание медиа: внешние расширения человека / пер. с англ. В.Г. Николаева. Москва; Жуковский: "Канон-пресс-Ц", "Кучково поле", 2003. 464 с.

23. Маклюэн М. Телевидение. Робкий гигант. *Современные проблемы личности*. 2001. № 1. С. 138-148.

24. Прудникова О.В. Феномен інформаційної культури: онтологічний статус та соціоантропологічні детермінанти: монографія; за заг. ред. О.П. Дзьобаня. Харків: Право, 2017. 496 с.

25. Рябініна О.В., Коваленко І.І. Простір Homo Virtualis і пост-цифрова естетика музики. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2018. № 4. С. 214-221.

26. Сілютіна І.М. Інформаційна діяльність в мереженому суспільстві. *Гілея: науковий вісник*: зб. наукових праць. 2017. Вип. 120 (5). С. 170-173.

27. Бодрийяр Ж. Симулякры и симуляции / пер. с фр. А. Качалова. Москва: ПОСТУМ, 2016. 238 с.

28. Пархоменко О.В., Пархоменко В.Д. Людина майбутнього в умовах формування інформаційно-знаннєвої парадигми цивілізаційного розвитку. *Наука, технології, інновації*. 2017. № 4 (4). С. 3-9.

29. Скіннер К. Людина цифрова. Четверта революція в історії людства, яка торкнеться кожного. Київ: Фабула, 2020. 272 с.

30. Сучасне суспільство, людина, право в умовах глобальних трансформацій: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. Харків: Право, 2020. 344 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-6548-5457.

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ТА ОСОБЛИВОСТІ ЛОКАЛІЗАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ: КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *Розглянуто загальносвітові тенденції та особливості локалізації персональних даних у деяких зарубіжних країнах (ЄС, США, Індонезія, Малайзія, Індія, Узбекистан, Казахстан, РФ). Узагальнено деякі аспекти здійснення зберігання, обробки та передачі персональних даних у межах юрисдикції держав. Деталізовано законодавче забезпечення штрафних санкій за порушення нормативних вимог локалізації персональних даних, їх конфіденційності та приватності. Визначено позитивні аспекти та здобутки використання світового сервісу "InCountry". Регламентовано особливості здійснення передачі персональних даних на умовах аутсорсингу. Окреслено шляхи удосконалення вітчизняного законодавства у сфері локалізації персональних даних.*

Ключові слова: *персональні дані, приватність, конфіденційність, локалізація, захист, IT-технології, провайдери, оператори, аутсорсингові послуги.*

Summary. *The global trends in the localization of personal data are considered. Peculiarities of localization of personal data in some foreign countries (EU, USA, Indonesia, Malaysia, India, Uzbekistan, Kazakhstan and Russian Federation) are investigated. Some aspects of the storage, processing and transfer of personal data within the jurisdiction of states are summarized. The legislative support of penalty sledges for violation of regulatory requirements for localization of personal data, their confidentiality and privacy is detailed. The positive aspects and achievements of using the world "InCountry" service are identified. The peculiarities of outsourcing of personal data transfer are regulated. The directions of improvement of the domestic legislation in the field of personal data localization are outlined.*

Keywords: *personal data, privacy, confidentiality, localization, protection, IT technologies, providers, operators, outsourcing services.*

Аннотация. *Рассмотрены общемировые тенденции и особенности локализации персональных данных в некоторых зарубежных странах (ЕС, США, Индонезия, Малайзия, Индия, Узбекистан, Казахстан, РФ). Проведено обзор некоторых аспектов осуществления хранения, обработки и передачи персональных данных в пределах юрисдикции государств. Детализировано законодательное обеспечение штрафных санкций за нарушения нормативных требований локализации персональных данных, их конфиденциальности и приватности. Определены положительные аспекты и достижения использования мирового сервиса "InCountry". Регламентированы особенности осуществления передачи персональных данных на условиях аутсорсинга. Определены пути усовершенствования отечественного законодательства в сфере локализации персональных данных.*

Ключевые слова: *персональные данные, приватность, конфиденциальность, локализация, защита, IT-технологии, провайдеры, операторы, аутсорсинговые услуги.*

Постановка проблеми. Одним з найбільш проблемних правових питань в еру інформаційних технологій є захист персональних даних. До того ж у світі, поглибленому глобалізацією, дані користувача однієї країни можуть використовувати треті особи з будь-якого куточка світу, у тому числі й незаконно.

Останнім часом світова спільнота активно переймається питаннями локалізації персональних даних у межах національних кордонів з метою забезпечення їхнього збереження у форматі захисту цифрових прав громадян, особливо щодо приватних та конфіденційних відомостей користувачів пристроїв. На цьому фоні невиконання вимог щодо локалізації інформаційних баз з персональними даними створює певну загрозу для захисту та безпеки громадян, безперебійного функціонування критичної інформаційної інфраструктури, мінімізує ефективність заходів боротьби з тероризмом, нівелює здобутки щодо забезпечення національної безпеки держави. У зв'язку з цим для будь-якої країни сучасного світу необхідним є прискорення в удосконаленні відповідних нормативно-правових актів, які мають регламентувати порядок та умови впровадження такої локалізації, з одночасним запровадженням санкцій та відповідальності за правопорушення прав людини. Динамічне розширення сфери застосування сучасних технологій та комунікацій створює додаткові умови для зростання рівня кіберзлочинності.

Глобальні та кардинальні зміни у сфері ІТ-технологій, що відбуваються останнім часом, вимагають адекватного коригування та адаптації вітчизняного законодавства з метою встановлення превентивних заходів щодо профілактики та попередження протиправних дій у зв'язку з поширенням несанкціонованих обробки та використання персональних даних. За таких умов, розгляд зарубіжних законодавчих ініціатив, які впроваджуються щодо посилення процесів локалізації персональних даних та підвищення рівня відповідальності операторів ІТ-ринку за такі порушення, є своєчасним та логічним.

Результати аналізу наукових публікацій. Питання організаційно-правових засад інституціоналізації та локалізації персональних даних, сучасні методи їх обробки та збереження досліджували у своїх наукових працях такі вчені, як: В. Брижко, В. Пилипчук [1], П. Гуйван [2], К. Мельник [3], Т. Обуховська [4], А. Тарасюк [5] та інші. Проте висвітлення кращих практик зарубіжного досвіду у сфері законодавчого забезпечення щодо локалізації персональних даних потребує подальших досліджень, зокрема щодо висвітлення особливостей роботи всесвітнього сервісу "InCountry".

Метою статті є визначення сучасних законодавчих ініціатив у провідних країнах світу з метою впровадження концептуальних засад локалізації персональних даних для їх забезпечення дотримання принципів приватності та конфіденційності у сучасних європейських правових стандартах.

Виклад основного матеріалу. Персональні дані – не тільки ім'я чи контактні дані певної фізичної особи, це також й IP-адреса, MAC-адреса, геолокація, які можуть використовувати персональні дані для відстеження контактів. Ще декілька років тому компанії, незалежно від юрисдикції держав, зберігали дані своїх користувачів де завгодно: деякі у межах країни, а інші – поза межами, в інших державах, або на серверах та площадках міжнародних ІТ-гігантів, на кшталт "Google", "Facebook" тощо.

Адже траплялося чимало випадків несанкціонованого або спеціального витоку персональних даних або їх використання у злочинних цілях, що привезло до необхідності посилення заходів збереження та обробки персональних даних. Таким чином, загальноприйнятим трендом в сучасному світі є активізація процесу локалізації персональних даних з дотриманням вимог політики конфіденційності та приватності. Метою політики конфіденційності й приватності є забезпечення захисту прав і свобод людини і громадянина при обробці його персональних даних, в тому числі захисту прав на недоторканність приватного життя від несанкціонованого доступу і розголошення. По мірі того, як активно прогресує та просувається інформаційна епоха, важливість географічного місцязнаходження для конфіденційності даних стає дедалі важливішою. На цьому фоні актуальним питанням стає така ознака як резидентність даних, тобто їхня

локалізація у межах певної держави. Так, останнім часом, у багатьох країнах світу таких, як ЄС, Канада, Австралія, США, Аргентина та інших, компанії, які мають доступ до обробки та зберігання персональних даних громадян, зобов'язані зберігати їх виключно на території своїх країн, тобто в межах їх національних юрисдикцій. Тому кожна держава світу розробляє та впроваджує власні системні заходи з метою збереження персональних даних громадян у межах національних сегментів кіберпростору. Також кожна країна розробляє норми регулювання персональних даних з метою встановлення правил їх зберігання та використання.

В травні 2018 року для міжнародного ІТ-ринку усіх держав-членів ЄС було запроваджено оновлені правила обробки персональних даних на підставі Загального Регламенту ЄС 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)" від 27 квітня 2016 року (General Data Protection Regulation – GDPR) [6].

Загальний Регламент захисту даних встановив більш суворі вимоги до принципів обробки та використання персональних даних. Вони полягають в тому, що персональні дані мають збиратися законно, правомірно, прозоро та відповідно до цільового призначення. В умовах поширення глобалізації та прискореного інформаційно-технологічного прогресу стало конче необхідним посилити захист основоположних прав людини в сфері захисту персональних даних за умов впровадження заходів, які мають гарантувати недоторканність приватного життя та забезпечити цифрові права пересічених громадян. Тобто виконання приписів GDPR передбачає для усіх держав-членів ЄС схвалення нових національних програм захисту персональних даних з чіткою системою контролю, яка має орієнтуватися на виконання принципів та правил забезпечення приватності та конфіденційності [7].

Що стосується питання захисту персональних даних в інших країнах, традиційно, найбільш розвиненою юрисдикцією вважається США. Однією із причин необхідності розвитку такого законодавства є значна кількість порушень у сфері персональних даних. У зв'язку з цим у 2020 році у штаті Каліфорнія був прийнятий новий Закон про захист персональних даних. Насамперед, його важливість полягає в тому, що в Каліфорнії знаходяться такі компанії, як "Facebook", "Google", "Apple", що працюють з персональними даними користувачів по всьому світу. Завданням цього законодавчого акту стала необхідність посилення захисту персональних даних, які обробляють юридичні особи приватного права та є розпорядниками такої інформації. Саме тому цим Законом користувачам надається право дізнатися відомості про те, як компанія розпоряджається їхніми даними, а також можливість вимагати видалення інформації про себе та зупинення її розповсюдження. За невиконання нормативних вимог закону передбачені значні штрафи, навіть, якщо компанія порушує законодавство через необережність. Таким чином, завдяки впровадженню цього Закону Каліфорнія підвищила дисциплінованість та відповідальність юридичних осіб під час збирання та обробки персональних даних фізичних осіб [8].

Так, у 2012 році в Індонезії уряд схвалив нормативний акт, спрямований на дотримання вимог державними організаціями, установами та закладами, які надають відповідні електронні послуги, зокрема створення центрів обробки даних на території цієї країни. Встановлено, що експлуатація державної електронної операційної системи передбачає створення Центру аварійного реагування. Окрім того, Міністерство зв'язку цієї країни запровадило загальну вимогу щодо функціонування Центрів обробки даних для більш широкого кола державних інституцій, які використовують інформаційні

технології з метою надання відповідних послуг громадянам. Також електронний системний оператор має забезпечити зберігання даних про усі трансакції в Індонезії. Вимога щодо зберігання персональних даних між постачальниками електронних систем та їх клієнтами в Індонезії застосовується як приватними, так і публічними постачальниками електронних систем.

У Малайзії Законом про захист персональних даних ще з 2010 року запроваджено заборону на передачу персональних даних за межі країни. Транскордонна передача персональних даних можлива лише за умови виконання певних передумов і тільки у виключних випадках. За фабулою Закону повинна бути отримана згода суб'єктів персональних даних, якщо існує необхідність виконання договору між суб'єктом та оператором, який було укладено за запитом або в інтересах суб'єкта персональних даних.

В Індії, згідно із засадами державної інформаційної політики, обробка усіх даних, які зібрані з використанням державних ресурсів, має віжбуватися виключно на території Індії. Також встановлена вимога щодо провайдерів послуг електронної пошти стосовно розміщення своїх серверів тільки у цій країні. В сучасних умовах у рамках закону Індії про телекомунікації, уся інформація про клієнтів та користувачів, окрім інформації про наданий роумінг, повинна зберігатися тільки у межах цієї країни, а віддалений доступ до такої інформації заборонений з-за кордону.

В Узбекистані у 2019 році набули чинності зміни до законодавства про персональні дані, що зобов'язують зберігати такі дані виключно на території цієї країни. Законодавчо встановлено, що персональні дані громадян повинні оброблюватися на технічних засобах та пристроях, які фізично розташовані на території Узбекистану та зареєстровані у відповідному Державному реєстрі. Вимоги щодо локалізації даних поширюються на обробку даних з використанням інформаційних технологій, у тому числі й за допомогою мережі Інтернет. Нормативний обов'язок щодо зберігання даних покладається на володільця або оператора бази даних, при цьому володільцем є власник бази даних, а оператором – особа, яка обробляє персональні дані. Вимога щодо локалізації передбачає збір, систематизацію та зберігання персональних даних.

Згідно із Законом Узбекистану "Про персональні дані", який набув чинності 1 жовтня 2019 року, персональні дані – це зафіксована на електронному, паперовому або іншому матеріальному носії інформація, яка відноситься до певної фізичної або юридичної особи, яка надає змогу провести її ідентифікацію. Запроваджено систему санкцій за порушення законодавства про локалізацію персональних даних, включаючи настання кримінальної відповідальності – позбавлення волі на строк до 3 років. Законом покладено обов'язок щодо локалізації серверів з персональними даними виключно на території Узбекистану.

У Казахстані Закон "Про персональні дані" був прийнятий у 2013 році, а у 2015 році до нього були внесені зміни у зв'язку із запровадженням загальної вимоги про зберігання (локалізацію) персональних даних у цій країні. Вимога щодо зберігання персональних даних у Казахстані набула чинності з 1 січня 2016 року. Хоча у Законі відсутні вимоги щодо передачі персональних даних до інших держав світу, у випадку передачі даних за кордон, обов'язковим є копіювання та зберігання такої інформації на серверах на території Казахстану. У Казахстані Законом "Про персональні дані" передбачається як адміністративна, так і кримінальна відповідальність за порушення вимог щодо їхнього захисту. Під санкції підпадають дії, спрямовані на незаконний збір, обробку персональних даних, недотримання власником, оператором або третьою особою заходів щодо захисту таких даних, несвоєчасне забезпечення власником або

володільцем інформаційних систем, які містять персональні дані заходів щодо їх фізичного захисту тощо. Кримінальна відповідальність настає у випадку спричинення значної шкоди правам та законним інтересам особам в результаті незаконного збору або обробки персональних даних. Законодавчо встановлено, що зберігання є активною поведінкою суб'єкта щодо повноцінного забезпечення одночасно приватності й конфіденційності персональних даних.

Загальновідомо, що до персональних даних відносяться: стан здоров'я, розмір заробітної плати, інша інформація, яка не підлягає розголошенню у форматі тексту, фотографій або відео. Інформація про релігійну належність, світогляд, політичні переконання, стиль приватного життя, дані про судимість та стан здоров'я є спеціальними персональними даними та їхня обробка забороняється, крім випадків власного навмисного поширення у загальнодоступних джерелах. Більшість сервісів як мінімум оброблюють персональні дані – мобільні оператори, Інтернет-магазини, соціальні мережі, пошукові системи тощо. Наприклад, кожен раз, коли людина здійснює у сервісах "Google" будь-які дії, ця компанія автоматично збирає та зберігає дані про неї. Аналіз нормативних актів різних країн світу засвідчує, що оптимальним рішенням локалізації даних є перенесення персональних даних, їхня обробка, збір та зберігання з використанням можливостей саме дата-центрів або буферного серверу у межах певної країни.

В сучасних умовах отримав світове схвалення та визнання сервіс "InCountry" [9]. Він став першим постачальником послуг з локалізацією масивів даних, який надає змогу впроваджувати свою послугу навколо світу, управляти даними у понад 90 країнах. Завдяки цьому сервісу надійно зберігаються персональні відомості у межах національних кордонів. Геопросторові дані між браузерами користувачів та веб-додатками глобально проксируються через смуги присутності у чітко визначених країнах.

Сервіс "InCountry" пропонує швидкі та ефективні рішення з метою інтеграції персональних даних. Його впровадження сприяє локалізації даних та є оптимальним рішенням для компаній, які прагнуть здійснювати масштабування та повинні дотримуватися законодавчих вимог щодо зберігання персональних даних. Повноцінна робота з постачальниками послуг у форматі "InCountry" є запорукою гарантування, що інформація буде збиратися, оброблюватися та зберігатися у відповідності до національних вимог й стандартів тієї чи іншої країни. За допомогою сервісу "InCountry" до персональних даних, які можуть збиратися та оброблятися відносяться: дані про співробітників, фінансові й податкові дані, дані про стан здоров'я, платіжні дані.

Підтримка локалізації даних дає два потужних сигнали: по-перше, бізнес підтримує локалізацію даних та поважає конфіденційність; по-друге, цей сервіс відповідає встановленим регіональним вимогам захисту даних та конфіденційності.

Загалом локалізація даних має різноманітні форми, у той час як деякі країни запроваджують повну заборону на таку передачу даних, багато з них відносяться до конкретних секторів, включаючи особисті та фінансові дані, податкові та медичні відомості тощо. Сервіс "InCountry" підтримується глобальними компаніями, які стикаються з обмеженнями встановленими регіональними законами про забезпечення конфіденційності, тому партнерство з "InCountry" – найшвидший спосіб дотримуватися нормативних правил розміщення даних.

Практика застосування чинного законодавства переконливо свідчить про недостатню ефективність існуючих заходів реагування на правопорушення у сфері інформаційних технологій та поширення інформації в інформаційно-комунікаційних мережах. У зв'язку з цим політичне керівництво провідних держав світу посилює заходи

відповідальності за порушення у сфері обробки даних та поширення інформації з урахуванням кращих практик міжнародного та зарубіжного досвіду у цій площині.

Так, у Німеччині за порушення провайдерами телекомунікаційних послуг запитів про передачу інформації, що запитується, у тому числі й у випадку порушення механізмів шифрування, уповноважений компетентний орган може накласти штраф у розмірі до 500 тис. Євро, частково або повністю зупинити діяльність провайдера.

У Великобританії штраф за порушення вимог уповноважених органів складає до 50 тис. фунтів, а також передбачена кримінальна відповідальність до двох років тюремного ув'язнення.

У Туреччині законодавчо встановлений штраф за невиконання норм про умови зберігання інформації та організації доступу до неї у розмірі до 100 тис. турецьких лір, відмова обмежити доступ до інформації – до 300 тис. турецьких лір.

У 2019 році в Росії був схвалений Федеральний Закон про введення штрафів за порушення вимог локалізації обробки персональних даних громадян. Законом передбачено, що за перше порушення вимог про локалізацію компанія, яка обробляє дані громадян РФ, може бути піддана штрафу на 2-6 млн. російських рублів, а за повторне – 6-18 млн. російських рублів. Альтернативою штрафів є можливість внесення доменних імен та мережевих адресатів у реєстр порушників прав суб'єктів персональних даних. Відповідно до нормативних вимог про локалізацію, під час збору персональних даних, у тому числі й з використанням мережі Інтернет, оператор зобов'язаний забезпечити запис, систематизацію, накопичення, зберігання та уточнення (оновлення, зміна) персональних даних. Вимоги про виконання правил локалізації не є перепоною для передачі персональних даних в зарубіжні країни. Персональні дані першочергово вносяться до бази даних на території РФ та актуалізуються, а згодом можуть надалі передаватися до баз даних, які розташовані за межами РФ. Головне завдання, щоб під час такої передачі виконувалися загальні вимоги щодо транскордонної передачі персональних даних (наприклад, для передачі даних до США необхідно отримати письмову згоду відповідного суб'єкта). Вимога про локалізацію даних застосовується до іноземних компаній без фізичної присутності у РФ, якщо вони проводять діяльність у цій країні. Так, наприклад, Інтернет-сайт вважається таким, що проводить діяльність у РФ у таких випадках: сайт використовує доменне ім'я, пов'язане з РФ, сайт має російськомовну версію, сайт надає можливість сплачувати за товар у російських рублях; на сайті можливо укласти договори з виконавцем у РФ, на сайті ведеться реклама російською мовою, інші обставини, які переконливо демонструють інтерес власника сайтів до аудиторії. Технічно закон про локалізацію даних застосовується до усіх російських компаній, філій та представництв іноземних компаній та корпорацій, має відношення до інших юридичних осіб, поширюється на операторів, зареєстрованих за межами РФ, які не мають офіційної присутностіі, проте здійснюють господарську діяльність на місцевих ІТ-ринках.

Також слід вказати, що чимало іноземних ІТ-холдингів стикаються з проблемою локалізації персональних даних, коли постає питання щодо їхнього використання головною організацією, тобто материнською компанією, яка перебуває за кордоном тієї чи іншої країни, тобто поза межами її юрисдикції. У такому випадку важливо розуміти спектр заходів, які можуть здійснюватися щодо захисту персональних даних за кордоном в умовах забезпечення нормативного процесу суцільної локалізації.

На цьому фоні актуальною проблемою залишаються передачі персональних даних за допомогою аутсорсингової компанії. Останнім часом, послуги аутсорсингу стають дедаля більш затребуваними. Однак, здійснюючи передачу провайдеру певних функцій, досить часто йому передають доступ до персональних даних, у зв'язку з чим постає

питання щодо виконання провайдером правил їх локалізації, оскільки він не є відповідальним за збереження та захист персональних даних. Так, якщо компанія-оператор персональних даних надає аутсорсинговій компанії тільки виключно доступ до своїх баз даних для виконання певних функцій за договором (наприклад, для здійснення рекламних розсилок), то у цьому випадку відповідальність щодо захисту персональних даних покладається на замовника. У випадку, коли компанія передає свою базу даних організації-аутсорсеру (наприклад, у випадку надання бухгалтерських послуг), то у договорі необхідно вказати про права провайдера щодо аутсорсингових послуг та визначити його обов'язки щодо застосування заходів захисту отриманих персональних даних та конфіденційності інформації. У такому випадку саме аутсорсингова компанія стає оператором персональних даних, який зобов'язаний дотримуватися нормативних вимог про їх локалізацію.

Висновки.

1. Тренди на світових ринках кібербезпеки формуються під впливом динамічного розвитку міжнародного та національного законодавства й масштабів поширення загроз. Локалізація персональних даних та окремих процесів обробки персональних даних – необхідна вимога сучасності. На цьому фоні кожна держава світу здійснює активну законотворчу роботу, яка нормативно спрямовується на розробку та впровадження додаткових вимог, у першу чергу, щодо посилення захисту та локалізації персональних даних в інформаційних та інформаційно-комунікаційних системах, впровадження нормативних вимог та правил у сфері локалізації персональних даних. Посилаючись на позитивний зарубіжний досвід, можно констатувати, що усі компанії – постачальники електронних послуг зобов'язані локалізувати свої сервери, у іншому випадку настають санкції – штрафи та блокування їх роботи, формування державою "чорних списків" провайдерів.

Узагальнючи викладене, можна визначити важливі кроки, які фіксуються у законодавствах передових країн світу, практична реалізація яких сприятиме активізації процесів локалізації персональних даних у межах національних кордонів, зокрема, це:

- проведення інвентаризації усіх інформаційних систем або баз даних;
- визначення місця знаходження інформаційних систем та баз даних, їхніх серверів за принципом екстериторіальності, оскільки обов'язкова вимога щодо локалізації персональних даних означає, що саме на території відповідної держави має відбуватися первинний збір таких даних, хоча обробка та зберігання ймовірно можуть здійснюватися й за кордоном;
- запровадження штрафів та санкцій з посиленням відповідальності порушників нормативних вимог.

2. Для України в сучасних реаліях масштабного переходу на дистанційний режим роботи в умовах пандемії коронавірусу та запровадження локдауну, тематика локалізації персональних даних є досить актуальною.

Вітчизняні суб'єкти господарювання й підприємці, які використовують відповідні сервіси, збирають персональні дані українців, навіть не повідомляючи останніх про те, що їхні дані досить часто передаються за кордон. Більш того, особи, які використовують такі сервіси у власній діяльності, зазвичай не мають будь-яких внутрішніх норм про обробку даних, обмеження щодо кола осіб, які мають доступ до таких даних. Такі особи іноді не дуже звертають увагу на проблеми захисту персональних даних. Переважно суб'єкти даних не обізнані про те, як використовують і поширюють їхні дані, або взагалі не мають відомостей, у які країни їх дані передаються й, звичайно, де перебувають відповідні сервери.

Отже, з точки зору вимог вітчизняного законодавства, досить часто відбуваються його порушення, що потребує посилення відповідальності за недотримання нормативів приватності та конфіденційності персональних даних.

На практиці мінімізація ризиків здійснюється наступним чином: локалізація відповідного сервісу; розроблення належної документації в сфері обробки персональних даних; постійний контент-аналіз процесу здійснення обробки персональних даних. З цією метою доцільно періодично проводити аудит порядку обробки персональних даних для усунення недоліків, якщо такі були виявлені.

За таких умов, потребує удосконалення Закон України "Про захист персональних даних" з урахуванням: загальносвітових тенденцій посилення спроможностей держав у напрямку суцільної локалізації персональних даних; встановлення більш жорстких правил щодо забезпечення приватності та конфіденційності, які відповідають нормативним стандартам захисту персональних даних у державах-членах ЄС; посилення штрафних санкцій за порушення законодавчих вимог приватності та конфіденційності.

Використана література

1. Защита персональных данных / В. Брыжко, Ю. Базанов та ін. Київ: Национальное агентство по вопросам информатизации при Президенте Украины, 1998 г. 128 с.; Права человека и защита персональных данных / В. Брыжко, Ю. Базанов та ін. – (Государственный комитет связи и информатизации Украины). Харьков: Фолио, 2000. 280 с.; Становлення і розвиток правових основ та системи захисту персональних даних в Україні / В.Г. Пилипчук, В.М. Брижко та ін.: монографія. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

2. Гуйван П.Д. Особливості національного та міжнародного регулювання обробки окремих категорій персональних даних. *Журнал європейського і порівняльного права.* 2018. № 2. С. 42-56.

3. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 97-103. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_18

4. Обуховська Т.М. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. *Вісник Національної академії державного управління при Президентові України*. 2014. № 1. С. 95-103. URL: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_17

5. Тарасюк А.В. Вплив загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України. *Інформація і право*. №1(24)/2018. С. 28-35.

6. The General Data Protection Regulation (GDPR). URL: https://ec.europa.eu/info/law/law-topic/data-protection_en; – (переклад) Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

7. Брижко В.М., Пилипчук В.Г. Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми. *Інформація і право*. № 1(36)/2021. С. 17-28.

8. Фісун В. Проблеми захисту персональних даних: досвід України та інших країн. *Юридична газета*. 2020. № 10 (716). URL: https://yur-gazeta.com/publications/practice/informaciyne - pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html

9. Global Apps, Local Compliance. URL: https://incountry.com

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 347.121.1

ГОЛОВКО О.М., *кандидат юридичних наук,* старший науковий співробітник
Інституту інформації, безпеки і права НАПрН України,
старший викладач кафедри публічного права
НТУУ "КПІ ім. Ігоря Сікорського".

ПРАВОВІ ЗАСАДИ ПРОТИДІЇ МОВІ ВОРОЖНЕЧІ: РЕТРОСПЕКТИВНИЙ ОГЛЯД ТА АНАЛІЗ ПЕРСПЕКТИВ

Анотація. *В статті представлено ретроспективний огляд українського законодавства та аналіз перспектив законотворчого процесу щодо протидії мові ворожнечі, в тому числі в медіапросторі. Представлено критерії для кваліфікації hate speech злочинного спрямування та інших, які не є кримінально караними, які тягнуть за собою юридичну відповідальність або без такої. Висновки зроблені з огляду на європейську практику класифікації злочинів на ґрунті ненависті. Встановлено, що в основі формування законодавства з протидії мові ворожнечі має бути визнання людини найвищою соціальною цінністю, незалежно від тих особливостей, які роблять її не схожою на інших. Виявлено проблематику нових проектів законів, що покликані протидіяти мові ворожнечі в медіапросторі.*

Ключові слова: *права людини, інформаційна безпека, мова ворожнечі, злочини ненависті, дискримінація.*

Summary. *The article reflects the retrospective review of Ukrainian legislation and an analysis of the prospects of the lawmaking process on countering hate speech, including in the media space. Criteria for the hate speech and other non-criminal criminal qualification, which entail legal liability or without one, are presented. The conclusions are drawn from the European practice of classifying hate crimes. It has been established that the basis of legislation to combat hate speech should be recognition of the highest social value of a person, regardless of those features that make him or her unlike any other. The problems of new draft laws aimed at counteracting hate speech in the media space have been identified.*

Keywords: *human rights, information security, hate speech, hate crimes, discrimination.*

Аннотация. *В статье представлен ретроспективный обзор украинского законодательства и анализ перспектив законотворческого процесса по противодействию языку вражды, в том числе в медиапространстве. Представлены критерии для квалификации hate speech преступной направленности и других, которые не являются уголовно наказуемыми, и которые влекут за собой юридическую ответственность или без таковой. Выводы сделаны с учетом европейской практики классификации преступлений на почве ненависти. Установлено, что в основе формирования законодательства по противодействию языку вражды должно быть признание человека высшей социальной ценностью, независимо от тех особенностей, которые делают ее не похожей на других. Выявлено проблематику новых проектов законов, призванных противодействовать языку вражды в медиапространстве.*

Ключевые слова: *права человека, информационная безопасность, язык вражды, преступления ненависти, дискриминация.*

Постановка проблеми. В юридичній англомовній літературі існує та використовуються словосполучення *hate crimes* (укр. – "злочин ненависті") та *hate speech* (укр. – "мова ворожнечі"). На відміну від *hate crimes*, "мова ворожнечі" рідко розглядається в правому контексті національного законодавства України, оскільки має міждисциплінарний характер. Як поняття "мова ворожнечі" не закріплено в

національному законодавстві України, хоча має своє відображення в деяких нормативно-правових актах з огляду на взяті державою Україна міжнародні зобов'язання, зокрема, з протидії дискримінації та різним видам ксенофобії (ратифікація Україною Міжнародної конвенції про ліквідацію всіх форм расової дискримінації, Міжнародний пакт про громадянські та політичні права). При цьому, вказане узгоджується з Конституцією України як основного закону держави, в якій зазначено засади рівності всіх громадян України перед законом. Саме тому протидія такому негативному явищу як "мова ворожнечі" має здійснюватись правовими інструментами, дослідженню яких присвячена ця стаття*.

Результати аналізу наукових публікацій. Теоретичною основою цієї роботи стали національні та міжнародні нормативно-правові акти, а також думки відомих вчених з питань, пов'язаних з тематикою дослідження. У науковому дослідженні використовуються праці таких науковців як Бенедек Ф., Бєляков К.І., Дзьобань О.П., Долуда В.В., Золотар О.О., Кеттеман М., Мануйлов Є.М., Онупрієнко С. Г., Шопіна І. М. та інші.

Метою статті є визначення правових засад протидії мові ворожнечі на національному рівні та з урахуванням європейської практики.

Виклад основного матеріалу. "Мова ворожнечі" (*hate speech)* визначається в юридичній літературі як мова, яка виражає (або прагне сприяти, або потенційно підвищує) ненависть по відношенню до людини або групи людей за певною особливістю, яка їм належить [1]. Іншими словами, це мова, яка використовується для вираження ненависті до цільової групи або має намір принизити чи образити членів групи [2]. В деяких підходах використовується поняття групової ідентичності, де мова ворожнечі – це навмисна атака на конкретну групу людей, мотивована особливостями цієї групи [3]. З огляду на визначення, прояв мови ворожнечі можливий з огляду на наявні соціальні зв'язки з позицій приналежності людини до певної соціальної групи за конкретною ознакою (колір шкіри, національність, гендер, мовна ознака тощо).

Цікавим видається підхід Американської асоціації адвокатів, яка не дає офіційного визначення "мови ворожнечі", однак тлумачить її як мову, яка сприяє злочинному діянню та може бути покарана як частина "злочину ненависті" – *hate crimes* [4]. Такий підхід відрізняється від попередніх, адже передбачає наявність завданої шкоди або намір завдати її в результаті застосування мови ворожнечі.

Згідно статті 3 Конституції України: "Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визначаються в Україні найвищою соціальною цінністю" [5]. Тобто, цей правовий припис визначає Україну як людиноцентристську державу, головним обов'язком якої є забезпечення прав і свобод конкретної людини за умов врахування загроз для інших людей.

Відповідно до положень статті 24 Конституції України визначено засади рівності всіх громадян України перед законом. Серед положень цієї статті встановлено: "Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних,

* *Примітка.* Статтю створено на підставі дослідження проведеного в межах виконання міжнародного проекту в сфері освіти "European Integration: legislation and the IoT" ("Європейська інтеграція: законодавство та Інтернет речей") у межах напряму Жан Моне "Модуль" програми "Erasmus+" №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проект НТУУ "КПІ ім. Ігоря Сікорського", Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС). Підтримка Європейською комісією випуску цієї роботи не означає схвалення змісту, який відображає лише думки авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься в ній.

релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками" [5] .

По суті, Конституцією чітко встановлений об'єкт охорони та захисту з боку держави, що корелює з тим, що визначено Кодексом України про адміністративні правопорушення та Кримінальним кодексом України.

Правовим ядром охорони та захисту від посягань, спричинених мовою ворожнечі, є Кримінальний кодекс України (далі – КК України), а саме стаття 161 "Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками" [6]. За роки незалежності вона зазнала ряду змін, на яких варто зосередитись окремо, оскільки є рефлексією на ставлення в державі до правопорушень на ґрунті ненависті та фактичним визнанням *hate speech* передумовою для *hate crimes*.

Станом на момент прийняття КК України від 5 квітня 2001 року, зазначена стаття була сформульована як діяння у вигляді порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії. Законом України від 05.11.09 р. № 1707-VI та від 18.06.14 р. № 1519-VII до неї було внесено зміни та доповнення як в частині опису даного діяння (диспозиції), так і в частині виду та розміру кримінальної відповідальності за його вчинення (санкції).

В 2008 році було винесено на розгляд та обговорення проект закону України "Про внесення змін до Кримінального кодексу України щодо відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості" [7]. В результаті зміни було внесене до статей 115 (Умисне вбивство), 121 (Умисне тяжке тілесне ушкодження), 122 (Умисне середньої тяжкості тілесне ушкодження), 126 (Побої і мордування), 127 (Катування), 129 (Погроза вбивством), 161 (Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками), 300 (Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості) в частині включення законодавцем мотиву расової, національної чи релігійної нетерпимості як обтяжуючої ознаки злочину.

Серед запропонованих змін до ст. 161 КК України було підняті питання заміни слова "громадянин" на "людина", адже потерпілим від цього злочину може стати будь-хто незалежно від правової приналежності до певної держави. Однак, відповідно до висновку Головного науково-експертного управління на даний проект від 30.07.08 р., заміна у тексті ст. 161 КК України слова "громадян" словом "людей" визначено зайвим, оскільки "у доктрині кримінального права та на практиці на даний час вжите у цій статті слово "громадян" розуміється у тому сенсі, що потерпілими від даного злочину можуть бути як громадяни України, так і іноземці або особи без громадянства" [8]. Проблема цієї аргументації в непотрібності заміни потерпілого даної статті з категорії "громадянин" категорією "людина" є досить сумнівною, адже вносить нове оціночне поняття про сприйняття чітко визначеної правової категорії. Завдання будь-якого нормативно-правового акту – врегулювати найважливіші суспільні відносини таким чином, щоб в матеріально-правовій нормі не було можливості довільного трактування, адже це створює додаткові загрози для уникнення правопорушником відповідальності. Таким чином, думка законодавця у прийнятті даних змін є очевидною, адже оціночні поняття та судження ускладнюють процес встановлення справедливості.

По суті, до цих змін в антидискримінаційній нормі містився дискримінаційний аспект, оскільки потерпілим могла бути тільки та особа, яка є громадянином, тобто має стійкий правовий зв'язок з державою. Виходячи з того, що йдеться про статтю КК України, потерпілим за старою нормою міг бути тільки громадян України.

Ініціатори даних змін до КК України зробили акцент на зафіксовані станом на початок 2008 року 29 інцидентів з учиненням насильства над іноземцями в Україні. Як було зазначено в супровідній записці до проекту закону України "Про внесення змін до Кримінального кодексу України (щодо відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості)" – "на думку міжнародних експертів такі злочини мали потенційну можливість бути кваліфікованими як ті, що вчинені з мотивів расової нетерпимості чи ксенофобії". Кількість подібних проявів станом на дату внесення цих змін перевищувала аналогічну статистику за весь 2007 рік. При цьому "абсолютна більшість випадків не фіксуються правоохоронними структурами або ж жертви не звертаються до органів МВС у зв'язку з відсутністю надії на реагування" [9].

Така офіційна думка додатково підкреслює латентний характер злочинів, мотивованих расовою, національною чи релігійною нетерпимістю. Окрім цього, дана категорія злочинів є специфічною напрямом діяльності представників організованої злочинності, відповідальність за яку передбачена, зокрема, в ч. 3 ст. 161 КК України. Через підвищення загрози такої діяльності виникла пропозиція з підвищення меж покарання за цей злочин:

1) До внесення змін від 05.11.2009 р. санкція передбачала – позбавлення волі на строк від 2 до 5 років.

2) Пропозиція ініціаторів внесення змін до цієї статті – позбавлення волі на строк від 3 до 10 років.

3) Після внесення змін від 05.11.2009 р. – від 5 до 8 років.

Через призму аналізу цієї правової норми (ч. 3 ст. 161 КК України) бачимо разючу зміну в підході законодавця до юридичної відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості. Вона виявляється в тому, що пропозиція змін виглядала досить суворою, оскільки передбачала кардинальне підвищення мінімальної та максимальної меж покарання за даний злочин. Втім, результатом обговорення став альтернативний варіант з підвищення максимальної межі до п'яти років, одна зменшення мінімальної строком до 8 років позбавлення волі. Результатом таких змін стала відносна постійність санкцій даної статті, адже їх не було змінено з 2009 до 2020 року, що вказує на доцільність прийнятого компромісного рішення з встановлення чинної досі санкції.

Втім, наразі виникають нові загрози, пов'язані з розпалюванням ворожнечі в медіапросторі, які є реальним провокуючим чинником до збільшення показників злочинів ненависті. Задля реагування на них в тому числі розпочата активна законотворча діяльність, пов'язана з реформуванням діяльності ЗМІ, що становить окрему частину цього дослідження. На основі попередніх досліджень дефініції "медіапростір" було запропоновано розглядати його як динамічну віртуальну систему, яка складається з масових дистанційних комунікацій, що функціонує в умовах наявного медіадискурсу, задовольняючи інформаційні потреби споживача [10, с. 145]. Ознака віртуальності медіапростору є ключовою в даному визначенні, оскільки відмежовує його від простору фізичного, однак вказує на їх взаємозв'язок через здатність медіа задовольнити інформаційні потреби споживача. Ця здатність становить в собі загрози, які мають бути попереджені правовими засобами. Серед цих загроз значне місце посідає саме мова ворожнечі.

Окремої уваги потребують прояви мови ворожнечі у віртуальному просторі не тільки з боку представників медіа, однак і звичайних користувачів соціальних мереж. Існує думка, що соціальні медіа сприяють антисоціальній поведінці, включаючи домагання в Інтернеті (*online harassment*), кібербулінг (*cyberbullying*) та мову ненависті [11]. Дійсно, прояви ненависті у Всесвітній мережі Інтернет можна визначити через

категорії кібер-ненависті (*cyberhate*) та кібербулінгу, що по суті охоплюють категорію мови ворожнечі зі специфікою у її просторовому вираженні.

Варто розглянути мову ворожнечі через призму актуальної нині проблеми у світі – спалаху COVID-19.

З початку лютого 2020 року у Великобританії було зафіксовано та знаходиться у провадженні North Yorkshire Police чотири расистські випадки, пов'язані із спалахом коронавірусу; посол Китаю у Великобританії засудив "ненависть" до китайців після спалаху [12]. Незважаючи на лише чотири підтверджені випадки COVID-19 у Великобританії, китайська громада відзначила помітно расистську реакцію на світову кризу в галузі охорони здоров'я; китайський центр Манчестера отримав безліч скарг на расистські інциденти, що стосуються дітей у школах по всьому регіону [13].

Таким чином, випадки прояву мови ворожнечі за ознакою приналежності до нації, в країні якої вірус було виявлено першим, спричинило хвилю ненависті до конкретної соціальної групи, викликаної страхом зараження. Результатом цього стали випадки прояву агресії до представників зазначеної групи. Почуття страху зараження COVID-19 підсилюється повідомленнями, отриманими зі ЗМІ, що може провокувати вкрай непередбачувану реакцію споживачів такої інформації.

Більше того, існує підхід до тлумачення злочинів на ґрунті ненависті як комунікативних дій, які часто провокуються негативними соціальними подіями, що підбурюють прагненням до помсти певній групі осіб, яка має схожі характеристики з "винними" у цих негативних подіях [14]. Дана теорія підтверджується спалахом ворожої реакції до осіб азіатського походження за зовнішністю, які фактично могли ніколи не бути в Китаї та мати від народження громадянство іншої держави. Однак, це не зупиняє ворожо налаштованих осіб, у яких китайці викликають асоціацію з поширенням COVID-19. Дискурс ворожнечі, як і в будь-якому конфлікті досягає ескалації, а потім йде на спад. Проблематика використання соціальних мереж в даному контексті може штучно спричиняти провокування та продовження періоду ескалації.

Окрім цього, неможливо не зробити акцент на резонансному рішенні Верховного Суду у складі колегії суддів Першої судової палати Касаційного цивільного суду, який набрав законної сили 10 березня 2021 року по Справі № 331/5291/19 щодо відсторонення дитини позивачки від занять у зв'язку із відсутністю щеплень, встановлених законом [15]. Позивачка уважала, що ст. 15 Закону України "Про захист населення від інфекційних хвороб" є дискримінаційною. Мова йде про заборону відвідувати дитячий заклад дітям, які не отримали профілактичних щеплень згідно з календарем щеплень. На перший погляд здається, що така норма обмежує право дитини на освіту, адже вона не допускається до навчального закладу. Окрім цього, можливо, певні щеплення не рекомендовано робити дитині з певними вадами здоров'я, оскільки це може спричинити погіршення її загального стану. З іншого боку, в мотивувальній частині рішення Верховного Суду зазначено, що завданням держави є забезпечення дотримання оптимального балансу між реалізацією права дитини на освіту та інтересами інших дітей. Ще одним аргументом на користь відсутності дискримінації в цьому положенні закону є те, що ст. 9 Закону України "Про освіту" визначено право обрати альтернативну форму отримання загальної середньої освіти у випадку, якщо реалізація очної форми навчання є неможливою. Тобто наявність альтернативи говорить про можливість реалізації права дитини на освіту іншим шляхом, який є безпечним для всіх учасників навчального процесу.

І хоча з точку зору закону рішення Верховного Суду є абсолютно аргументованим, однак вона викликало хвилю обурення серед населення саме з точки зору наявності мови ворожнечі з боку держави щодо не щеплених дітей. В даній ситуації, на нашу

думку, проблематика полягає не в наявності мови ворожнечі, а у відсутності інформаційної кампанії держави, зокрема, в медіапросторі щодо роз'яснення обґрунтованості даного рішення, яке відповідає вимогам закону.

Деякими дослідниками було виявлено, що Інтернет є новим спільним простором з формування так званої "колективної ідентичності" для раніше відокремлених груп ненависті, що може спричинити появу "глобальної расистської субкультури", якщо не реагувати на явище кібер-ненависті [16]. Інше дослідження доводить, що розширення та розвиток платформ соціальних медіа супроводжується збільшенням рівня кібер-ненависті [17], що, в свою чергу, підвищує ризики злочинів на ґрунті ненависті в реальному просторі.

Досить інноваційним в цьому контексті виглядає підхід Європейського суду з прав людини (далі – ЄСПЛ). У Справі "Buturugă v. Romania" була наявна скарга на діяння у вигляді кібер-переслідування (*cybertracing*) з боку чоловіка заявниці. Суд встановив порушення статті 3 Конвенції про захист прав людини і основоположних свобод (заборона нелюдського чи принизливого поводження) та статті 8 (право на повагу до приватного та сімейного життя та на листування), класифікувавши дії порушника як кібер-насильство. Суд зазначив, що в даний час кібербулінг вважається аспектом насильства, яке може набувати різноманітних форм, включаючи порушення конфіденційності, вторгнення в комп'ютер жертви, захоплення, обмін та маніпулювання даними та зображеннями, включаючи приватні дані [18].

Як зазначалось раніше, злочини з мотивів расової, національної чи релігійної нетерпимості мають латентний характер. Це пов'язано не тільки з тим, що жертви не заявляють про скоєне щодо них правопорушення з огляду на страх подальшого переслідування, однак і з тим, що не завжди виявляється реальний мотив скоєних злочинів як такий, що вчинений безпосередньо на ґрунті ненависті. З цього приводу доречно звернутися до розмежування мотивів вчинення злочину мірою їх домінування: 1) домінуючі (основні); 2) факультативні (додаткові) [19, с. 31-32]. Такий підхід не заохочується у доктрині кримінального права, оскільки використовує більше психологічні, аніж правові критерії оцінки вини злочинця, втім, на нашу думку, він може стати ключовим при виявленні та кваліфікації мотиву ненависті до представників певної соціальної групи.

Так, якщо в 2009 році акцент здійснювався на формуванні спеціального законодавчого врегулювання *hate crimes*, то зараз актуалізовано проблематику застосування специфічних організаційних зусиль при виявленні цього мотиву. Правова оцінка таких дій, яка включає кримінально-правову кваліфікацію потребує чіткого підходу для максимального усунення суб'єктивізму в юридичному аналізі певної ситуації. Так, на допомогу приходить європейська практика з розробки критеріїв виявлення та ідентифікації мови ворожнечі як такої, що спричинила або з високою вірогідністю могла спричинити злочини на ґрунті ненависті.

Так, найбільш вагомим видається Рабатський план дій щодо заборони пропаганди національної, расової чи релігійної ненависті [20]. Цей документ передбачає три підходи:

- мова ворожнечі як кримінально каране діяння (кримінальна відповідальність);
- мова ворожнечі, яка не становить загрози кримінального характеру, але може спричинити реакцію у вигляді цивільного позову або адміністративної санкції (цивільна, адміністративна, майнова відповідальність);
- мова ворожнечі, яка не породжує юридичної відповідальності, оскільки не передбачається законом, але викликає стурбованість щодо загрози толерантності, доброзичливості та повазі до прав інших людей.

Найбільш чіткими є критерії до першої групи діяння, пов'язаного з мовою ворожнечі, адже злочини на ґрунті ненависті становлять найбільшу загрозу для суспільства та людства в цілому. До цих критеріїв відносять:

1) зміст заяви, яка містить мову ворожнечі ставить певну соціальну групу у домінуючу позицію щодо іншої станом на час висловлювання (ознака "іншості" в негативній конотації щодо конкретної цільової групи);

2) статус особи, у висловлюванні якої наявна мова ворожнечі, адже він прямо пов'язаний із здатністю впливати на аудиторію (ознака публічності автора висловлювання);

3) наявність наміру особи підбурювати конкретну групу осіб, оскільки недбалість не може призвести до такого підбурювання, який передбачено в термінології статті 20 Міжнародного пакту – "Будь-який виступ на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства, повинен бути заборонений законом" (наявність прямого умислу на підбурення);

4) зміст і форма висловлювання, які є ключовими елементами для аналізу (контент та контекстуальна ознака, зокрема, врахування серйозності висловлювання);

5) ступінь поширення заяви, включаючи аналіз кількості аудиторії, до якої було подано заяву, способу її поширення, чи заява була публічною та доступною для широкої громадськості тощо (ознака публічності з позиції джерела висвітлення вислову, який містить мову ворожнечі);

6) можливість та невідворотність настання наслідків після заяви, які повинні бути оцінені державними органами в процесі її аналізу через призму стандарту розумності (передбачення юридичної відповідальності; оціночна категорія "розумності", яка виноситься на розсуд уповноважених органів).

Серед визначених ознак наявні як суб'єктивні (внутрішні), так і об'єктивні (зовнішні). Виходячи з аналізу даних критеріїв з позиції складу злочину здійснимо таке розмежування: до особи, яка безпосередньо вчиняє діяння (суб'єкта) в даному переліку віднесено критерій № 2; до внутрішнього ставлення особи до вчиненого діяння – № 1 – 5; до суспільних відносин, на які здійснено посягання (об'єкта) – № 1; до діяння, яке безпосередньо вчинено та його наслідків (об'єктивна сторона) – № 5, 6.

Даний аналіз дає змогу зробити висновок, що при кваліфікації злочину, ускладненого виявленням мотиву у вигляді певного виду ворожнечі робиться акцент саме на суб'єктивній стороні діяння, де найважливішим є виявлення наявності чи відсутності умислу особи.

Інший підхід до встановлення критеріїв виявлення мови ворожнечі представлений практикою ЄСПЛ. Прикладом є частина рішення "Заклики до насильства та "мови ненависті" по Справі "Perinçek v Switzerland" [21], де суд мав визначити: по-перше, чи були аналізовані висловлювання здійснені в умовах напруженого політичного чи соціального становища (збройні зіткнення, тюремні бунти, інтеграція іммігрантів, відносини з національними меншинами); по-друге, чи піддалися ці висловлювання тлумаченню та чи були вони розглянуті як у безпосередньому, так і в широкому контексті як такі, що містили прямі чи опосередковані заклики до насильства, ненависті, нетерпимості або їх виправдання (негативний контекст щодо цілих етнічних, релігійних та інших груп, пов'язування їх з терористичними актами, іншими злочинами, проголошенням їх зв'язку з поширенням соціально небезпечних інфекційних захворювань; прямі заклики до насильства щодо певної соціальної групи); спосіб та форма висловлювань та його здатність – пряма чи непряма – спричиняти шкідливі наслідки (у вигляді поезії, виборчих листівок; у ЗМІ та конкретних форматах передач,

наприклад, плюралістичного характеру телевізійна дискусія, що зменшило негативний ефект висловлювання; тримання символіки, яка передбачає мовчазну незгоду щодо масового заходу).

Як зазначено в пункті 208 Справи "Perinçek v Switzerland", у всіх зазначених випадках результат діяльності визначався саме взаємозв'язком між різними чинниками, а не будь-яким із них, розглянутими ізольовано. Таким чином, підхід ЄСПЛ до такого типу справ є особливо контекстний, що корелює з попередніми критеріями, представленими в Рабатському плані.

Більше того, підхід ЄСПЛ дає можливість визначити дві основні тенденції кваліфікації мови ворожнечі, які полягають у встановленні причинно-наслідкового зв'язку між злочинами ненависті та висловлюваннями, що їм передують, а також щодо обов'язкової наявності прямого чи непрямого умислу на розпалювання ворожнечі та/або провокування до вчинення hate crimes.

Дослідження практики ЄСПЛ стосовно випадків розпалювання мови ворожнечі через медіа дає можливість повернутися до підходів українського законодавця щодо попередження цього негативного явища.

Відповідно до ст. 28 Закону України "Про інформацію", серед ознак неприпустимості зловживання правом на інформацію виокремлено таку інформацію, яка не може бути використана для розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [22].

Відповідно до ч. 2 ст. 6 Закону України "Про телебачення і радіомовлення", не допускається використання телерадіоорганізацій для розпалювання національної, расової чи релігійної ворожнечі та ненависті та пропаганди винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження [23].

Як бачимо, цей перелік корелює з деякими критеріями детермінації мови ворожнечі, описаними вище.

Втім, 2019 – 2020 роки ознаменувалися новими підходами до регулювання діяльності ЗМІ. Це проявилось в ряді пропозицій у вигляді нових законопроектів. Одним з них став проект закону "Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації", винесений на публічне обговорення 20 січня 2020 року. Він містить нове для українського законодавства положення щодо мови ворожнечі. Відповідно до п. 2 ч. 4 ст. 26 проекту, запропоновано віднести *hate speech* до підставам для відмови у наданні та припиненні раніше наданої акредитації іноземного журналіста. Норма була б більш справедливою, якби застосовувалась і до українських журналістів урівнюючи їх в правах з іноземними колегами. Більше того, в цій нормі можна виявити ознаки упередженості до іноземних журналістів, що може становити ознаку нетерпимості на ґрунті громадянства та/або професійної діяльності, а тому проект потребує доопрацювання в цьому аспекті.

Проект закону "Про медіа" від 27 грудня 2019 року став ще одним актом, запропонованим законодавцем для розгляду на початку 2020 року. Відповідно до п. 2. ч. 1 ст. 37 даного проекту, на території України (в тому числі суб'єктам у сфері медіа) забороняється поширювати висловлювання, що розпалюють національну, расову чи релігійну ворожнечу чи ненависть до окремих осіб чи їх груп, що відповідає загальним положенням чинного законодавства, фактично дублюючи їх.

Ця норма також повторюється в п. 2 ч. 4 ст. 110 зазначеного проекту як "грубе порушення в межах відповідальності суб'єктів у сфері аудіовізуальних медіа". За змістом

даного проекту грубе порушення становить найвищий ступінь суспільної небезпеки, що також є спірним, адже суспільно-небезпечні діяння передбачені виключно в КК України, а отже поряд з цим проектом закону має бути внесено зміни до КК України, щоб дана норма реально могла діяти. Однак, саме потенційне визнання мови ворожнечі діянням, що становить найвищий ступінь суспільної небезпеки є позитивним явищем, особливо коли йдеться про джерела масової інформації. Підкреслимо кореляцію даного положення з міжнародними критеріями, зокрема в категорії поширення на аудиторію та загалом щодо ознаки публічності джерела інформації.

Новелою даного проекту є право на відповідь та спростування, що має особа у випадку, якщо відомості, поширені суб'єктом у сфері медіа призвели до приниження честі, гідності чи ділової репутації. Цікаво, що це право нівелюється, оскільки п. 3 ч. 7 ст. 44 проекту передбачено, що суб'єкт у сфері медіа може відмовити в поширенні спростування або відповіді у випадку, якщо його текст містить мову ворожнечі або іншу інформацію, поширення якої заборонено відповідно до чинного законодавства України. З огляду на те, що "мова ворожнечі" є оціночним поняттям та не має чітко окреслених критеріїв визначення виходить, що особа фактично позбавляється можливості встановлення об'єктивної істини через те, що суб'єкт у сфері медіа розцінив її повідомлення як мову ворожнечі. Тобто йдеться про порушення презумпції невинуватості, адже особа вважатиметься винною у прояві мови ворожнечі неналежним суб'єктом без наявних на те законних підстав. Дана норма є абсолютно неправомірною і має бути виключена задля усунення потенційних порушень, які легалізуються цією потенційною нормою. Жодна особа не може бути визнана винною у *hate speech* без рішення суду та належної на те процедури.

Окрім цього, п. 2 ч. 1 ст. 119 проекту передбачено обмеження щодо змісту інформації у медіа, пов'язаних зі збройною агресією, серед яких встановлено заборону на поширення "недостовірних матеріалів щодо збройної агресії та діянь держави-агресора (держави-окупанта), її посадових осіб, осіб та організацій, що контролюються державою-агресором (державою-окупантом), у разі, якщо наслідком цього є розпалювання ворожнечі та ненависті…". Проблематика такого формулювання також наявна, адже вона фактично дублює загальну норму про порушення у вигляді спричинення мови ворожнечі, однак постає проблема механізму реалізації цієї норми. Більш доречним в цій частині було б передбачити ознаку недостовірності матеріалів щодо збройної агресії як обтяжуючу ознаку при кваліфікації hate speech.

Таким чином, існує потреба в розробці чіткого механізму притягнення до кримінальної відповідальності за скоєння злочинів на ґрунті ненависті шляхом виявлення даного мотиву як основного чи додаткового. Окремої уваги потребує розробка критеріїв виявлення та оцінки мови ворожнечі судами, що створить умови для єдності в підходах до правової оцінки таких справ. Також, на обговорення спільноти правників та юристів варто винести питання встановлення адміністративної відповідальності за правопорушення на ґрунті ненависті.

Висновки.

Мова ворожнечі виступає підставою посилення потужності антагоністичних сил, мета яких – руйнування та знищення, війна не заради миру, а заради нової війни. Усвідомлення цього факту сприятиме відмежуванню користувача цифрових технологій від потоку ненависті, який має місце у соціальних мережах Інтернету, особливо, коли йдеться про політичні декларації та гострі соціально-економічні питання. Дуже важливим при цьому є те, що найбільш інтенсивної маніпуляції людина зазнає тоді, коли йдеться про загрозу її особистій безпеці, що може бути ключовим чинником у

поширенні масової ненависті до певних осіб або соціальних груп, які, як може вважати людина, на цю безпеку посягають.

Отже, завдання права та нормативно-правового упорядкування, як превентивних інструментів з врегулювання правовідносин, що можуть виникати через мову ворожнечі, полягає в попередженні злочинних посягань з мотивів расової, національної, релігійної та інших видів нетерпимості. Однозначно існує потреба в чіткому визначенні критеріїв правової оцінки мови ворожнечі. Підхід ЄСПЛ щодо цього вважається найбільш доречним з огляду на вже існуючу практику застосування цих критеріїв на різних видах правовідносин та правових конфліктах, що вже виникали в різних державах. Імплементація даних критеріїв у національну правозастосовну практику надасть можливість розмежовувати мову ворожнечі, яка потребує втручання держави, та передбачати чіткі межі серед видів юридичної відповідальності, що має бути застосована у справах, пов'язаних з *hate speech*, адже ця ознака може бути як основним, так і додатковим мотивом для вчинення протиправних дій. Окрім цього, розмежування мотиву на основний та додатковий може стати ключовим аспектом розмежування злочинів та адміністративних правопорушень, вчинених на ґрунті ненависті.

З огляду на це надважливим є формування відчуття відповідальності за мову ворожнечі, усвідомлення своїх висловлювань як таких, що можуть нанести шкоду, спричинити насилля, що може проявлятися через крайню форму – злочини ненависті. Необхідним є актуалізація загрози мови ворожнечі, в тому числі, у віртуальному просторі залежно від негативного забарвлення висловлювання, що містить мову ворожнечі; публічності автора висловлювання та платформи, на якій воно висвітлюється; адресата висловлювання у вигляді конкретної соціальної групи за певною ознакою; наявність умислу (прямого чи непрямого) на спричинення ворожнечі щодо конкретного адресата; зміст та форма висловлювання з урахуванням ступеня його значущості при формуванні суспільної думки; реальності та потенційності негативних наслідків.

Використана література

1. Herz M., Molnar P. The content and context of hate speech: Rethinking regulation and responses. Cambridge: Cambridge University Press, 2012. 544 p.

2. Davidson T., Warmsley D., Macy M. W., Ingmar W. Automated Hate Speech Detection and the Problem of Offensive Language. *ICWSM*. 2017. P. 512-515.

3. Ona G., Naiara P., Aitor G.-P., Montse C. Hate Speech Dataset from a White Supremacy Forum. In: 2nd Workshop on Abusive Language Online. 2018.

4. Wermiel, S.J. The Ongoing Challenge to Define Free Speech. *Human Rights Magazine*. 2018. № 43 (4). P. 1-4.

5. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 14.12.2020).

6. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 14.01.2021).

7. Про внесення змін до Кримінального кодексу України щодо відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості: Закон України від 05.11.09 р. № 1707-VI. URL: https://zakon.rada.gov.ua/laws/show/1707-17 (дата звернення: 07.02.2021).

8. Висновок Головного науково-експертного управління на проект закону України "Про внесення змін до Кримінального кодексу України (щодо відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості)" від 30.07.08 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=32154 (дата звернення: 07.02.2021).

9. Супровідна записка до проекту закону України “Про внесення змін до Кримінального кодексу України (щодо відповідальності за злочини з мотивів расової, національної чи релігійної нетерпимості)” від 28.03.08 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf 3511=32154 (дата звернення: 07.02.2021).

10. Головко О.М. Медіабезпека людини: засади інформаційно-правової політики: монографія. Київ: Видавничий дім “АртЕк”. 2019. 168 с.

11. Elsherief M., Nilizadeh S., Nguyen D., Vigna G., Belding E. Peer to Peer Hate: Hate Speech Instigators and Their Targets. Web and Social Media: materials of International AAAI Conference (ICWSM). 12 April, 2018. URL: https://arxiv.org/pdf/1804.04649.pdf (accessed 23 November 2019).

12. North Yorkshire Police probe racist coronavirus-related incidents. *BBC*. URL: https://www. bbc.com/news/uk-england-york-north-yorkshire-51407641 (дата звернення: 25.02.2020).

13. Chinese in UK report 'shocking' levels of racism after coronavirus outbreak. *The Guardian*. URL: https://www.theguardian.com/uk-news/2020/feb/09/chinese-in-uk-report-shocking-levels-of-racism -after-coronavirus-outbreak (дата звернення: 25.02.2020).

14. Hanes E., Stephen M. Hate Crime in the Wake of Terror Attacks: Evidence from 7/7 and 9/11. *Journal of Contemporary Criminal Justice*. 2014. № 30. P. 247-267.

15. Постанова Верховний Суду від 10 березня 2021 р., судова Справа № 331/5291/19. URL: https://reyestr.court.gov.ua/Review/95642825 (дата звернення: 30.03.2021).

16. Perry B., Olsson P. Cyberhate: The Globalisation of Hate. *Information & Communications Technology Law*. 2009. № 18. P. 185-199.

17. Williams M.L., Burnap P. Crime sensing with big data: The affordances and limitations of using open source communications to estimate crime patterns. *British Journal of Criminology*. 2015. № 57 (2). P. 320-340.

18. Judgment of the European Court of Human Rights in the case “Buturugă v. Romania” from 15 October 2020. Application no. 56867/15. Official web-page of the European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200842%22]} (accessed 12 February 2020).

19. Савченко А.В. Мотив і мотивація злочину. Київ: “Атіка”, 2002. 144 с.

20. Human Rights Council. Twenty-second session Agenda. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General from from 11 January 2013. The Office of the High Commissioner for Human Rights (UN Human Rights). URL: https://www.ohchr.org/Documents/Issues/Opinion/Seminar Rabat/Rabat_draft_outcome.pdf (accessed 13 December 2019).

21. Judgment of the European Court of Human Rights in the case “Perinçek v Switzerland” from 15 October 2020. Application no. 27510/08. Oficial web-page of the European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-158235%22]} (accessed 12 February 2020).

22. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. URL: https://zakon.rada. gov.ua/laws/show/2657-12 (дата звернення: 17.02.2020).

23. Про телебачення і радіомовлення: Закон України від 21.12.93 р. № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12 (дата звернення: 19.02.2020).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Правова інформатика

УДК 342.951

ГЛУЩЕНКО Б.І., старший судовий експерт Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-0731-1077.

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЕРЖАВНОГО СЕКТОРУ: КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *Окреслено загальносвітову тенденцію розвитку Хмарних технологій та сервісів. Розглянуто засади та пріоритети американської концепції "Cloud First". Досліджено моделі законодавчого забезпечення Хмарних технологій у передових зарубіжних країнах та КНР. Визначено особливості використання Хмарних сервісів для потреб державного сектору. Деталізовано шляхи розбудови вітчизняної композитної стратегії "Cloud First". Висвітлено концепти законодавчих ініціатив, присвячених розвитку Хмарних сервісів в Україні.*

Ключові слова: *цифрова трансформація, державний сектор, кіберзагроза, Хмарні технології, Хмарні послуги, державна політика, оператор Хмарних послуг, державне управління.*

Summary. *The global trend of development of cloud technologies and services is outlined. The principles and priorities of the American Cloud First concept are considered. The models of legislative support of cloud technologies (services) in the advanced foreign countries and the People's Republic of China are researched. Peculiarities of using cloud services for the needs of the public sector are determined. The directions of building the domestic composite Cloud First strategy are detailed. The concepts of domestic legislative initiatives dedicated to the development of cloud services in Ukraine are highlighted.*

Keywords: *digital transformation, public sector, cyber threat, Cloud Technologies, Cloud Services, state policy, Cloud Services operator, public administration.*

Аннотация. *Очерчена общемировая тенденция развития Облачных технологий и сервисов. Рассмотрены основы и приоритеты американской концепции "Cloud First". Исследованы модели законодательного обеспечения Облачных технологий в передовых зарубежных странах и КНР. Определены особенности использования Облачных сервисов для нужд государственного сектора. Детализированы направления развития отечественной композитной стратегии "Cloud First". Высветлены концепты законодательных инициатив, посвященных развитию Облачных сервисов в Украине.*

Ключевые слова: *цифровая трансформация, государственный сектор, киберугрозы, Облачные технологии, Облачные услуги, государственная политика, оператор Облачных услуг, государственное управление.*

Постановка проблеми. Впровадження Хмарних технологій (обчислень) та сервісів є загальносвітовою тенденцією динамічного економічного зростання. Використання Хмарних сервісів у державному секторі є запорукою успішного розвитку будь-якої країни сучасності, незалежно від географічного місця розташування у світовому геопросторі. Стрімка цифровізація призводить до необхідності інтеграції сфери державних послуг та узгодження роботи ІТ-систем у багатьох сферах держави, таких, як: освіта, охорона здоров'я, соціальна допомога, електронний уряд тощо.

Єдиним стратегічним рішенням, спрямованим на об'єднання цього конгломерату, у цій площині стали саме Хмарні технології та їх широкомасштабне використання у державному секторі. На цьому фоні спостерігається поступовий розвиток ринку Хмарних сервісів. Хмарні технології стали одним із найбільш динамічно зростаючих напрямків світового ІТ-ринку.

Оскільки цифрова трансформація розширює можливості несанкціонованого проникнення в корпоративні та державні мережі, тому як приватні компанії, так і державний сектор спрямовують власні зусилля та значні інвестиції саме у захищеність Хмарних технологій. Тому більшість Хмарних проектів реалізуються з урахуванням необхідності забезпечення сучасних стандартів безпеки. Для України актуальним залишається тенденційне використання Хмарних сервісів державними підприємствами та органами державної влади, оскільки у цьому напрямку здійснюються лише перші важливі та поступальні кроки. Проте в Україні все ще масово використовуються застарілі інструменти та методи побудови ІТ-інфраструктур, що уповільнює оперативність здійснення реального цифрового прогресу, а можливість повноцінного використання Хмарних сервісів як доступного інструменту для вирішення ІТ-потреб кожного підприємства та органу державної влади залишається, на жаль, далекою перспективою. Хмарний ринок стрімко розвивається, тому вже сьогодні необхідно прискорити регулювання та гармонізацію моделей використання Хмарних сервісів державними органами та підприємствами стратегічних галузей економіки у першу чергу.

Враховуючи викладене, актуальним та своєчасним є висвітлення успішних моделей законодавчого забезпечення Хмарних технологій (сервісів) у законодавстві передових зарубіжних країн в контексті необхідності прискорення опанування й адаптації кращих світових практик у вітчизняному форматі, особливо щодо посилення спроможностей держави у цьому напрямку.

Результати аналізу наукових публікацій. Хмарні технології та проблеми їх правового регулювання й використання досліджували у своїх працях: М. Вітер [1], О. Юдін [2], Н. Чігіна [3], Р. Скриньковський [4] та інші. Питання зарубіжного досвіду юридичного визначення та використання Хмарних технологій на науковому рівні розглядали: Ю. Носенко [5], Ю. Запорожченко [6], В. Брижко [7] тощо. Проте висвітлення кращих практик передового зарубіжного досвіду щодо запровадження державних програм у зазначеній сфері у працях вказаних авторів не здійснювалось, що посилює тематичну актуальність цієї публікації.

Метою статті є визначення особливостей та вірогідних моделей ефективного впровадження у практичну площину роботи державних інституцій Хмарних технологій в контексті інноваційної стратегії "Cloud First", яка знайшла своє відображення у відповідних новелах законодавства провідних зарубіжних країн.

Виклад основного матеріалу. Починаючи з 2011 року, провідні країни світу (США, Великобританія, Німеччина, Сінгапур, Індія, Республіка Корея, Австралія, Канада, Саудівська Аравія) розпочали впроваджувати стратегії цифрової трансформації, а технології Хмарних обчислень (Хмарні технології, сервіси) стали обов'язковим атрибутом та інструментом державного управління та складовою функціонування державного сектору.

Одним із базових фундаментів цих процесів стала американська концепція "Cloud First". Вперше вона з'явилася на початку XXI століття та суттєво простимулювала появу аналогічних революційних підходів до Хмарних технологій в інших кранах світу.

Загалом концепція "Cloud First" являє собою довгострокову програму як важливу складову державної політики, яка змінює моделі створення та споживання будь-яких ІТ

сервісів у держсекторі. Її концепти визначають поступовий перехід від закупівлі стандартного обладнання та програмного забезпечення до використання Хмарних сервісів, що виробляються приватним сектором, завдяки чому відбувається суттєва економія бюджетних коштів, включаються механізми забезпечення цифрового суверенітету. Практична реалізація концепції "Cloud First" сприятиме активізації залучення інвестицій в інформаційну інфраструктуру на усіх рівнях за рахунок приватного сектору, що забезпечує ефективну протидію зростаючим кіберзагрозам та географічне розподілення цифрових ресурсів держави. За таких умов формується сприятлива екосистема державно-приватного партнерства.

Концепця "Cloud First" була започаткована та розроблена уперше в США як комплексна ідея впровадження Хмарних технологій у сфері державного управління. Зародження цієї ідеї відбулося ще у 2002 році, коли стартував національний проект "E-Government", одним з елементів якого стали саме Хмарні технології. Проте потужний імпульс ця концепція отримала у 2010 році, коли співробітник адміністрації Президента США В. Кундра виступив з ініціативою, яка згодом отримала назву "Cloud First". Змістом цієї концепції стала масова міграція державних ІТ-інфраструктур та її сервісів до Хмар – приватних, публічних (комерційних) та гібридних. Однією з особливостей "Cloud First" стало те, що вона визначала лише загальні принципи побудови та експлуатації інфраструктур, а вибір технологій, сервісів та операторів залишався правом тих, хто буде замовником Хмари – державні структури різних рівнів. У переліку активних користувачів Хмарних сервісів – Національне управління аеронавтики та вивчення космічного простору (NASA), Міністерство внутрішніх справ, Міністерство охорони здоров'я та соціальних служб США, Пентагон тощо. Навіть американське військове відомство замовляє Хмарні сервіси у світових комерційних операторів на мільярди доларів.

У рамках "Cloud First" достатньо чітко визначені основні критерії надійності та безпечності інфраструктури Хмарних операторів, які планують розміщувати в себе державні ІТ-сервіси. До речі, нормативно передбачено, що це може бути виключно американський оператор, який має зберігати та оброблювати дані на території США.

Проте існують певні застереження, в залежності від того, яка інформація оброблюється. Якщо замовником Хмарних сервісів виступає Пентагон або ЦРУ, то має забезпечуватися максимальний рівень захисту інформації та її конфіденційність, а якщо це вимоги до сервісів місцевого значення, то вони не такому високому рівні. У будь-якому випадку, оператори, особливо найбільші, намагаються створити спеціальні сервіси, які повною мірою відповідають усім вимогам "Cloud First". У свою чергу, компанія "Microsoft" пропонує платформу "Cloud for Government", яка, окрім цієї послуги, пропонує набір інших сервісів (Microsoft 365, Dynamics 365 CRM Online Government тощо). Їх відрізняє підвищений рівень захисту, у зв'язку з чим надаються послуги на 3-х рівнях. Перший рівень надійності має назву "Government Community Cloud" (GCC) – такі Хмари підходять для більшості державних структур без особливих вимог до безпеки; другий рівень – "GCC High" – відповідає підвищеним критеріям захищеності ІТ-структур та даних у Хмарних сервісах; максимальний рівень безпеки позначається як "DoD Cloud" – це сервіс рівня Міністерства оборони США (DoD – Department of Defense).

Таким чином, понад десять років у США концепція "Cloud First" успішно впроваджується як на рівні федеральних органів, так і в діяльності офіційних структур окремих штатів та інших адміністративних одиниць. Наприкінці 2020 року ця концепція була удосконалена і вже існує у новому форматі як концепція "Cloud Smart", яка є логічним продовженням першої. У положеннях цієї концепції враховані помилки та прорахунки

попередніх років та негативного досвіду роботи відповідних сервісів. Також у концепції "Cloud Smart" регламентовано використання нових технологій, таких як блокчейн, штучний інтелект тощо. Адже оцінити загальний вплив концепції "Cloud First" досить складно, проте на експертному рівні одноголосно визначено її позитивний та сприятливий ефект. Так, завдяки використанню Хмарних сервісів, державний сектор заощадив понад $20,5 млрд. тільки на процесах розробки нових додатків. Такі державні структури, як Комісія з цінних паперів США, Командування сил спеціальних операцій використовуючи Хмарні технології заощаджують $3 млн. щорічно.

У свою чергу, країни Європи створили спільну стратегію у сфері Хмарних технологій, при цьому не тільки у приватному секторі, а й у державному управлінні ще у 2013 році. Кожна країна ЄС, розуміючи важливість та актуальність цифрового прогресу та позитивно оцінюючи ефект впровадження нових технологій у реалії сьогодення, має власні програми розвитку Хмарних технологій на державному рівні. Наприклад, у Франції подібна ініціатива отримала назву "Andromede", у Німеччині – "Trusted Cloud", у Великобританії – "G-Cloud". Для держав ЄС використання Хмарних технологій – це найшвидший та надефективний спосіб подолати цифрову нерівність та отримати безперешкодний доступ до нових сервісів та безлімітних можливостей. Розвинута телекомунікаційна інфраструктура у поєднанні з Хмарними інструментами надає змогу, у тому числі, навчати та працевлаштовувати співробітників з віддалених регіонів та паралельно розвивати електронну комерцію, сфери розробки програмного забезпечення тощо.

У 2011 році у Великобританії було оприлюднено програмний документ – "Державна ІКТ – стратегія" (Government ICT Strategy), у складі якої була визначена "Державна Хмарна стратегія" (Government Cloud Strategy або скорочено – G-Cloud). Згодом ці документи багаторазово доповнювалися та корегувалися, проте загальний стратегічний курс використання Хмарних технологій залишається незмінним та пріоритетним вже понад десять років. Ключовим аспектом Державної Хмарної стратегії Великобританії стало визначення, що "державна Хмара" – це не просто технологія, а постійний інтерактивний процес, під час реалізації якого виникають нові функціональні можливості та ліквідуються помилки попередніх етапів. Також було схвалено рішення про обов'язковість використання у державному секторі Хмарних технологій, які мають сприяти удосконаленню моделей закупівлі та експлуатації ІКТ.

При цьому розробники національної стратегії чітко визначили різницю між такими поняттями, як "державна Хмара" та "Хмара, яка належить державі". У першому випадку замовником виступають міністерства та департаменти країни, які отримують у своє розпорядження необхідні обсяги IT-ресурсів за конкурентними цінами, замовляючи їх у довірених комерційних операторів. У другому – це значні фінансові та тимчасові витрати з непередбачуваним результатом. Таким чином, починаючи з 2012 року Хмарна стратегія активно впроваджується у Великобританії, у зв'язку з чим відбулася масова міграція державних структур у Хмари. При цьому, кожне відомство має право обирати оператора на свій розсуд – головне, щоб оператор забезпечував виконання національних вимог у сфері захисту інформації та надійності інфраструктури. З метою сприяння даному процесу була створена спеціальна онлайн-площадка "Digital Marketplace", де постачальники Хмарних послуг пропонують свої сервіси державним організаціям, які, у свою чергу, обирають найбільш зручні сервіси.

Така модель стимулює операторів пропонувати послуги відразу на вигідних умовах, оскільки конкуренція досить велика, оскільки маркетплейс об'єднує сотні приватних компаній. На відміну від класичних тендерів та аукціонів вибір постачальників послуг державною організацією здійснюється без конкурсу – тобто кожна державна структура

замість витрачання часу та ресурсів на проведення тендерних процедур обирає для себе найкращий варіант. Станом на 2020 рік обіг додатків для державних структур Великобританії "Government Application Store" перевищує 5,5 млрд. фунтів стерлінгів. При цьому, 80 % від загального обсягу закупівель перепадає на центральні органи влади, залишок – на регіональні структури. Завдяки широкому застосуванню Хмарних технологій у сферах державного управління, Сполучене Королівство заощаджує на IT-інфраструктурі понад 4 млрд. фунтів щорічно. Тільки у період 2012 – 2015 рр. впровадження Хмарних технологій державними органами Великобританії (модель "G-Cloud" – "урядова Хмара") дозволило зменшити витрати державних органів на цифровій трансформації та інформаційних технологіях на 3,56 млрд. фунтів стерлінгів. Таким чином, використання Хмарних технологій та сервісів є найбільш оптимальним та ефективним способом подолати цифрову нерівність, отримати додаткові трудові резерви та підвищити корисний ефект від використання IT-бюджетів у державному секторі.

Системи Хмарних обчислень досить активно впроваджуються у сфері державного управління в розвинених європейських країнах. Так, зазначена вище урядова ініціатива "урядова Хмара", що діє у Сполученому Королівстві, покликана заохочувати та значно спростити використання державними органами саме систем Хмарних обчислень. Прикладами впровадження успішних проектів у рамках цієї ініціативи є, зокрема: міграція даних усіх податкових інспекторів Королівської податкової та митної служби до Хмари; проект Національної служби охорони здоров'я зі зберігання інформації про стан здоров'я пацієнтів у Хмарі; перехід парламенту Сполученого Королівства на Хмарні сервіси (включаючи електронну пошту, спільну роботу над файлами, використання прикладних програм та зберігання інформації) тощо.

У Данії організація одного з муніципалітетів, відповідальна за здійснення закупівель, повністю перенесла послуги із закупівель до Хмари, а в Норвегії усі органи місцевого самоврядування одержали дозвіл на використання Хмарних продуктів. Поширюється використання Хмарних технологій публічним сектором і в Швеції. Запозичуючи кращі практики американського та європейського досвіду у цій площині, у 2019 році навіть Саудівська Аравія схвалила власну концепцію "Cloud First Strategy", яка спирається на передовий досвід своїх стратегічних партнерів: США, Великобританії та Австралії.

Не відстає у реалізації Хмарних технологій і Китай, який стає потужним гравцем у світовій цифровій економіці. При цьому важлива роль відводиться саме технологіям Хмарних сервісів. Завдяки міцній державній підтримці Хмарний ринок у цій країні демонструє зростання майже у три рази за останні п'ять років. Проте КНР притаманні свої особливості. Так, не кожен провайдер може надавати послуги державним структурам. Це є прерогативою виключно великих надійних та авторитетних компаній, а вимоги до Хмарних інфраструктур періодично корегуються та доповнюються. Останні зміни вносилися у вересні 2019 року.

Нові нормативи передбачають запровадження більш жорсткого контролю за діяльністю операторів, які надають Хмарні послуги для державних компаній. У 2019 році згідно зі звітом Китайського інформаційного мережевого Інтернет центру (China Internet Network Information Center) понад 90 % місцевих урядів у провінціях та 70 % муніципалітетів успішно використовують Хмарні платформи або перебувають в процесі їх запровадження. При цьому кожна державна структура самостійно обирає для себе технології та провайдера. Навіть пропонується певна альтернатива. Дозволяється будувати власну Хмару, користуватися послугами сертифікованого оператора або поєднувати ці рішення комплексно, оскільки жодних обмежень законодавчо не встановлено. Проте, щоб отримати сертифікат на 3 роки, спеціальна комісія має вивчити діяльність компанії –

провайдера не тільки у частині технічних спроможностей та інфраструктури, але й за іншими напрямками. Для цього оператор повинен надати повний доступ до будь-якої інформації про свою діяльність, включаючи відомості про усіх співробітників. У такий спосіб у КНР намагаються запобігти несанкціонованому витоку даних.

Навіть Республіка Білорусь активізувала діяльність у цьому напрямку та створила власну централізовану державну Хмару під назвою "Government Cloud" ("G-Cloud"). З цією метою у 2016 – 2017 роках був створений спеціальний республіканський центр обробки даних, оператором якого виступає приватна компанія "BeCloud". Це є першим захищеним Хмарним сервісом такого формату у цій країні. Його основне завдання передбачає надання інфраструктури для обробки та зберігання масивів даних державних структур Білорусі.

Таким чином, брендом номер один у світі в сфері розвитку інформаційно-комунікаційних технологій є широке використання істеблішментом багатьох держав світу саме Хмарних обчислень та реалізація політики переваги (пріоритету) Хмарного середовища ("Cloud First") у таких сферах, як: державне управління, освіта, наука, соціальна допомога, безпека та оборона, правоохоронна діяльність та інші, що має на меті сприяти більш ефективної взаємодії держави та суспільства. Передумови, за якими стратегія "Cloud First" стає актуальною, однакові практично у всіх вищевказаних країнах.

Для порівняння, поточна ситуація в Україні є більш складною і саме з цієї причини вимагає радикальних змін у підходах, що пов'язано із зростаючою залежністю від декількох глобальних постачальників, серед яких виділяється: нерівномірний розвиток внутрішнього ринку сервісів в порівнянні із зовнішніми ринками; гальмування вітчизняних органів державної влади щодо можливості працювати швидко при впровадженні інновацій, формуванні технічних завдань та бюджетів, а також при закупівлі компонентів для державних інформаційних систем тощо. Внаслідок цього також стримується і сам розвиток інформаційно-комунікаційних технологій в Україні, зокрема у сфері електронного урядування, освіти та науки.

Висновки.

Загальносвітова тенденція світовій сучасності – схвалення державних програм та прискорення міграції державних органів у Хмарні сервіси.

Починаючи з 2019 року на державному рівні в Україні тривають активні дискусійні обговорення вітчизняної версії світової загальновідомої стратегії "Cloud First", яка має запровадити стандарти Хмарних інструментів для потреб держави та заощадити мільярди державних фінансових ресурсів. Проте цей процес йде досить повільно. У вітчизняних реаліях використання Хмарних технологій у державному секторі є необхідним, враховуючи курс України до євроінтеграції. У ЄС, як і в США, сектор Хмарних послуг розвинутий досить добре, чимало держав схвалюють власні стратегії Хмарних технологій. Водночас, переважно державні організації входять до переліку найбільших замовників таких сервісів та послуг.

Тому для України впровадження власної моделі концепції "Cloud First" має передбачати залучення великих IT-підприємств, законодавчих та регуляторних органів до цієї проблематики з метою пошуку найкращого варіанту використання Хмарних сервісів для потреб державного сектору з урахуванням здобутків зарубіжного досвіду. Розробка, схвалення та практична реалізація власної стратегії сприятиме прискоренню цифрової трансформації на рівні усієї держави та її регіонів.

У середині 2020 року у першому читанні навіть було схвалено проект закону "Про Хмарні послуги" від 20.12.19 р. № 2655 [8], який має стати основою національної концепції використання Хмарних сервісів у державному секторі, надасть змогу створити передумови

для обробки та захисту даних при використанні технології Хмарних обчислень, наданні Хмарних послуг та визначенні особливостей використання Хмарних послуг органами державної влади, а також більш ефективного використання державних ресурсів шляхом впровадження новітніх технологій. Серед основних позитивних очікувань схвалення цього законодавчого акта має стати підвищення ефективності роботи усіх державних суб'єктів владних повноважень, а також державних підприємств, установ та організацій за рахунок більш оптимального використання коштів державного бюджету та суттєвого зменшення витрат на створення обчислювальних потужностей, їх обслуговування та безпеку.

Це свідчить про спробу закласти фундамент для вітчизняної стратегії "Cloud First". Очікується, що створення легітимних передумов для використання суб'єктами владних повноважень та державними підприємствами, установами та організаціями новітніх інформаційних технологій та впровадження систем ефективної взаємодії держави та суспільства дозволить створити потужну екосистему надавачів Хмарних послуг всередині країни, стимулюватиме перехід на Хмарну модель більшості секторів української економіки, дасть імпульс до прискореного розвитку ринку розробок програмного забезпечення для внутрішнього ринку, створюватиме додану вартість сектору ІТ та значно знизить ризики корупційної складової при здійснені закупівель за бюджетні кошти. Враховуючи викладене, одним із першочергових завдань держави є законодавче врегулювання використання Хмарних технологій та сервісів, виходячи із кращих практик та моделей зарубіжного досвіду у цій площині, що у свою чергу, сприятиме створенню потужних корпоративних ІТ-спільнот у державному секторі.

Використана література

1. Вітер М.Б. Використання Хмарних технологій у системі інформаційної взаємодії державних органів. *Науковий вісник НЛТУ України.* 2014. Вип. 24.9. С. 340-347.

2. Юдін О.К., Зюбіна Р.В. Нормативно-правові аспекти використання Хмарних технологій. *Наукоємні технології.* 2014. № 3(23). С. 303-306.

3. Чігіна Н.В. Поняття та основні правові проблеми упорядкування відносин у сфері Хмарних технологій. *Правова інформатика.* № 2(46)/2015. С. 17-24.

4. Скриновський Р. Принципи правового регулювання використання Хмарних технологій для обробки персональних даних URL: https://ideas.repec.org/a/pos/journl/60-2.html (дата звернення 25.03.2021).

5. Носенко Ю. Зарубіжний досвід використання Хмарних технологій в інклюзивній освіті. *Збірник наукових праць Уманського державного педагогічного університету.* 2017. № 2.

6. Запорожченко Ю.Г. Використання засобів ІКТ для підвищення якості інклюзивної освіти. *Інформаційні технології в освіті*: *зб. наук. праць.* Херсон: ХДУ, 2013. № 15. С. 138-145.

7. Брижко В.М. Приватність даних у Хмарних технологіях. *Інформація і право.* № 4(19)/2016. С. 47-59.

8. Про Хмарні послуги: проект закону України від 20.12.19 р. № 2655. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67744 (дата звернення: 25.03.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УКД 341.9+342.7

КОНЮШ М.Р., магістрант кафедри міжнародної інформації
Національного університету "Львівська політехніка".

ВЕЛИКІ ДАНІ ЯК ЗАГРОЗА ПРАВУ ЛЮДИНИ НА НЕДИСКРИМІНАЦІЮ

Анотація. *У статті розкрито проблему важливості і необхідності модернізації та адаптації права на недискримінацію в еру Великих даних та автоматизованих систем обробки даних. Запропоновано низку підходів, які потенційно можуть полегшити вирішення цієї проблеми, зокрема щодо попередньої та подальшої обробки даних. Проаналізовано концепцію "коду як права", яка допомагає краще зрозуміти вплив цифрових технологій на дискримінацію і знайти нові способи для протидії цьому явищу.*

Ключові слова: *дискримінація, Великі дані, "код як право", цифровий розрив.*

Summary. *This article reveals the problem of the importance and necessity of modernization and adaptation of the right to non-discrimination in the era of Big data and automated data processing systems. A number of approaches that could potentially facilitate the solution of this problem is proposed, in particular with regard to pre- and post-processing of data. The concept of "code as law" is analyzed, which helps to understand the impact of digital technologies on discrimination and to find new ways to combat this phenomenon.*

Keywords: *discrimination, Big data, "code as law", digital divide.*

Аннотация. *В данной статье раскрыта проблема важности и необходимости модернизации и адаптации права на недискриминацию в эру Больших данных и автоматизированных систем обработки данных. Предложен ряд подходов, которые могут облегчить решение этой проблемы, в частности относительно предыдущей и последующей обработки данных. Проанализирована концепция "кода как права", которая помогает лучше понять влияние цифровых технологий на дискриминацию и найти новые способы противодействия этому явлению.*

Ключевые слова: *дискриминация, Большие данные, "код как право", цифровой разрыв.*

Постановка проблеми. Розвиток системи прав людини у теперішньому швидкоплинному світі пов'язаний як із глобалізацією, так і з надзвичайно швидким удосконаленням різного роду інформаційних та комунікаційних технологій. Упродовж останніх декількох десятків років з'явилася необхідність правового захисту людини не лише у реальному світі, але й у мережі. З-поміж багатьох інших прав це стосується також і права на недискримінацію. Саме це право означає надання індивіду низки можливостей, важливих для нормального життя у сучасному суспільстві, які закріплені у більшості правових систем розвинених держав.

Завдяки розвитку технологій, які набули назву "Великі дані" (англ. – *Big data*) з часом проблема дискримінації може стати настільки ж масштабною, як і забруднення довкілля, особливо якщо вчасно не звертати на це увагу та не перейматися забезпеченням права осіб на недискримінацію у новому цифровому оточенні.

Метою статті є окреслення історії утвердження права на недискримінацію у системі прав людини та міжнародних документах, охарактеризування впливу Великих даних на це право, а також визначення потенційних шляхів вирішення проблеми дискримінації в сучасну епоху.

Результати аналізу досліджень і публікацій. Принцип недискримінації у своїх роботах досліджували багато вчених, зокрема О. Банчук, О. Васильченко, П. Рабінович,

Г. Христова, С. Шевчук, О. Панкевич, С. Погребняк, З. Равлінко та інші. Однак у контексті застосування сучасних технологій та трансформації інформаційних відносин цей принцип досліджено недостаньо. Зважаючи на наявні тренди в інформаційній сфері, доцільним є вивчення реального і потенційного впливу Великих даних на право людини на недискримінацію.

Виклад основного матеріалу.

Право на недискримінацію у міжнародних документах. Перш ніж розпочати обговорення права на рівність та недискримінацію, важливо розглянути саму концепцію дискримінації та її взаємозв'язок з принципом недискримінації. Загальновизнано, що рівність та недискримінація є позитивним та негативним твердженнями одного принципу. Інакше кажучи, рівність можна визначити як відсутність дискримінації та дотримання принципу недискримінації поміж усіма соціальними групами. Основною метою даного принципу є надання всім людям рівних та справедливих можливостей, доступних кожному [17].

До 1945 р. заборона дискримінації регулювалася лише так званими договорами про меншини (наприклад, Малий Версальський договір від 1919 р., укладений для захисту польських етнічних меншин у післявоєнний період [7]). Проте з прийняттям Статуту ООН положення про недискримінацію стало загальновизнаним елементом міжнародного права. Ідеї про те, що ООН повинна стати міжнародним захисником прав людей, виникла і утвердилася після трагічного досвіду Другої Світової війни та жахливих і масових порушень прав людини.

Важливим кроком світового співтовариства на шляху до мінімізації проявів дискримінації можна вважати прийняття Загальної декларації прав людини у 1948 р. [3]. Основні моменти щодо захисту від дискримінації були окреслені у її ст. 7, яка закріпила право людини на захист від дискримінації, а також у п. 2 ст. 23, котра гарантувала право на працю з гідною оплатою без будь-якої дискримінації.

Згодом у 1950 р. була прийнята Конвенція про захист прав та основоположних свобод [5], у ст. 14 якої визначені основні ознаки, що підпадають під захист від дискримінації, а саме: стать, раса, колір шкіри, мова, релігія, політичні чи інші переконання, національне чи соціальне походження, приналежність до національної меншини, майновий стан та низка інших ознак. Пізніше вона була доповнена положеннями Протоколу № 12, ст. 1 якого встановлює загальну заборону будь якої дискримінації [9].

У Європейському Союзі прояви дискримінації за національною ознакою та ознакою статі були заборонені установчими договорами, інші ж підстави дискримінації були додані після підписання Амстердамського договору від 1997 р. [1]. У теперішній час Договір про функціонування ЄС [2] забороняє будь-яку дискримінацію за ознаками національності, статі, раси, етнічного походження, релігії чи переконань, інвалідності, віку та сексуальної орієнтації. Також принцип недискримінації закріплений у ст. 21 Хартії Європейського Союзу про основні права від 2000 р. [11].

Не менш важливими інструментами є міжнародні договори та інші документи, які стосуються протидії дискримінації найуразливіших груп населення. З-поміж них можна виділити Конвенцію про права осіб з інвалідністю від 2007 р. [6], Міжнародну конвенцію про ліквідацію всіх форм расової дискримінації від 1965 р. [8], Конвенцію ООН про ліквідацію всіх форм дискримінації щодо жінок від 1979 р. [4], а також Стратегію Європейської Комісії щодо ЛГБТ від 2020 р. [10].

Великі дані. Великі дані – це загальна назва структурованих та неструктурованих даних у значних обсягах (що підлягають обробці та аналізу не лише програмними

інструментами, але й різного роду аналітиками у значно менших обсягах), які прийшли на заміну традиційним структурам керування базами даних наприкінці 2000-х рр. [12]. Терміном "Великі дані" прийнято описувати обробку великих масивів різноманітної інформації зі складною, неоднорідною або взагалі невизначеною структурою. Ця інформація може бути структурована або неструктурована [13]. Оскільки ми живемо у "мережевому світі", кількість структурованих числових та неструктурованих даних невпинно збільшується.

Одним з найтривожніших аспектів використання Великих даних є зростання ризиків щодо їх застосування з метою дискримінації людей. Варто зазначити, що дискримінація певною мірою корелюється з нерівністю, адже шкода, спричинена дискримінацією, часто призводить до нерівності. Іншим важливим моментом у дослідженні цієї проблеми є потенційна неготовність правових систем до боротьби з дискримінацією, яка виникає чи багатократно збільшується внаслідок використання Великих даних.

Ці небезпеки висвітлені у звіті Білого Дому про впровадження антидискримінаційної політики в моделях статистичного моделювання [21]. Зокрема, у ньому йдеться про проблеми використання алгоритмів та статистичних моделей при наявності таких характеристик як раса, стать, вік; доцільність заборони збору даних про расу та стать для використання у сфері іпотеки та страхування; впровадження прозорої системи роботи алгоритмів.

Надзвичайно важливим фактором також є цифровий розрив (або цифрова нерівність) [14], який утворюється через недостатній рівень фінансового забезпечення разом з неможливістю отримати сучасний пристрій для доступу до мережі, а також через високу ціну на доступ до мережі.

Враховуючи вищезазначене, можна виділити окремі загрози у сфері дискримінації, зумовлені поширенням Великих даних:

- мережа може стати упередженою щодо певних груп людей [16];
- предикативна функція Великих даних для попередження злочинів може дискримінувати частіше одну групу населення через значну кількість схожих порушень у цієї групи [15].

Підходи до вирішення проблеми дискримінації, зумовленої використанням Великих даних. Зважаючи на масштабність проблеми, окремі спеціалісти та дослідники вже зараз пропонують її практичні рішення. Найчастіше йдеться про розробку методу, який допомагав би розпізнавати та усувати дискримінацію. Зокрема, можна застосувати методи:

- попередньої обробки даних, які виключатимуть можливість створення нової моделі дискримінації;
- подальшої обробки даних, які проводитимуть певний аудит даних для виявлення потенційних дискримінаційних моделей [19].

Запровадження більш "прозорих процесів" збирання даних може допомогти уникати завданню шкоди та несправедливості. Для імплементації зазначених процесів збирання даних потрібно розробляти нові методи інтелектуального аналізу даних, що включають створення нового алгоритму та обґрунтування логічності кроків для простеження того, як поведінка й вибір людини будуть інтерпретовані алгоритмом.

Іншим потенційно можливим способом вирішення проблеми можна вважати вдосконалення системи збереження конфіденційності та способів отримання інформації, адже дискримінацію важко повністю викорінити, якщо в систему інтегрована модель, яка виключає конфіденційність інформації [18].

Щодо правового регулювання, то його потрібно здійснювати з урахуванням особливостей програмного та апаратного забезпечення, які самі собою можуть чинити значний вплив на суспільні відносини. Інакше кажучи, технічні засоби можуть посилювати або послаблювати ефективність правового регулювання. Як у свій час зазначав Л. Лессінг, "код – це право" [20], тобто програмний код як елемент архітектури Інтернету здатен певною мірою обмежувати дії людини або схиляти їх у певному напрямку.

Проте, на відміну від звичних традиційних правових норм, які вказують на можливість чи необхідність певної дії, включаючи утримання від неї, особливості коду та апаратного забезпечення безпосередньо визначають поле можливого і виключають будь-яке втручання третіх сторін у прийняття рішення щодо поведінки особи. Яскравим прикладом регулювання кодом є біткойн або будь-яка інша криптовалюта. Це фінансові системи, які функціонують на основі строгих правил, що закладені безпосередньо у коді. Якщо ж говорити про дискримінацію, що є наслідком роботи алгоритму або коду, то такі випадки зустрічаються при використанні автоматичних систем фіксації порушень у великих містах. Наприклад, об'єктом уваги алгоритму щодо пошуку підозрюваних у скоєнні правопорушень частіше стають афроамериканці [16].

Висновки.

Зміни, які відбуваються у сучасному глобалізованому світі, із кожним новим стрибком у технологічному прогресі створюють нові виклики як для суспільства, так і для права, головною функцією якого є врегулювання суспільних відносин. З-поміж них важливе місце займає проблема дискримінації, особливо у контексті поширення Великих даних та процесів, коли автоматизовані системи змінюють та витісняють людей з певних галузей прийняття рішень.

Незважаючи на те, що західні дослідники приділяють цій проблемі багато уваги, і напрямки, у котрих вони рухаються, дають підстави сподіватися на краще, все ж досі існує вірогідність зіткнутися зі значними труднощами у процесі розробки і упровадження механізмів, покликаних зменшити ймовірність дискримінаційних проявів, спричинених Великими даними.

По-перше, не дивлячись на спроби адаптуватися до викликів, пов'язаних з дискримінацією, виникають суперечки щодо того, чи зможе алгоритм або код убезпечити від таких проявів, і наскільки такі ініціативи сумісні з принципом прозорості правового регулювання, а також із принципом свободи особи.

По-друге, залишається відкритим питання, наскільки ефективним буде таке регулювання і чи не породить воно збільшення дискримінації у інших сферах.

По-третє, необхідно з'ясувати, чи можливо створити і адаптувати алгоритм, який міг би ефективно, чітко та швидко приймати правильні рішення без необхідності сторонньої допомоги – спеціаліста, який за потреби вносив би правки або вручну вводив би рішення для остаточного врегулювання ситуації.

Використана література

1. Амстердамський договір від 1997 р. URL: https://pidru4niki.com/2015101166769/politologiya/amsterdamskiy_dogovir

2. Договір про функціонування Європейського Союзу від 1957 р. URL: https://zakon.rada.gov.ua/laws/show/994_017#Text

3. Загальна декларація прав людини: Резолюція ООН від 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

4. Про ліквідацію всіх форм дискримінації щодо жінок: Конвенція ООН від 1979 р. URL: https://zakon.rada.gov.ua/laws/show/995_207#Text

5. Про захист прав та основоположних свобод: Конвенція ООН від 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

6. Про права людей з інвалідністю: Конвенція ООН від 2006 р. URL: https://zakon.rada.gov.ua/laws/show/995_g71#Text

7. Малий Версальський договір від 1919 р. URL: https://uk.wikipedia.org/wiki/Малий_ Версальський _договір

8. Про ліквідацію всіх форм расової дискримінації: Конвенція ООН від 1965 р. URL: https://zakon.rada.gov.ua/laws/show/995_105#Text

9. Протокол № 12 до Конвенції про захист прав людини та основоположних свобод від 2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_537#Text

10. Стратегія рівності ЛГБТ 2020 – 2025 від 2020 р. URL: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/lesbian-gay-bi-trans-and-intersex-equality/lgbtiq-equality-strategy-2020-2025_en

11. Про основні права: Хартія Європейського Союзу від 2000 р. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text

12. Шаховська Н.Б., Болюбаш Ю.Я. Модель Великих даних "сутність – характеристика". *Вісник Національного університету "Львівська політехніка". Серія: "Інформаційні системи та мережі"*. 2015. № 814. С. 186-196.

13. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право.* № 1(20)/2017. С. 51-67.

14. Barocas S., Selbst A. Big Data's Disparate Impact. *California Law Review*. 2016. 104. P. 671-732. URL: https://ssrn.com/abstract=2477899

15. Burgess M. UK police are using AI to inform custodial decisions – but it could de discriminating against the poor. *Wired.* 2018. URL: https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit

16. Courtland R. Bias detectives: the researches striving to make algorithms fair. *Nature.* 2018. P. 357-360. URL: https://www.nature.com/articles/d41586-018-05469-3

17. Glossary of summaries: non-discrimination principle. URL: https://eur-lex.europa.eu/summary/glossary/nondiscrimination_principle.html

18. Hildebrandt M., Kroops B-J. The challenges of ambient law and legal protection in the profiling era. *The Modern Law Review*. 2010. P. 273-307. URL: https://www.academia.edu/702736/The_challenges_of_ambient_law_and_legal_protection_in_the_profiling_era

19. Kamiran F., Žliobaitė I., Calders T. Quantifying explainable discrimination and removing illegal discrimination in automated decision making. *Knowledge and Information Systems*. 2013. 35. P. 613-644. URL: https://doi.org/10.1007/s10115-012-0584-8

20. Lessig L. Code and other law of cyberspace. *Review.* 1999. P. 179-180. URL: http://surl.li/ofap

21. Pope D., Sydnor J. Implementing Anti-Discrimination Policies in Statistical Profiling Models. *American Economic Journal: Economic Policy*. Vol 3. 2011. P. 206-301. URL: https://pdfs.Semanticscholar.org/0532/ad6127c0ffef23258bff42e33d314d28f6bb.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

ЦЯПА С.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-9263-1050.

ОГЛЯД ЗАРУБІЖНИХ ЗАКОНОДАВЧИХ ІНІЦІАТИВ СТРАТЕГІЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ УМОВАХ

Анотація. *Проаналізовано окремі акти зарубіжного законодавства, присвячені питанням технологічного розвитку штучного інтелекту. Визначено пріоритети та галузі використання штучного інтелекту. Обґрунтовано результативні показники впровадження штучного інтелекту у соціальній сфері, економіці та державному управлінні. Розглянуто ініціативи, які схвалені на державному та міжнаціональному рівнях з метою нормативного врегулювання використання штучного інтелекту у військовій сфері. Окреслені загальносвітові тенденції динамічного розвитку штучного інтелекту в сучасних умовах.*

Ключові слова: *штучний інтелект, цифрові технології, когнітивні технології, нейронні мережі, кібербезпека, кіберзагроза, кібератака, кіберзахист, державна політика, цифровізація, блокчейн, військова сфера.*

Summary. *Some acts of foreign legislation devoted to the issues of technological development of artificial intelligence are analyzed. Priorities and areas of artificial intelligence use have been identified. The effective indicators of introduction of artificial intelligence in the social sphere, economy and public administration are substantiated. The initiatives approved at the state and international levels for the purpose of normative regulation of the use of artificial intelligence in the military sphere are considered. The general world`s tendencies of dynamic development and distribution of technological support of artificial intelligence in modern conditions are outlined.*

Keywords: *artificial intelligence, digital technologies, cognitive technologies, neural networks, cybersecurity, cyberthreat, cyberattack, cyberdefense, state policy, digitalization, blockchain, military sphere.*

Аннотация. *Проанализированы отдельные акты зарубежного законодательства, посвященные вопросам технологического развития искусственного интеллекта. Определены приоритеты и отрасли использования искусственного интеллекта. Обоснованы результативные показатели внедрения искусственного интеллекта в социальной сфере, экономике и государственном управлении. Рассмотрены инициативы, одобренные на государственном и межнациональном уровнях с целью нормативного урегулирования использования искусственного интеллекта в военной сфере. Очерчены общемировые тенденции динамического развития искусственного интеллекта в современных условиях.*

Ключевые слова: *искусственный интеллект, цифровые технологии, когнитивные технологии, нейронные сети, кибербезопасность, киберугроза, кибератака, киберзащита, государственная политика, цифровизация, блокчейн, военная сфера.*

Постановка проблеми. Тотальна епоха цифровізації, розширених технічних та технологічних можливостей кардинально змінює існуючу глобальну соціально-економічну модель світу. Останнім часом технологічне забезпечення штучного інтелекту та його розвиток є сучасним прогресивним напрямком, яким охоплені розвинуті держави світу. Саме когнітивні технології розширюють потенціал інформаційних технологій

з метою вирішення завдань, які традиційно вважалися прерогативою людини та які позбавляють необхідності робити вибір між швидкістю, витратами та якістю. Починаючи з 2017 року, у всесвітніх масштабах розпочалася боротьба за світове лідерство у сфері розвитку штучного інтелекту. З метою унормування подальшого розвитку технологій штучного інтелекту протягом 2017 – 2019 років понад 30 країн світу розробили відповідні національні стратегії (Канада, Сінгапур, КНР, Данія, Італія, Німеччина, Франція), визначивши штучний інтелект одним із важливих пріоритетів державної політики. За таких умов стрімкий розвиток та динамічне використання технологій штучного інтелекту розповсюджується на дедалі більшу кількість сфер та галузей економіки, супроводжуючись значним зростанням як державних, так і приватних інвестицій у їх розвиток. У світових масштабах можна спостерігати навіть конкуренцію між провідними державами у цій сфері. Так, Китай неодноразово заявляв про своє світове лідерство у сфері передових технологій штучного інтелекту вже до 2030 року. У планах офіційного Пекіну прискорені темпи розвитку індустрії штучного інтелекту у сфері проектування та виробництва чипів, у зв'язку з чим влада має намір виділити 16,4 млрд. Євро. Такі самі амбіційні плани у глобальних масштабах останнім часом демонструє і держава-агресор.

На цьому фоні можна констатувати, що провідні країни світу серйозно опікуються цією проблематикою, постійно удосконалюють національне законодавство, присвячене розвитку штучного інтелекту. В умовах цифрових трансформацій кількість як національних інституцій, державних, так і приватних компаній, які тією чи іншою мірою використовують технологічні можливості штучного інтелекту зростає в геометричній прогресії. Практично в сучасних умовах на ринку кібербезпеки вже з'явилися системи з використанням штучного інтелекту. Так, у сфері захисту веб-ресурсів ці системи аналізують середовище та події, які у ньому відбуваються, розпізнають реальні та потенційні загрози, вживають заходів з метою їх усунення та блокування. Інструменти штучного інтелекту оптимізують роботу сайтів, контенту та самостійно налаштовують системи захисту, блокуючи при цьому шкідливий трафік та забезпечуючи надходження безпечного контенту. Адже застосування штучного інтелекту не обмежується виключно захистом веб-ресурсів. Ще однією поширеною сферою його застосування є суттєве зменшення уразливостей та ризиків в системах забезпечення кібербезпеки. Адже не можна недооцінювати роль та значення технологій штучного інтелекту, особливо в умовах транснаціонального розповсюдження гібридних загроз, кібератак, глобального поширення пандемії, коли тренд переходу на віддалений режим роботи задає високу планку та нові вимоги до сучасних систем безпеки.

В сучасних умовах Україна робить лише перші поступальні кроки з метою нормативного забезпечення процесів розробки та впровадження технологій штучного інтелекту у загальну концепцію побудови безпеки цифрових сервісів та електронних послуг. Тому висвітлення проблемних питань використання штучного інтелекту у сфері забезпечення кібербезпеки, визначення подальших шляхів удосконалення законодавчих основ у цій площині є актуальним та своєчасним, особливо враховуючи проголошений курс України на тотальну цифровізацію усіх сфер суспільного життя у рамках реалізації з 2019 року амбіційного проекту "Держава у смартфоні".

Результати аналізу наукових публікацій. Технології штучного інтелекту та їх вплив на стан забезпечення кібербезпеки певною мірою досліджували у своїх працях такі науковці: В. Брижко [1], О. Бусол [2], О. Радутний [3], В. Савченко [4], тощо. Питання правового врегулювання засад розвитку штучного інтелекту розглядали: О. Баранов [5], А. Бежевець [6], О. Косілова [7], О. Кривецький [8], К. Міліцина [9] та ін.

Проте вбачаються недостатньо висвітленими сучасні зарубіжні законодавчі ініціативи, які останнім часом впроваджуються з метою правового врегулювання сфери застосування технологій штучного інтелекту, що посилює актуальність цієї роботи.

Метою статті є оцінка нормативно-правових актів окремих держав світу та узагальнення стратегічних напрямів розбудови вітчизняної екосистеми інноваційних розробок у сфері технологій штучного інтелекту.

Виклад основного матеріалу. Світовою спільнотою було розроблено такий показник, як "Індекс готовності урядів до впровадження штучного інтелекту" (Government Artificial Intelligence Readiness Index) [10]. Так, у 2020 році Україна посіла 57-е місце у цьому загальносвітовому рейтингу держав світу, країна – агресор (РФ) 33-е місце, а Білорусь – 66. На цьому фоні, наша держава також розвиває власне законодавство та формує концептуальні засади державної політики в галузі штучного інтелекту, наближаючи його до кращих практик міжнародного досвіду, переслідуючи мету створення конкурентоспроможного середовища у соціально-економічній, науково-технічній, оборонній та інших сферах життєдіяльності. За таких умов, у вітчизняних реаліях технології штучного інтелекту повинні сприяти прискоренню трансформації економіки, ринку праці, державних інституцій та суспільства в цілому.

З метою проведення порівняльно-правового аналізу, розглянемо концептуальні засади регулювання технологій штучного інтелекту в Республіці Білорусь. Так, Концепція інформаційної безпеки, яка затверджена Постановою Ради Міністрів Республіки Білорусь 18 березня 2019 року [11], нормативно регламентує прагнення політичного керівництва цієї країни прискорити запровадження цифрової трансформації економіки як важливої складової формування інформаційного суспільства, що має призвести до того, що усі галузі, ринки, сфери життєдіяльності держави мають бути переорієнтовані на нові цифрові економічні моделі. Зазначається, що в Білорусі активно розвиваються інноваційні цифрові технології, засновані на системах штучного інтелекту, нейронних мереж, що забезпечують роботу з численними інформаційними ресурсами, у тому числі й масивами Великих даних, технології реєстру блоків трансакцій (блокчейн). При цьому акцентовано, що у цій країні ступінь цифровізації галузей економіки є диференційованою, що значно знижує очікуваний синергічний ефект від запровадження синхронної інформатизації, у зв'язку з чим цифрова політика держави має орієнтуватися на реалізацію пілотних проектів цифровізації та їх галузеве масштабування, створення центрів компетенції з питань цифрової трансформації. Задекларовано, що у якості найбільш вірогідних джерел загроз кібербезпеки виступають: збої технічних засобів та програмного забезпечення в інформаційних та телекомунікаційних системах, протиправна діяльність окремих осіб та злочинних угрупувань, помилки персоналу інформаційних систем, які проявляються у порушенні встановлених регламентів їх експлуатації та правил обробки інформації, залежність Білорусі від інших держав – виробників програмних та апаратних засобів при створенні та розвитку інформаційної інфраструктури. Кібербезпека національного сегменту мережі Інтернет забезпечується переважно за рахунок відбиття основного обсягу кібератак на інформаційні системи та мережі передачі даних шляхом блокування шкідливих комунікацій між суб'єктами та об'єктами впливу. Тобто, "людський фактор" залишається, у тому числі, однією із актуальних загроз кібербезпеці держави, що диктує необхідність використання технологій штучного інтелекту з метою нівелювання цієї загрози.

Постановою Ради Міністрів Республіки Білорусь від 2 лютого 2021 року № 66 була затверджена Державна програма "Цифровий розвиток Білорусі на 2021 – 2025 роки" [12]. Цим програмним документом проголошено курс на прискорення впровадження

цифрових інновацій та технологій “розумних міст”, забезпечення інформаційної безпеки таких рішень. Передбачається виконання заходів щодо створення сучасної інформаційно-комунікаційної інфраструктури та комплексної цифрової трансформації процесів державного управління, регіонального та галузевого розвитку, у тому числі й у таких сферах як: охорона здоров’я, освіта, екологічна безпека, стабільний розвиток населених пунктів тощо.

Також визначено засади та перелік заходів, реалізація яких надасть змогу впровадити у реалії життя передові інформаційні технології, прискорити інтеграцію економіки Білорусі у світовий економічний цифровий простір. При цьому достатня увага приділяється штучному інтелекту в контексті розв’язання сучасних цифрових рішень й завдань. Розвиток інформаційних технологій, заснованих на впровадженні технічних рішень, державних електронних сервісів, має призвести до необхідності безперервного удосконалення інструментів, які мають забезпечувати стабільність їх роботи та захист даних державних інформаційних систем (цифрових платформ).

Очікується, що практична реалізація положень цієї Державної програми дозволить: підвищити рівень інформаційної безпеки даних та технологій її забезпечення у рамках створення розгалуженої цифрової інформаційної екосистеми; забезпечити конкурентоздатність вітчизняних розробок та технологій інформаційної безпеки; створити ефективну систему захисту прав та законних інтересів громадян, бізнесу та держави від загроз інформаційної безпеки. Ключовим завданням впровадження технологій штучного інтелекту у сфері забезпечення інформаційної безпеки має стати зміцнення довіри громадян, забезпечення умов для безпечного надання та отримання електронних послуг, включаючи розробку програмних та програмно-апаратних комплексів захисту інформаційних ресурсів, інформаційно-телекомунікаційних систем, формування та удосконалення технічних умов з метою надійної ідентифікації в рамках надання державних послуг та здійснення адміністративних процедур в електронній формі.

Узагальнюючи вищевикладене, можна констатувати, що в Білорусі під штучним інтелектом розуміють глибокі штучні нейронні мережі та технологію на їх основі, які дозволяють вирішувати складні завдання обробки масивів інформації. Технології штучного інтелекту покликані імітувати когнітивні функції людського інтелекту, що дозволяє системі здійснювати обробку та інтерпретувати інформацію, аналізувати її та робити висновки, використовуючи й адаптуючи ці знання для досягнення мети, з якою ця технологія була впроваджена. Застосовуючи штучний інтелект та алгоритми глибокого навчання у сфері кібербезпеки, можливо виграти час, що є критичним елементом у будь-якій ситуації під час поширення кібератак. Для Білорусі штучний інтелект виступає революційною технологією у сфері забезпечення кібербезпеки, при цьому саме технології машинного навчання та комп’ютерного зору відкривають нові перспективи для розвитку сучасних засобів захисту інформації. Типовими формами його практичної реалізації є розробка та впровадження відповідних пілотних проектів. Наприклад, в Мінському обласному управлінні Департаменту охорони МВС Республіки Білорусь у січні 2020 року стартував пілотний проект моніторингу безпеки території за допомогою штучного інтелекту. При цьому у якості основи інфраструктури системи комплексної безпеки були обрані інтелектуальні модулі, засновані на нейронних мережах.

Держава-агресор (РФ) з метою реалізації своїх імперських задумів та проведення наступальних операцій, у першу чергу, в кіберпросторі, особливо проти України, ще у жовтні 2019 року схвалила Національну стратегію розвитку штучного інтелекту до 2030 року [13]. Невипадково нормативно задекларовано амбіційне прагнення РФ посісти

міжнародні лідерські позиції у сфері розвитку та використання технологій штучного інтелекту у всіх сферах життєдіяльності, включаючи такі сегменти як оборона та безпека.

Цікавим видається досвід Узбекистану у цій площині, країни, де першочерговим пріоритетом визначено штучний інтелект та технології його впровадження. У зв'язку з цим Президент цієї країни 17 лютого 2021 року підписав Постанову "Про заходи щодо створення умов для прискорення впровадження технологій штучного інтелекту" [14]. Цим документом заплановано розробку Національної стратегії розвитку штучного інтелекту, яка передбачатиме підготовку цільової державної програми підтримки наукових досліджень та інноваційних проектів у сфері штучного інтелекту, "дорожню карту" реалізації положень Стратегії, цільові показники (індикатори) розвитку цієї сфери; підвищення доступності та якості цифрових даних, розробку програмних продуктів; створення сучасної високотехнологічної інфраструктури та апаратних комплексів для вирішення завдань у сфері штучного інтелекту; організацію підготовки кваліфікованих спеціалістів у цій сфері, в тому числі й із залученням зарубіжних викладачів, цільового навчання кадрів для пріоритетних галузей економіки, соціальної сфери, системи державного управління; розробку комплексної системи регулювання питань впровадження та застосування технологій штучного інтелекту, загальних керівних принципів та норм, а також єдиних стандартів й правил обробки цифрових даних; удосконалення системи контролю та запобігання ризикам у сфері штучного інтелекту, у тому числі забезпечення безпечного функціонування програм, розроблених на основі технологій штучного інтелекту, а також профілактики потенційних ризиків, а також конфіденційності використаних даних. Також передбачається схвалення на національному рівні міжнародних стандартів у сфері штучного інтелекту, створення та запровадження спеціального правового режиму щодо застосування технологій штучного інтелекту.

Стратегічним напрямком визначена розбудова вітчизняної екосистеми інноваційних розробок у сфері штучного інтелекту, що передбачатиме: утворення науково-дослідного інституту розвитку цифрових технологій та штучного інтелекту, запровадження механізмів спільного фінансування (краудфандингу) у стартап-проєктах у сфері штучного інтелекту, проведення відкритих занять у закладах освіти. Достатня увага також приділяється питанням: формування інвестиційної привабливості та здійснення розробок у сфері штучного інтелекту; забезпечення доступу вітчизняних підприємств та спеціалістів до інформаційних ресурсів у сфері штучного інтелекту, налагодження плідного міжнародного співробітництва у сфері штучного інтелекту та технологій його застосування. Нормативно заплановано впровадження технологій у сфері штучного інтелекту в Узбекистані протягом 2021 – 2022 років у таких галузях: сільське господарство, банківський сектор, фінанси, транспорт, охорона здоров'я, електронне урядування. Загальний обсяг фінансування, закладений з метою виконання цих програм, складає 200 млрд. Сумів.

Нормативно задекларовано, що з метою стимулювання залучення інвестицій у технологічне оснащення штучного інтелекту повинні бути розроблені інструменти державно-приватного партнерства, запроваджені фінансові та податкові пільги для розробників та інвесторів, включаючи венчурне фінансування. Для побудови ефективних рішень на базі штучного інтелекту у таких сферах як безпека, освіта, охорона здоров'я потребується запровадження єдиної системи збору та аналізу даних з уніфікованим доступом та суцільною деперсоналізацією. Таким чином, Узбекистан, адаптуючи кращі практики зарубіжного досвіду, розробив та впроваджує власну модель технологічного забезпечення штучного інтелекту цивільного сектору, активно опікується питаннями розробки власної нормативно-правової бази, яка визначатиме

єдині критерії та вимоги, засади відповідальності й безпечності під час розробки та використання технологій штучного інтелекту в провідних галузях економіки та соціальній сфері, системі державного управління.

Україна також не стоїть осторонь процесів удосконалення правового регулювання технологій штучного інтелекту та виражає прагнення зайняти значний сегмент світового ринку технологій штучного інтелекту, провідні позиції у міжнародних рейтингах. Зокрема, у грудні 2020 року в Україні була схвалена Концепція розвитку штучного інтелекту [15], практична реалізація якої сприятиме інтеграції інноваційних технологій в економічно важливі сектори держави. Очікується, що технології штучного інтелекту сприятимуть трансформації економіки, ринку праці, державних інституцій та суспільства загалом. Їх застосування надасть можливість зменшити обсяги витрат і підвищити ефективність виробництва, якість товарів та послуг. Метою цієї Концепції є визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління. Пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, нормативно визначені: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя. Згідно із положеннями чинного законодавства штучний інтелект – організована сукупність інформаційних технологій, із застосуванням яких можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.

Особлива увага у її положеннях присвячена розвитку штучного інтелекту саме у сфері кібербезпеки. Чинним законодавством України встановлено, що основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об’єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян. Комплексне розв’язання проблем кібербезпеки у цьому форматі вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок штучного інтелекту у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей Хмарних обчислень. Оновлення стандартів та розроблення нових необхідно здійснювати з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032.

Загалом можна констатувати, що у питаннях розроблення стандартів у сферах новітніх технологій, зокрема штучного інтелекту, наша держава виходить з того, що всесвітня глобальна мережа має залишатися глобальною та відкритою, технології повинні орієнтуватися на людину, забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас, у зв'язку з ускладненням міжнародної безпеки в кіберпросторі Україна займає більш проактивну позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері забезпечення кібербезпеки, зменшуючи актуальні небезпеки мілітаризації кіберпростору. За таких умов, одним із ключових завдань для держави залишається прискорення впровадження технологій штучного інтелекту в національній системі кібербезпеки, посилення спроможностей її відповідальних суб'єктів.

Розглянемо деякі ініціативи, які схвалюються як на державному, так і міжнаціональному рівнях з метою нормативного врегулювання використання штучного інтелекту саме у військовій сфері. Так, розуміючи актуалізацію сучасних тенденцій поширення технологій штучного інтелекту у світових масштабах, на початку 2020 року Пентагон схвалив етичні принципи для впровадження штучного інтелекту в свою діяльність. Успіхи РФ та КНР у військовій сфері, прискорений розвиток сучасних оборонних технологій сприймаються в американському оборонному відомстві як серйозний і потужний виклик, що провокує активізацію розробок у сфері високих технологій з використанням нейтронних мереж. Невипадково, у цих принципах закладено базові основи етичного проектування, розробки та використання штучного інтелекту міністерством оборони США.

Слід вказати, що нові технології, такі як штучний інтелект, автономні та квантові технології змінюють характер діяльності НАТО. Розуміючи ризики та можливості, які несуть нові технології Північноатлантичному Альянсу, міністри оборони держав-членів НАТО на щорічному саміті у лютому 2021 року схвалили стратегію впровадження нових та революційних технологій. Загальна мета цього програмного документа – розробка власної інноваційної системи комплексної взаємодії в рамках Альянсу, яка надасть змогу використовувати тотожні підходи та однакові технології для усіх учасників блоку. Для загального управління цим процесом запропоновано створити власну інституцію (агентство), а з метою здійснення фінансування – інвестиційний банк НАТО з венчурним фондом, який буде функціонувати за рахунок внесків держав-членів, забезпечуючи надання субсидій та грантів на перспективні проекти. Очікується, що влітку 2021 року НАТО схвалить власну стратегію, присвячену питанням розвитку сфери технологій штучного інтелекту та обробки даних, оскільки цей напрямок є і залишається загальною частиною загальної стратегії інвестицій НАТО в нові та революційні технології. Ця стратегія визначатиме шляхи заохочення та захисту розробок у сфері штучного інтелекту та його технологій з метою збереження технологічного домінування НАТО у глобальній військовій сфері, буде містити плани стандартизації взаємодії та розвитку технологій, включати рекомендації відповідального використання платформ з підтримкою штучного інтелекту. Запланована плідна співпраця НАТО з партнерами, науковими установами, приватним сектором, включаючи стартапи з метою зміцнення економічного потенціалу та промислової бази союзників.

У рамках реалізації повістки "НАТО – 2030" важливе місце також посідають оборонні інновації, спрямовані на покращення трансатлантичного співробітництва у сфері впровадження та розвитку критично важливих технологій. Тобто кінцевою метою є прагнення Альянсу зберегти технологічне домінування та перемогти Китай, Росію та інших великих гравців під час гонки технологічного озброєння. У фокусі уваги НАТО сконцентровані такі питання як: створення оперативної мережі інноваційних центрів, просування успішних інноваційних бізнес-моделей та оперативних моделей, підвищення спроможностей й рівня технічної та цифрової грамотності персоналу.

Висновки.

Роль та значення технологій штучного інтелекту у світових масштабах не можна недооцінювати. В сучасних умовах у світі відбувається прискорення впровадження технологічних рішень, розроблених на основі штучного інтелекту у різних галузях економіки, державного управління та сферах суспільних відносин. Практичне використання технологій штучного інтелекту передбачає обробку великих масивів даних та машинне навчання, за якого програми та алгоритми постійно удосконалюються. Штучний інтелект дозволяє практично повністю виключити людський фактор з процесів забезпечення захисту інформації та залишає лише допоміжні функції моніторингу та корекції. У зв'язку з цим штучний інтелект є технологією майбутнього. За оцінками експертів, очікується, що завдяки впровадженню таких рішень зростання світової економіки у 2024 році дорівнюватиме $1 трлн. Штучний інтелект та його технології відкривають нові горизонти в епоху цифровізації та розпочинають активно використовуються у цивільній та військовій сферах.

Кожна держава світу, розуміючи переваги штучного інтелекту намагається законодавчо врегулювати сфери його використання. Аналіз висвітлених нормативно-правових актів дає змогу визначити форми впровадження технологій штучного інтелекту у тій чи іншій країні світу, якими виступають: розробка та реалізація пілотних проектів, запровадження фінансових та податкових пільг для розробників та інвесторів, затвердження керівних принципів та етнічних норм використання штучного інтелекту тощо. Ключовим питанням для країн світу залишається формат фінансування відповідних розробок та обсяг залучених інвестицій для розвитку технологій штучного інтелекту.

Як не парадоксально, навіть країни третього світу із значним технологічним відставанням, на кшталт Узбекистану, переймаються проблемою актуалізації прискорення впровадження технологій штучного інтелекту у реалії повсякденного життя. За таких умов у світі спостерігається активізація та динамічний розвиток цієї сфери, а для деяких країн світу вимальовуються перспективи нарощування потужностей з метою протистояння та боротьби за глобальне технологічне домінування. Також чином, можливо підсумувати, що саме технології штучного інтелекту беззаперечно є рушійною силою у питаннях забезпечення безпеки та оборони, про що яскраво свідчать останні кроки та ініціативи, які здійснюють Пентагон та НАТО. Світ поступово переходить у нову еру протистояння та реагування на виклики й загрози за допомогою штучного інтелекту, у тому числі й у військових конфліктах, про що свідчить започаткована гонка технологічних озброєнь між провідними країнами світу (США, КНР, РФ) з метою встановлення й опанування світового цифрового лідерства.

Використана література

1. Брижко В.М., Фурашев В.Н. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право*. № 1(20)/2017. С. 51-67.

2. Бусол О.Ю. Потенційна небезпека штучного інтелекту. *Інформація і право*. № 2(14)/2015. С. 121-127.

3. Радутний О.Е. Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект. *Інформація і право*. № 2(25)/2018. С. 158-170.

4. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації*. 2020. № 4 (44). С. 6-11.

5. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.

6. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. *Інформація і право*. № 1(28)/2019. С. 61-67.

7. Косілова О.І., Солодовнікова Х.К. Права і свободи людини і громадянина v.s. штучний інтелект: проблемні аспекти. *Інформація і право*. № 4(35)/2020. С. 56-66.

8. Кривецький О. До проблеми правового регулювання штучного інтелекту. *Громадська думка про правотворення*. 2018. № 14. С. 15-19. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=3728:do-problemi-pravovogoregulyuvannya-shtuchnogo-intelektu&catid=8 &Itemid=350

9. Міліцина К. Об'єкти, створені за допомогою штучного інтелекту і штучним інтелектом безпосередньо, та авторське право США. *Підприємництво, господарство і право*. 2019. № 5. С. 343-346.

10. Government Artificial Intelligence Readiness Index 2020. URL: https://www.oxfordinsights.com/government-ai-readiness-index-2020 (дата звернення: 20.02.2021).

11. О Концепции информационной безопасности Республики Беларусь: Постановление Совета Министров Республики Беларусь от 18 марта 2019 года № 1. URL: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (дата звернення: 20.02.2021).

12. О государственной программе "Цифровое развитие Беларуси" на 2021 – 2025 годы: Постановление Совета Министров Республики Беларусь от 2 февраля 2021 года № 66. URL: https://pravo.by/document/?guid=12551&p0=C22100066&p1=1&p5=0

13. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 года № 490. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/#1000 (дата звернення: 20.02.2021).

14. О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта: Постановление Президента Республики Узбекистан от 17 февраля 2021 года № 4996. URL: https://lex.uz/docs/5297051(дата звернення: 20.02.2021).

15. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 20.02.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Інформаційна і національна безпека

УДК 32.019.51:323.28:323.2(477)

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-2488-7377.

ТЕРОРИЗМ: ІНФОРМАЦІЙНО-ПРАВОВИЙ ВИМІР

Анотація. *У статті висвітлені теоретико-правові аспекти інформаційного тероризму. Наведено класифікацію видів інформаційного тероризму в інформаційному просторі. Міститься аналіз нормативних актів України у сфері інформаційної безпеки. Запропоновано визначення інформаційного тероризму.*

Ключові слова*: тероризм, інформаційний тероризм, інформаційні технології, інформаційне насильство, кібертероризм.*

Summary*. The article highlights the theoretical and legal aspects of information terrorism. The classification of types of information terrorism in the information space is given. The analysis of regulatory acts of Ukraine in the field of information security is provided. The definition of information terrorism is offered.*

Keywords*: terrorism, information terrorism, information technologies, information violence, cyberterrorism.*

Аннотация*. В статье освещены теоретико-правовые аспекты информационного терроризма. Приведена классификация видов информационного терроризма в информационном пространстве. Содержится анализ нормативно-правовых актов в области информационной безопасности. Предложено определение информационного терроризма.*

Ключевые слова*: терроризм, информационный терроризм, информационные технологии, информационное насилие, кибертерроризм*.

Постановка проблеми. Стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж та процес побудови інформаційного суспільства обумовили виникнення нових загроз в інформаційній сфері, однією з яких на часі є використання виникаючих можливостей в терористичній діяльності, що заподіює шкоду життєво важливим інтересам особи, суспільства і держави. Рівень загрози інформаційного тероризму стрімко зростає в сучасних умовах глобалізації та набуває надзвичайно деструктивного значення. Особливу загрозу світовим інформаційним системам складає поєднання технологічного та наукового потенціалу провідних країн світу. Високотехнологічні терористичні акції здатні продукувати системну кризу для всієї світової спільноти. Україна, перебуваючи у стані гібридної війни, зазнає негативного інформаційного впливу, наслідки якого сьогодні гостро відчуваються у суспільстві.

Результати аналізу наукових публікацій. Теоретичні аспекти протидії інформаційному тероризму досліджували Лабенко Л.В. [1], Бураєва Л.А. [2], Банк Р.О. [3], Пилипчук В.Г., Дзьобань О.П. [4] та ін. Особливості інформаційного тероризму як одного із засобів інформаційної війни, а також види та застосування інформаційної

зброї висвітлені у працях Почепцова Г.Г. [5], Брижка В.М. [6], Коршунова В.О. [7], Рижова І.М. [8], Яцик Т.П. [9] та ін. Серед зарубіжних теоретиків і практиків, які займалися дослідженням інформаційного тероризму як засобу введення інформаційної війни в умовах глобалізації та розвитку кіберпростору, слід зазначити Д. Белла [10], Ж. Бодрійара [11], Е. Тоффлера [12], Б. Хофмана [13], А. Шміда [14] та ін. Міжнародно-правові та кримінально-правові аспекти протидії інформаційному тероризму висвітлені в працях Ковлагина Д.А. [15], Настюка В.Я., Трофімова С.А. [16], Молчанова М.А., Матевосової Є.К. [16].

Водночас, серед науковців відсутні єдині підходи до визначення поняття "інформаційний тероризм". Існують також розбіжності поглядів щодо форм і різновидів інформаційного тероризму.

Метою статті є удосконалення визначення інформаційного тероризму з урахуванням підходів, вироблених вітчизняними і зарубіжними вченими.

Виклад основного матеріалу. Законодавство України не містить визначення інформаційного тероризму. Закон України "Про боротьбу з тероризмом" згадує поняття "технологічний тероризм", під яким слід розуміти кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру (ст. 1) [18]. Наведене визначення не збігається з дефініцією інформаційного тероризму, яке є ширшим за змістом.

Закон України "Про основні засади забезпечення кібербезпеки України" містить визначення "кібертероризму" [19], який можна визнати лише одним з різновидів інформаційного тероризму, про що мова буде іти далі.

Доктрина інформаційної безпеки [20] визначає лише актуальні загрози та пріоритети державної політики в інформаційній сфері. З-поміж загроз згадуються спеціальні інформаційні операції, інформаційна експансія, інформаційне домінування, зміст яких лише частково охоплює поняття інформаційного тероризму.

Стратегія національної безпеки України [21] основним завданням розвитку системи кібербезпеки визначає гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації (п. 52), а серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів виділяється активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам. У Стратегії згадується "інформаційна зброя", яку застосовує Російська Федерація для зміцнення своїх позицій у Європі, а також поширення міжнародного тероризму у кіберпросторі як загроза національній безпеці України.

Очевидно, що визначення інформаційного тероризму має знайти відображення у Стратегії інформаційної безпеки України, розробка якої випливає з положень Стратегії національної безпеки України (п. 66).

Зауважимо, що визначення інформаційного тероризму не містять й міжнародні правові акти, серед яких виділяються Конвенція Ради Європи про запобігання тероризму (2005 р.), Конвенція про кіберзлочинність (2001 р.) Аналіз зазначених актів дає підстави для висновку, що кібертероризм є частиною або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму [3, с. 112].

Таким чином, аналіз нормативно-правових актів у сфері боротьби з тероризмом свідчить про те, що поняття інформаційного тероризму не знайшло відображення у чинному законодавстві України. Однак, як зазначалося раніше, на доктринальному рівні це поняття досліджувалося як вченими, так і практичними фахівцями у сфері інформаційних технологій. На думку більшості зарубіжних дослідників, інформаційний тероризм є різновидом терористичної діяльності, яка пов'язана з досягненнями у сфері інформаційних технологій.

На думку О. Ісакова, інформаційний тероризм – це сфера негативного впливу на особу, суспільство, державу за допомогою всіх видів інформації з метою послаблення або повалення конституційного ладу [22].

Схожої думки додержується І.М. Глотіна, на думку якої інформаційний тероризм як багатогранне, мінливе явище є формою негативного впливу на особу, суспільства, державу за допомогою використання інформаційно-комунікаційний технологій. Вільний доступ, анонімність користувачів, масовість аудиторії, обмежені можливості контролю, недосконаліть законодавства є чинниками, які сприяють поширенню інформаційного тероризму [23, с. 134].

Окремі дослідники розглядають інформаційний тероризм в межах виключно інтелектуальної сфери. Так, А. Кота вважає інформаційний тероризм одним з найбільш перспективних видів тероризму, який діє в інтелектуальній сфері і породжує новий вид пов'язаного з кіберпростором насильства, яке може бути спрямоване проти будь-кого, а його успіх забезпечується не грубою силою, а нейронами [24, с. 56]. Дійсно, різного роду маніпуляції суспільною свідомістю негативно впливають на інтелектуальний розвиток людства, а інформаційний тероризм можна визнати різновидом деструктивного інформаційно-психологічного впливу на масову свідомість людей [25].

З точки зору американського професора У. Тафойа, інформаційним тероризмом є залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об'єктів критичної інфраструктури або знищення інформації [26].

Слід зазначити, що визначення інформаційного тероризму висвітлюються і в дослідженнях вітчизняних вчених.

В.О. Коршунов під інформаційним тероризмом пропонує розуміти новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [7, с. 6].

Т.П. Яцик вважає, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних з національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [9, с. 57].

На кримінально-правові аспекти інформаційного тероризму звертає увагу Р.О. Банк, який вважає за доцільне передбачити у законодавстві відповідальність за інформаційний терористичний акт. Під таким актом пропонується розуміти дії інформаційно-психологічного та інформаційно-технічного впливу, спрямовані на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктних ситуацій з метою маніпуляції та зомбіювання свідомості особи чи

широкого кола осіб шляхом реалізації способів і методів інформаційного насильства, застосування інформаційної зброї [3, с. 115].

Аналіз національного законодавства та наукової літератури з порушеного питання дає підстави для висновку, що інформаційний тероризм – доктринальне поняття теорії інформаційної безпеки, під яким розуміють: 1) різновид форми суспільно небезпечного діяння, яким є "тероризм"; 2) форму деструктивного інформаційно-психологічного впливу на особистість, суспільство і державу; 3) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади і управління, пов'язані із розповсюдженням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій в державі, нагнітання страху і напруги у суспільстві [1]; 4) певний насильницький пропагандистський вплив на психіку людини, який не дає йому можливості критично оцінювати отриману інформацію [2]; 5) новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної. структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [7]; 6) множину інформаційних війн та інформаційних спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [9]; 7) злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [27]; 8) ідеологічно обґрунтовану практику впливу, направленого на залякування населення, на прийняття рішення або вчинення дії (бездіяльності) органом влади, органом місцевого самоврядування, міжнародною організацією, соціальною групою, юридичною особою або фізичною особою в межах інформаційного простору, пов'язаного з використанням інформації, інформаційних технологій і (або) інформаційного ресурсу [15].

Основою інформаційного тероризму є інформаційне насильство, з-поміж властивостей якого виділяється: несиловий, ідеальний характер, вихід за межі фізичних закономірностей; нелінійність; порушення закону збереження речовини й енергії, кумулятивний характер, можливість бурхливого зростання інформації; широке розповсюдження; можливість ідеального клонування; нелокалізованість у часі; опосередкований характер і прихованість впливу; віртуальний характер впливу; можливість фіксування; селективність; легкість доступу, злому інформаційних систем [28].

Залежно від спрямованості умовно можна виділити два види інформаційного тероризму: 1) "психологічний" (пропаганда тероризму, створення атмосфери страху і паніки в суспільстві і т.д.); 2) "технічний" (контролювання або блокування каналів передачі масової інформації, порушення функціонування об'єктів інформаційної інфраструктури та ін.) [17].

Залежно від злочинної мети та використання інструментів (засобів) її досягнення інформаційний тероризм теж поділяється на два види: медіа-тероризм та кібертероризм.

Медіа-тероризм – зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, сприяння вчиненню теракту). Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо. [3, с. 114].

Кібертероризм – навмисна, політично вмотивована атака на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій [4]. Закон України "Про основні засади забезпечення кібербезпеки України" визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1) [19]. Кібертероризм є серйозною суспільно-політичною загрозою для людства, у порівнянні навіть з ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози через свою новизну, не до кінця ще усвідомлений і вивчений. Світовий досвід свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні мережі та організації віддаленої кібератаки на інформаційні ресурси жертви [29, с. 42-43].

Також небезпечними проявами інформаційного тероризму є релігійні, псевдорелігійні, сектантські організації, в середовищі яких зароджуються ідеї тероризму, а масовий інформаційний вплив на людей забезпечує поширення ідеології прихильників таких організацій [25, с. 7].

Викладене свідчить про необхідність визначення на законодавчому рівні поняття "інформаційний тероризм", а також формування системи запобігання тероризму з урахуванням його інформаційних різновидів. У ст. 3 Закону України "Про боротьбу з тероризмом" передбачено принцип пріоритетності попереджувальних заходів. Кінцевим підсумком реалізації державної політики у сфері запобігання тероризму має стати усунення причин і умов, що сприяють виникненню цього негативного явища. Курс на пріоритетність запобігання тероризму обумовлюється такими чинниками: 1) доктринальним визначенням стратегії запобіжної діяльності; 2) прогнозуванням змін і тенденцій тероризму та його проявів; 3) визначенням порядку, методики, форм і засобів запобіжної діяльності; 4) інформаційним забезпеченням реалізації визначених завдань; 5) розробкою програм, планів запобігання тероризму; 6) координацією запобіжної діяльності суб'єктів боротьби з тероризмом; 7) здійсненням контролю за виконанням; 8) матеріальним та іншим ресурсним забезпеченням [30].

Завдання, основні принципи та напрями вдосконалення загальнодержавної системи боротьби з тероризмом з огляду на сучасні терористичні загрози національній безпеці України та прогноз їх розвитку визначені Концепцією боротьби з тероризмом в Україні, напрями реалізації якої передбачають: визначення та аналіз причин і умов, що призводять до поширення тероризму; удосконалення правових та організаційних основ боротьби з тероризмом; удосконалення існуючих, розроблення та впровадження нових методів боротьби з тероризмом; оптимізація шляхів та способів захисту життя і безпеки, прав і свобод людини і громадянина, захисту інтересів суспільства та держави від терористичних посягань; поліпшення інформаційного, наукового, кадрового та матеріально-технічного забезпечення суб'єктів боротьби з тероризмом [31].

Одним з визначених Концепцією пріоритетів боротьби з тероризмом є інформаційне, наукове та інше забезпечення боротьби з тероризмом. Відповідно до Концепції таке забезпечення має включати здійснення моніторингу стану і тенденцій поширення тероризму; проведення постійного системного аналізу і багатовимірного комплексного оцінювання причин та умов, що впливають на виникнення і поширення

тероризму, постійного і своєчасного обміну між суб'єктами боротьби з тероризмом інформацією про терористичні загрози; уніфікації програм навчання, підготовки та перепідготовки особового складу та працівників суб'єктів боротьби з тероризмом; застосування сучасних систем безпеки на об'єктах можливих терористичних посягань; забезпечення суб'єктів боротьби з тероризмом необхідною ресурсною базою [31].

Реалізація зазначених заходів безумовно сприятиме запобіганню різним проявам тероризму, у т.ч. інформаційного. Проте, на законодавчому рівні залишається невизначеним поняття "інформаційний тероризм", його ознаки та види. Це, у свою чергу, ускладнює реалізацію антитерористичної політики держави.

Висновки.

Таким чином, як узагальнююче можна надати наступне визначення поняття "інформаційний тероризм": *Інформаційний тероризм – антисоціальне явище, для якого характерним є умисне застосування інформаційно-психологічного та інформаційно-технічного впливу, спрямованого на маніпуляцію чи залякування населення або заподіяння шкоди суспільству чи окремим особам з метою примусити публічну владу, міжнародну організацію, юридичну чи фізичну особу (групу осіб) вчинити якусь дію (або утриматися від її вчинення) в межах інформаційного простору, пов'язаного з використанням інформації, інформаційних технологій і (або) інформаційного простору*.

Закріплення такого поняття на законодавчому рівні сприятиме реалізації державної інформаційної політики в контексті протидії правопорушенням в інформаційній сфері, забезпеченню інформаційної безпеки як складової національної безпеки України.

Використана література

1. Лабенко Л.В. Інформаційний тероризм: поняття та ознаки. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3439/%D0%9B%D0%B0%D0%B1%D0%B5%D0%BD%D0%BA%D0%BE.pdf?sequence=1&isAllowed=y (дата звернення: 04.02.2021).

2. Бураева Л.А. Информационный терроризм как угроза национальной безопасности Российской Федерации. URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoy-federatsii/viewer (дата звернення: 04.02.2021).

3. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* № 1(16)/2016. С. 110-116.

4. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.

5. Почепцов Г.Г. Информационные войны. – (Серия: Образовательная библиотека). Издательство: Рефл-бук, 2001. 576 с.

6. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

7. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. …канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

8. Рижов І.М., Строгий В.І. Концептуальні засади соціально-інформаційних технологій упередження кризових явищ соцілального характеру (на прикладі моніторингу тероризму). *Науковий вісник Львівського державного університету внутрішніх справ*. *Серія: "Юридичні науки"*. 2014. № 3. С. 219-228.

9. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право).* 2014. № 2(65). С. 55-60.

10. Livingstone M.H. International terrorism in the contemporary World. Westport (Conn.). 1978.

11. Жан Бодрийяр. Дух терроризма. Войны в заливе не было (сборник). Москва: “РИПОЛ классик”, 2016. 930 с.

12. Тоффлер Э., Тоффлер Х. Война и антивойна: Что такое война и как с ней бороться. Как выжить на рассвете XXI века. Москва: АСТ: Транзиткнига, 2005. 412 с.

13. Хоффман Б. Терроризм – взгляд изнутри / пер. с анг. Е. Сажина. Москва: Ультра. Культура, 2003. 252 с.

14. Шмид А. Статистика терроризма: задачи определения тенденций в глобальном масштабе: *Форум по проблемам преступности и общества*. Т. 4. № 1, 2. Декабрь 2004 г. С. 51-71.

15. Ковлагина Д.А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия: дис. ...канд. юрид. наук: спец. 12.00.08. ФГБОУ ВПО Саратовская государственная юридическая академия, 2016. 270 с.

16. Настюк В.Я. Трофімов С.А. Міжнародно-правовий режим протидії тероризму: монографія. Харків: Право, 2008. 350 с.

17. Молчанов Н.А., Матевосова Е.К. Информационный терроризм в международно-правовом контексте. *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2018. № (5). С. 94-103.

18. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 04.02.2021).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.02.2021).

20. Доктрина інформаційної безпеки: Указ Президента України від 25.02.17 р. № 47. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 04.02.2021).

21. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 04.02.2021).

22. Исаков А.И. Информационный терроризм. *Обозреватель-Observer.* – (Научно-аналитический журнал). URL: http://observer.materik.ru/observer/N5-6_02/5-6_10.htm (дата звернення: 04.02.2021).

23. Глотина И.М. Информационный терроризм и его влияния на экономику. *Экономическая глобализация и проблемы национальной международной безопасности*. 2014. С. 132-134. URL: file:///C:/Users/%D0%91%D0%BE%D1%80%D0%B8%D1%81/Downloads/informatsionnyy-terrorizm-i-ego-vliyanie-na-ekonomiku.pdf (дата звернення: 04.02.2021).

24. Кота А. Эпоха терроризма. *Международный терроризм и право*. Москва, 2004. С. 56-60.

25. Арчаков В. О понимании проблемы информационного терроризма в глобальном и региональном масштабе. URL: https://beldumka.belta.by/isfiles/000167_885379.pdf (дата звернення: 04.02.2021).

26. Tafoya W.L. Cyber Terror. *FBI Law Enforcement Bulletin.* 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcementbulletin/november-2011/cyber-terror (дата звернення: 04.02.2021).

27. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *NATO Library at: Terrorismand political violence*. Vol. 12, no. 2. Summer 2000. P. 97-122.

28. Дзьобань О.П. Насильство інформаційне. – (Енциклопедія соціогуманітарної інформології). Київ: Видавничий дім “Гельветика”, 2020. Т. 1. С. 151-155.

29. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия: доклады ТУСУРа, 2010. № 1(21). Ч. 1. С. 41-45.

30. Леонов Б.Д. Запобігання та протидія тероризму: теоретичні підходи. *Часопис Національного університету “Острозька академія”. Серія: “Право”*. 2012. № 2(6). URL: http://lj.oa.edu.ua/articles/2012/n2/12lbdttp.pdf

31. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL:https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 04.02.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 343.326

БІЛАН І.А., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1237-1565.

ПРОТИДІЯ ТЕРОРИЗМУ: ДОСВІД ЄС

***Анотація**. У статті аналізується досвід ЄС у сфері протидії тероризму. Розкриваються проблеми реалізації державної політики у цій сфері. Досліджуються вжиті країнами ЄС заходи, спрямовані на запобігання тероризму. Проаналізовано національне законодавство окремих європейських країн з питань протидії тероризму. Зроблено висновок, що сучасна міжнародна політика боротьби з тероризмом характеризується прийняттям актів, які враховують необхідність криміналізації всіх суспільно небезпечних проявів терористичної діяльності, посиленням міжвідомчого співробітництва, налагоджуванням зв'язків між регіональними антитерористичними структурами правоохоронних органів та спеціальних служб.*

***Ключові слова**: тероризм, протидія, запобігання, терористична загроза, ЄС.*

***Summary**. The article analyzes the EU experience in the field of counter-terrorism. Problems of implementation of the state policy in this sphere are explored. Measures taken by EU countries to prevent terrorism are being examined. The national legislation of some European countries on counter-terrorism is analyzed. The article concludes that the current international counter-terrorism policy is characterized by the adoption of acts that take into account the need to criminalize all socially dangerous acts of terrorism, strengthen interdepartmental cooperation between law enforcement and special services of foreign countries, establish links between regional counterterrorism structures.*

***Keywords**: terrorism, counteraction, prevention, terrorist threat, EU.*

***Аннотация**. В статье анализируется опыт ЕС в области противодействия терроризму. Раскрываются проблемные вопросы реализации государственной политики в этой области. Исследуются принятые в странах ЕС мероприятия, направленные на предотвращение терроризма. Проанализировано национальное законодательство отдельных европейских стран по воспросу противодействия терроризму. Сделан вывод о том, что современная международная политика борьбы с терроризмом характеризуется принятием актов, которые учитывают необходимость криминализации всех общественно опасных проявлений террористической деятельности, усилением межведомственного сотрудничества, усовершенствованием связей между региональными антитеррористическими структурами правоохранительных органов и специальных служб.*

***Ключевые слова**: терроризм, противодействие, предотвращение, террористическая угроза, ЕС.*

Постановка проблеми. Терористична загроза в світі знаходиться нині на досить високому рівні. Від неї потерпають як країни в яких тривають збройні конфлікти (передусім на Близькому Сході та в Африці), так і країни Заходу, які до останнього часу вважалися цілком безпечними з огляду на розвинену систему правоохоронних органів і спецслужб [1]. Якщо за період 2007 – 2013 рр. кількість терористичних актів в країнах ЄС зменшилася майже вчетверо, то в 2013 р. зафіксовано зростання на 39 %, а у 2015 р. спостерігався абсолютний пік (1077 випадків), що вдвічі перевищує показник 2013 р. [2].

Протидіяти цій загрозі стає дедалі важче [1], про що свідчить криваві теракти січня та листопада 2015 р. у Парижі, березня 2016 р. у Брюсселі, травня 2017 року в Манчестері.

Результати аналізу наукових публікацій. Окремі аспекти протидії тероризму в іноземних країнах висвітлено в працях вітчизняних науковців: В.Ф. Антипенка, А.А. Вознюка, В.М. Дрьоміна, В.Н. Кубальського, Б.Д. Леонова, В.В. Мокляка, С.М. Мохончука, І.В. Михальчук, Д.Й. Никифорчука, М.В. Рибачука, М.М. Руденка, О.Г. Семенюка, М.В. Семикіна, О.В. Шамари та ін. Водночас, недостатньо врахованим для вітчизняного законодавця залишається позитивний досвід країн ЄС у протидії тероризму.

Метою статті є оцінка законодавчих ініціатив і практичних заходів ЄС в контексті вдосконалення сучасної стратегії протидії тероризму.

Виклад основного матеріалу. Аналіз наявних міжнародних антитерористичних структур, які займаються запобіганням тероризму, дозволяє констатувати, що існує міжнародний (інтернаціональний), регіональний [3] та (субрегіональний) рівень організації боротьби з тероризмом.

Найважливішим нормативним актом, спрямованим на запобігання тероризму, є Глобальна контртерористична стратегія ООН, прийнята у 2006 р. З того часу вже неодноразово (у 2008, 2010, 2014 рр.) були здійснені її огляди, у результаті чого Генеральна Асамблея ООН підтвердила Глобальну контртерористичну стратегію ООН та її компоненти [3].

12 грудня 2016 року на засіданні Ради Безпеки ООН було прийнято Резолюцію № 2322 (одним з авторів є Україна), яка закликає держави до укріплення та розширення міждержавної взаємодії та взаємодопомоги у сфері боротьби з тероризмом, обміну інформацією щодо терористичних організацій та бойовиків-терористів, включаючи їх біометричні та біографічні дані. Прикладом тривалої співпраці з питань протидії тероризму є взаємодія США з країнами Європейського Союзу (передусім Францією, Німеччиною та Великобританією), яка розширюється з 2001 року, коли адміністрація Джорджа Буша-молодшого підписала ключову угоду з поліцейською службою ЄС (Європол). Угода надала можливість здійснювати обмін стратегічною та технічною інформацією з питань протидії тероризму, відмивання грошей, протиправної торгівлі наркотиками, ядерними, радіологічними речовинами та людьми. У 2002 році додаткова угода між Європолом та компетентними органами США дозволила обмінюватись персональними даними підозрюваних осіб, а також запровадила інститут офіцерів зв'язку. З того часу взаємодія ЄС та США розширюється та охоплює також питання протидії фінансуванню тероризму, нелегальній міграції, іноземним бойовикам-терористам. В лютому 2015 року відповідні служби США підписали дві нові угоди з Європолом щодо протидії нелегальній міграції та іноземним бойовикам. Це забезпечило платформу для обміну інформацією щодо осіб, які забезпечують вербування та переправлення іноземних бойовиків, а також джерел їх фінансування [1].

Довгий час очільники ЄС не приділяли достатньої уваги цьому загрозливому явищу. У Стратегії європейської безпеки (2003 р.) констатуються очевидні факти: тероризм ставить під загрозу життя людей, намагається підірвати відкритість і толерантність суспільств, може застосовувати необмежене насильство, набув глобального масштабу, що може спричинити значні жертви [2].

Як справедливо зазначає Р. Паркес, раніше в ЄС головна увага була прикута до таких питань, як підвищення ефективності прикордонного контрою, захист населення від пожеж, покращення діяльності структур охорони здоров'я тощо. На периферії нагальних проблем, що вимагають розв'язання, опинилися теми запобігання терористичним актам, лісовим пожежам, іншим стихійним лихам [4, с. 1].

В рамках ЄС правову базу для спільних дій у сфері боротьби з тероризмом складає Конвенція Ради Європи про запобігання тероризму (2006 року) та Додатковий протокол

до неї (2015 року), положення якого передбачають зобов'язання для держав встановити кримінальну відповідальність за вчинення таких дій, як участь у терористичній організації або групі (ст. 2), проходження навчання тероризму (ст. 3), виїзд за кордон з терористичною метою (ст. 4), фінансування виїзду за кордон з метою терористичної діяльності (ст. 5), організацію чи сприяння іншим способом виїзду за кордон з метою терористичної діяльності (ст. 6).

Реалізація політики ЄС у сфері боротьби з тероризмом проводиться через формування співробітництва правоохоронних органів і спеціальних служб європейських країн, посилення взаємодії з Євроюстом, Європолом, іншими регіональними (субрегіональними) структурами у цій сфері. У ЄС вжито низку заходів, спрямованих, у першу чергу, на підвищення ефективності взаємодії та обміну інформацією між національними спеціальними та поліцейськими службами, а також посилення прикордонного контролю. У 2016 році на основі інформації Антитерористичної групи (м. Гаага) створено єдину базу даних, до якої в режимі реального часу мають доступ понад 20 європейських спецслужб. Розроблено та заплановано реалізацію пілотного проекту щодо автоматизованого обміну даними між правоохоронними органами держав-членів ЄС щодо осіб, які мають судимість [1].

Крім цього, активізується робота з введення в дію Європейської інформаційної системи авторизації подорожей. У грудні 2016 року Єврокомісією було представлено комплекс заходів по боротьбі з фінансуванням тероризму, посилення прикордонного контролю, удосконалення Шенгенської інформаційної системи (далі – SIS) [5]. В рамках таких заходів пропонується внесення у зазначену базу даних SIS щодо: осіб, які підозрюються у причетності до терористичної діяльності; осіб, яким заборонено в'їзд до Євросоюзу; мігрантів, стосовно яких видано санкцію на депортацію. Також ЄС пропонує забезпечити необмежений доступ державам-членам ЄС до баз даних Європолу. За попередніми оцінками, запровадження цих заходів коштуватиме близько 70 млн. Євро.

Сьогодні на рівні глав міністерств внутрішніх справ ЄС досягнуто згоду щодо посилення і покращення взаємного доступу до даних, що мають вирішальне значення для запобігання і припинення терактів. Спільна заява міністрів внутрішніх справ ЄС також вказує на необхідність вдосконалення європейського поліцейського партнерства, запобігання радикалізації, обміну інформацією про осіб, що представляють терористичну загрозу або загрозу насильницького екстремізму, запобігання проникненню в ЄС іноземних бойовиків-терористів, незалежно від того, чи є вони громадянами держави-члена Євросоюзу чи ні [6].

Як стверджують А. Шміт та Д. Теннес, останнім часом увага європейської спільноти до тероризму актуалізувалася не лише у зв'язку зі зростанням кількості терористичних актів, а через небувалу хвилю мігрантів, головним чином із мусульманських країн. Вони застерігають від легковажних висновків і вказують на відсутність серйозних наукових досліджень на перетині двох феноменів (тероризму та міграції) [7, с. 3].

Посилення міграційних процесів створює додаткові можливості для активізації діяльності міжнародних терористичних організацій. З огляду на це, уряди країн з найбільшими міграційними потоками (у першу чергу держави-члени ЄС) вживають заходи щодо посилення прикордонного контролю, впровадження ефективних систем спостереження за мігрантами та запобігання нелегальній міграції, як важливих елементів системи попередження вчинення терористичних актів [1]. На думку лідерів держав-членів ЄС, захист і контроль на зовнішніх кордонах ЄС необхідно посилити.

Зокрема, компетентним органам держав ЄС необхідно чітко знати, хто в'їжджає в Шенгенську зону, і хто подорожує по ній [8].

З метою протидії поширенню тероризму та здійснення скоординованої діяльності антитерористичних організацій в Європейському контртерористичному центрі Європолу (ЕСТС) створено Групи Інтернет-досліджень (European Internet Referral Unit – IRU), які уповноважені на співробітництво з правоохоронними органами не лише держав-членів Європейського Союзу, а й інших держав, а також із приватним сектором [2].

28 квітня 2015 року у Страсбурзі представлено план боротьби з тероризмом та кіберзлочинністю, який передбачає три пріоритети безпекової політики, серед яких – запобігання тероризму і протидія радикалізації, боротьба з організованою злочинністю та боротьба з кіберзлочинністю. Також ЄС планує покращити співпрацю з третіми країнами для подолання такого явища, як іноземні військові найманці [9].

У січні 2016 р. в ЄС створено новий Антитерористичний центр, який працює на базі Європолу. До повноважень центру віднесено вирішення питання боротьби проти іноземних бойовиків, незаконного обігу вогнепальної зброї та фінансування тероризму [10]. Принагідно зазначимо, що за даними Європолу на теперішній момент зареєстровано більше 5 тис. міжнародних організованих злочинних угруповань, кількість яких різко зросла за останні кілька років (до 45 % проти 33 % в 2013 році). З моменту запровадження наприкінці січня 2016 року спеціальної бази даних Європолом затримано 24 особи з числа найбільш розшукуваних злочинців Європи [11].

У лютому 2016 р. Єврокомісія прийняла План дій щодо боротьби з фінансуванням тероризму [12], зміст якого передбачає заходи, спрямовані на вирішення питання боротьби з відмиванням грошей та незаконним рухом готівки, що пов'язані з тероризмом і злочинністю, шляхом заморожування і конфіскації активів, а також через удосконалення механізмів виявлення та відстеження потоків фінансування терористів.

В багатьох країнах запроваджено та виконуються спеціалізовані програми, спрямовані на недопущення поширення у суспільстві екстремістських поглядів, запобігання втягування молоді до участі у терористичних організаціях, застосовуються процедури амністії окремих осіб, які брали участь в терористичній діяльності, їх адаптації та ресоціалізації. З огляду на зростання терористичної загрози низкою країн було змінено національне законодавство з питань протидії тероризму, у т.ч. надано додаткових повноважень правоохоронним органам і спеціальним службам [1].

У Великобританії у 2015 році набув чинності Закон "Про безпеку та протидію тероризму" (*Counter-Terrorism and Security 2015*), який передбачає: 1) повноваження правоохоронних органів тимчасово витребувати документи, якщо підозрювана особа має намір виїзду в іншу країну з терористичною метою; 2) обмеження Інтернет-сайтів, де поширюються екстремістські матеріали; 3) профілактику тероризму та екстремізму органами місцевої влади, пенітенціарної служби, шкільними та лікарняними закладами; 4) посилення покарання за фінансові злочини, у т.ч. відмивання грошей, отриманих злочинним шляхом [13].

У 2016 році Уряд Великобританії оприлюднив план заходів, який передбачає збільшення на 15 % (на 1900 осіб) штату співробітників служби зовнішньої розвідки (МІ6), тоді як бюджет боротьби з тероризмом заплановано збільшити (на 30 %) з урахуванням необхідності придбання та утримання нової військової та спеціальної техніки, у т.ч. для підтримки сил швидкого реагування [14].

Після терактів, що сталися у Парижі 13 листопада 2015 року, Парламент Франції у квітні 2016 році прийняв новий Закон "Про боротьбу з тероризмом", норми якого розширюють повноваження правоохоронних органів, зокрема, у частині: проведення

обшуків у нічний час, у т.ч. у приватних будинках, технічного оснащення для здійснення електронного спостереження, спостереження в мережі Інтернет за сайтами і публікаціями, які містять заклики до вчинення терактів [15]. Також цей Закон передбачає: збільшення термінів покарання у виді позбавлення волі за терористичну діяльність (до довічного ув'язнення без права дострокового звільнення); організацію більш суворого режиму виконання покарань; встановлення обставин, які обтяжують покарання за вчинення окремих злочинів членами організованих угруповань у зв'язку з терористичними діями. Парламент також посилив адміністративний контроль над районами проведення антитерористичних операцій та затвердив положення про створення паризького суду, спеціалізацією якого є боротьба з кіберзлочинністю. Крім того, до Кримінального кодексу Франції внесені нові норми про злочини, зокрема, криміналізована діяльність із створення сайтів терористичної спрямованості за межами Франції. Також посилено боротьбу з відмиванням грошей і фінансуванням тероризму, зокрема, введено заборону на поповнення або використання банківських карт, які не можуть бути пов'язані з ідентифікованим користувачем [1].

24 червня 2016 р. у ФРН прийнято Закон "Про заходи з протидії тероризму", яким передбачається: запровадження більш жорстких правил реєстрації власників передплаченого зв'язку; організація автоматизованого обміну даними між національними спецслужбами та правоохоронними органами, а також із спецслужбами іноземних держав; збільшення термінів зберігання відповідної інформації; розширення оперативної складової у діяльності поліції, особливо у контексті протидії нелегальній міграції; зменшення з 16 до 14 років мінімального віку громадян, за якими дозволено здійснювати стеження [1; 16].

Також було внесено зміни до Закону "Про Федеральну розвідувальну службу" (далі – BND), якими розширюються її повноваження. Зокрема, передбачено надання цій службі права щодо зняття інформації з телекомунікаційних каналів на території ФРН, у т.ч. й прослуховування громадян країни (до цього BND не мала повноважень здійснювати такі заходи на території країни), зберігати інформацію про користувачів Інтернету та передавати її до партнерських спецслужб. Серед інших додаткових заходів, спрямованих на протидію тероризму в Німеччині, також можна виокремити: прийняття земельним парламентом Баварії закону, який передбачає посилення контролю з боку спецслужб у сфері зв'язку й обміну інформацією; надання Федеральному відомству із захисту конституції необмеженого доступу до баз даних та архівів організацій зв'язку та обміну інформацією, у т.ч. до клієнтської бази за умови отримання відповідного дозволу від комісії, що забезпечує виконання вимог конституції про таємницю листування, пошти та телефонного спілкування. Надається також право на обшуки, спостереження і використання агентів під прикриттям; підвищення спроможностей спецслужб з виявлення та припинення протиправної діяльності у кіберпросторі [1]. В межах нового законодавства передбачається підвищення ефективності координації діяльності підрозділів спеціального призначення; збільшення кількості особового складу спеціальних служб та поліції на 4600 осіб; розвиток систем відеоспостереження у містах.

У 2016 році у Польщі прийнято новий антитерористичний Закон, який надає спецслужбам додаткові повноваження для протидії терористичним загрозам, зокрема: припиняти масові заходи та публічні зібрання у разі підвищення рівня цієї загрози; з дозволу суду затримувати підозрілих осіб строком до 14 діб (на даний момент таке затримання не може більше 48 годин) до пред'явлення обвинувачення. За новим Законом обшуки і затримання можна буде здійснювати цілодобово [1]. Також Закон

передбачає невідкладну депортацію іноземців, які являють загрозу для країни, право, спрощення доступу спецслужб до баз даних, а також обов'язкову реєстрацію телефонних карт передоплати і швидкий доступ до особистих даних громадян через Агентство внутрішньої безпеки [17].

Висновки.

Оцінка законодавчих ініціатив і практичних заходів в контексті імплементації кращих світових практик ЄС у сфері боротьби з тероризмом свідчить про таке.

Сучасна міжнародна політика боротьби з тероризмом характеризується прийняттям актів, які враховують необхідність криміналізації всіх суспільно небезпечних проявів терористичної діяльності, посиленням міжвідомчого співробітництва правоохоронних органів та спеціальних служб іноземних країн, налагоджуванням зв'язків між регіональними антитерористичними структурами. У першу чергу, це стосується питань обміну інформацією, покращення взаємодії спецслужб та правоохоронних органів, посилення контролю за перетином державних кордонів та протидії фінансуванню тероризму. Важливе значення для України має посилення взаємодії з іншими країнами з питань протидії тероризму, налагодження обміну інформацією між уповноваженими органами як на міжнародному, так і на національному рівнях.

Політика більшості країн світу виходить із необхідності створення комплексної системи протидії тероризму з боку світової спільноти, що включає: удосконалення нормативно-правової бази з питань боротьби з тероризмом; посилення взаємодії правоохоронних органів, надання допомоги та сприяння в боротьбі з тероризмом; налагодження співпраці оперативних та розвідувальних органів; максимальний тиск на країни, які підтримують тероризм, використовуючи комплексні засоби протидії, в тому числі й військові; відмова в задоволенні вимог терористів; активізація діяльності силових структур та інші заходи. Комплексний підхід до проблем протидії тероризму є одним з визначальних факторів успішного протистояння терористичній загрозі.

На національному рівні провідні держави світу вживають додаткових заходів, спрямованих на профілактику тероризму, вдосконалюють антитерористичне законодавство, розширюють повноваження правоохоронних органів та спецслужб, надаючи їм додаткові інструменти, прагнуть покращити взаємодію та обмін інформацією між уповноваженими органами, створюють нові координуючі органи для боротьби з тероризмом, посилюють відповідальність за участь у терористичній діяльності [1].

Викладене дає підстави для висновку про невідповідність чинної Концепції боротьби з тероризмом [18] сучасним викликам і загрозам, що зумовлює необхідність її перегляду з урахуванням позитивного міжнародного досвіду у цій сфері. Її зміст, зокрема, має передбачати: підвищення ризиків тероризму у зв'язку зі збройними конфліктами; виникнення нових форм втягування людей у такі конфлікти для здійснення терористичної діяльності; появу внутрішньо демобілізованих військовослужбовців, які мають значний досвід роботи з вибуховими пристроями й речовинами, як категорій, особливо привабливих для вербування терористами з метою їх використання в терористичній діяльності.

Потребує удосконалення робота суб'єктів боротьби з тероризмом з населенням з питань запобігання тероризму. Активне залучення населення до цієї діяльності дозволить підвищити ефективність антитерористичної діяльності і збільшити рівень довіри населення до суб'єктів боротьби з тероризмом.

Використана література

1. Іноземний досвід протидії тероризму: висновки для України. – (Аналітична записка). URL: http://www.niss.gov.ua/articles/2446 (дата звернення: 28.02.2021).

2. Тероризм та безпекова політика ЄС. *Зовнішні справи*. 2020. № 7-8. URL: https://uaforeignaffairs.com/uk/category/bezpeka/terorizm-ta-bezpekova-politika-yes (дата звернення: 28.02.2021).

3. Форноляк В.М. Особливості співробітництва антитерористичних організацій країн європейського союзу щодо протидії тероризму. URL: http://www.academy.ssu.gov.ua/ua/page/page_1581428561.htm (дата звернення: 28.02.2021).

4. Parkes R. Migration and terrorism: the new frontiers for European solidarity. European Union Institute for Security Studies, Brief Issue 37. December 2015. 4 pp.

5. ЄС має намір закрити всі шляхи фінансування тероризму. URL: https://dt.ua/WORLD/yes-maye-namir-zakriti-vsi-shlyahi-finansuvannya-terorizmu-228210_.html (дата звернення: 28.02.2021).

6. ЄС хоче розширити обмін даними для боротьби з тероризмом. URL: https://www.dw.com/uk/yes-khoche-rozshyryty-obmin-danymy-dlia-borotby-z-teroryzmom/a-55596576 (дата звернення: 28.02.2021).

7. Schmid A.P., Tennes J. Terrorism and Migration: An Exploration. The Hague: International Centre for Counter Terrorism (ICCT), 2016. 63 pp.

8. ЄС посиить співпрацю у боротьбі з тероризмом. URL: https://www.dw.com/uk/yes-posylyt-spivpratsiu-dlia-borotby-z-teroryzmom/a-55558939 (дата звернення: 28.02.2021).

9. В ЄС представили новий план боротьби з тероризмом та кіберзлочинами. URL: http://tyzhden.ua/News/135332 (дата звернення: 28.02.2021).

10. Євросоюз створив власний Антитерористичний центр. URL: https://tsn.ua/svit/yevrosoyuz-stvoriv-vlasniy-antiteroristichniy-centr-578144.html (дата звернення: 28.02.2021).

11. Кількість злочинних угруповань в ЄС зросла до 5 тисяч – (Європол). URL: http://www.eurointegration.com.ua/news/2017/03/9/7062765 (дата звернення: 28.03.2021).

12. Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing COM(2016)050 final, Strasbourg, 2.2.2016. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0050

13. Тереза Мэй. Великобритания ужесточает антитеррористические законы. URL: http://tass.ru/mezhdunarodnaya-panorama/1593746 (дата звернення: 28.03.2021).

14. Великобритания увеличит число шпионов для борьбы с терроризмом. URL: http://korrespondent.net/world/3748242-velykobrytanyia-uvelychyt-chyslo-shpyonov-dlia-borby-s-terroryzmom (дата звернення: 28.02.2021).

15. Во Франции вступил в силу антитеррористический закон. URL: http://www.interfax.ru/world/418373 (дата звернення: 28.02.2021).

16. В Германии согласовали принципы борьбы с терроризмом. URL: http://odnako.su/news/world/-501039-v-germanii-soglasovali-principy-borby-s-terrorizmom (дата звернення: 28.02.2021).

17. Антитеррористический закон в Польше. URL: http://polomedia.ru/news/sobytiya/antiterroristicheskiy-zakon-v-polshe-2016 (дата звернення: 28.02.2021).

18. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/53/2019?find=1&text=%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D1%96%D0%BA%D1%82#Text (дата звернення: 28.02.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.922:351.74 (477)

ПОЛІЩУК С.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-3142-9163.

УДОСКОНАЛЕННЯ ЗАГАЛЬНОДЕРЖАВНОЇ СИСТЕМИ БОРОТЬБИ З ТЕРОРИЗМОМ

Анотація. *У статті аналізуються сучасні терористичні загрози. Міститься аналіз нормативно-правових актів з питань боротьби з тероризмом. Висвітлюється позитивний досвід США щодо визначення рівнів терористичних загроз. Визначено шляхи удосконалення загальнодержавної системи боротьби з тероризмом.*

Ключові слова: *тероризм, терористична загроза, рівні терористичної загрози, загальнодержавна система боротьби з тероризмом.*

Summary. *The article analyzes modern terrorist threats. It is noted that today the level of terrorist threat in Ukraine is determined by a number of factors, both external and internal. The article contains an analysis of regulations on combating terrorism. The positive experience of the United States in determining the levels of terrorist threats is highlighted. Ways to improve the national system of combating terrorism have been identified.*

Keywords: *terrorism, terrorist threat, levels of terrorist threat, national system of countering terrorism.*

Аннотация. *В статье анализируются современные террористические угрозы. Содержится анализ нормативно-правовых актов по вопросам борьбы с терроризмом. Освещается позитивный опыт США касательно определения уровней террористических угроз. Определены пути совершенствования общегосударственной системы борьбы с терроризмом.*

Ключевые слова: *терроризм, террористическая угроза, уровни террористической угрозы, общегосударственной системы борьбы с терроризмом.*

Постановка проблеми. Відповідно до Концепції боротьби з тероризмом терористична загроза – існуючі та потенційно можливі чинники, що створюють небезпеку вчинення терористичного акту щодо об’єкта можливих терористичних посягань та настання негативних наслідків від нього. Сьогодні серед терористичних загроз виділяється: активізація в Україні сепаратистських рухів та провокування таких настроїв у місцях компактного проживання національних меншин; агресивні дії Російської Федерації відносно України; зростання рівня злочинності, пов’язаної з незаконним обігом вогнепальної зброї, боєприпасів, вибухових і отруйних речовин та інших засобів масового ураження; посилення інтересу до України з боку міжнародної організованої злочинності у сферах незаконної міграції, легалізації (відмивання) доходів, одержаних злочинним шляхом, контрабанди зброї, небезпечних матеріалів та наркотичних засобів, відходів біологічних та хімічних речовин, ядерних матеріалів; внутрішні міграційні процеси, в тому числі спричинені збройною агресією Російської Федерації проти України, а також загострення міграційної кризи у світі [1].

Актуалізує терористичну загрозу наявність на території України потенційно небезпечних та уразливих у терористичному плані об’єктів, які з огляду на світовий досвід можуть розглядатися як потенційні цілі терористів [1; 2].

Результати аналізу наукових публікацій. Проблеми удосконалення загальнодержавної системи боротьби з тероризмом досліджували у своїх роботах Антипенко В.Ф., Ємельянов В.П., Крутов В.В., Леонов Б.Д., Мокляк В.В., Семенюк О.Г., Кубальський В.Н., Рижов І.М., Ткачов І.В. та ін.

Водночас, терористичні загрози постійно трансформуються, з'являються нові види таких загроз, що актуалізує дослідження заходів з їх нейтралізації. Крім цього, досі невирішеною залишається проблема антитерористичного захисту потенційно небезпечних об'єктів, визначення порядку їх віднесення до об'єктів можливих терористичних посягань, розробки особливих правил антитерористичної безпеки. Підвищення стійкості України до терористичної загрози потребує певного удосконалення антитерористичного законодавства України, оновлення моделі взаємодії спеціальних служб і правоохоронних органів з населенням з питань запобігання і протидії тероризму, а також мінімізації наслідків вчинення терактів. У цих процесах має бути врахований як досвід проведення АТО на території окремих районів Донецької і Луганської областей, так і передовий іноземний досвід [3, с. 4].

Метою статті є удосконалення загальнодержавної системи боротьби з тероризмом на підставі аналізу терористичних загроз, що постали перед Україною.

Виклад основного матеріалу. Чинна сьогодні Стратегія національної безпеки України [4] до актуальних терористичних загроз національній безпеці України відносить: 1) агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, а саме: розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму, створення і всебічна підтримка, зокрема військова, маріонеткових квазідержавних утворень на тимчасово окупованій території частини Донецької та Луганської областей (п. 3.1); 2) неефективність системи забезпечення національної безпеки і оборони України: діяльність незаконних збройних формувань, зростання злочинності, незаконне використання вогнепальної зброї (п. 3.2); 3) загрози безпеці критичної інфраструктури: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій (п. 3.8).

За рівнем терористичних загроз ситуація, що склалася в Україні, є унікальною у межах Єврозони та створює осередок нестабільності в усьому регіоні. Діяльність терористичних організацій і диверсійних груп, ведення гібридної війни сусідньою країною спрямовані на повалення конституційного ладу в Україні. У нинішніх умовах діяльність міжнародних терористичних організацій не лише негативно позначається на безпековому середовищі, а й становить безпосередню загрозу для національної безпеки України [3, с. 4]. Сьогодні рівень терористичної загрози в Україні визначає низка факторів як зовнішнього, так і внутрішнього характеру.

Агресія Російської Федерації проти України утворила живильне середовище для терористичної діяльності. Активне використання оснащених та підготовлених Росією терористичних угруповань для реалізації її агресивних планів, підтримка нею терористичних утворень у Донецькій і Луганській областях створюють загрозу зростання масштабів і поширення терористичної діяльності на інші регіони України [5, с. 6, 7]. Бойовики, які діють в Україні, користуються постійною підтримкою з території Російської Федерації, що здійснює масштабні поставки озброєння, військової техніки, боєприпасів, надає значні матеріальні та фінансові ресурси, а також проводить їх підготовку на своїх військових полігонах [3, с. 4]. За даними офісу Генерального

прокурора, за ст. 258 КК України у 2014 – 2019 рр. обліковано 5644 кримінальних провадження, вручено повідомлення про підозру в 130 провадженнях, направлено до суду 1875 кримінальних проваджень. Більшість злочинів, кваліфікованих за ст. 258 КК України, стосується членів незаконних збройних формувань у контексті захоплення контролю над частинами територій Донецької та Луганської областей та подальшого збройного конфлікту [6].

Для підвищення в Україні рівня терористичної загрози підґрунтям стають низка зовнішніх чинників, серед яких, зокрема, виділяється тенденція до збільшення в Україні кількості осіб – вихідців із держав, в яких нестабільні економіка і політична ситуація та на територіях яких активно діють терористичні організації [1].

За оцінками міжнародних організацій, національних урядів, спецслужб, неурядових організацій та незалежних фахівців наразі найбільшу терористичну загрозу у світі становлять ісламістські або джихадистські організації та групи. Більшість терористичних актів пов'язано саме з активністю таких угруповань [3, с. 11].

З огляду на активізацію діяльності міжнародних терористичних організацій та угруповань у державах Близького Сходу та Центральної Азії, Євросоюзу, Північної Африки, а також загальну військову та суспільно-політичну ситуацію в Україні особливу небезпеку становить діяльність міжнародної терористичної організації "Ісламська держава", представники якої намагаються активно використовувати канали нелегальної міграції для переховування та переправлення бойовиків з Північного Кавказу, Центральної Азії та Європи транзитом через територію України. Отже, небезпечною залишається тенденція підвищеної заінтересованості до території України як транзитної зони з боку міжнародних злочинних угруповань, які діють, зокрема, у сферах незаконної міграції, нелегального переміщення зброї, небезпечних матеріалів та наркотичних засобів, фінансового та іншого забезпечення діяльності міжнародних терористичних організацій [7, с. 119]. Збільшується вірогідність використання ними в Україні терористичних методів як способу досягнення політичної мети або привернення уваги громадськості до своїх ідеологічних чи інших поглядів [7, с. 8]. Можливість використання міжнародними терористами території України для транзиту, відпочинку і оздоровлення, незаконного перевезення зброї, людей, наркотичних речовин в умовах збройного конфлікту на Донбасі та відсутності контролю за ділянкою державного кордону в районі проведення антитерористичної операції може бути використана РФ як для виправдання можливих агресивних дій, під виглядом боротьби з тероризмом, так і у ході інформаційної кампанії проти України [3, с. 4].

Потенціальною загрозою для України є формування за її межами потужних законспірованих ланок міжнародних терористичних організацій, метою яких є вчинення терористичних актів у різних регіонах світу, передусім в країнах, що беруть участь у міжнародних антитерористичних операціях. Зауважимо, що Україна бере активну участь в урегулюванні тривалих збройних конфліктів, міжнародних антитерористичних операціях, що є одним з чинників підвищення рівня терористичної загрози в нашій державі [8, с. 18].

З огляду на сучасні терористичні загрози розроблено нову редакцію Концепції боротьби з тероризмом, яка проголошує, що терористичні загрози, що постали перед Україною, вимагають удосконалення функціонування загальнодержавної системи боротьби з тероризмом. Пунктом 1 Плану заходів з реалізації Концепції боротьби з тероризмом в Україні, затвердженим Розпорядженням Кабінету Міністрів України від 05.01.21 р. № 7-р, передбачено провести аналіз загальнодержавної системи боротьби з тероризмом, за результатами сформувати модель загальнодержавної системи боротьби з

тероризмом з урахуванням потенційних терористичних загроз національній безпеці України та фінансово-економічних можливостей держави [9].

Рівні терористичних загроз та заходи реагування суб'єктів боротьби з тероризмом на загрозу вчинення або вчинення терористичного акту визначаються Положенням про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (далі – Положення), затвердженим Постановою Кабінету Міністрів України від 18.02.16 р. № 92 [10].

Згідно з п. 7 Положення залежно від наявної інформації про загрозу вчинення або вчинення терористичного акту встановлюються такі рівні терористичних загроз:

- "сірий (можлива загроза)" – за наявності факторів (умов), що сприяють вчиненню терористичного акту;
- "синій (потенційна загроза)" – за наявності інформації, що потребує підтвердження, про підготовку до вчинення терористичного акту;
- "жовтий (імовірна загроза)" – за наявності достовірної (підтвердженої) інформації про підготовку до вчинення терористичного акту;
- "червоний (реальна загроза)" – у разі вчинення терористичного акту [10].

Рішення про встановлення, зміну, скасування рівня терористичної загрози, строк та район дії рівня терористичної загрози приймає керівник Антитерористичного центру за письмовим дозволом Голови СБУ. Про прийняте рішення керівник Антитерористичного центру негайно інформує Президента України (п. 8 Положення) [10].

До речі, схожа система рівнів терористичної загрози функціонує в США. Спробуємо її охарактеризувати, оскільки ця країна має величезний досвід розв'язання цієї проблеми.

Систему рівнів терористичної загрози (або рівнів терористичної небезпеки) було розроблено у США після подій 11 вересня 2001 р. у відповідь на численні скарги громадян країни про те, що держоргани не надають роз'яснень про ступінь такої небезпеки в той чи інший момент. Систему було введено з березня 2002 р. Вона складається з п'яти рівнів, що розрізняються за кольором: зелений, синій, жовтий, помаранчевий і червоний. Найменший ступінь небезпеки, що відповідає повсякденній нормі – це зелений колір, найвищий – червоний (синій рівень відповідає заклику "бути насторожі", жовтий характеризується як "серйозний", помаранчевий – як "критичний"). Визначення рівня терористичної загрози відбувається згідно з інформацією про активність різних екстремістських організацій (у тому числі терористичних), що отримують спеціальні служби США. Оголошення того чи іншого "кольору" (як правило, міністром юстиції) спричиняє певні дії влади. У випадках із "зеленим" і "синім" рівнями жодних надзвичайних заходів не вживають. "Жовтий" рівень передбачає посилене спостереження за об'єктами, які можуть зазнати терористичної атаки. При цьому діяльність різних департаментів, таких як Національне агентство внутрішньої безпеки, має бути максимально скоординованою. У випадку з "помаранчевим" рівнем у США вживають додаткових заходів безпеки на військових базах, у морських портах, аеропортах і на залізниці; посилюють охорону кордонів, мостів, тунелів, АЕС, а за межами США – американських посольств і представництв. У разі оголошення "червоного" рівня припиняють роботу і закриваються громадські та урядові установи. Увесь персонал евакуюється у спеціально відведені місця, зокрема, в підземні бункери. [11]. Останнім часом загрозливою залишається тенденція щодо залучення до терористичної діяльності безпосередньо громадян країн, які є об'єктами терористичних нападів. Терористичні напади у США, вчинені за останні два роки від імені "Ісламської держави", скоїли радикалізовані громадяни цієї країни, а не мігранти. У цьому контексті найбільша загроза

полягає у використанні терористичними організаціями, перш за все "Ісламською державою", осіб (іноземців), які брали участь у бойових діях у зонах конфліктів у складі відповідних угруповань та повертаються до своїх країн (*foreign terrorist travellers*) [3, с. 7].

Враховуючи позитивний досвід США та з огляду на потребу вжиття заходів щодо систематизації матеріалів вивчення зарубіжного досвіду боротьби з тероризмом (п. 17 Плану), слушними слід визнати пропозиції щодо внесення до Закону України "Про боротьбу з тероризмом" статті, яка має наголошувати, що "ступінь терористичної загрози визначається відповідно до п'ятибальної шкали, а дії, спрямовані на протидію тероризму, мають відповідати ступеню терористичної загрози" [12, с. 459].

Не останню роль у боротьбі з тероризмом відіграє належна організація та проведення антитерористичної операції – комплексу скоординованих спеціальних заходів, спрямованих на попередження та припинення злочинних діянь, здійснюваних з терористичною метою, звільнення заручників, ліквідацію терористів, мінімізацію наслідків терористичного акту чи іншого злочину, вчиненого з терористичною метою.

Зокрема, до таких спеціальних дій і заходів сил охорони правопорядку належать спеціальні операції, які проводяться в разі, коли терористичний акт загрожує загибеллю багатьох людей чи іншими тяжкими наслідками або якщо його вчинено одночасно на території кількох областей, районів чи міст; ситуація, пов'язана з учиненням або загрозою вчинення терористичного акту, є невизначеною щодо причин та обставин її виникнення і подальшого розвитку; вчинення терористичного акту зачіпає міжнародні інтереси України та її відносини з іноземними державами; реагування на вчинення дій з ознаками терористичного акту належить до компетенції різних правоохоронних та інших державних органів; очевидна неможливість попередження або припинення терористичного акту силами правоохоронних та місцевих органів виконавчої влади окремого регіону [12, с. 459].

Координуючу функцію у діяльності суб'єктів боротьби з тероризмом, у попередженні терористичних актів стосовно державних діячів, критичних об'єктів життєзабезпечення населення, об'єктів підвищеної небезпеки, актів, що загрожують життю і здоров'ю значної кількості людей, та їх припинення здійснює Антитерористичний центр – постійно діючий орган при СБ України. Тому посилення ролі цього органу є необхідним заходом у сфері боротьби з тероризмом [3, с. 4, 7; 14, с. 113].

Висновки.

Сьогодні Україною не вироблена комплексна стратегія дій ані щодо терористичної діяльності як форми злочинної діяльності, ані щодо тероризму як негативного суспільно небезпечного явища, яка має бути всеохоплюючою, не прив'язаною до специфіки загрози, довгостроковою й такою, що визначає необхідні реформи та новації за стадіями терористичної діяльності залежно від ступеня суспільної небезпечності.

Реалізація державної політики у сфері боротьби з тероризмом передбачає застосування комплексного підходу, який має знайти втілення у положеннях згаданої стратегії, зміст якої має визначати такі форми контролю: превентивну, регулятивну і репресивну [7, с. 304], а також основи організації, координації і оптимізації діяльності держави з урахуванням нових терористичних загроз.

Аналіз Концепції боротьби з тероризмом та Плану заходів з її реалізації свідчить про те, що окремі заходи, частина яких була передбачена ще Планом заходів 2013 р. [14], залишалися невиконаними. Зокрема, йдеться про розробку та затвердження критеріїв віднесення об'єктів незалежно від форми власності до переліку об'єктів можливих терористичних посягань, методики їх ідентифікації; розроблення механізму стимулювання фізичних і юридичних осіб до співпраці із суб'єктами боротьби з

тероризмом (п. 8, 13 Плану) [15]. Частину передбачених Планом 2013 р додаткових організаційних заходів механічно перенесено до нового Плану. Це, зокрема, поглиблення взаємодії суб'єктів боротьби з тероризмом з недержавними суб'єктами охоронної діяльності з питань запобігання вчиненню та недопущення терористичних проявів (п. 4 Плану) [14]. Підпунктом 1 пункту 4 Плану передбачено завдання з внесення змін до статті 24 Закону України "Про боротьбу з тероризмом" щодо визначення критеріїв та порядку визнання організації терористичною [9], реалізація якого було заплановано ще п/п. 1 п. 1 Рішення РНБО України від 25.05.12 р. "Про заходи щодо посилення боротьби з тероризмом в Україні" (уведене в дію Указом Президента України від 08.06.21 р. № 388).

Концепція боротьби з тероризмом не передбачає підвищення ризиків тероризму у зв'язку з появою внутрішньо демобілізованих військовослужбовців, які мають значний досвід роботи з вибуховими пристроями й речовинами, як категорій, особливо привабливих для вербування терористами з метою їх використання в терористичній діяльності.

У зв'язку з цим Кабінету Міністрів України доцільно вжити в установленому порядку заходів щодо внесення змін до Концепції боротьби з тероризмом та Плану заходів з її реалізації. Зокрема, існує потреба ведення (з використанням інформаційних автоматизованих систем) спеціального обліку осіб, що пройшли спеціальну підготовку з диверсійної, розвідувальної чи контррозвідувальної діяльності, після їх виходу у відставку чи припинення ними служби з інших причин, а також осіб, котрі брали участь у збройних конфліктах, з метою їх реабілітації й адаптації до інших соціальних умов, що знизить вірогідність використання їх досвіду кримінальними структурами, у т.ч. терористичними угрупованнями.

Використана література

1. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: http://zakon2.rada.gov.ua/laws/show/230/2013

2. Щодо оцінки стану транскордонної і транснаціональної організованої злочинності та її впливу на суспільно-політичні процеси в державі. Критерії оцінки криміногенної ситуації в Україні. Перспективи застосування на території України міжнародних миротворчих операцій з підтримання миру і безпеки у світі: методичні рекомендації / Гребенюк М.В., Марчук М.П., Шепетько С.А., Вітик І.Р. та ін. Київ: МНДЦ при РНБО України, 2016. 82 с.

3. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доповідь / Резніков О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є.; за заг. ред. О.О. Резнікової. Київ: НІСД, 2017. 60 с.

4. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26.05.15 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070

5. Про внутрішнє та зовнішнє становище України у сфері національної безпеки: аналітична доповідь Національного інституту стратегічних досліджень до позачергового Послання Президента України до Верховної Ради України. Київ: НІСД, 2014. 148 с.

6. Розслідування окремих злочинів терористичної спрямованості (оновлено). – (Харківська правозахисна група). Харків: Інформаційний портал "Права людини в Україні". URL: http://khpg.org/1607669591 (дата звернення: 20.02.2021).

7. Леонов Б.Д. Запобігання тероризму: кримінологічний аспект: монографія. Київ: Видавничий дім "АртЕк". 2015. 435 с.

8. Боротьба з тероризмом: підруч. / кол. авт.; за заг. ред. Є.Д. Скулиша. Київ: Наук.-вид. центр НА СБ України, 2012.

9. План заходів з реалізації Концепції боротьби з тероризмом: Розпорядження Кабінету Міністрів України від 05.01.21 р. № 7-р. *Урядовий кур'єр* від 15.01.2021. № 9.

10. Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків: Постанова Кабінету Міністрів України від 18.02.16 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF

11. Системы уровней террористической угрозы в мире. URL: http://ria.ru/spravka/201206 16/674808393.html

12. Жаровська Г.П. Теорія та практика протидії транснаціональній організованій злочинності в Україні: дис. …докт. юрид. наук: спец. 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Київ, 2019. 593 с.

13. Ткачов І.В., Басін К.В., Леончик Я. Ю. Нормативно-правове закріплення терористичних загрозу: ретроспективний аналіз. Роль і місце національної спецслужби в історії українського державотворення. Київ: ВПЦ "Київський Університет". 2017. 183 с.

14. План заходів з реалізації Концепції боротьби з тероризмом на 2013 – 2017 роки: Розпорядження Кабінету Міністрів України від 11.07.13 р. № 547-р. *Урядовий кур'єр* від 15.08.2013. № 147.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 35.076+342.5(477)+351.746.1(477)

ГОРДІЄНКО С.Г., *доктор юридичних наук, доцент*, завідувач кафедри національної безпеки навчально-наукового інституту права ім. князя Володимира Великого МАУП.
ORCID: https://orcid.org/0000-0003-0392-2601.
ДОРОНІН І.М., *доктор юридичних наук, доцент,* завідувач наукової лабораторії Інституту інформації, безпеки і права НАПрН України.
ORCID: https://orcid.org/0000-0002-5991-6713.

ДЕРЖАВНА БЕЗПЕКА УКРАЇНИ В СУЧАСНИХ УМОВАХ: ПРОБЛЕМИ КОМПЕТЕНЦІЇ ДЕРЖАВНИХ ОРГАНІВ

Анотація. *У роботі розглядаються проблеми розвитку поняття "державна безпека" в Україні, її правового виміру, належного визначення компетентних державних органів, відповідальних за її забезпечення. Виходячи з того, що усталеним для вітчизняної правової науки є визначення держави як організації політичної влади, її безпека залежить від політичної, економічної, наукової та науково-технологічної складових, які є фундаментом інноваційної політики України. У сучасному світі рушійною силою економіки стають якісно нові знання, тому структуру економіки, як інноваційної, можна звести до наступної формули: "загальна економіка = економіка науки + науково-технологічна економіка + економіка матеріального виробництва". Економіку ж, на нашу думку, схематично можна відобразити так: "економіка науки (інформація => інформаційні ресурси => інноваційна діяльність => якісно нові знання => інтелектуальні ресурси), науково-технологічна економіка та економіка матеріального виробництва". У такому контексті безпека держави залежить від її політичної складової із забезпечення економічної безпеки суспільства. Систематизація повноважень Верховної Ради України, Президента України, Ради національної безпеки України, Кабінету Міністрів України, місцевих органів влади та органів із забезпечення безпеки на сьогодні далека від досконалої. Визначається, що безпеку держави забезпечує не лише законодавчо визначений орган – Служба безпеки України, а й інші органи влади та управління. Водночас питання розмежування компетенції між ними у зазначеній сфері залишається складним і потребує ґрунтовних досліджень.*

Ключові слова: *національна безпека, безпека держави, політична безпека, економічна безпека, воєнна безпека, органи влади і управління, повноваження державних органів.*

Summary. *This paper examines the problem of development of the term "state security" in Ukraine, legal context of implementation, adequate definitions for state authorities` competence in sphere of security. Based on traditional theoretical legal definition of state as organization of political power, security of state depends on the components of security such as politics, economy, scientific and technological policy as the foundation of innovation policy. In today's world economics is driven by knowledge. Therefore, structure of innovation economy may be described as conditional pattern "common economy = economy of science + economy of technics + economy of production (real economy)". The economy in this context may be described as "economy of science (information => information resources => innovations => qualitatively new knowledge => intellectual resources), economy of technics and economy of production". In this sense state security depends on political component of economic security. Systematization of competence of Verkhovna Rada of Ukraine (national parliament), President of Ukraine, National Security and Defense Council of Ukraine, Cabinet of Ministers of Ukraine, local authorities in the sphere of security is far from perfect. The authors argue that the state security is not only within the competence of Security Service of Ukraine according to prescriptions of the law. These objectives are subjects for other state authorities. However, the problems of separation of competence for state powers and state authorities are complex and need following studies.*

Keywords: *national security, state security, political security, economic security, military security, state authorities, competence of state authorities.*

Аннотация. *В работе рассматриваются проблемы развития понятия "государственная безопасность" в Украине, ее правового измерения, надлежащего определения компетентных государственных органов, ответственных за ее обеспечения. Исходя из того, что устойчивым для отечественной правовой науки есть определения государства как организации политической власти, ее безопасность зависит от политической, экономической, научной и научно-технологической составляющих, которые являются фундаментом инновационной политики Украины. В современном мире движущей силой экономики становятся качественно новые знания, поэтому структуру экономики, как инновационной, можно свести к следующей формуле: "общая экономика = экономика науки + научно-технологическая экономика + экономика материального производства". Экономику же, по нашему мнению, схематично можно отобразить так: "экономика науки (информация => информационные ресурсы => инновационная деятельность => качественно новые знания => интеллектуальные ресурсы), научно-технологическая экономика и экономика материального производства". В таком контексте безопасность государства зависит от ее политической составляющей из обеспечения экономической безопасности общества. Систематизация полномочий Верховной Рады Украины, Президента Украины, Совета национальной безопасности Украины, Кабинета Министров Украины, местных органов власти и органов из обеспечения безопасности на сегодня далекая от совершенной. Определяется, что безопасность государства обеспечивает не только законодательно определенный орган – Служба безопасности Украины, а и другие органы власти и управление. Вместе с тем вопрос размежевания компетенции между ними в указанной сфере остается сложным и нуждается в грунтовних исследований.*

Ключевые слова: *национальная безопасность, безопасность государства, политическая безопасность, экономическая безопасность, военная безопасность, органы власти и управление, полномочие государственных органов.*

Постановка проблеми. Чергове звернення авторів до проблематики визначення сутності та змісту державної безпеки України зумовлене новими реаліями соціального, політичного та державного будівництва України, а також наявністю публікацій за даною тематикою, що з'явились останнім часом. Беззаперечним вважаємо, що державна незалежність і безпека є базовою політичною цінністю, а їх зміцнення й розвиток – головною стратегічною метою сучасної української держави.

Незалежність передбачає спроможність і готовність держави захистити свою цілісність та непорушність кордонів; вести незалежну зовнішню політику винятково на підставі національних інтересів; мінімізувати зовнішню залежність. Державна незалежність є головною умовою успішної реалізації державного курсу на створення комплексної, цілісної, інтегрованої системи національної безпеки на суспільному, державному та політичному рівнях.

Результати аналізу наукових публікацій. У загальному розумінні національна безпека України – це спосіб самозбереження українського народу, який досяг рівня організації у формі незалежної держави. Відповідно до пропозицій ЮНЕСКО, вона може розумітись як система державних і суспільних гарантій стабільного розвитку нації, захисту її базових цінностей та інтересів, джерел духовного і матеріального добробуту від зовнішніх та внутрішніх загроз. Традиційно безпеку визначають як певну характеристику якісного стану системи та її основних частин.

О.В. Українчук одним із перших визначив, що національна безпека – це специфічний вид суспільних відносин, які складаються між людьми та їх колективами у процесі здійснення цілеспрямованої діяльності щодо досягнення стану оптимального

функціонування і розвитку суспільства та його структур шляхом правильного вибору перспективних цілей, ефективної централізації загроз, що виникли, стимулювання і створення позитивних процесів [1]. У подальшому вивчення проблем безпеки української державності перебувало в полі зору багатьох вчених, зокрема С.Г. Гордієнка, О.Г. Данільяна, О.П. Дзьобанья, І.М. Дороніна, В.С. Картавцева, В.Г. Пилипчука, О.В. Сосніна, В.А. Ященка та інших.

Національна безпека України забезпечується діяльністю суспільних інститутів, спрямованою на створення і вдосконалення умов та чинників (гарантій) ефективної життєдіяльності народу. Відповідні суспільні інститути утворюють систему забезпечення національної безпеки України.

Однією із важливих ключових складових національної безпеки є державна безпека, тому національну безпеку не можна звужувати до державної, адже таке загрожуватиме пріоритетом інтересів держави над інтересами народу.

У системі національної безпеки одними із головних пріоритетів є державно-політичний та соціально-економічний аспекти.

Державно-політичний аспект полягає у забезпеченні територіальної цілісності України, недоторканності її кордонів, внутрішніх і міжнародних інтересів Української держави та її впливу на світовій арені, захисту державно-політичного ладу від спроб ліквідувати чи змінити його неконституційним шляхом, а також прав та свобод громадян, виживання у випадках катастроф, стихійних лих і мінімізації їх наслідків.

Соціально-економічний аспект забезпечує стійкість соціально-економічної системи держави, вдосконалення структури народного господарства, захищеність його від зовнішніх та внутрішніх загроз, подолання кризових явищ в економіці і соціальній сфері.

Загрози національній безпеці України (внутрішні та зовнішні, реальні та потенційні) безпосередньо впливають на якісний стан безпеки держави.

Метою статті є визначення компетенції державних органів у забезпеченні безпеки держави щодо її спроможності до обороноздатності та здатності протистояти антиконституційним проявам в українському суспільстві.

Виклад основного матеріалу. Поняття “національна безпека” стало невід’ємним атрибутом більшості воєнно-політичних концепцій, аналітичних і прогностичних розробок довгострокового, глобального характеру. Але для різних видів безпеки відсутня загальновизнана дефініція, і до того ж розбіжності між науковими школами та окремими дослідниками досить радикальні. Це саме стосується і поняття “державна безпека”.

Відповідно до законодавства України державну безпеку забезпечує лише Служба безпеки України та й то від загроз невоєнного характеру. Але забезпечення безпеки випливає із мети діяльності досить великого кола державних органів. Тобто, гіпотетично, безпеку держави, як апарату влади та управління, забезпечує сукупність органів зі своєю компетенцією.

Таким чином, варто погодитись із пропозиціями В.А. Ященка, що визначення поняття “національної безпеки України” та “державної безпеки України” відповідно до Закону України “Про національну безпеку України” потребує уточнення, хоча б до такого: − це “надійне, стабільне функціонування суспільства та держави і нарощування їх потенціалу як умови їх існування і захищеності від реальних та потенційних загроз” [2].

Потрібно враховувати, що зміст поняття “безпека” дещо ширший, ніж статичний “стан захищеності” соціальної системи від внутрішніх і зовнішніх загроз, а тим більше – “стан непорушності”.

Можливо передбачити, що безпека соціальної системи залежить від її здатності ефективно нейтралізувати (у т.ч. через запобігання) внутрішні та зовнішні загрози, що виникли; стимулювати та використовувати у своїх інтересах позитивні явища, фактори і процеси, що впливають на соціальну систему, а також створювати їх; стимулювати трансформацію нейтральних щодо даної системи факторів у позитивні і водночас протидіяти їх трансформації у негативні фактори, процеси, явища.

Отже, безпека соціальної системи є станом її оптимального функціонування і розвитку за умов правильного вибору перспективних цілей, ефективної нейтралізації загроз, що виникають, стимулювання і створення позитивних процесів.

Зустрічаються юридичні визначення державної безпеки. Таким шляхом йдуть законодавці тих країн, де в нормативному акті після наведення поняття надається розлоге його пояснення через визначення мети, завдань і принципів діяльності. Майже у всіх визначеннях державна безпека розглядається як стан суспільного та державного ладу або його основ, що характеризується певними якостями, а саме: міцністю, непорушністю, незалежністю, захищеністю. На нашу думку, перспективною є ідея поєднання поняття "державна безпека" з категорією "відносини".

Отже, зрозуміло, що поняття "державна безпека" досить складне, багатоаспектне, інтегроване із багатьох понять і відповідно висвітлює безпеку не тільки держави, але й окремої особи та суспільства в цілому [3].

Хоча кожне визначення має свої особливості, зазначимо, що сучасне трактування безпеки як "стану захищеності" конкретного соціального об'єкта (особи, суспільства, держави) позитивно сприймається у політичних та наукових колах.

Вивчаючи суспільні відносини, можливо стверджувати, що спецслужба будь-якої країни не спроможна (й не має таких повноважень) забезпечити безпеку у повному обсязі усіх без винятку суспільних відносин. З огляду на це Служба безпеки України (враховуючи визначену законом мету діяльності) має забезпечувати пріоритетні інтереси суспільства через забезпечення безпеки держави в основних сферах діяльності України. Однак, і це принципово, держава має бути тільки ефективним засобом, суб'єктом виконання завдань, що необхідно вирішувати суспільству.

Отже, враховуючи призначення і мету діяльності із забезпечення державної безпеки, статус та сутність діяльності СБ України може визначатися таким чином: Служба безпеки України – державний орган, який забезпечує безпеку держави спеціальними силами, засобами, методами та формами шляхом виявлення, попередження та припинення протиправної діяльності (розвідувально-підривної діяльності спеціальних служб іноземних держав та посягань на суверенітет України) організацій, груп та осіб у політичній, економічній, науково-технічній, воєнній та соціальній сферах діяльності України.

На сьогодні термін "державна безпека" автоматично підміняє поняття "безпека держави", яке конкретніше та точніше, ніж перше, але не таке придатне для політичного вжитку. Історично вжиття зазначених термінів у законодавчих актів відбулось після внесення у 1990 році змін до Конституції УРСР, які містили згадування термінів і "державна безпека", і "безпека держави" (нової редакції ст. 7 щодо заборони створення і діяльності партій та громадських організацій і рухів, що ставлять за мету окрім іншого підрив безпеки держави, ст. 49 щодо можливості встановлення обмежень об'єднання у політичні партії, інші громадські організації в інтересах у тому числі державної безпеки). А у 1992 році до Конституції України були внесені зміни, що передбачали ужиття терміну "національна безпека".

Однак якщо взяти за вихідне те твердження, що термін “державна безпека” відображає тільки забезпечення безпеки держави, можна уникнути низки протиріч. Застосувавши теорію домовленості, можна створити, звичайно, недосконалу, але систему класифікації “безпек”: національна безпека, суспільна безпека, безпека держави, воєнна безпека, політична безпека, економічна безпека тощо.

Таким чином, поняття “безпека держави – як здатність системи суспільних відносин (у державно-політичній та соціально-економічній сферах діяльності суспільства), що безпосередньо пов’язана із забезпеченням оптимального функціонування її інститутів (у першу чергу державної влади) забезпечити безпеку особи, суспільства і держави при конкретному балансі їх життєве важливих інтересів” знаходить своє підтвердження [4].

Спроба аналізу сутнісних і змістовних характеристик різних “безпек”: нації, народу, етносу, політичної нації, території, країни та держави приводить до вкрай простого висновку, що обсяг понять і їх “вага”, а саме – безпеки нації, політичної нації, етносу, народу, території, території держави, країни, держави та суверенної держави є різним. Ми погоджуємося, що у системі національної безпеки головними пріоритетами є державно-політичний та соціально-економічний аспекти.

З урахуванням зазначеного, термін “державна безпека”, має визначатися як якісно визначений законодавством стан функціонування держави, як політичного інституту влади, який досягається шляхом прогнозування, попередження, виявлення та мінімізації негативного впливу існуючих і ймовірних загроз основним ознакам держави (насамперед, інститутам державної влади, територіальній цілісності, суверенітету, грошово-кредитній та податковій системам) та дозволяє державі ефективно реалізовувати своє соціальне призначення щодо забезпечення подальшого розвитку людини, суспільства та держави.

Виходячи з того, що найбільш прийнятним визначенням держави є визначення її як організації політичної влади (складова суспільства, яка його організовує), можемо зазначити що безпека держави, як системи політичної влади в Україні залежить від її політичної, економічної, наукової та науково-технологічної складових, які є фундаментом інноваційної політики України.

Тобто, державна безпека – це безпека державно-політичного, конституційно легітимізованого політичного ладу держави від змін його неконституційним шляхом; безпека державотворення і конструктивної політики задля стабільності суспільства; наявність політичного суверенітету; територіальна цілісність України і недоторканість її кордонів; безпека інститутів державної влади; безпека національно-державних інтересів у сфері економіки.

Таким чином, гіпотеза, що безпеку держави, як апарату влади та управління, забезпечує значна кількість її органів і у кожного з них є своя компетенція знаходить своє попереднє підтвердження.

Задля визначення складових державної безпеки, доцільним вважаємо, в першу чергу визначитися з такими феноменами як політика, безпека політичної системи та державного устрою України, політична економія та економіка. На нашу думку всі ці визначення дуже тісно пов’язані між собою, взаємопереходять одне в одне та найбільш реально дають можливість окреслити стратегічні, пріоритетні напрями державної діяльності, а отже і визначити напрями її забезпечення.

Політика – це і мистецтво можливого; і наука державного управління; і участь в справах держави; і напрям діяльності держави; і певні форми, мета, завдання, зміст діяльності держави. Сфера політики охоплює питання державного устрою, управління країною, керівництво соціальними спільнотами: класами, різними суспільними групами

людей, політичну боротьбу політичних партій, політичних рухів та ін. У політиці відображаються корінні, життєві інтереси соціальних спільнот, класів.

Пріоритетність того чи іншого виду національної безпеки (політичної, економічної, соціальної, екологічної, військової тощо) визначається об'єктивними чинниками: ступенем потреби людей у цьому виді безпеки; уразливістю людей і життєво важливих об'єктів від цього виду небезпек; наявністю широкого кола надзвичайних небезпек, яким повинна протистояти ця система безпеки.

Отже, можливо стверджувати, що політична безпека є сукупністю заходів з виявлення, попередження і усунення тих чинників, які можуть завдати збитків політичним інтересам країни, народу, суспільству, громадянам, зумовити політичний регрес і навіть політичну загибель держави. Існує багато небезпек, які здатні підірвати владу, правовий порядок, викликати хаос. Своєю чергою, накопичення цих загроз зумовлює необхідність створення дієвого механізму забезпечення політичної безпеки [5].

У такому разі політична безпека – один з найголовніших різновидів безпеки, що використовує політичні засоби для економічного та соціального балансу (або його відсутності) державного устрою. Беззаперечно, координаційна і керівна роль у процесі забезпечення політичної безпеки країни має належати державі, дії якої у цьому разі узгоджуються з інтересами економічної безпеки.

Аналізуючи викладене вище і власні напрацювання у теорії понять, припускаємо, що:

- політика – це стратегічна програма, як система засобів та методів реалізації її пріоритетів та напрямків управлінської діяльності держави, що відповідають інтересам особи, суспільства та саме держави, які проголошені владою, або її представниками і які забезпечуються державою в певному соціальному середовищі;
- політична безпека – це якісний стан політичної системи суспільства, який має визначатися законодавчо, і який досягається системою заходів, спрямованих на збереження конституційно легітимізованого політичного ладу тієї чи іншої держави, забезпечення державотворення і конструктивної політики стабільності суспільства при можливості: нації та державних інститутів самостійно вирішувати питання державного устрою; гарантований захист політичного суверенітету, територіальної цілісності, політичної незалежності та конституційного ладу держави; незалежно проводити внутрішню і зовнішню політику, що ґрунтується на балансі життєво важливих інтересів особистості, суспільства і держави.

Останнє передбачає в першу чергу чітку політику держави в соціально-економічній сфері її діяльності.

Економіка – найважливіша сфера суспільного життя, в якій на основі використання різноманітних ресурсів здійснюється виробництво, обмін, розподіл та споживання продуктів людської діяльності, формується і постійно розвивається система продуктивних сил і економічних відносин, якими управляють різні типи економічних законів. Економіка має складну структуру її матеріальною основою є система продуктивних сил, що відображає активне ставлення людини до природи у процесі праці й створення матеріальних та нематеріальних благ.

На всіх етапах розвитку людської цивілізації до системи продуктивних сил входили людина-працівник, засоби виробництва, сили природи, які використовувалися людьми. У XIX ст. новим елементом цієї системи стають форми і методи організації виробництва, у другій половині XX ст. – наука та інформація.

Останні наразі стають визначальними чинниками функціональної структури економіки і, як ми вважаємо, стають її основою.

Економіку, на нашу думку схематично можна відобразити так: “економіка науки” (інформація => інформаційні ресурси => інноваційна діяльність => якісно нові знання => інтелектуальні ресурси), “науково-технологічна економіка” та “економіка матеріального виробництва”.

Таким чином, під забезпеченням економічної безпеки держави розуміється: забезпечення від реальних, а за можливості і потенціальних збитків пріоритетним напрямам системи суспільних відносин, що стосуються економічної діяльності держави специфічним для кожного державного органу видом діяльності [6].

Економічна безпека – надійна захищеність національно-державних інтересів у сфері економіки від реальних та потенційних внутрішніх і зовнішніх загроз, а в першу чергу - прямих та опосередкованих економічних збитків. Стан економічної безпеки оцінюється системою параметрів, які визначають сприятливі умови функціонування економічної системи.

В сучасному світі рушійною силою економіки стають якісно нові знання, тому структуру економіки, як інноваційної можна звести до наступної формули: загальна економіка = економіка науки + науково-технологічна економіка + економіка матеріального виробництва.

Тобто, безпека держави залежить в першу чергу від її політичної складової із забезпечення економічної безпеки суспільства [7].

Розмежування повноважень між державними органами у забезпеченні національної безпеки та окремих видів безпеки, у т.ч. і державної, зумовлена низкою факторів негативного впливу. По-перше, в Україні існує конституційна невизначеність статусу глави держави, що зумовлює прогалини у визначенні відповідної компетенції Президента та так званих “допоміжних” органів при Президентові, що фактично виконують певні повноваження [8 – 10]. По-друге, тривалий час проводиться адміністративна реформа, що зумовлює існування державних органів з різним статусом [11, с. 28-29]. Зазначене негативно впливає на керованість ними особливо при загострення внутрішньополітичного протистояння. У літературі на це було звернуто увагу в контексті необхідності належного та ефективного організаційно-правового удосконалення системи забезпечення національної безпеки України [12].

Враховуючи вимоги законодавчих актів у цій сфері, пропонується систематизувати суб’єкти забезпечення безпеки наступним чином.

Верховна Рада України – орган законодавчої влади в Україні, який покликаний боронити суверенітет і незалежність України, дбати про благо країни і добробут Українського народу шляхом прийняття законів та інших нормативно-правових актів обов’язкових до виконання всіма органами влади та управління України, а також здійснення парламентського контролю у випадках, визначених законом.

Можливо систематизувати конституційно визначені повноваження Верховної Ради щодо забезпечення безпеки у таких сферах.

1. *Політична* – визначення основ національної безпеки; засад внутрішньої і зовнішньої політики; організації діяльності органів виконавчої влади; основ державної служби, державної статистики та інформатики; правового режиму державного кордону; контролю за діяльністю Кабінету Міністрів України; прийняття рішення щодо Програми діяльності Кабінету Міністрів України; відповідальності Кабінету Міністрів України та прийняття резолюції недовіри Кабінету Міністрів України; територіального устрою України; заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України; надання згоди на обов’язковість міжнародних

договорів України та денонсація міжнародних договорів України; парламентський контроль.

2. *Воєнна* – оголошення за поданням Президента України стану війни і укладення миру; схвалення рішення Президента України про використання Збройних Сил України та інших військових формувань у разі збройної агресії проти України; організації Збройних Сил України; порядку допуску та умов перебування підрозділів збройних сил інших держав на території України; порядку направлення підрозділів Збройних Сил України до інших держав; затвердження указів Президента про введення воєнного чи надзвичайного стану в Україні або в окремих її місцевостях, про загальну або часткову мобілізацію; правовий режим воєнного стану.

3. *Економічна* – визначення основ зовнішньоекономічної діяльності та митної справи; засади формування Державного бюджету України і бюджетної система України; засади використання природних ресурсів, виключної (морської) економічної зони, континентального шельфу, освоєння космічного простору, організації та експлуатації енергосистем, транспорту і зв'язку; засади створення і функціонування фінансового, грошового, кредитного та інвестиційного ринків; затвердження Державного бюджету України та внесення змін до нього, контроль за виконанням Державного бюджету України, прийняття рішення щодо звіту про його виконання; затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля; затвердження переліку об'єктів права державної власності, що не підлягають приватизації, визначення правових засад вилучення об'єктів права приватної власності; порядок випуску та обігу державних цінних паперів, їх види і типи; порядок утворення і погашення державного внутрішнього і зовнішнього боргу; правовий режим власності; система оподаткування, податки і збори; статус національної валюти, а також статус іноземних валют на території України; затвердження указів Президента про оголошення окремих місцевостей зонами надзвичайної екологічної ситуації; правовий режим надзвичайного стану; правовий режим зон надзвичайної екологічної ситуації.

4. *Сфера правосуддя* – визначення засад забезпечення громадського порядку; засад організації та діяльності адвокатури; засад судової експертизи; засад організації і діяльності прокуратури, нотаріату, органів досудового розслідування, органів і установ виконання покарань; порядку виконання судових рішень; судоустрою, судочинства та статусу суддів;

Президент України є главою держави і виступає від її імені, є гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, є гарантом реалізації стратегічного курсу держави.

Конституційно визначеними повноваженнями Президента України у політичній, воєнній, економічній та судовій сферах, можливо назвати вжиття заходів щодо:

1. *Політична сфера*: захищеності державного суверенітету, державної незалежності і правонаступництва держави від реальних та потенційних загроз; захищеності територіальної цілісності від реальних та потенційних загроз; захищеності демократичного конституційного ладу від реальних та потенційних загроз; керівництва у сфері безпеки держави; представництва держави в міжнародних відносинах; керівництва зовнішньополітичною діяльністю держави, ведення переговорів та укладення міжнародних договорів; подання про призначення Верховною Радою України Прем'єр-міністра, Міністра оборони, Голови Служби безпеки та Міністра закордонних справ України; призначення та звільнення з посад половини складу Національної ради України з питань телебачення і радіомовлення; головування у Раді національної безпеки і оборони

України; ветування прийнятих Верховною Радою України законів (крім законів про внесення змін до Конституції України) з наступним поверненням їх на повторний розгляд Верховної Ради України; видання декретів, указів і розпоряджень.

2. *Воєнна сфера*: Головнокомандування Збройними Силами України; призначення та звільнення з посад вищого командування Збройних Сил України та інших військових формувань; керівництва у сфері оборони держави; внесення до Верховної Ради України подання про оголошення стану війни та у разі збройної агресії проти України прийняття рішення про використання Збройних Сил України та інших утворених відповідно до законів України військових формувань; про загальну або часткову мобілізацію та введення воєнного стану в Україні або в окремих її місцевостях у разі загрози нападу, небезпеки для незалежності України.

3. *Економічна сфера:* призначення та звільнення з посад половини складу Ради Національного банку України; призначення та звільнення з посад голів державних адміністрацій; зупинення дії актів Кабінету Міністрів України з мотивів невідповідності Конституції з одночасним зверненням до Конституційного Суду України щодо їх конституційності.

4. *Сфера правосуддя:* призначення та звільнення з посади за згодою Верховної Ради України Генерального прокурора; призначення на посади третину складу Конституційного Суду України; призначення та звільнення з посад суддів.

Рада національної безпеки і оборони України є координаційним органом при Президентові України, яка координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони.

Повноваженнями РНБО України у політичній, воєнній, економічній та судовій сферах є питання:

1. *Політична сфера:* розробки та розгляду на засіданнях питань, які належать до сфери державної безпеки та надання пропозицій Президентові України; виконання прийнятих Радою національної безпеки і оборони України рішень, введених в дію указами Президента України; здійснення поточного контролю та координації за діяльністю органів виконавчої влади в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують державній безпеці України, подання Президентові України відповідних висновків та пропозицій; ініціація розробки нормативних актів та документів з питань державної безпеки, узагальнення практики їх застосування та результатів перевірок їх виконання; внесення пропозиції Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері державної безпеки; визначення стратегічних національних інтересів України, концептуальних напрямів забезпечення державної безпеки у політичній, економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах; формування проектів державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів та документів з питань державної безпеки; удосконалення системи забезпечення державної безпеки, утворення, реорганізації та ліквідації органів влади у сфері національної безпеки; розробки та впровадження системи невідкладних заходів із розв’язання кризових ситуацій, що загрожують державній безпеці України.

2. *Воєнна сфера:* координації та контролю діяльності органів влади по відбиттю збройної агресії, організації захисту населення та забезпеченню його життєдіяльності, охороні життя, здоров'я, конституційних прав, свобод і законних інтересів громадян, підтриманню громадського порядку в умовах воєнного та надзвичайного стану та при виникненні кризових ситуацій, що загрожують державній безпеці України; координації та

контролю діяльності органів виконавчої влади у сфері оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують державній безпеці України; координації та контролю переведення центральних і місцевих органів виконавчої влади, а також економіки країни на роботу в умовах воєнного чи надзвичайного стану; координації та контролю діяльності органів місцевого самоврядування в межах наданих повноважень під час введення воєнного чи надзвичайного стану.

3. *Економічна сфера:* координації та контролю діяльності органів виконавчої влади у сфері державної безпеки у мирний час; законодавства про Державний бюджет України та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням державної безпеки; матеріального, фінансового, кадрового, організаційного та іншого забезпечення виконання заходів з питань державної безпеки; розробки, реалізації та контролю заходів політичного, економічного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України у сфері забезпечення державної безпеки; координації та контролю діяльності органів виконавчої влади з протидії корупції; оголошення стану війни, загальної або часткової мобілізації, введення воєнного чи надзвичайного стану в Україні або окремих її місцевостях, оголошення в разі потреби окремих місцевостей України зонами надзвичайної екологічної ситуації.

4. *Сфера правосуддя:* координує і контролює діяльність органів виконавчої влади з протидії корупції, забезпечення громадської безпеки та боротьби із злочинністю.

Вищим органом у системі виконавчої влади є Кабінет Міністрів України, що відповідальний перед Президентом України і Верховною Радою України, підконтрольний і підзвітний Верховній Раді України.

Кабінет Міністрів України у своїй діяльності керується Конституцією та законами України, виконує постанови Верховної Ради України та укази Президента України відповідно до правового режиму у державі.

Повноваженнями Кабінету Міністрів України у політичній, воєнній, економічній та судовій сферах є питання:

1. *Політична сфера*: забезпечення державного суверенітету і економічної самостійності України, здійснення внутрішньої і зовнішньої політики держави, виконання Конституції і законів України, актів Президента України; забезпечення реалізації стратегічного курсу держави; вжиття заходів із забезпечення прав і свобод людини і громадянина.

2. *Воєнна сфера*: здійснення заходів щодо забезпечення обороноздатності і державної безпеки України.

3. *Економічна сфера*: розробки проекту закону про Державний бюджет України і забезпечення виконання Державного бюджету України та подання Верховній Раді України звіту про його виконання; організація і забезпечення зовнішньоекономічної діяльності України, митної справи; розробки і здійснення загальнодержавних програм економічного, науково-технічного, соціального і культурного розвитку України; забезпечення проведення фінансової, цінової, інвестиційної та податкової політики; забезпечення проведення політики у сферах праці й зайнятості населення, соціального захисту, освіти, науки і культури, охорони природи, екологічної безпеки і природокористування; забезпечення рівних умов розвитку всіх форм власності; здійснення управління об’єктами державної власності.

4. *Сфера правосуддя*: здійснення заходів з забезпечення громадського порядку, боротьби зі злочинністю; здійснення заходів щодо забезпечення державної безпеки України.

Щодо місцевого рівня необхідно зазначити, що виконання державних і регіональних програм соціально-економічного та культурного розвитку, програм охорони довкілля (а в місцях компактного проживання корінних народів і національних меншин – також програм їх національно-культурного розвитку), реалізацію інших наданих державою, а також делегованих відповідними радами повноважень, забезпечують місцеві органи виконавчої влади.

Зазначені вище повноваження мають бути втіленими в доктрини, концепції, стратегії та програми діяльності органів влади та управління [13].

Окрім цього, слід звернути увагу на доволі значне розмаїття державних органів, які мають чітко визначену законодавством компетенцію у сфері забезпечення безпеки, що обумовлена відповідними основними завданнями. До числа суб'єктів забезпечення національної безпеки України законодавець прямо відносить 13 суб'єктів. 2 з них є міністерствами; 2 – центральними органами виконавчої влади зі статусом служби; 2 – центральними органами виконавчої влади зі спеціальним статусом; 2 – органи, з центральними органом виконавчої влади у своєму складі; 2 – військові формування, 1 – державний орган, 1 – державний правоохоронний орган спеціального призначення, 1 – державний орган спеціального призначення з правоохоронними функціями. До цього переліку можливо додати ще 1 міністерство з компетенцією забезпечення формування та реалізації оборонної політики та 1 державний орган (СЗР).

Із 15 перелічених вище лише 5 мають правовий статус, що відповідає системі, яка визначена Законом України "Про центральні органи виконавчої Владик, а 2/3 мають правовий статус, що є унікальним. Така унікальність негативно впливає на стан керованості, оскільки правовий статус служби чи агентства зумовлює підпорядкування відповідному Міністру, що не завжди можливо враховуючи специфіку завдань. Відповідна проблема може бути вирішена лише на рівні здійснення заходів адміністративної реформи (щодо організації державного управління), що триває у системі державного управління надто довго [14].

Висновки.

Таким чином, знаходить своє підтвердження теза, що державна безпека - це безпека: державно-політичного, конституційно легітимізованого політичного ладу держави від змін його неконституційним шляхом; державотворення і конструктивної політики задля стабільності суспільства; політичного суверенітету; територіальної цілісності України і недоторканності її кордонів; інститутів державної влади; національно-державних інтересів у сфері економіки задля ефективної реалізації соціального призначення держави – забезпечення подальшого розвитку особи, суспільства та держави

Ефективна реалізація соціального призначення органів влади та управління (якісні показники зазначених безпек мають бути викладені та закріплені належним чином із законодавчо визначеними формами та методами, силами і засобами із забезпечення подальшого розвитку особи, суспільства та самої держави в умовах конкретних правових режимів у політичній, економічній, воєнній, науково-технологічній та інших важливих сферах діяльності суспільства. Сукупність форм, методів, сил та засобів залежить від чіткого розмежування компетенції державних органів.

Забезпечення державної безпеки, як призначення, законодавчо визначено для Служби безпеки України. Водночас безпеку держави забезпечують інші державні органи. Основним негативним фактором впливу для належної організації діяльності у цій сфері є незакінчена адміністративна реформа, що має на меті уніфікацію системи центральних органів виконавчої влади. Також необхідним є належне визначення правового статусу так званих "допоміжних" органів при Президентові України та

виокремлення відповідного обсягу його повноважень, що безпосередньо пов'язані із гарантуванням державного суверенітету і територіальної цілісності держави.

Окрім цього, послідовність законодавчого визначення має здійснюватись від призначення державного органу через мету діяльності, завдання, функції та повноваження.

Використана література

1. Українчук О.В. Забезпечення національної безпеки в умовах формування в Україні громадянського суспільства та демократичної, правової, соціальної держави: автореф. дис. ...канд. юрид. наук. Харків, 1994. 18 с.

2. Ященко В.А. Щодо визначеності поняття "національна безпека України": зб. матеріалів круглого столу *Право національної безпеки та військове право: історія, сучасність і перспективи*, Київ, 28 берез. 2019 р. / упоряд.: М.М. Прохоренко, П.П. Богуцький; за заг. ред. М.М. Прохоренка. Київ: ФОП Ямчинський О.В., 2019. С. 45-48.

3. Гордієнко С.Г. Про поняття "державна безпека". *Науковий вісник Академії СБ України.* 1998. № 6 – 7. С. 33-41.

4. Гордієнко С.Г. Методологічні аспекти теорії державної безпеки України та захисту інтелектуальної власності Службою безпеки: матеріали наук.-практ. конференції *Концептуальні засади забезпечення державної безпеки України*, Київ, 9 черв. 2004 р. Київ: Вид-во НА СБ України, 2004. С. 70-73.

5. Кравчук О.Ю. Особливості політичної безпеки України. *Українська національна ідея: реалії та перспективи розвитку*. 2011. Вип. 23. С. 85-89.

6. Гордієнко С.Г. Забезпечення економічної безпеки держави контррозвідкою СБ України: матеріали наук.-практ. конференції *Проблеми контррозвідувального захисту економічної безпеки держави*, м. Харків, 19 груд. 2003 р. Харків: ФПС для СБ України (СФ) у складі Нац. юрид. акад. України, 2004. С. 55-61.

7. Гордієнко С.Г. Складові безпеки української державності за сферами її буття. *Юридична Україна.* 2020. № 9. С. 6-17.

8. Федоренко В.Л. Конституційно-правовий статус Ради національної безпеки і оборони України. *Бюлетень Міністерства юстиції України.* 2010. № 12. С. 32-39.

9. Цоклан В.І. Структура Ради національної безпеки і оборони України як важливий елемент її конституційно-правового статусу. *Часопис Київського університету права.* 2011. № 2. С. 90-93.

10. Коваль Н.В., Пухтинський М.О. Забезпечення впорядкування допоміжних структур при Президентові України на законодавчому рівні. *Вісник НАДУ при Президентові України. Серія: "Державне управління"*. 2017. № 4. С. 10-19.

11. Авер'янов В.Б. Система органів виконавчої влади: проблеми реформування у світлі конституційних вимог. *Право України.* 2003. № 9. С. 24-30.

12. Доронін І.М. Організаційно-правові аспекти трансформації системи сектору національної безпеки та оборони. *Порівняльно-аналітичне право.* 2019. № 6. С. 230-233.

13. Гордієнко С.Г. Повноваження державних органів у забезпеченні безпеки держави та напрями їх удосконалення. *Юридична Україна.* 2019, № 10. С. 6-17.

14. Мельниченко В. Правове забезпечення реформування системи центральних органів виконавчої влади в Україні: стан та перспективи. *Вісник Національної академії державного управління. Серія: "Державне управління"*. 2013. Вип. 1. С. 180-187.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.951

ГОРУН О.Ю., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-0447-1729.

ПРІОРИТЕТНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *Розглянуто пріоритети державної політики кібербезпеки. Визначено сучасні виклики та загрозливі тенденції у сфері забезпечення кібербезпеки. Деталізовано засади формування та реалізації державної політики кібербезпеки. Проаналізовано окремі акти вітчизняного законодавства, присвячені актуальним питанням забезпечення кібербезпеки. Обґрунтовано доцільність посилення спроможностей національної системи кібербезпеки України. Окреслено пріоритетні напрями розбудови критичної інформаційної інфраструктури. Визначено завдання та шляхи удосконалення нормативно-правового регулювання державної політики кібербезпеки.*

Ключові слова: *кібербезпека, кіберзагроза, кібератака, кіберзброя, кіберзахист, національна система кібербезпеки, кіберінцидент, кіберпростір, державна політика кібербезпеки, цифровізація.*

Summary. *The priorities of the state cybersecurity policy are considered. Modern challenges and threatening trends in the sphere of cybersecurity have been identified. The main principles of formation and implementation of the state cybersecurity policy are detailed. Some acts of domestic legislation devoted to the topical issues of cybersecurity are analyzed. The expediency of strengthening the capabilities of the national cybersecurity system of Ukraine is substantiated. The priority directions of development of the critical information infrastructure are outlined. The tasks and directions of improvement regulatory framework of state cybersecurity policy have been identified.*

Keywords: *cybersecurity, cyberthreat, cyberattack, cyberweapons, cyberdefense, national cybersecurity system, cyberincident, cyberspace, state cybersecurity policy, digitalization.*

Аннотация. *Рассмотрены приоритеты государственной политики кибербезопасности. Определены современные вызовы и угрожающие тенденции в сфере обеспечения кибербезопасности. Детализированы основы формирования и реализации государственной политики кибербезопасности. Проанализированы отдельные акты отечественного законодательства, посвященные актуальным вопросам обеспечения кибербезопасности. Обоснована целесообразность усиления возможностей национальной системы кибербезопасности. Очерчены приоритетные направления развития критической информационной инфраструктуры. Определены задачи и направления усовершенствования нормативно-правового регулирования государственной политики кибербезопасности.*

Ключевые слова: *кибербезопасность, киберугроза, кибератака, кибероружие, киберзащита, национальная система кибербезопасности, киберинцидент, киберпространство, государственная политика кибербезопасности, цифровизация.*

Постановка проблеми. Кібербезпека була і залишається однією із важливих складових системи національної безпеки України. Питома вага, форми та види кіберзагроз в контексті національної безпеки постійно та динамічно зростають й трансформуються. Ця загрозлива тенденція в міру розвитку інформаційно-комп'ютерних (цифрових) технологій (далі – ІКТ) та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на

функціонування структур управління як національних, так і транснаціональних, формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів.

Реалізація зазначеного пріоритету забезпечує в епоху тотальної цифровізації повноцінну життєдіяльність політикуму держави, бізнесу та пересічених громадян і здійснюється шляхом посилення спроможностей національної системи кібербезпеки. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору. Це зумовлює нові можливості для цифровізації всіх сфер суспільного життя. Враховуючий такий стан справ, актуальним та своєчасним є уточнення та деталізація пріоритетних засад державної кібербезпекової політики.

Результати аналізу наукових публікацій. Проведення контент-аналізу та розгляд основ державної політики у сфері забезпечення кібербезпеки, пошук оптимальних шляхів її удосконалення здійснювали у своїх наукових працях такі фахівці, як: О. Бакалінська [1], Л. Веселова [2], Ю. Геращенко [3], Р. Лук'янчук [4] та ін. Адже з набуттям чинності 14 вересня 2020 року Стратегії національної безпеки України [5] пріоритетні засади державної кібербезпекової політики набувають неабиякої актуальності в епоху масштабного поширення ІКТ, суцільної світової діджіталізації та потребують уточнення на рівні науково-теоретичної проблеми.

Метою статті є визначення пріоритетних засад державної кібербезпекової політики з урахуванням загрозливих тенденцій та викликів сучасності, визначення шляхів, практична реалізація яких надасть змогу досягнути такого рівня захищеності кіберпростору, який забезпечує реалізацію національних інтересів України у кібернетичній сфері.

Виклад основного матеріалу. Основним правовим актом, положення якого визначають основні цілі, напрями та принципи державної політики у сфері кібербезпеки є Закон України "Про основні засади забезпечення кібербезпеки" від 05.10.17 р. [6]. Забезпечення кібербезпеки здійснюється відповідно до пріоритетних засад державної політики у цій сфері, яка включає формування, удосконалення та реалізацію організаційно-правових, науково-технічних, правоохоронних, економічних заходів забезпечення національної безпеки в кіберсфері. Обов'язком політичного керівництва будь-якої держави світу є забезпечення безперешкодного та надійного доступу громадян і суспільства до безпечного кібернетичного середовища шляхом упровадження та реалізації виваженої державної політики, спрямованої на мінімізацію наслідків будь-яких кібератак, кіберінцидентів та кіберзагроз, недопущення блокування спецслужбами іноземних держав або хакерськими групами діяльності стратегічно важливих інформаційно-комунікаційних мереж, електронних комунікацій, цілеспрямованих посягань на об'єкти національної критичної інформаційної інфраструктури.

Розуміючи загрозливий характер та масштаби поширення кіберзагроз у сучасному світі, і зокрема для України, у Посланні Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України в 2020 році" [7] визначено, що інформаційне протиборство з державою-агресором триває й у кіберпросторі.

Адже формування та реалізація пріоритетів державної кібербезпекової політики повинні враховувати сучасні виклики у сфері кібербезпеки, виходячи із внутрішніх та зовнішніх негативних факторів й загрозливих тенденцій, до яких можна віднести:

активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, змагальний характер розвитку засобів кібербезпеки та реалізації кіберзагроз у процесі швидких прогресуючих змін ІКТ щодо Хмарних обчислень, Великих Даних, Інтернету речей, 5G-мереж тощо; мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї, які надають можливість здійснювати приховане проведення противником кібератак та кібероперацій, віддаленого взяття під контроль систем управління, завдання шкоди та руйнування критичної інформаційної інфраструктури; зростання технологічного рівня протиправних зовнішніх посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій; вплив поширення пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинило швидку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням саме електронних сервісів та інформаційно-комунікаційних систем.

В сучасному світі передумовами динамічного поширення кіберзагроз все ще залишаються: недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування кіберзлочинів, низький рівень правової відповідальності за порушення вимог законодавства у цій сфері; відсутність у значної частини органів державної влади відповідних структурних підрозділів, фінансування робіт із кіберзахисту за залишковим принципом з технологічними помилками; відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів; незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Надзвичайно актуальною загрозою в сучасних умовах є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов’язана з проведенням спецслужбами іноземних держав, насамперед Російської Федерації, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об’єктів критичної інформаційної інфраструктури, передусім систем управління державою, об’єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій). Загальновідомо, що з 2014 року Росія активно використовує кіберпростір у форматі гібридної агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами та зброєю сил оборони, а також на об’єкти критичної інфраструктури. Держава-агресор постійно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей та спроможностей у сфері забезпечення кібербезпеки органами сектору безпеки і оборони.

Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних

країні-агресору та іншим країнам. Збільшення кількості інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах призвело до створення глобального ринку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет. Дедалі частіше спрямовані кібератаки не здійснюються напряму на уряди та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до великої кількості їх клієнтів та завдання масштабної шкоди. Популярні веб-сайти, соціальні мережі, реєстри збирають значну кількість різноманітних персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

В Україні в останні роки відчутно зросла загроза кібертероризму, що насамперед, пов'язано з кіберможливостями держави-агресора РФ, яка веде проти України кібервійну із застосуванням кіберзброї. Дедалі частіше спостерігається тенденція використання кіберпростору з метою фінансування терористичних угруповань. Водночас недостатньою є взаємодія України з міжнародними партнерами щодо опрацювання на взаємовигідній основі механізмів протидії кібертероризму. Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до ІКТ та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору з метою вчинення інших кримінальних правопорушень (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація значно ускладнюється через низький рівень кіберграмотності населення, зокрема, пересічних користувачів електронних послуг.

Держава зацікавлена у створенні системи захисту від ризиків, викликів та загроз для державних інформаційних ресурсів та об'єктів критичної інфраструктури, тобто забезпеченні такого важливого елементу, як "кіберстабільність". Слід вказати, що в Україні до 2021 року були відсутні концептуальні засади формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян, що значно гальмувало процес забезпечення розвитку усіх сфер суспільного життя відповідно до сучасних вимог, процесів глобальної цифровізації економіки, сфер життєдіяльності суспільства, які відбуваються у більшості країн світу. З метою розв'язання окреслених проблемних питань, останнім часом, спостерігається активна та плідна нормотворчість Уряду України з метою визначення пріоритетних напрямків щодо проведення послідовної та виваженої державної політики, спрямованої на досягнення інтеграційного курсу до європейського співтовариства та євроатлантичних спільнот, визначення та реалізації заходів, спрямованих на стрімкого розвитку цифрової економіки, підвищення кіберграмотності населення України.

Так, протягом останнього часу, були схвалені: Національна економічна стратегія на період до 2030 року (Постанова Кабінету Міністрів України від 03.03.21 р. № 179) [8], та Концепція розвитку цифрових компетентностей (Розпорядження Кабінету Міністрів України від 03.03.21 р. № 167) [9]. Аналіз вказаних нормативно-правових актів дає змогу констатувати, що прискорена цифрова трансформація є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Впровадження нових

технологій, цифрових послуг та механізмів взаємодії громадян з державою, включаючи виборчий процес, створює значну кількість прихованих взаємозв'язків на рівні технологій і процесів. Проте, за відсутності системного підходу до кібербезпеки та оцінки ризиків існує ймовірність втрати довіри громадян до процесів цифрової трансформації, актуалізації поширення кіберзагроз. Адже обов'язок політичного керівництва України – це створення безпечних інформаційних систем та відкриття доступу до них задля суспільного блага.

Важливим та актуальним напрямком залишається розбудова національної системи кібербезпеки. Держава має розбудовувати національну систему кібербезпеки, ґрунтуючись на: всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей України), неухильному захисті національних інтересів України у сфері кібербезпеки; перманентності заходів з удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо її актуалізації відповідно до безпекових умов, що змінюються; орієнтованості на суспільство, що сприятиме його економічному і соціальному зростанню; використанні принципу мінімальної достатності ролі держави у процесах розвитку та забезпечення безпеки кіберпростору, встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту, повазі до основоположних цінностей, прав людини і особи на свободу вираження думки, такому самому захисті загальновизнаних основоположних прав в онлайн-середовищі, як і в офлайновому; засудженні практики перевищення встановлених меж необхідності щодо обмеження прав громадян та юридичних осіб під час використання кіберпростору та ІКТ; відкритості та створенні умов для активної участі всіх заінтересованих сторін з урахуванням їх потреб і зобов'язань в умовах, коли кібербезпека цифрового середовища набула надважливого значення для держави, суспільства і громадян; визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності, застосування стимулюючих механізмів та обміну унікальними знаннями і досвідом; ризик-орієнтованому підході в частині заходів забезпечення кібербезпеки та кіберзахисту тощо.

Узагальнюючи викладене, державними пріоритетами забезпечення кібербезпеки України виступають такі складові:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки.

З метою реалізації вказаних пріоритетів держава повинна не лише створити та розвивати ефективні (у тому числі кадрові та технологічні) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну організаційно-правову та технологічну модель їх функціонування та застосування, що неможливо уявити без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності. Україна має забезпечити проведення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів

держави, суспільства і окремих громадян. Правоохоронні та державні органи спеціального призначення з правоохоронними функціями мають посилити спроможності для мінімізації загроз кіберзлочинності, свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів. Важливим напрямком залишається створення необхідних умов задля забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору.

Держава об'єктивно зацікавлена у створенні системи захисту від ризиків, викликів та загроз у тому числі й для державних інформаційних ресурсів та об'єктів критичної інфраструктури, тобто забезпеченні такого важливого елементу, як "кіберстійкість". З цією метою актуальним завданням держави має стати посилення національної кіберготовності, що являє собою здатність суб'єктів сектору безпеки і оборони своєчасно й ефективно реагувати на кібератаки, забезпечувати штатний режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед, об'єктів критичної інформаційної інфраструктури. Актуальним при цьому, залишається забезпечення гарантій з боку держави щодо надійності та безпеки цифрових послуг.

У рамках реалізації пріоритетних напрямів державної політики у сфері забезпечення безпеки критичної інфраструктури, з метою вдосконалення правової основи захисту критичної інфраструктури та створення системи її державного управління РНБО України ухвалила Рішення "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29.12.16 р., що затверджено Указом Президента України від 16.01.17 р. № 8/2017 [10], яким, зокрема, передбачалося:

створення державної системи захисту критичної інфраструктури;

визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;

визначення функцій, повноважень та відповідальності центральних органів виконавчої влади, інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;

запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;

запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації тощо.

На підставі вказаного Постановою Кабінету Міністрів України була затверджена "Концепція створення державної системи захисту критичної інфраструктури" від 06.12.17 р. № 1009 [11]. Реалізація положень цієї Концепції мала сприяти: створенню державної системи захисту критичної інфраструктури, здатної забезпечувати належний рівень захисту такої інфраструктури від усіх видів загроз; виробленню механізмів ефективного реагування у разі виникнення кризових ситуацій та ліквідації їх наслідків, а також швидкому відновленню функціонування об'єктів критичної інфраструктури; налагодженню ефективної взаємодії між усіма суб'єктами державної системи захисту критичної інфраструктури за активної підтримки суспільства, місцевих громад, засобів масової інформації та недержавних дослідних інституцій, що вивчають проблеми безпеки та оборони; гармонізації законодавства України у сфері захисту критичної інфраструктури із законодавством ЄС; міжнародному співробітництву у сфері захисту критичної інфраструктури.

У рамках реалізації спроможностей держави у вказаному сегменті, відповідальні суб'єкти національної системи кібербезпеки мали розробити Національний перелік об'єктів критичної інфраструктури. На жаль, станом на 2021 рік, такий перелік все ще не сформульований, хоча останнім часом було схвалено декілька нормативно-правових актів, присвячених поступовому вирішенню цього стратегічного завдання держави. Зокрема, за цією тематикою було прийнято низку актів Уряду України, серед яких виділяються Постанови Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.19 р. № 518 [12] та "Деякі питання об'єктів критичної інформаційної інфраструктури" від 09.10.20 р. № 943 [13].

Також в нашій державі відсутній уніфікований законодавчий акт про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури. Не випадково в умовах технологічного відставання від світових країн-лідерів у сфері високих технологій вітчизняна ІТ-інфраструктура, в тому числі й об'єкти критичної інформаційної інфраструктури, ще й досі залежні від імпортних програмно-апаратних комплексів та відповідного програмного забезпечення.

Аналіз положень чинного законодавства надає підстави констатувати про відсутність у нашій державі системних правових актів є прямим свідченням того, що на сьогодні існують та поширюються загрозливі тенденції в кіберпросторі, які безпосередньо впливають на цілісність державної політики у сфері кібербезпеки. Очевидним фактом є також недостатня нормативна урегульованість міжвідомчої координації з питань забезпечення кібербезпеки, відсутність схваленої на державному рівні оновленої Стратегії кібербезпеки на 2021 – 2025 роки.

Таким чином, у сучасних умовах державна політика у сфері забезпечення кібербезпеки повинна бути сконцентрована на досягненні вагомих результатів з метою створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України та блокування будь-яких посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; зниження рівня вразливості об'єктів кіберзахисту; приєднання до європейської системи та дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення міжнародної кібербезпеки.

Забезпечення кібербезпеки як важлива складова державної політики залишається комплексною проблемою, яка потребує, у першу чергу, схвалення законодавчих та нормативно-правових актів, спрямованих на розв'язання проблемних питань у цій сфері. Основною метою реалізації державної політики у сфері забезпечення кібербезпеки є: створення політико-правових, фінансово-економічних, організаційних та матеріально-технічних умов для формування її сучасної моделі, орієнтованої на позитивний досвід ЄС та НАТО; підвищення ефективності використання усіх видів інформаційно-телекомунікаційних ресурсів і управління елементами інформаційно-комунікаційної інфраструктури, державної підтримки виробництва вітчизняної ІТ-продукції, забезпечення розвитку та дієвого захисту кіберпростору.

Висновки.

Пріоритетні засади державної політики України у сфері забезпечення кібербезпеки мають формуватися комплексно, виходячи із сфери національних інтересів, балансу інтересів людини, суспільства і держави. Формування державної політики забезпечення кібербезпеки передбачає реалізацію дієвих заходів організаційно-правового, технічного, фінансово-економічного, виховного і наукового спрямування та зовнішньополітичного характеру.

Серед організаційно-правових заходів, зокрема, виділяється: прискорення схвалення Стратегії кібербезпеки на 2021 – 2025 роки, затвердження Національного переліку об'єктів критичної інфраструктури, розроблення та запровадження індикаторів стану кібербезпеки на основі системного моніторингу виявлення і прогнозування кіберзагроз, що надасть змогу фіксувати досягнення або недоліки функціонування системи кібербезпеки.

Технічні заходи в рамках державної політики забезпечення кібербезпеки мають бути спрямовані на: створення технологічної складової національної системи кібербезпеки, зокрема формування конкурентного середовища у сфері електронних комунікацій; розвиток технологій кіберзахисту, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку; удосконалення технічного захисту інформації, забезпечення регламентації процедури підтвердження відповідності засобів технічного захисту інформації; створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення; тотальну модернізацію програмно-апаратного оснащення комплексів, що забезпечують роботу (CERT-UA); розробку та практичне впровадження галузевих індикаторів стану кібербезпеки; удосконалення системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних ІКТ (включаючи технології онлайн-доступу); розробку нових методів запобігання кібератакам, кіберінцидентам.

Фінансово-економічні заходи мають бути спрямовані на створення економічних передумов для розвитку і забезпечення безпеки критичної інформаційної інфраструктури держави та її ресурсів, активізації інвестиційної діяльності держави у сферу високих технологій та покращення інвестиційного клімату української ІТ-індустрії, збільшення державного бюджетного фінансування на потреби реалізації заходів щодо забезпечення кібербезпеки, збільшення обсягів на фінансування сектору безпеки і оборони України; створення конкурентоспроможної національної системи виробництва ІТ-продукції, розвинутої інформаційно-комунікаційної інфраструктури; сприяння розвитку конкуренції, вдосконалення антимонопольної політики в інформаційній сфері, зокрема шляхом розроблення і вжиття комплексу заходів, спрямованих на запобігання надходженню контрафактної продукції, захист вітчизняного інформаційного ринку, вітчизняного ІТ-виробника та споживачів. Обсяги бюджетного фінансування потрібно визначати щороку під час складання проектів бюджетів на відповідний рік виходячи із завдань та фінансових можливостей держави.

Заходи державної політики у сфері забезпечення кібербезпеки виховного та наукового спрямування мають передбачати: налагодження процесу підготовки кадрів у сфері кібербезпеки, забезпечення внесення змін до навчальних планів і програм середньої та вищої школи, підготовки наукових та науково-педагогічних кадрів, що спрямовані на інформування основних цільових груп про кіберзагрози та методи протидії їм; посилення державної підтримки розвитку основних напрямів науки і техніки як основи створення високих ІКТ; забезпечення створення необхідних умов для реалізації прав інтелектуальної власності в кіберпросторі України; розробку загальнодержавних програм підвищення рівня обізнаності населення щодо кіберзагроз. Потребують державної підтримки вітчизняні фундаментальні та прикладні дослідження, розробки у сфері інформатизації, телекомунікацій і зв'язку, необхідні активні загальнодержавні зусилля, спрямовані на підтримку та формування кадрового потенціалу у сфері забезпечення кібербезпеки.

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки залишається поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. Таким чином, у зовнішньополітичній сфері діяльність держави має бути зосереджена на постійному забезпеченні вільного доступу громадян до мережі Інтернет в аспекті вільного користування зарубіжними та міжнародними інформаційними ресурсами; формуванні позитивного міжнародного іміджу України на світовій арені; налагодженні тісного співробітництва з міжнародними партнерами України; забезпеченні поглиблення співпраці України з ЄС та НАТО для посилення спроможностей держави у сфері кібербезпеки; забезпеченні участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки, неухильному дотриманні взятих на себе міжнародних зобов'язань у сфері кібербезпеки; організації та проведенні науково-практичних заходів, зокрема конференцій, семінарів, форумів, симпозіумів з питань забезпечення кібербезпеки і захисту інформації в кіберпросторі на міжнародному рівні.

Таким чином, український вектор зовнішньої політики має бути сфокусований на активізацію міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримку міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, продовження комплексної взаємодії з питань кібербезпеки за участю органів державної влади і відповідних структур НАТО шляхом співпраці на двосторонній основі, впровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування (CERT) на кіберінциденти, поглиблення співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ. Світова спільнота в рамках міжнародного співробітництва також повинна спрямувати свої ініціативи щодо недопущення проведення локальних та міжнародних війн у кіберпросторі, посилити міжнародно-правову відповідальність держав за протиправну діяльність в Інтернеті та в кіберпросторі.

Ефективність заходів державної політики у сфері забезпечення кібербезпеки може бути набагато результативнішою, якщо держава обере композитну стратегію активного учасника міжнародного інформаційного ринку, що вимагає налагодження виробництва та захисту власного ІТ-продукту, створення умов для його просування на відповідні світові ринки. Державна політика у сфері забезпечення кібербезпеки сконцентрована на досягненні вагомих результатів з метою створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України та блокування будь-яких посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; зниження рівня вразливості об'єктів кіберзахисту; приєднання до міжнародної системи та дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю і кібертероризмом; забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки.

Використана література

1. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія: "Юридичні науки"*. 2019. № 2. С. 23-28.

3. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Державне управління"*. 2019. № 1. С. 140-145.

4. Лук'янчук Р. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. № 3. С. 110-117. URL: http://nbuv.gov.ua/UJRN/Vnadu_2015_3_18 (дата звернення: 20.03.2021).

5. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.03.2021).

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

7. Про внутрішнє та зовнішнє становище України у 2020 році: послання Президента України до Верховної Ради. URL: https://www.president.gov.ua/news/poslannya-prezidenta-ukrayini-volodimira-zelenskogo-do-verho-64717 (дата звернення: 20.03.2021).

8. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.21 р. № 179. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-nacionalnoyi-eko-a179 (дата звернення: 20.03.2021).

9. Концепція розвитку цифрових компетентностей: Розпорядження Кабінету Міністрів України від 03.03.21 р. № 167. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text (дата звернення: 20.03.2021).

10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури": Указ Президента України від 16.01.17 р. № 8/2017. URL: https://zakon.rada.gov.ua/laws/show/8/2017#n2 (дата звернення: 20.03.2021) .

11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 06.12.17 р. № 1009. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р#Text (дата звернення: 20.03.2021).

12. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 20.03.2021).

13. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.20 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text (дата звернення: 20.03.2021).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.951

ГУРЖІЙ С.В., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-7863-8456.

ЗАСАДИ ІНСТИТУЦІОНАЛЬНО-ФУНКЦІОНАЛЬНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Анотація. *Окреслено кіберзагрози в умовах поширення викликів сучасності. Регламентовано заходи з метою посилення спроможностей національної системи кібербезпеки. Деталізовано пріоритетні засади інституційно-функціонального забезпечення розвитку національної системи кібербезпеки. Проаналізовані заходи, які вживаються з метою інституціонального посилення безпеки у кіберпросторі у деяких зарубіжних країнах Висвітлено засади формування вертикалі контролю й координації заходів у сфері кібербезпеки. Окреслено повноваження Національного координаційного центру з кібербезпеки як робочого органу Ради національної безпеки і оборони України. Уточнено повноваження деяких суб'єктів національної системи кібербезпеки з метою уникнення дублювань. Визначено шляхи удосконалення пріоритетних засад інституційно-функціонального забезпечення кібербезпеки виходячи із загрозливих тенденцій сучасності.*

Ключові слова: *кібербезпека, кіберпростір, кіберзагрози, цифровізація, національна система, кібербезпека, оптимізація, інституціонально-функціональне забезпечення кібербезпеки, сектор безпеки і оборони, критична інформаційна інфраструктура.*

Summary. *Cyber threats in the context of the spread of modern challenges are outlined. The measures to strengthen the capacity of the national cybersecurity system are regulated. The priority principles of institutional and functional support for the development of the national cybersecurity system are detailed. The measures taken to institutionally strengthen security in cyberspace in some foreign countries are analyzed. The principles of forming the vertical of control and coordination of measures in the field of cybersecurity are highlighted. The powers of the National Coordination Center for Cyber Security as a working body of the National Security and Defense Council of Ukraine are outlined. The capacities of some actors in the national cybersecurity system have been clarified in order to avoid duplication. The directions of improvements of the priority principles of institutional and functional support of cybersecurity based on the threatening trends of today have been identified.*

Keywords: *cybersecurity, cyberspace, cyberthreats, digitalization, national cybersecurity system, optimization, institutional and functional support of cybersecurity, security and defense sector, critical information infrastructure.*

Аннотация. *Определены киберугрозы в условиях распространения вызовов современности. Регламентировано мероприятия с целью усиления возможностей национальной системы кибербезопасности. Детализированы приоритетные основы институционально-функционального обеспечения развития национальной системы кибербезопасности. Проанализированы меры, которые принимаются с целью институционального усиления безопасности в киберпространстве в некоторых зарубежных странах Освещены основы формирования вертикали контроля и координации мероприятий в сфере кибербезопасности. Очерчены полномочия Национального координационного центра по кибербезопасности как рабочего органа Совета национальной безопасности и обороны Украины. Уточнены полномочия некоторых субъектов национальной системы кибербезопасности во избежание дублирования. Определены пути совершенствования приоритетных основ институционально-функционального обеспечения кибербезопасности исходя из угрожающих тенденций современности.*

Ключевые слова: *кибербезопасность, киберпространство, киберугрозы, цифровизация, национальная система, кибербезопасность, оптимизация, институционально-функциональное обеспечение кибербезопасности, сектор безопасности и обороны, критическая информационная инфраструктура.*

Постановка проблеми. Інтенсивний розвиток інформаційно-комунікаційних технологій (далі – ІКТ), їх широке застосування в усіх сферах життєдіяльності людини створили передумови для формування глобальної інформаційної інфраструктури. У сучасному суспільстві інформаційно-комунікаційні технології є фактором, який визначає рівень соціально-економічного розвитку та стан національної безпеки. Саме тому забезпечення кібербезпеки безпосередньо впливає на розвиток та інформатизацію суспільства, певним чином стимулюючи економічне зростання держав світу. На сьогодні розвиток інформаційного суспільства, поширення інформаційних цифрових технологій в усі сфери життєдіяльності людини та суспільства стали нормою подальшої глобальної еволюції цивілізації. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя.

Становлення та динамічний розвиток ІКТ, та, як наслідок, входження в нову інформаційну еру, формування сучасного інформаційного суспільства в провідних країнах світу, з одного боку, а також переосмислення ролі та значення людини, її прав і свобод щодо інтересів держави в ракурсі її пріоритету, з іншого, спричинили необхідність динамічного розвитку вітчизняного та міжнародного законодавства у сфері кібербезпеки, яке повинно відповідати сучасним викликам шляхом формування ефективних механізмів протидії можливим правопорушенням та загрозам у кіберпросторі, вироблення моделі адекватного реагування на їх поширення та суцільну ліквідацію.

Прискорений розвиток та взаємопроникнення ІКТ поряд з потужними соціально значимими перевагами супроводжується масштабуванням кіберзагроз у всіх сферах життєдіяльності, їх еволюцією в бік високотехнологічних рішень та урізноманітненням інструментарію реалізації. Докорінно змінюючи світовий життєустрій, пандемія коронавірусу COVID-19 матиме довготривалий вплив на світовий порядок. Зростає залежність від цифрових комунікацій, що робить вразливим процес обміну інформацією, захисту інформації та персональних даних. Кіберзлочинці, максимально використовуючи тему пандемії, від її початку дедалі більше застосовують нові методи проведення кібератак, що змушує національні уряди впроваджувати додаткові механізми протидії, збереження доступу до необхідних пристроїв, належного функціонування всіх потрібних для життя та роботи важливих електронних ресурсів і відповідних систем. З огляду на це, висвітлення проблемних питань оптимізації інституційної системи забезпечення кібербезпеки залишається важливим та актуальним як з позиції фундаментальної базової теорії, так і практики її застосування.

Результати аналізу наукових публікацій. Питання організаційно-правового забезпечення кібербезпеки досліджували у своїх наукових працях такі фахівці: І. Діордиця [1], І. Доронін [2], Н. Ткачук [3], В. Шеломенцев [4] та інші. Проте деталізацію засад перспективного інституційно-функціонального забезпечення розвитку кібербезпеки жоден із вказаних авторів не здійснював, особливо в умовах масштабного поширення гібридних загроз та глобального інформаційного протистояння.

Метою статті є визначення перспективних засад інституційно-функціонального забезпечення кібербезпеки в умовах поширення гібридних загроз та викликів сучасності.

Виклад основного матеріалу. З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами, а також на об'єкти критичної інфраструктури. Держава-агресор невпинно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей забезпечення кібербезпеки органами сектору безпеки і оборони. Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед РФ, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій).

За таких умов, активізація посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань на планових засадах, спрямованих на досягнення визначених цілей. Враховуючи викладене, для України актуальним залишається інституціональна розбудова національної системи кібербезпеки, оскільки як переконливо доводить набутий досвід, діяльність її суб'єктів залишається недостатньо скоординованою й такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан та ефективність реалізації Стратегії кібербезпеки України за визначеними показниками не перевищує 40 %. Невирішеними залишаються питання оперативного обміну інформацією про кіберзагрози, налагодження ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства.

Однією із виявлених сучасних проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Протягом 2014 – 2020 років повільно здійснювався розвиток спроможностей основних суб'єктів національної системи кібербезпеки, була зафіксована обмеженість ресурсного забезпечення функціонування цієї системи, відсутність належної державної підтримки розвитку її інституційного забезпечення. Таким чином, інституціоналізація сфери забезпечення кібербезпеки – це перманентний процес створення відповідних органів державного управління, належного правового регулювання відносин у кіберпросторі, які виникають між громадянами, суспільством, державою, з метою недопущення будь-яких проявів кібертероризму, запобігання кіберзагрозам і кібератакам, ефективності заходів боротьби з кіберзлочинністю. Кардинальні зусилля держави мають бути спрямовані та активізовані на створення потужної багаторівневої інституційної системи кібербезпеки, яка була би здатна захистити не тільки громадян і суспільство, а й державні органи, приватний сектор. Інституційна система кібербезпеки має включати сукупність компонентів, серед яких важливе місце посідають: цифрова грамотність та обізнаність населення, сучасні засоби захисту особистої інформації в кіберпросторі, кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, розроблення методів запобігання кібератакам та оприлюднення інформації про них, упровадження механізмів попередження та профілактики кіберзагроз тощо.

Поширення ландшафту загроз та ускладнення інструментарію їх реалізації спонукає уряди провідних країн удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам. Вносяться зміни до моделі протидії кіберзагрозам, які пов'язані з розумінням недостатньої можливості побудувати абсолютно невразливі системи захисту. Як демонструє практика, будь-які інформаційно-комунікаційні системи можуть бути уражені внаслідок кібератаки незалежно від рівня їх захисту. Тому набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Глобальне протистояння в кіберпросторі є небезпечною складовою гібридної війни, розв'язаної проти України, у зв'язку з чим Україні потрібно швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів забезпечення кібербезпеки. Таким чином, крім відпрацювання ефективного реагування на кібератаки та кіберінциденти, доцільно вибудувати активний захист кіберпростору, створюючи належні умови для інституційно-функціонального забезпечення кібербезпеки. Проте становлення інституційної системи кібербезпеки ускладнюється низкою поточних факторів, серед яких передусім виділяється невідповідний та неефективний механізм міжвідомчої координації, наявність широких дублювань у сфері їх функціональності та компетенції.

Розуміючи сучасний стан та актуальність проблеми забезпечення кібербезпеки, більшість країн світу вживають комплексних заходів щодо безпеки в кіберпросторі, які пов'язані передусім з розробкою та вдосконаленням нормативно-правової бази, що регулює питання сфери кібербезпеки, а також створюють відомчі та державні структури, що відповідають за забезпечення кібербезпеки. Спеціальні служби різних країн вивчають методи діяльності хакерських груп, а іноді навіть активно співпрацюють з ними, використовуючи їхні знання та навички при проведенні кібернетичних операцій, пропонуючи їм натомість лояльність та захист. У рамках посилення інституційних спроможностей забезпечення кібербезпеки на початку 2019 року керівники трьох американських спецслужб ЦРУ, АНБ і ФБР офіційно заявили, що смартфони Huawei та ZTE можуть стежити за користувачами та здійснювати шпигунську діяльність.

Можна констатувати, що переважна більшість країн світу на державному рівні опікується питаннями створення та ефективного функціонування парадигми кібербезпеки, яка має такі інституційні ознаки: формуються відповідні правові норми переважно у форматі стратегій кібербезпеки та спеціальних актів законодавства, розробляються пріоритетні засади державної політики у сфері забезпечення кібербезпеки, створюються уповноважені державні органи, які відповідають за стан забезпечення кібербезпеки, динамічно розвиваються нові інтерактивні сфери, що орієнтуються на запобігання кібератакам, системну боротьбу з кіберзлочинністю, кібертероризмом, розробляються та постійно вдосконалюються технології захисту інформації та апаратно-програмного забезпечення в інформаційно-комунікаційних мережах тощо.

У сучасному світі понад 65 держав мають власні національні стратегії кібербезпеки, в яких акцент робиться на зменшенні та усуненні факторів ризиків для суспільства і громадськості. При цьому кожна країна визначає найбільш важливі для неї загрози та вразливості в кіберпросторі, тому не існує однакових національних стратегій кібербезпеки. Аналіз переважної більшості стратегій кібербезпеки надає змогу визначити їх основні позиції: підтримка та гарантування безпечного та захищеного кіберпростору, створення довірчого середовища електронних комунікацій; усунення ризиків для ІКТ; посилення спроможностей і стійкості критичної інформаційної інфраструктури; підтримка та підвищення рівня економічного потенціалу, соціального

благополуччя населення. Наприклад, у квітні 2014 року Національний конгрес Бразилії затвердив т.зв. "Біль Марко", більш відомий як "Інтернет-Конституція Бразилії", яким задекларовано права та свободи особи й громадянина в Інтернет-просторі, а також механізми їх забезпечення й додержання. Цей закон став відправною точкою для створення власної, окремої від США, національної системи в кібернетичній сфері. Із набранням чинності цим законом державним службовцям та військовослужбовцям Бразилії нормативно заборонено використання в службовій діяльності послуг постачальників електронної пошти з США. У 2015 році в Бразилії розпочато реалізацію великомасштабного проекту щодо прокладання Інтернет-кабелю з Європи до Бразилії по дну Атлантичного океану в обхід США, а в перспективі очікується також створення аналогічних Інтернет-мереж між Бразилією та Африкою. У 2017 році Уряд Бразилії схвалив рішення про створення підрозділів кіберполіції та активізував інституціоналізацію співробітництва в цьому напрямі між Бразилією та Європолом.

Індія посідає одне з перших місць у світі за кількістю скоєних кіберзлочинів на душу населення та масштабами поширення шкідливого програмного забезпечення. У 2013 році в Індії створено Національний центр захисту об'єктів критичної інфраструктури та розпочала свою діяльність кіберполіція. У лютому 2017 року команда реагування на кіберінциденти (CERT-In) розпочала впровадження проекту "Cyber Swachha Kendra", який є частиною ініціативи Уряду "Цифрова Індія" під егідою Міністерства електроніки та інформаційних технологій щодо створення безпечного кіберпростору шляхом виявлення інфікованих ботнетів та аналізу шкідливих програм кінцевих користувачів.

У Південно-Африканській Республіці (ПАР) ще у 2010 році вперше були створені спеціальні підрозділи кіберполіції, основним завданням яких стало відстеження та боротьба з кіберзлочинністю. У 2016 році Уряд ПАР оприлюднив регламент "Про кіберзлочинність", у положеннях якого першочерговим завданням визначено суцільну інформатизацію суспільства, органів державної влади та правоохоронних органів як складових забезпечення національної безпеки. На виконання положень цього програмного документа у 2017 році за сприяння Уряду країни було утворено Центр кібербезпеки при Національному університеті Йоганнесбурга, який здійснює підготовку кадрів, розробляє нормативно-правові основи регулювання інформаційного простору ПАР, забезпечує інформаційно-технічну підготовку кадрів для урядових структур та проводить науково-дослідницьку діяльність у сфері кібербезпеки.

Провідну роль у системі інформаційного захисту Фінляндії відіграє Стратегія кібербезпеки 2013 року, що стала першим самостійним документом у цій сфері. У Стратегії визначено ключові орієнтири стосовно забезпечення кібербезпеки, а також реальні для виконання положення щодо досягнення бажаного кінцевого результату захисту інформаційного простору та гарантування цифрового суверенітету. Так, відповідальними за розробку та реалізацію політики у сфері захисту національного кіберпростору у Фінляндії є урядові та неурядові структури, які здійснюють постійний нагляд і контроль за поточним станом інформаційного захисту. Із 2014 року у Фінляндії функціонує Національний центр з кібербезпеки, діяльність якого спрямована на забезпечення безпеки в кіберпросторі, надання гарантованого захисту та доступу користувачам (державним і приватним), які використовують інформаційно-комунікаційні мережі загального та спеціального зв'язку, долаючи при цьому всі можливі кіберзагрози, а також створення сприятливих умов для підтримки найважливіших соціальних функцій держави. У зв'язку з подальшим поширенням використання у злочинній діяльності ІКТ правоохоронним органам слід розробляти нові

методологічні підходи у боротьбі з новими видами злочинної діяльності та створювати відповідні організаційні структури.

Таким чином, інституційна система забезпечення кібербезпеки – сукупність організаційних структур, які забезпечують функціонування державного механізму забезпечення безпеки в кіберпросторі та дієвого кіберзахисту державних інформаційних ресурсів й об'єктів критичної інформаційної інфраструктури, а її оптимізація – один з аспектів організаційного розвитку. Метою оптимізації інституційної системи забезпечення кібербезпеки є визначення заходів та механізмів, завдяки яким гарантується безпека в кіберпросторі, що, у свою чергу, передбачає проведення у стислі терміни огляду наявних сил, засобів і можливостей нарощування потенціалу для реагування на кіберзагрози та кіберінциденти за участю усіх компетентних державних органів, впровадження в практичну площину механізмів взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки. З огляду на це важливим аспектом діяльності державного апарату в напрямі розбудови системи кібербезпеки залишається визначення алгоритму роботи різних національних структур для виконання покладених на них функцій відповідно до вимог сучасного вітчизняного законодавства.

Крім того, має бути побудована чітка вертикаль контролю і координації заходів у сфері кібербезпеки, впроваджені дієві механізми мобілізації ресурсів та оперативного реагування на кіберзагрози з використанням принципу асиметричної відповіді. Саме критична інформаційна інфраструктура є технологічним плацдармом життєдіяльності інформаційного суспільства, від сталого та надійного функціонування всіх її складових залежить стан забезпечення кібербезпеки, можливість управління державою, забезпечення потреб оборони та безпеки, функціонування промисловості, кредитно-фінансової та банківської систем, енергетичних, транспортних інфраструктур, комунального господарства, цивільного захисту, адже в державі ще й досі не сформовано повної та систематизованої бази даних про топологію і наявні ресурси телекомунікаційних мереж загального користування, що перебувають у приватній власності, а також відомчих телекомунікаційних мереж, побудованих за державні кошти.

Отже, кібербезпека відноситься до заходів безпеки та дій, які можуть використовуватися для захисту кіберпростору як у цивільній, так і військовій сферах, від таких загроз, які пов'язані або можуть пошкодити міжнародні інформаційно-комунікаційні мережі або об'єкти критичної інформаційної інфраструктури. Завдяки кібербезпеці забезпечується доступність і цілісність мереж та інфраструктури, а також конфіденційність інформації, яка в них циркулює. Проте ще й досі держава не володіє достовірними даними щодо сталості та надійності цих мереж, стану завантаженості, динаміки розвитку. Відсутні також достатні технічні вимоги до телекомунікаційних мереж щодо забезпечення сталості та живучості, у зв'язку з чим унеможливлюються: організація централізованого моніторингу стану мережевих та інформаційних ресурсів, моніторингу кібератак; контроль сталості кібербезпеки і ефективного використання ресурсів усіх мереж в умовах критичних ситуацій, надзвичайного або воєнного стану відповідно до чинного законодавства. Інакше кажучи, навіть, якщо захист державних інформаційних систем має регламентовані законодавством механізми, то, наприклад, налагодження комплексної взаємодії приватного сектору та держави щодо кіберзахисту об'єктів критичної інформаційної інфраструктури передбачає розробку нових методик з урахуванням інтересів IT-бізнес-середовища та відповідного стимулюючого ефекту, оскільки більшість таких об'єктів перебуває у віданні саме комерційних структур. Також необхідною є розробка методики оцінки та управління ризиками в вітчизняному сегменті кіберпростору.

Оскільки державні органи та правоохоронні структури – суб'єкти забезпечення кібербезпеки фізично не мають можливості захистити комерційні підприємства та організації, вони повинні самостійно забезпечувати власну кібербезпеку, при цьому державні структури виконують координаційні та контрольні функції. За таких умов необхідно: законодавчо визначити, що відповідальність за забезпечення кіберзахисту об'єкта критичної інформаційної інфраструктури покладається на його власника, який зобов'язаний надавати суб'єктам забезпечення кібербезпеки відомості про об'єкт критичної інформаційної інфраструктури; утворювати у своїй структурі підрозділ забезпечення кібербезпеки або уповноважувати окремих осіб на виконання функцій такого підрозділу та забезпечувати їх функціонування; негайно інформувати Держспецзв'язку про будь-які спроби вчинення стосовно об'єкта критичної інформаційної інфраструктури кібератак та інших несанкціонованих дій, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків. Формування чіткої вертикалі контролю й координації заходів у сфері кібербезпеки передбачає ієрархічну побудову системи її компетентних органів, у межах якої відповідальними суб'єктами надається розпорядницька та звітна інформація в чітко встановлені строки про здобуті результати з метою подальшого інформування керівництва держави, а в разі необхідності – світової спільноти.

Водночас координування з питань забезпечення кібербезпеки має відбуватися на двох рівнях – стратегічному та оперативному. Стратегічне координування є сферою відповідальності РНБО України, а саме Національного координаційного центру кібербезпеки як робочого органу РНБО України, оперативне – Кабінету Міністрів України. Адже недостатня координація досить часто призводить до негативних явищ у сфері практичних дій суб`єктів забезпечення кібербезпеки. З огляду на це, завданням держави є розробка та впровадження ситуативної моделі управління ризиками в кіберпросторі, визначення алгоритму дій суб`єктів забезпечення кібербезпеки, порядку та умов їх комплексної взаємодії, здійснення поточної та перспективної оцінки стану забезпечення кібербезпеки, контролю за результатами виконання планово-звітної документації.

Актуальним та важливим напрямком стало посилення спроможностей Національного координаційного центру кібербезпеки як робочого органу РНБО України. У зв'язку з тим було змінено формат його діяльності, зокрема, до його роботи відповідно до Указу Президента України від 28.01.20 р. № 27 залучено фахівців з приватного сектору, які спеціалізуються на кіберзахисті. Одночасно було акцентовано увагу на головній меті діяльності Національного координаційного центру кібербезпеки: залучити технологічний та інженерний потенціал прямих виробників до співпраці з Центром; використати існуючу в Україні інсталяційну базу на об'єктах критичної інфраструктури; поглибити співпрацю із суб'єктами кібербезпеки та приватними компаніями у рамках державно-приватного партнерства. В даному контексті слід вказати, що ефективність системи забезпечення кібербезпеки безпосередньо залежить від можливостей її постійного вдосконалення на фоні щоденного виникнення нових загроз у кіберпросторі, оскільки результати успішних інцидентів у кіберпросторі обмежуються не лише тимчасовими незручностями, але й призводять до тяжких наслідків для держави в економічній та соціальній площинах.

Розбудову інституційної системи забезпечення кібербезпеки також неможливо уявити без створення оптимальної управлінської організаційної ланки та залучення професійного людського кадрового ресурсу. Така модернізація вимагає часу та достатніх як фінансових, так і технічних ресурсів, відповідного кадрового потенціалу. Адже побудова дієвої системи кіберзахисту без її поступової модернізації деградує, передусім, через те, що інформаційні системи досить швидко розвиваються, а процес

створення відповідних систем захисту іноді не встигає за динамічним ІТ-розвитком. Хоча існують й здобутки у цій сфері. Так, у Національному координаційному центрі кібербезпеки РНБО України було створено реєстр обміну інформацією щодо кіберінцидентів з метою вчасного реагування на них у режимі реального часу та прямого зв'язку. Подібні центри вже існують в усіх передових державах світу, а їх робота визнається ефективною та результативною. Ці структури повинні обмінюватися інформацією. Отже, Національний координаційний центр кібербезпеки РНБО України має тісно взаємодіяти з міжнародними партнерами для вчасного реагування на кіберзагрози. Однак, на жаль, з точки зору розвитку системи кібербезпеки можна констатувати, що для спільної протидії викликам та загрозам в кіберпросторі не вистачає координованості зусиль як між державними структурами, міжнародними партнерами, так і між державою та приватним сектором.

Останнім часом Україна залишається мішенню для російських та проросійських кіберзлочинців. Кібератаки, також фіксувалися і проти інших держав, зокрема під час попередньої президентської кампанії у США та голосувань у країнах Європи (Великобританія, Нідерланди, Франція). Наведемо кілька останніх прикладів: Британія звинуватила хакерів, підконтрольних СЗР РФ, у втручанні в парламентські вибори 2019 року. Крім того, Лондон, Вашингтон та Оттава звинуватили Кремль у спробі вкрасти дані про вакцину від COVID-19. Також, нещодавно ЄС застосував санкції до російських хакерів, які були причетні до атаки "NotPetya", яка, зокрема, була встановлена за допомогою українських правоохоронців.

Загалом кібератаки завдали мільярдних збитків. Вони дали зрозуміти, наскільки ефективна кіберзброя в руках противника аби паралізувати будь-яку країну. Важливим завданням українського політичного істеблішменту є також залучення фахівців до кола суб'єктів забезпечення кібербезпеки, використання сучасних технічних засобів, апаратно-програмних комплексів, високоякісної ІТ-продукції. Забезпечення кібербезпеки неможливо уявити без людських ресурсів. Однак рівень кадрового забезпечення відомств відповідними фахівцями у сфері кібербезпеки все ще є незадовільним.

Оскільки структурно забезпечення кібербезпеки здійснюється у двох стратегічних напрямах: цивільному та військовому секторах, то важливим завданням держави в умовах оптимізації інституційної системи забезпечення кібербезпеки залишається дієвість і контрольованість заходів, спрямованих на підтримку зазначених векторів, які повинні розвиватися комплексно та системно.

У контексті військового сектору необхідно вказати, що спеціальні завдання, які здатна виконувати ворожа кіберзброя, мають переважно чітко виражений військовий характер. Тому для України доцільним є запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони. Йдеться про утворення у складі Збройних Сил України окремого роду військ – "Сили кібероборони" ("MilCert"), їх забезпечення належними фінансовими, кадровими і технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору. З цією метою слід розробити загальнодержавний план кібероборони в контексті забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів та оглядів у сфері кібербезпеки тощо.

Актуальним напрямом діяльності держави щодо оптимізації інституційної системи забезпечення кібербезпеки також залишається інформаційно-роз'яснювальна робота з метою профілактичного впливу на свідомість суспільства щодо негативних наслідків і масштабів збитків від кіберзагроз, кіберзлочинності та кібертероризму. У зв'язку із цим

необхідними є проведення просвітницької роботи з населенням з питань забезпечення кібербезпеки, роз'яснення методів протидії сучасним кіберзагрозам, надання консультативної допомоги в питаннях протидії злочинній діяльності в кіберпросторі, створення вітчизняних експертних інформаційно-аналітичних центрів, які б спеціалізувалися на питаннях кіберзахисту.

З огляду на це, слід зазначити, що незалежно від політичного курсу будь-якої країни світу Інтернет став технологічною інновацією, що наразі потребує інноваційного підходу до інституційної та регуляторної сфери. Надмірна політизація питання управління Інтернетом та нормативних засад розвитку кіберпростору знижують ефективність інституційних платформ, що сьогодні діють у цій сфері. У зв'язку з цим невирішеними залишаються питання протидії кібершпигунству, ідентифікації суб'єктів у кіберпросторі, мережевої нейтральності, юрисдикції в мережі Інтернеті тощо. Крім того, множинність інституційних механізмів може зрештою призвести до небажаної фрагментації екосистеми Інтернету.

Гібридна війна, розгорнута державою-агресором проти України, поряд з класичними воєнними діями та інформаційно-психологічними операціями, включає в себе й проведення кібероперацій. Державне управління процесами забезпечення сфери кібербезпеки має бути спрямоване на вирішення таких функціональних завдань щодо:

планування та контролю – оцінка ризиків та заходи щодо їх усунення, координація діяльності суб'єктів її забезпечення;

забезпечення кіберзахисту – проектування та практична реалізація заходів захисту критичної інформаційної інфраструктури, розроблення вимог щодо захисту державних інформаційних ресурсів та контроль за їх виконанням, розроблення вимог щодо безпечного використання Інтернету та електронних послуг;

оперативного реагування – оперативне реагування на кіберінциденти, розроблення методики попередження кіберінцидентів;

науково-методологічної підтримки – проведення наукових досліджень у сфері кібербезпеки, розроблення відповідних галузевих стандартів;

розслідування та попередження кіберзлочинів – розслідування кіберзлочинів, запровадження особливостей щодо судового провадження у сфері кіберзлочинів.

За таких умов для України прискорення оптимізації інституційної системи забезпечення кібербезпеки є дієвим інструментом, який передбачає два ключових напрями: правовий та організаційний.

Правовий полягає в ініціативній розробці необхідної нормативної бази та її постійному удосконаленні з метою формування відповідних правових норм, які знаходять відображення в Стратегії кібербезпеки та Законі України "Про основні засади забезпечення кібербезпеки України".

Організаційний – у підвищенні ефективності діяльності відповідальних інституційних структур – суб'єктів забезпечення кібербезпеки, міністерств, інших центральних органів виконавчої влади та інституцій громадянського суспільства завдяки підвищенню їх спроможностей, усуненню дублювань під час реалізації своїх повноважень, об'єднання зусиль під егідою робочого органу РНБО України – Національного координаційного центру кібербезпеки з урахуванням кращих практик міжнародного та європейського досвіду в цій площині.

Відповідно до компетенції РНБО України відповідає за координацію діяльності у сфері забезпечення кібербезпеки як важливої складової національної безпеки України. На жаль, в Україні відсутній комплексний звіт на національному рівні про процеси, пов'язані із поширенням та оцінкою стану кіберзлочинності, в якому можуть бути

окреслені загрози та визначені рекомендації щодо їх подолання та недопущення, в тому числі й транснаціонального характеру. Як переконливо демонструє провідний зарубіжний досвід, інституційно-функціональне забезпечення кібербезпеки передбачає два основних напрями: утворення підрозділів кіберполіції, розширення їх компетенції та утворення Національних центрів з кібербезпеки. В Україні актуальним залишається питання динамічної розбудови національної системи кібербезпеки. Важливим здобутком стало відкриття створеного Держспецзв'язку Центру реагування на кіберзагрози ("Cyber Threat Response Centre" – CRC) як центрального компоненту та ядра національної системи кіберзахисту. У своїй діяльності Центр реагування на кіберзагрози використовує кращі світові аналоги сучасних технологічних та аналітичних систем. Головним завданням вказаної структури стало запобігання кібератакам та максимальна локалізація можливих та потенційних уражень.

Ретельний аналіз положень Закону України "Про основні засади забезпечення кібербезпеки України" [5] надає змогу констатувати, що в його положеннях чітко розмежовуються функції між правоохоронними органами та вітчизняною спецслужбою. За стратегічне управління та координацію діяльності відомств, що забезпечують кібербезпеку, відповідає РНБО, якій підпорядкована Держспецзв'язку. Остання має розробляти комплексну систему кіберзахисту стратегічних об'єктів і контролює діяльність компаній, які проводять аудит таких стратегічних об'єктів. Держспецзв'язку підпорядкований Державний центр реагування на кібератаки, підрозділ якого – CERT-UA проводить моніторинг і виявляє потенційні кіберзагрози. Кіберполіція України відповідає за стан запобігання та розслідування кіберзлочинів. Міноборони та Генштаб забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та надзвичайного стану. СБУ здійснює запобігання терористичним атакам в кіберпросторі та має право перевіряти об'єкти критичної інфраструктури. Перелік об'єктів, що належать до критичної інфраструктури, визначає Кабінет Міністрів України, а кібербезпекою в банківській сфері опікується Національний банк України.

Однак законодавчо не визначено сфер відповідальності між різними державними та правоохоронними органами. Іншими словами, Закон України "Про основні засади забезпечення кібербезпеки України" [5] визначає базові поняття та передбачає, з одного боку, відповідальність керівників підприємств, установ та організацій за можливі кіберінциденти, з іншого боку, за кібербезпеку відповідають усі державні структури: Кабінет Міністрів України, Нацполіція, СБУ, Держспецзв'язку та Міноборони, НБУ, але виключно абстрактно.

Отже, якщо Україну раптом знову вразить вірус на військових об'єктах, то відповідальність мають нести Міноборони чи Генштаб і СБУ, якщо кібератака розцінюється як терористичний акт. Проте практично впровадити систему кіберзахисту, передбачену вказаним законом, навіть у державних органах досить складно. У рамках розбудови інституційного забезпечення кібербезпеки необхідно врегулювати організаційно-правові засади, на яких має бути побудована архітектура кібербезпеки об'єктів критичної інфраструктури, оскільки в Законі України "Про основні засади забезпечення кібербезпеки України" не визначено переліку об'єктів, що належать до такої інфраструктури, а також ще й досі не розроблені підзаконні акти, які мають регулювати нормативи кібербезпеки на таких об'єктах. Ураховуючи викладене, потребує удосконалення механізм співпраці та комплексної взаємодії між суб'єктами забезпечення кібербезпеки шляхом створення єдиної інтерактивної бази даних про кіберінциденти для ключових потреб Міноборони, Держспецзв'язку, СБУ, НПУ, НБУ, розвідувальних органів. Доцільним є також прискорення імплементації у вітчизняне

законодавство Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року щодо заходів із підвищення загального рівня безпеки мереж та інформаційних систем.

У зазначеному контексті важливим кроком має стати розбудова національної системи кібербезпеки, що передбачає: координацію дій та заходів, які вживаються державними органами, іншими суб'єктами забезпечення кібербезпеки, посилення спроможностей сектору безпеки і оборони, консолідацію зусиль та об'єднання знань, досвіду, потенціалу та ситуативної інформованості державного і приватного секторів. Також посилення спроможностей національної системи кібербезпеки неможливе без урегулювання питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет в операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам захисту інформації; щорічного збільшення видатків на фінансування з метою модернізації ситуаційних центрів з кібербезпеки СБУ та Держспецзв'язку; забезпечення суцільної модернізації та розширення функціональних можливостей системи інформаційного обміну про кіберзагрози між відповідальними суб'єктами; активізації співпраці між СБУ та Держспецзв'язку із зарубіжними партнерами щодо протидії кібератакам на критичну інформаційну інфраструктуру, проведення спільних розслідувань таких кібератак, установлення причин і умов, що сприяли їх вчиненню, а також щодо залучення міжнародної технічної допомоги для забезпечення кіберзахисту державних електронних інформаційних ресурсів.

Висновки.

З метою покращення координації діяльності суб'єктів забезпечення кібербезпеки в Україні у 2016 році було утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки на правах робочого органу, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері. На цьому фоні Україна має необхідний потенціал для нарощування спроможностей у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.

Проте, на жаль, в сучасних умовах зберігається загрозлива тенденція активного застосування й поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Зокрема, держава-агресор активно впроваджує концепцію інформаційного протиборства, яка базується на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України.

Провідні держави ЄС, держави-члени альянсу НАТО, провідні міжнародні корпорації та експерти одностайно визнають РФ та її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її активна розвідувально-підривна діяльність у кіберпросторі є частиною гібридної війни, яку вона веде проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі, яке проявлятиметься, насамперед, у розширенні кола держав, які намагатимуться сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі. Очікується розроблення інструментарію, що передбачає накопичення великих масивів даних та інформації щодо оцінки відомостей про людину, соціальних груп та використовує їх у сфері штучного інтелекту.

Важливим компонентом розвитку інституціонального забезпечення кібербезпеки для України є обов'язкове щорічне оприлюднення публічного звіту про стан реалізації та виконання Стратегії кібербезпеки за загальними оцінками. Саме Національний координаційний центр кібербезпеки у визначених законодавством формах має забезпечувати планування та забезпечення виконання заходів з реалізації Стратегії кібербезпеки, координує їх проведення і контролює стан виконання та ефективність. У рамках посилення інституціонального забезпечення кібербезпеки доцільно розширити мережі обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз на базі технологічної платформи Національного координаційного центру кібербезпеки, охопивши всі державні органи та об'єкти критичної інфраструктури, уніфікації форматів обміну інформацією; запровадити за досвідом держав-членів ЄС скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем під егідою Національного координаційного центру кібербезпеки, запровадити механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки держави. Також актуальним є запровадження обов'язкового надання в режимі реального часу інформації про кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами до Національного координаційного центру кібербезпеки.

Важливим та ефективним напрямом має стати розробка нових національних стандартів у сфері кібербезпеки, зокрема впровадження міжнародного стандарту ISO 27001, розвиток організаційно-технічної моделі кіберзахисту, впровадження механізмів своєчасної ідентифікації кіберзагроз, виявлення кібератак з метою оперативного й адекватного реагування на них та швидкого відновлення стабільної роботи за їх наслідками; запровадження загальнонаціональної програми виявлення уразливостей інформаційно-комунікаційних систем, проведення на регулярній основі аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість тощо.

Використана література

1. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. *Jurnalul juridic naţional: teorie şi practică.* 2016. № 6(22). С. 33-38.

2. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* № 1(20)/2017. С. 104-111.

3. Ткачук Н. Стан та проблемні питання реалізації стратегії кібербезпеки України. *Інформація і право.* № 1(28)/2019. С. 129-134.

4. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/ boz_2014_2_44

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

МАНУІЛОВ Я.С., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8149-2745.

ЩОДО КОНЦЕПЦІЇ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ МОДЕЛІ КІБЕРЗАХИСТУ

Анотація. *Визначено актуальні загрози кібербезпеці в сучасних умовах. Регламентовано складові функціонування національної системи кібербезпеки. Окреслено повноваження Держспецзв'язку у сфері побудови ефективного кіберзахисту на вітчизняних теренах. Деталізовано напрямки розбудови організаційно-технічної моделі національної системи кіберзахисту. Узагальнено компоненти організаційно-технічної моделі кіберзахисту. Актуалізовано доцільність прискорення схвалення на державному рівні Концепції організаційно-технічної моделі кіберзахисту.*

Ключові слова: *гібридна загроза, сектор безпеки і оборони, кібербезпека, кіберзагроза, кібератака, кіберзахист, кіберпростір, організаційно-технічна модель кіберзахисту, національна система кібербезпеки, цифровізація.*

Summary. *The current threats to cyber security in modern conditions have been identified. The components of the functioning of the national cyber security system are regulated. The powers of the State Special Communications Service in the field of building effective cyber defense in the domestic territory are outlined. The directions of development of organizational and technical model of the national cyber defense system are detailed. The components of the organizational and technical model of cyber defense are generalized. The expediency of accelerating the approval at the state level of the Concept of the organizational and technical model of cyber defense has been updated.*

Keywords: *hybrid threat, security and defense sector, cyber security, cyber threat, cyber attack, cyber defense, cyberspace, organizational and technical model of cyber defense, national cyber security system, digitalization.*

Аннотация. *Определены актуальные угрозы кибербезопасности в современных условиях. Регламентированы составляющие функционирования национальной системы кибербезопасности. Определены полномочия Госспецсвязи в сфере построения эффективной киберзащиты на отечественных просторах. Детализировано направления развития организационно-технической модели национальной системы киберзащиты. Обобщены компоненты организационно-технической модели киберзащиты. Актуализировано целесообразность ускорения принятия на государственном уровне Концепции организационно-технической модели киберзащиты.*

Ключевые слова: *гибридная угроза, сектор безопасности и обороны, кибербезопасность, киберугроза, кибератака, киберзащита, киберпространство, организационно-техническая модель киберзащиты, национальная система кибербезопасности, цифровизация.*

Постановка проблеми. В сучасному світі поширення кіберзагроз вражає своїми масштабами та наслідками. Адже загрози кібербезпеці останнім часом актуалізуються через дію таких негативних чинників, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів від потужних кіберзагроз; безсистемність заходів кіберзахисту критичної інформаційної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів тощо.

За таких умов є потреба активізації зусиль з боку держави щодо кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури з метою забезпечення безперебійного функціонування національної телекомунікаційної мережі та прискорення упровадження організаційно-технічної моделі національної системи кіберзахисту, вироблення єдиного підходу до питань оперативного реагування на кібератаки та кіберінциденти. У зв'язку із викладеним класичні моделі політичного, соціально-економічного та державного управління потребують перегляду в умовах суттєвої зміни кіберсередовища, особливо в умовах здійснення тотальної цифровізації усіх сфер життєдіяльності держави та суспільства. Викладене потребує активізацію діяльності владних структур держави у контексті забезпечення стану кібербезпеки, у першу чергу, прискорення створення та запровадження організаційно-технічної моделі кіберзахисту, висвітлення отриманих здобутків у цьому сегменті, відстеження динаміки відповідних процесів.

Результати аналізу наукових публікацій. Питання правового забезпечення розбудови організаційно-технічної моделі кіберзахисту досліджували у своїх працях: О. Бакалінська [1], О. Довгань [2], П. Рогов [3], В. Шеломенцев [4] та інші. Проте аналіз та узагальнення здобутків у сфері впровадження організаційно-технічної моделі кіберзахисту недостатньо висвітлено вказаними авторами, особливо в умовах масштабного поширення гібридних загроз, агресивної поведінки РФ у кіберпросторі, що посилює актуальність тематичного напрямку цього дослідження.

Метою статті є визначення подальших кроків з метою прискорення схвалення та впровадження у практичну площину Концепції організаційно-технічної моделі кіберзахисту як важливої складової менеджменту кібербезпеки в сучасних умовах масштабного поширення гібридних загроз у кіберпросторі.

Виклад основного матеріалу. Забезпечення кібербезпеки неможливе без прийняття виважених та послідовних управлінських рішень на планових засадах, що передбачає розробку та вжиття необхідних заходів, визначення алгоритму спільних дій з боку державних органів та інших суб'єктів забезпечення кібербезпеки, встановлення конкретних строків та відповідальних за їх виконання структур. Національна система кібербезпеки – органічна системна сукупність загальних і спеціальних суб'єктів її забезпечення та взаємопов'язаних і взаємоузгоджених між ними заходів організаційно-технічного, навчально-виховного, нормативно-правового, соціально-економічного, правоохоронного, оборонного, інформаційного характеру. Її основою є державні органи, правоохоронні структури, які відповідно до покладених завдань та в рамках взаємодії виконують функції із забезпечення безпеки кіберпростору України, громадські об`єднання, підприємства, установи, організації незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Першочерговими заходами щодо розбудови національної системи кібербезпеки є: вдосконалення державного управління у цій сфері; створення нормативно-правової бази для забезпечення такої діяльності; запровадження протоколів спільних дій суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів; підвищення спроможностей суб'єктів забезпечення кібербезпеки з виявлення, попередження та припинення правопорушень, пов'язаних із несанкціонованими доступом та діями, порушенням приватності, конфіденційності, цілісності та автентичності, поширенням та продажем даних і інформації, насамперед з обмеженим доступом; профілактика, виявлення та усунення умов і факторів загроз кібербезпеці держави; запровадження активних дієвих заходів у сфері боротьби з кібертероризмом, зокрема терористичними

актами та диверсіями у кіберпросторі, кібератаками на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури.

В умовах нарощування російської агресії, найвищим національним пріоритетом є подальше зміцнення складових сектору безпеки і оборони. Тільки успішна і послідовна державна політика, що виходить із максимально ефективного використання власних людських, фінансових, матеріально-технічних та інформаційних ресурсів, неухильне просування у напрямі європейської і євроатлантичної інтеграції, а також всебічний розвиток взаємодії зі стратегічними союзниками, у тому числі з НАТО, надасть змогу захистити інтереси України і створити синергетичний ефект національної єдності та міжнародної співпраці. За таких умов модель сектору безпеки і оборони України має бути суттєво змінена, що передбачає передусім уточнення повноважень, взаємоузгодження функцій та завдань суб'єктів сектору безпеки і оборони з метою унеможливлення виконання ними дублюючих або невластивих їм функцій, розпорошення сил та засобів. Має запрацювати чіткий механізм керівництва сектором безпеки і оборони як функціональним об'єднанням з визначенням особливостей його функціонування в мирний час, у кризових ситуаціях та в особливий період, що неможливо без формування відповідної нормативно-правової бази.

Важливою складовою нормального та безперебійного функціонування національної системи кібербезпеки є прискорення впровадження організаційно-технічної моделі кіберзахисту з метою оперативного (кризового) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості усіх комунікаційних систем. На цьому фоні актуальним та своєчасним питанням є визначення та узагальнення шляхів удосконалення вітчизняної організаційно-технічної моделі кіберзахисту, яка є важливою складовою менеджменту кібербезпеки у сучасному світі.

Згідно із чинним законодавством саме на Держспецзв'язку покладено обов'язок розробки, впровадження і поширення організаційно-технічної моделі кіберзахисту. Тобто у рамках компетенції та відповідно до функціональності саме Держспецзв'язку є регулятором з кібербезпеки для органів державної влади, а для інших галузей має виконувати роль координатора – сприяє розслідуванню та відновленню нормального стану після кібератак, сповіщає бізнес-структури (приватний сектор) про нові реальні та потенційні кіберзагрози. Запорукою ефективної діяльності складових національної системи кібербезпеки оптимальним є ініціювання, розробка та запровадження під егідою Держспецзв'язку на підставі спільних нормативно-правових актів механізму оперативної комплексної взаємодії в межах компетенції та згідно із функціональністю її суб'єктів з метою виявлення і нейтралізації кібератак та кіберзагроз із протидії їм, боротьби з кібертероризмом та кіберзлочинністю, забезпечення дієвого кіберзахисту, інформаційного обміну в режимі реального часу між суб'єктами забезпечення кібербезпеки та Національним координаційним центром кібербезпеки при РНБО України. Так, організаційно-технічна модель національної системи кіберзахисту, передбачає, передусім, забезпечення безперебійного функціонування автоматизованих систем органів військового та державного управління, оскільки в сучасних умовах з метою ефективного відбиття кібератак та гарантування надійного кіберзахисту вказані системи повинні вдосконалюватися в напрямі підвищення ступеня їх автоматизації та комп'ютеризації.

Ураховуючи викладене, актуальною та сучасною вимогою сьогодення є перегляд принципів побудови автоматизованих систем органів військового та державного управління кібербезпекою як у мирний, так і у воєнний час. Також у контексті

розбудови національної системи кібербезпеки важливим напрямком залишається перспективне використання її інтелектуальної підсистеми. Саме інтелектуальна підсистема кібербезпеки надасть можливість не тільки оперативно виявляти нові, невідомі та нетипові кібератаки в процесі моніторингу кіберпростору, але й системно аналізувати виявлені кіберзагрози й автоматично обирати параметри функціонування автоматизованих систем в умовах деструктивних впливів без погіршення їх основних характеристик.

Крім вдосконалення складових функціонування автоматизованих систем органів військового та державного управління, у рамках розбудови організаційно-технічної моделі національної системи кіберзахисту мають бути реалізовані можливості щодо: автоматичної зміни властивостей та параметрів підсистем і засобів забезпечення кібербезпеки залежно від зміни стану кіберпростору (виявлення активності потенційних джерел кіберзагроз, виявлення кібератак) та результатів проведених кібератак; автоматичної оцінки змін захищеності автоматизованих систем органів військового та державного управління від кіберзагроз при диференційованих умовах функціонування; автоматизованої підтримки прийняття рішень щодо протидії кібератакам та автоматичного впливу на джерело кібератаки; автоматизованої підтримки прийняття рішень щодо перерозподілу ресурсів систем та засобів забезпечення кібербезпеки на випадок їх функціонального ураження в результаті кібератак; обліку у процесі посилення кібербезпеки всіх взаємопов'язаних та взаємодіючих факторів, які можуть впливати на рівень її забезпечення; контролю та зниження нецільового навантаження на комплекси засобів автоматизації систем кібербезпеки; прогнозування на підставі отриманих у процесі експлуатації програмно-апаратних комплексів знань та факторів, що можуть впливати на рівень захищеності автоматичних систем управління від усіх видів кіберзагроз.

Також важливими елементами організаційно-технічної моделі кіберзахисту є розробка та використання сучасних засобів і методів, відповідних алгоритмів, завдяки яким в системі слід передбачити можливості реалізації запобіжних апаратно-програмних впливів та завдання ударів на виявлені джерела кібератак або на відповідні інформаційні системи і ресурси. Отже, важливою умовою створення організаційно-технічної моделі кіберзахисту є застосування апаратної та програмної платформ у складі довіреного програмно-апаратного середовища як сукупності технічних і програмних засобів, організаційних заходів, які забезпечують створення, застосування та розбудову систем спеціального призначення, що відповідають за умови забезпечення кібербезпеки.

Для забезпечення безпеки інформаційних ресурсів можуть використовуватися такі програмно-технічні рішення, як: обладнання комп'ютерів антивірусними програмами та засобами, які гарантують надійний захист від шкідливого програмного забезпечення, що може міститися в Інтернет-ресурсах та в додатках електронної пошти; міжмережеве екранування з метою обмеження несанкціонованого доступу до комп'ютерів через мережу; використання системи DLP, яка забезпечує захист інформації від копіювання на змінні носії, незареєстровані ресурси в зовнішній мережі; застосування програмно-технічних рішень для забезпечення контролю фізичного доступу до інформаційних та інформаційно-комунікаційних систем.

Як слушно зазначають А.В. Чунарьова та А.В. Чунарьов, роль організаційних заходів щодо захисту інформації в системі заходів кібербезпеки визначається своєчасністю, адекватністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації. Проведення організаційно-технічних та організаційно-правових заходів здійснюються завдяки таким принципам захисту інформації: науковий

підхід до організації захисту інформації; планування захисту; керування системою захисту; безперервність процесу захисту інформації; мінімальна достатність організації захисту; системний підхід до організації та проектування систем і методів захисту інформації; комплексний підхід до організації захисту інформації; відповідність рівня захисту інформації; гнучкість захисту; багатозональність захисту, що передбачає розміщення джерел інформації в зонах із контрольованим рівнем її безпеки; обмеження кількості осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації [5].

Таким чином, основою організаційно-технічної моделі кіберзахисту є система функціонування автоматизованих систем органів військового та державного управління, яка включає такі складові: постійний моніторинг кіберпростору, комплексний захист інформації, оперативне оповіщення про кібератаки або кіберзагрози та протидія їм; впровадження стандартів управління кібербезпекою. Загальноприйнятим є розуміння постійного моніторингу кіберпростору як сукупності апаратно-програмних систем і засобів, що дають змогу здійснювати оцінку ситуації (обстановки) в кіберпросторі, систематично збирати, обробляти та аналізувати інформацію про можливі кіберзагрози, наявні кіберінциденти завдяки цифровому проникненню в зовнішні мережі та комп'ютери, що потребує розробки передових розвідувальних кібертехнологій.

Комплексний захист інформації в інформаційних та інформаційно-телекомунікаційних системах має базуватися на таких підсистемах: попередження та виявлення комп'ютерних атак, криптографічний захист інформації, контроль стану й функціональної стабільності автоматизованих систем. Оперативне оповіщення про кібератаки або кіберзагрози передбачає вибір оптимальної стратегії запобігання та протидії кібератакам за допомогою програмно-апаратних і телекомунікаційних засобів, які призначені для своєчасного доведення до відповідних суб'єктів забезпечення кібербезпеки оперативної інформації в режимі реального часу про можливі або виявлені кіберзагрози або кібератаки, їхні параметри та зміст, а також вибору дієвих та доступних заходів кіберзахисту.

Впровадження організаційно-технічної моделі кіберзахисту неможливе без запровадження на підприємствах, в установах та організаціях, що належать до об'єктів критичної інфраструктури, ефективних систем менеджменту кібербезпеки, вжиття відповідних заходів щодо їх сертифікації згідно з міжнародними стандартами, наприклад, ISO/IEC 27032:2012 "Information technology – Security techniques – Guidelines for cybersecurity" – підвищення рівня кібербезпеки в глобальній мережі Інтернет. Тому для установ, організацій, підприємств, які провадять діяльність на міжнародному рівні, важливою умовою підвищення ефективності цієї діяльності є наявність сертифікату відповідності міжнародним стандартам серії ISO/IEC 27001 (оцінки й управління інформаційною безпекою) "Інформаційні технології – засоби забезпечення безпеки", що ґрунтуються на авторитетних британських стандартах BS 17799 (з 2000 року визнаних міжнародними у форматі "International Standart ISO/IEC 17799. Information technology – Code of practice for information security management".

У рамках вказаного стандарту тезаурус кібербезпеки повинен бути узгоджений із понятійним апаратом базових термінів у сфері інформаційної безпеки, при цьому стандарт являє собою керівні принципи у вигляді рекомендацій за такими напрямами: оцінка потенційних ризиків; дотримання вимог безпеки користувачами Інтернету; забезпечення кібербезпеки організаціями – провайдерами. Уважається, що завдяки використанню рекомендацій ISO/IEC 27032:2012 провайдери Інтернет-послуг зможуть підвищити загальний рівень кібербезпеки, забезпечити кіберзахист ресурсів

комп'ютерних мереж загального користування. Упровадження сучасної організаційно-технічної моделі кіберзахисту надасть змогу посилити координацію діяльності складових сектору безпеки і оборони України, їх техніко-технологічні можливості в рамках цілісної управлінської системи для боротьби з кіберзагрозами незалежно від способу, мети та суб'єкта їх реалізації, надасть можливість векторно спрямувати науковий та людський потенціал державних органів на забезпечення безпеки кіберпростору.

Виходячи із вищевикладеного, пріоритетними завданнями держави у цій площині залишаються: створення сучасної гнучкої національної системи кібербезпеки з метою ефективної взаємодії уповноважених органів під час реалізації заходів, спрямованих на її забезпечення; створення сприятливих умов для співпраці між державним і приватним секторами з питань протидії кіберзагрозам; активізація міжнародного співробітництва у сфері забезпечення кібербезпеки; формування передумов для забезпечення кіберзахисту інформаційної інфраструктури держави, передусім – об'єктів критичної інформаційної інфраструктури; прискорення розробки та практичного впровадження сучасної організаційно-технічної моделі забезпечення кіберзахисту.

Задля забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту щорічно проводяться планові заходи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість, тобто оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законодавства України, установ і організацій незалежно від форм власності.

Водночас, в нашій країні здійснюються поступальні кроки у напрямку розбудови вітчизняної організаційно-технічної моделі кіберзахисту. Протягом останніх років реалізовано низку практичних рішень, спрямованих на розробку організаційно-технічної моделі кіберзахисту. Так, окреслено державний контур кіберзахисту, активно та динамічно розвивається Національна телекомунікаційна мережа, працює Центр реагування на кіберзагрози, проведено масштабну модернізацію системи захищеного доступу до Інтернету. Також на виконання положень Закону України "Про основні засади забезпечення кібербезпеки в Україні" [6] Держспецзв'язку було офіційно презентовано Концепцію організаційно-технічної моделі кіберзахисту як важливої складової національної системи кібербезпеки [7]. У підготовці проекту "Організаційно-технічної моделі кіберзахисту" взяли участь фахівці і науковці Національного інституту стратегічних досліджень, Держспецзв'язку, Національної академії державного управління при Президентові України, фахівці приватних компаній та незалежні експерти.

За задумом "Організаційно-технічна модель кіберзахисту" складатиметься з трьох вертикально та горизонтально інтегрованих інфраструктур.

Перший рівень – це організаційно-керуюча інфраструктура кіберзахисту, її складовими елементами є суб'єкти національної системи кібербезпеки.

Другий рівень являє собою технологічну інфраструктуру кіберзахисту, яка складається з сукупності сил та засобів кіберзахисту. Це відповідні технологічні підрозділи суб'єктів кіберзахисту різних секторів (військовий та цивільний). На цьому рівні забезпечується відповідна комплексна взаємодія технологічних підрозділів, тобто обмін інформацією, моніторинг, забезпечення сталої безпеки кіберпростору тощо. Технологічна інфраструктура має три горизонти – національний, галузевий (регіональний) та об'єктовий.

Третій рівень – це базисна інфраструктура кіберзахисту, що забезпечує основні спроможності кіберзахисту. Базисна інфраструктура складається з двох шарів: захищена інформаційна інфраструктура та обізнане суспільство (громади та громадяни). Важливими питаннями впровадження цієї моделі залишаються її ресурсне забезпечення та механізми її імплементації.

Аналіз положень вказаної моделі дозволив визначити, що кіберзахист – це цілеспрямована діяльність із забезпечення безпеки кіберпростору та важлива складова національної системи кібербезпеки.

Також акцентовано увагу розробників на посиленні ризиків глобальної цифровізації, у зв'язку з чим існує вірогідність збільшення кількості кібератак та кіберзагроз, що потребує схвалення адекватних системних заходів реагування і відповідно, додаткових ресурсних витрат за напрямком посилення спроможностей відповідальних суб'єктів у сфері забезпечення кібербезпеки.

Висновки.

З метою розвитку технологічної платформи для розгортання національної системи кібербезпеки сьогодні вживаються заходи з розвитку її організаційно-технічної моделі як сукупності систем, комплексів і заходів, призначених для забезпечення кібербезпеки об'єктів критичної інфраструктури та кіберзахисту державних електронних інформаційних ресурсів, а також її телекомунікаційної платформи — Національної телекомунікаційної мережі. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки відповідно до ч. 5 ст. 8 Закону України "Про основні засади забезпечення кібербезпеки в Україні" здійснює Державний центр кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

У контексті посилення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки ключовим елементом оргтехмоделі є виконання відповідних завдань Центром реагування на кіберзагрози Держспецзв'язку, який було відкрито на початку 2018 року. З метою забезпечення ефективного обміну інформацією про кіберінциденти, аналізу загрозливих тенденцій, виявлення основних джерел кіберінцидентів, організації навчання щодо протидії кіберзагрозам, а також забезпечення належного рівня функціонування Центру реагування на кіберзагрози Держспецзв'язку, сьогодні розгортається єдина інтерактивна база даних про кіберінциденти для потреб основних суб'єктів забезпечення кібербезпеки як складових її національної системи.

На жаль, в Україні все ще спостерігаються повільні темпи, незавершеність заходів, спрямованих на повноцінне та повноформатне впровадження організаційно-технічної моделі кіберзахисту, яка має відповідати та адекватно реагувати на сучасні гібридні загрози, попереджувати їх негативні наслідки, нівелювати виклики у кіберпросторі та сприяти впровадженню глобальних тенденцій у розвиток індустрії кібербезпеки. У зв'язку із викладеним, в сучасних умовах, доцільно прискорити схвалення на державному рівні Концепції організаційно-технічної моделі кіберзахисту як фундаментального документа у цій площині.

Використана література

1. Бакалінська О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право.* 2019. № 9. С. 100-108.

2. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право.* № 3(26)/2018. С. 94-103. URL: http://nbuv.gov.ua/ UJRN/Infpr_2018_3_11

3. Рогов П.Д., Воровичб Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: зб. наук. праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського. 2017. № 1. С. 64-72. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13

4. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/ boz_2014_2_44

5. Чунарьова А.В., Чунарьов А.В. Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах. URL: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. В Україні презентовано Організаційно-технічну модель кіберзахисту. URL: https://cip.gov.ua/ua/news/klyuchovi-predstavniki-sub-yektiv-nacionalnoyi-sistemi-kiberbezpeki-ukrayini-obgovorili-organizaciino-tekhnichnu-model

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 343.45:340.5

ПОНОМАРЕНКО О.А., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7203-1859.

ОСОБЛИВОСТІ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ЗА ЗАКОНОДАВСТВОМ США

Анотація. *Стаття присвячена визначенню особливостей кримінально-правової охорони державної таємниці за законодавством США. Розглянуто систему нормативних актів США у сфері охорони державної таємниці. Наведено класифікацію видів державної таємниці. Визначені підстави кримінальної відповідальності за злочини у сфері охорони державної таємниці. Наведені заходи кримінально-правового впливу, що застосовуються до осіб, які вчинили такі злочини.*

Ключові слова: *державна таємниця, національна безпека, кримінальна відповідальність, законодавство, США.*

Summary. *The article is devoted to determining the features of criminal law protection of state secrets under US law. The system of US regulations in the field of protection of state secrets is considered. The classification of types of state secrets is given. The grounds for criminal liability for crimes in the field of protection of state secrets have been determined. The measures of criminal and legal influence applied to the persons who have committed such crimes are revealed.*

Keywords*: state secret, national security, criminal liability, legislation, USA.*

Аннотация. *Статья посвящена определению особенностям уголовно-правовой охраны государственной тайны по законодательству США. Рассмотрено систему нормативных актов США в области охраны государственной тайны. Приведена классификация видов государственной тайны. Определены основания уголовной ответственности за преступления в области государственной тайны. Приведены меры уголовно-правового влияния, которые применяются к лицам, совершившим такие преступления.*

Ключевые слова: *государственная тайна, национальная безопасность, уголовная ответственность, законодательство, США.*

Постановка проблеми. Сучасні процеси глобалізації, інтернаціоналізації та триваючої конвергенції потребують глибшого знання не тільки власного законодавства, а й законодавства, в тому числі кримінального, зарубіжних країн. Як слушно зазначає М.І. Хавронюк, у кримінальному законодавстві України змішані елементи національно-самобутнього з елементами запозиченого чужого – це законодавство завжди розвивалося під певним впливом кримінального законодавства інших держав, а також під впливом міжнародного права, який з часом стає усе більш потужним [1, с. 13].

Сьогодні Україна прагне стати повноправним членом Європейського Союзу і НАТО, а тому має привести своє законодавство у відповідність до європейських стандартів. Стратегічний курс держави на набуття повноправного членства України в Організації Північноатлантичного договору проголошено в Конституції України.

Охорона державної таємниці є важливою та невід'ємною частиною існування кожної держави світу для аналізу і подальшого розвитку законодавства у цій сфері необхідно звернути увагу на іноземний досвід, подальше використання якого є значним кроком уперед в інтегруванні української держави у світове співтовариство [2, с. 103].

Результати аналізу наукових публікацій. Дослідженням проблем захисту державної таємниці за законодавством зарубіжних країн займалися багато вчених: О.Ф. Бантишев [3], Д.П. Василенко [4], К.Є. Ковальов, Б.Д. Леонов [5], В.М. Лопатін, В.В. Макаренко, А.В. Савченко [6], О.Г. Семенюк, М.І. Хавронюк [1], О.В. Шамсутдінов [7], В.М. Шлапаченко [8], Д.С. Усов [2] та ін.

Одними з перших у світі, хто запровадив систему захисту інформації на законодавчому рівні, вважають американців [4, с. 128]. Сучасні засади державної безпекової політики США демонструють, що ця країна визначає державну таємницю як важливу складову національної безпеки та докладає значних зусиль з метою її охорони та забезпечення правового регулювання. Законодавча система США з безпеки інформації є однією з найнадійніших у світі, що робить її майже бездоганною й такою, на яку всі повинні рівнятися [4, с. 129]. Враховуючи стратегічний курс нашої держави на набуття повноправного членства України в НАТО, а також прагнення України посилити співпрацю з цією країною, розглянемо окремі норми кримінального законодавства США, що встановлює відповідальність за злочини у сфері охорони державної таємниці.

Метою статті є визначення особливостей кримінально-правової охорони державної таємниці за законодавством США.

Виклад основного матеріалу. Кримінальне право США, яке запозичило положення англійського кримінального права, відрізняється своєрідністю. При цьому вироблено власний варіант англійської правової системи [9, с. 446].

У Сполучених Штатах Америки закони, що стосуються сфери захисту інформації, діють з 1974 року [10]. Питання про охорону державної таємниці у США ретельно розроблені та юридично закріплені у низці нормативно-правових актів (законах, президентських виконавчих наказах, інструкціях тощо) [6]. Норми кримінально-правового характеру зібрані в основному у розділі 18 Зводу законів США, реформованого ще в 1948 р. (це так званий "Федеральний кримінальний кодекс США") [11; 7]. В окремих штатах діють свої кодекси: КК штату Нью-Йорк 1965 р., що являє собою главу 40 Зводу законів цього штату, КК Аляски 1978 р. тощо.

Відповідно до § 1 "Визначення" Закону про процедури із таємною інформацією від 15 жовтня 1980 р. (додаток № 3 до Розділу 18 Зводу законів США) поняття "таємна (класифікована) інформація" (*classified information*) означає "будь-яку інформацію чи матеріал, визначений урядом Сполучених Штатів відповідно до виконавчого наказу, закону, керівництва, що вимагають здійснення захисту проти її несанкціонованого розкриття в інтересах забезпечення національної безпеки, та будь-які відомості з обмеженим доступом, про що визначено у параграфі "r" ст. 11 Закону про атомну енергію 1954 р. (ст. 2014 (y) Розділі 42 Зводу законів США)" [11]. З наведеного визначення вбачається, що окремі федеральні закони, серед яких виділяються закони "Про національну безпеку" від 1947 р., "Про атомну енергію" 1954 р., "Про внутрішню безпеку" 2002 р., безпосередньо стосуються захисту державної таємниці.

Можна дійти висновку, що за законодавством таємна інформація в США поділяється на два види: оборонну (відомості про сферу національної безпеки) та службову (відомості з обмеженим доступом, наприклад, відомості про науково-технічний потенціал США в галузі розвідки, зв'язку, криптографічної системи, інформація про оперативну діяльність правоохоронних органів, про кадрову політику того чи іншого державного відомства та інші матеріали) [13, с. 449].

Норми, що встановлюють відповідальність за розголошення державної таємниці, містяться у Розділі 18 Зводу законів США ("Кримінальне право та процес"), у Розділі 50 ("Війна і національна безпека") та в інших розділах Зводу законів [12, с. 222]. Ці норми

відрізняються надзвичайною казуїстичністю, особливо при перерахуванні секретних об'єктів або способів злочинних посягань на державну таємницю [13, с. 450].

Так, Федеральний Звід законів у §793 передбачає кримінальну відповідальність за умисне повідомлення, передачу, надіслання матеріалів чи інформації щодо національної оборони "будь-якій особі, неуповноваженій на її одержання", або спробу чи сприяння вчиненню таких дій, якщо особа "має підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане на користь іноземній державі". Для цього складу злочину характерним є спеціальний суб'єкт: особа, яка на законних підставах має доступ, контролює чи володіє довіреними їй відповідними матеріалами чи інформацією [14, с. 40].

Для притягнення до кримінальної відповідальності за розголошення інформації щодо національної оборони, намір завдати шкоди не потрібний. Достатньо того, що обвинувачений усвідомлював важливість інформації, оскільки в даному випадку, як заявив Юридичний комітет Сенату, "йдеться про профілактичні заходи, щоб секретний матеріал не міг потрапити до ворога, а не про боротьбу з активним шпигунством" [12, с. 224].

Якщо аналізований злочин виявляється у формі втрати таємних документів (п. "f" § 793), то він є винятково посяганням у сфері охорони державної таємниці. Це посягання наявне тоді, коли той, кому довірені або хто на законній підставі володіє чи здійснює контроль над будь-яким документом, шифрувальною книгою, книгою сигналів, ескізом, фотографією, негативом, світлокопією, планом, картою, моделлю, приладом, обладнанням, записом або інформацією, що стосуються національної оборони: 1) через грубу недбалість допускає їхнє видалення (вилучення) з місця належного зберігання, або передачу будь-якій особі на порушення виявленої йому довіри, або втрату, викрадення, відокремлення або знищення; 2) знаючи, що вони незаконно видалені (вилучені) з місця належного зберігання, або передані будь-якій особі на порушення виявленої йому довіри, або втрачені, викрадені, відокремлені або знищені, негайно не сповіщає про це службовій особі вищого рівня, – карається штрафом або тюремним ув'язненням на строк до 10 років, або обома покараннями разом[13, с. 450-451]. Таким чином, § 793 (f), за суттю, містить описи двох злочинів: перший являє собою втрату через грубу недбалість предметів чи інформації оборонного характеру спеціальним суб'єктом – особою, якій вони довірені; інший полягає в неповідомленні про втрату цих предметів керівникові вищого рівня такою самою особою, яка знає, що зазначені предмети зникли [13, с. 450-451].

Розголошення таємної (класифікованої) інформації (§ 798) – це злочин, при якому той, хто свідомо та навмисно передає, постачає, доставляє будь-яку таємну інформацію або іншим чином робить її доступною для неуповноваженої особи, або публікує, або використовує її будь-яким іншим чином, що заподіює шкоду безпеці чи інтересам Сполучених Штатів або вчиняється на користь іноземного уряду на шкоду Сполученим Штатам. При цьому таємна інформація стосується: 1) природи, розробки або використання будь-якого коду, шифру, криптографічної системи Сполучених Штатів або будь-якої іноземної держави; 2) розробки, створення, використання, експлуатації або ремонту будь-якого пристрою, апарату чи приладу, який використовується, готується або планується для використання Сполученими Штатами або будь-якою іноземною державою у криптографії чи в цілях розвідувальних повідомлень; 3) розвідувальних повідомлень Сполучених Штатів або будь-якої іноземної держави; 4) отримання її шляхом передачі розвідувальних відомостей з повідомлень будь-якої держави. Караються такі дії тюремним ув'язненням на строк до 10 років та/або штрафом (додатковим покаранням є конфіскація майна) [6; 13, с. 450-451].

Очевидно, що розголошення таємної інформації може бути вчинене різними діями, зокрема наданням доступу неуповноваженій особі. Проте, на відміну від злочину,

передбаченого § 793, таке розголошення може бути здійснено будь-якою особою, а не тільки тією, яка володіє таємною інформацією на законній підставі [6; 13, с. 451].

Крім того, у федеральному законодавстві встановлена кримінальна відповідальність за необережне ("через грубу недбалість") видалення з місць зберігання чи передачу будь-якій неуповноваженій особі зазначених у §793 d матеріалів чи інформації або неповідомлення вищестоящій посадовій особі вищого рівня про таке видалення чи передачу при вказаних вище суб'єктивних ознаках, тобто маючи підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане у нагоді іноземній державі [5, с. 91-92; 7]. Суб'єктом у даному випадку виступає як особа, якій довірена або котра володіє чи контролює таку інформацію, тобто спеціальний суб'єкт (§ 793 f Зводу законів США), так і особа, яка незаконно володіє, має доступ чи контролює інформацію оборонного характеру, тобто загальний суб'єкт (§ 793e) Зводу законів США) [11]. Кожне з цих діянь тягне за собою покарання у вигляді штрафу в розмірі до $10 тис. чи тюремного ув'язнення на строк до 10 років, або обидва покарання одночасно [11].

Федеральне законодавство передбачає кримінальну відповідальність також за незаконне фотографування або зарисовку важливих оборонних об'єктів, за публікацію або продаж таких фотографій, малюнків тощо [5, с. 91-92]. Порушники цих правил, незалежно від їх суб'єктивних намірів чи "підстав вважати", можуть бути позбавлені волі на строк до 1 року або оштрафовані на $1 тис. (§§ 795-797 Зводу законів США) [11].

Не менш активною є боротьба з витоком офіційної інформації про діяльність американських розвідувальних служб, про їх співробітників і агентуру. Так, Закон про захист особового складу розвідки (1982 р.) за розголошення зазначених відомостей передбачає штраф у розмірі до $50 тис. чи тюремне ув'язнення строком до 10 років, або обидві міри покарання одночасно [7].

У федеральному законодавстві США встановлена також кримінальна відповідальність за розголошення кодів, шифрів, криптографічних систем, різних апаратів та пристроїв, що використовують для забезпечення секретності інформаційних зв'язків США чи інших держав [7]. Розкриття відповідних відомостей неуповноваженій на ознайомлення з ними особі, а також їх публікація чи будь-яке використання на шкоду інтересам США караються позбавленням волі на строк до 10 років чи штрафом (§ 796 Зводу законів США) [11]. Такому ж покаранню підлягає винна особа за публікацію або розкриття будь-якій особі кодів чи змісту дипломатичного листування (§ 952 Зводу законів США). Окремо регулюється охорона секретів, пов'язаних з дослідженнями в галузі атомної енергії (§§ 2271-2281 Розділу 42 Зводу законів США) [11].

Федеральне законодавство і КК штатів містять також загальні і спеціальні норми про різного роду зловживання службовим становищем і незаконне поширення та використання інформації. При цьому суб'єктами посадових злочинів можуть бути не тільки так звані публічні посадові особи, але й звичайні службовці та наймані робітники органів публічної адміністрації, публічних корпорацій і державних банків. Суб'єктами посадових злочинів можуть бути також і будь-які інші особи [5, с. 91-92].

У Главі 93 Розділу 18 Зводу законів США особливу групу зловживань становить діяльність чиновників у сфері використання службової інформації.

Так, вчиняє злочин, передбачений § 1902, посадова особа, службовець чи будь-яка особа, яка діє від імені США, департаментів або представництв, якщо вона в силу свого службового становища чи посади, володіючи якою-небудь інформацією, що має значення для торгівлі США та ринкової діяльності, свідомо й неуповноважено передає її особі, яка відповідно до закону або посадової інструкції не повинна отримувати таку інформацію [7]. Цей злочин карається штрафом до $10 тис. або (і) позбавленням волі на

строк до 10 років. До цієї ж групи посадових злочинів належить і поширення інформації щодо діяльності Корпорації фінансової реконструкції (§ 1904). За такий злочин передбачене покарання у вигляді штрафу до $10 тис. або (і) позбавлення волі на строк до 5 років [11].

Крім зазначених випадків розголошення спеціальної інформації, Глава 93 (§1905) містить норму про відповідальність за розголошення секретних відомостей загального характеру. Відповідно до цієї норми, якщо посадова особа чи службовець державних установ США, що за родом своєї служби володіє секретною інформацією, пов'язаною з проваджуваним розслідуванням, даними анкет або секретами торгівлі, управління, стилю роботи, даними про персонал, устаткування, статистичними даними, сумами чи джерелами доходів, прибутками чи витратами якої-небудь особи, фірми, компанії, корпорації, неуповноважено опубліковує, розкриває, розголошує чи яким-небудь іншим способом поширює таку інформацію, то вона карається штрафом у розмірі до 1000 дол. або позбавленням волі строком до 1 року [7]. Крім того, особа, засуджена за вчинення цього злочину, повинна бути звільнена з посади чи з місця роботи [11].

Для нормативного регулювання питань охорони державної таємниці важливе значення мають накази Президента США. Наприклад, Виконавчий наказ "Про таємну інформацію, що стосується національної безпеки" від 25 березня 2003 р. № 12958 встановлює поділ секретної інформація на три рівні: цілком таємна, таємна та конфіденційна [13, с. 450-451]. Цей наказ встановлює, що порушення порядку обігу таємної інформації стосовно національної безпеки, полягає у трьох формах: 1) будь-яке свідоме, злонавмисне чи необережне діяння, яке могло обґрунтовано викликати наслідок у виді несанкціонованого розкриття таємної інформації; 2) будь-яке свідоме, злонавмисне чи необережне діяння, яке полягає у здійсненні класифікації інформації чи продовженні здійснення її класифікації всупереч вимогам цього наказу чи його виконавчих директив; 3) будь-яке свідоме, злонавмисне чи необережне діяння, яке полягає у створенні програми спеціального доступу до інформації чи її продовженні всупереч вимогам цього наказу [13, с. 450-451].

Як бачимо, у США немає єдиного підходу до законодавчого встановлення кримінально-правової охорони державних секретів. В структурі правових джерел і в класифікації норм федерального законодавства та окремих штатів спостерігається помітне розмаїття [7].

З одного боку, діє Закон про покарання за розголошення офіційної інформації (1985), який за дане діяння передбачає покарання у вигляді штрафу в розмірі $15 тис. чи трьох років тюремного ув'язнення, або обидва види покарання одночасно [3, с. 26]. З іншого боку, існує Директива міністерства оборони США "Про нерозголошення важливої технічної інформації" (1984), відповідно до якої винному загрожує тюремне ув'язнення або штраф – $1 млн. чи на суму, що вп'ятеро перевищує вартість збитків, завданих розголошенням [3, с. 26].

При розгляді у суді виникає необхідність розкриття окремих аспектів державної таємниці. В такому разі суди США керуються Законом "Про процедури з секретною інформацією". Відповідно до цього Закону в разі, якщо суддя вважатиме, що розкриття секретних відомостей є необхідним для вирішення питання про невинність підсудного, він має право вимагати розкриття таких відомостей. Якщо в розкритті таких відомостей буде відмовлено відповідним органом, то судове переслідування припиняється. Як показує практика, в більшості випадків, коли виникали подібні ситуації, судове переслідування припинялося [15, с. 170].

Висновки.

Очевидно, що система нормативних актів США в галузі охорони секретної інформації надто розгалужена, складна і громіздка, що, однак, пояснюється особливостями системи загального права, до якої належить і американське право Ця система є надто специфічною та має як свої переваги, так і свої недоліки.

У законодавстві США існує значна кількість кримінально-правових норм, які передбачають диференційовану відповідальність за розголошення державної таємниці. Причому критерієм диференціації даних норм виступає, насамперед, предмет злочину, суб'єкт і зміст суб'єктивних чинників [13, с. 451-452]. Інакше кажучи, кожній категорії офіційної інформації відповідає окрема норма федерального кримінального законодавства [5, с. 92; 6]. Зокрема, в різних нормах американське федеральне законодавство передбачає відповідальність за умисне та необережне розголошення державної таємниці. Визначальною ознакою для розмежування розголошення державної таємниці з суміжними складами злочинів є предмет злочину. Також відзначається детальний опис понять і термінів, які стосуються державної таємниці.

Використана література

1. Хавронюк М.І. Кримінальне законодавство України та інших держав континентальної Європи: порівняльний аналіз, проблеми гармонізації: монографія. Київ: Юрисконсульт, 2006. 1048 с.

2. Усов Д.С. Захист державної таємниці за кримінальним законодавством інших країн на пострадянському просторі. *Публічне право*. 2013. № 3. С. 103-109. С. 103

3. Бантишев О.Ф. Як довести, що ти – не шпигун? *Політика і час*. 1994. № 8. С. 24-28.

4. Василенко Д.П., Маслак В.І. Законодавство провідних країн світу в сфері захисту інформації. *Вісник КДУ імені Михайла Остроградського*. Вип. 2/2010 (61). Ч. 1. 2010. С. 128-132.

5. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної та службової таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право*. № 1(20)/2017. С. 82-92.

6. Савченко А. На захисті державної таємниці: американський досвід. *Міліція України*. 2005. № 10. С. 24-25.

7. Леонов Б.Д., Шамсутдінов О.В. Особливості відповідальності за злочини у сфері охорони державної таємниці за кримінальним правом деяких зарубіжних держав (порівняльно-правова характеристика): навч. посібник. Київ: Наук.-вид. відділ НА СБУ, 2009. 92 с.

8. Шлапаченко В.М. Шляхи удосконалення нормативно-правового визначення державної таємниці. *Інформаційна безпека людини, суспільства, держави*. 2013. № 3. С. 41-44.

9. Кримінальне право України. Заг. частина; за ред. П.С. Матишевського, П.П. Андрушка, С.Д. Шапченка. Київ, 2000. 505 с.

10. Беляков К. Інформація організаційно-правової сфери. *Право України.* 2004. № 6. С. 88-92.

11. Federal Criminal Code and Rules. St. Paul, Minn., West Group, 2003. 1436 p.

12. Никифоров Б.С., Решетников Ф.М. Современное американское уголовное право. Москва: Наука, 1990. 256 с.

13. Савченко А.В. Порівняльний аналіз кримінального законодавства України та федерального кримінального законодавства Сполучених Штатів Америки: дис. …на здобуття наук. ступеня докт.-ра юрид. наук.: спец. 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Київ, 2007. 616 с.

14. Уголовное право Соединенных Штатов Америки: сб. нормативных актов / сост., отв. ред. И.Д. Козочкин. Москва: Изд-во Ун-та дружбы народов, 1986. 160 с.

15. Михайлуца М. Державна таємниця за законодавством України та зарубіжних країн світу: порівняльно-правовий аналіз. *Национальный юридический журнал*. 2016. С. 167-171.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

ПОЛЯКОВ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org /0000-0002-8984-1476.

АКТИВІЗАЦІЯ МІЖНАРОДНОЇ СПІВПРАЦІ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ШЛЯХИ УДОСКОНАЛЕННЯ В РЕАЛІЯХ СЬОГОДЕННЯ

Анотація. *Визначено стратегічні основи міжнародного співробітництва України у сфері кібербезпеки. Узагальнено завдання міжнародної взаємодії у сфері кібербезпеки. Проаналізовано міжнародні ініціативи, які впроваджуються з метою посилення захисту кіберпростору. Деталізовано напрямки здійснення модернізації політики інформаційної безпеки на рівні ООН. Окреслено ключові пріоритети міжнародного співробітництва у сфері забезпечення кібербезпеки між Україною та НАТО. Розглянуто перспективи діяльності в Україні Трастового фонду з кібербезпеки НАТО. Обґрунтовані сучасні світові тенденції, які впливають на безпекову політику НАТО і вимагають вжиття відповідних заходів реагування. На підставі узагальнення визначено шляхи удосконалення міжнародної співпраці у сфері забезпечення кібербезпеки.*

Ключові слова: *гібридна загроза, міжнародне співробітництво, сектор безпеки і оборони, інформаційна безпека, кібербезпека, кіберзагроза, кібератака, кіберзахист, кіберпростір, державна зовнішня політика, інформаційно-комунікаційні технології, НАТО, ООН.*

Summary. *The strategic bases of Ukraine's international cooperation in the field of cybersecurity have been identified. The tasks of international cooperation in the field of cybersecurity are generalized. The international initiatives implemented to strengthen the protection of cyberspace are analyzed. The directions of information security policy modernization at the UN level are detailed. The key priorities of international cooperation in the field of cybersecurity between Ukraine and NATO are outlined. Prospective activities of the NATO Cyber Security Trust Fund in Ukraine are considered. Modern world trends that affect NATO's security policy and require appropriate response measures are substantiated. On the basis of generalization, the directions to improve international cooperation in the field of cybersecurity have been identified.*

Keywords: *hybrid threat, international cooperation, security and defense sector, information security, cybersecurity, cyberthreat, cyberattack, cyberdefense, cyberspace, state foreign policy, information and communication technologies, NATO, UN.*

Аннотация. *Определены стратегические основы международного сотрудничества Украины в сфере обеспечения кибербезопасности. Обобщены задачи международного взаимодействия в сфере кибербезопасности. Проанализированы международные инициативы, которые внедряются с целью усиления защиты киберпространства. Детализированы направления осуществления модернизации политики информационной безопасности на уровне ООН. Очерчены ключевые приоритеты международного сотрудничества в сфере обеспечения кибербезопасности между Украиной и НАТО. Рассмотрены перспективы деятельности в Украине Трастового фонда по кибербезопасности НАТО. Обоснованы современные мировые тенденции, которые влияют на политику безопасности НАТО и требуют осуществления соответствующих мер реагирования. На основании обобщения определены направления усовершенствования международного сотрудничества в сфере кибербезопасности.*

Ключевые слова: *гибридная угроза, международное сотрудничество, сектор безопасности и обороны, информационная безопасность, кибербезопасность, киберугроза, кибератака, киберзащита, киберпространство, государственная внешняя политика, информационно-коммуникационные технологии, НАТО, ООН.*

Постановка проблеми. Активне впровадження сучасних цифрових технологій в економіці, соціальній сфері, управлінні, кредитно-банківській діяльності, безпеці та обороні, стрімкий розвиток інформаційно-телекомунікаційних технологій (далі – ІКТ) на основі використання глобальної інформаційної мережі Інтернет і спрощення доступу до неї широкого кола користувачів, зумовили зростання чисельних ризиків та загроз саме для кібербезпеки та її складових. Тобто ІКТ є важливою складовою майже усіх сфер існування людини й громадянина та провокують потребу комплексного міжгалузевого врегулювання їх захисту. В умовах тотальної глобалізації та стрімкого розвитку ІКТ жодна держава світу самостійно не здатна забезпечити надійного захисту свого цифрового простору та гарантувати кібербезпеку. Однак процес формування моделі міжнародної системи забезпечення кібербезпеки триває досить повільно та має непередбачуваний характер, що значно підвищує значимість розвитку двостороннього та багатостороннього співробітництва у питаннях вироблення єдиного стратегічного курсу з метою спільного запобігання сучасним кіберзагрозам гібридного характеру. Часом перевірено та доведено, що позитивний ефект міжнародного співробітництва полягає у підвищенні рівня кібербезпеки, при цьому цілеспрямовані спільні дії двох або більше держав, державних об'єднань (альянсів) у питаннях протидії кіберзагрозам дають змогу значно обмежити конфліктогенний потенціал агресивно налаштованих у кіберпросторі держав (РФ, КНР, Північна Корея), значно знизити їх деструктивний вплив на глобальну світову систему та її регіональні підсистеми. На цьому фоні важливим напрямом зовнішньої безпекової політики будь-якої держави світу виступає саме міжнародне співробітництво та перспективи його розвитку й удосконалення.

Україна є повноцінним членом глобальної системи безпеки, пріоритетами для якої залишаються розвиток міжнародного партнерства й співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглиблення тісної співпраці України з НАТО з метою підвищення спроможностей України у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри в кіберпросторі тощо. Україна відповідно до укладених нею міжнародних договорів проводить виважену державну політику у сфері вдосконалення співробітництва у сфері кібербезпеки. Враховуючи глобальну цифровізацію, зростання обсягів транснаціональної кіберзлочинності, загрозливі тенденції динамічного поширення кіберзагроз у світовому масштабі для України актуальним вбачається уточнення напрямків подальшого міжнародного співробітництва щодо посилення спроможностей України у сфері забезпечення кібербезпеки.

Результати аналізу наукових публікацій. Проблемні питання щодо пошуку оптимальної моделі розвитку та посилення міжнародного співробітництва у сфері забезпечення кібербезпеки перебували у фокусі уваги таких науковців: М. Гребенюка [1], С. Демедюка [2], В. Маркова [3], А. Марущака [4], Р. Лук'янчука [5], Є. Скулиша [6], В. Шемчука [7]. Аналіз опублікованих наукових праць вказаних фахівців переконливо засвідчує, що в сучасних умовах саме кібербезпека та її забезпечення для України мають стати одним з ключових пріоритетів міжнародної діяльності, посилюючи для цього потенціал зовнішньополітичних структур та загальний кіберпотенціал держави. Науковцями узагальнено, а експертами підтверджено, що з цією метою Україна розвиває мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва. Проте, розгляд засад міжнародної співпраці у сфері забезпечення кібербезпеки в умовах ескалації протиборства у кіберпросторі та поширення сучасних глобальних гібридних загроз жоден із вказаних авторів не здійснював. За таких умов висвітлення здобутків України та визначення шляхів

удосконалення міжнародної співпраці у сфері забезпечення кібербезпеки з метою їх деталізації є актуальним, своєчасним й таким, що відповідає засадам розвитку сучасної державної кібербезпекової політики.

Метою статті є деталізація шляхів удосконалення подальшого міжнародного співробітництва щодо посилення спроможностей сектору безпеки і оборони України у сфері забезпечення кібербезпеки.

Виклад основного матеріалу. Стаття 14 Закону України "Про основні засади забезпечення кібербезпеки України" [8] регламентує, що міжнародне співробітництво у сфері кібербезпеки наша держава здійснює на виконання укладених міжнародних договорів з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з транснаціональною кіберзлочинністю. Відповідно до чинного законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі. Розуміючи актуалізацію доцільності підвищення рівня кібербезпеки, у тому числі й завдяки міжнародній співпраці, Указом Президента України від 20 грудня 2019 року було уведено в дію рішення Ради Національної безпеки і оборони України від 7 грудня 2019 року "Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки" [9].

Виходячи із доктринальних засад чинного законодавства, Україна, відповідно до укладених нею міжнародних договорів, здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, насамперед держав-членів НАТО та ЄС, а також з міжнародними організаціями. Інформація з питань, пов'язаних із забезпеченням кібербезпеки, боротьбою з міжнародною кіберзлочинністю та кібертероризмом, подається іноземній державі на підставі укладених Україною міжнародних договорів. Такий формат охоплює широке коло питань нормотворчого, методологічного, практичного, наукового і навчально-виховного спрямувань, що передбачає проведення тематичних міжнародних семінарів та конференцій, надання іноземним партнерам методичної та практичної допомоги, організацію робочих контактів з провідними експертами в галузі кібербезпеки, що має позитивні результати вивчення та впровадження кращих практик кіберзахисту на вітчизняних теренах.

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози. Міжнародне співробітництво здійснюється з метою: зміцнення взаємної довіри у сфері кібербезпеки; вироблення спільних підходів до протидії кіберзагрозам; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних цілях; виконання Україною зобов'язань у рамках укладених міжнародних договорів у контексті співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також міжнародними організаціями; оптимізації надання міжнародної технічної допомоги.

В сучасних умовах ситуація, що склалася навколо майбутнього глобального кіберпростору, перебуває на перетині двох рівнозначних трендів. З одного боку, офіційні зусилля світової спільноти спрямовані на демілітаризацію кіберпростору та недопущення його перетворення на нове поле збройного конфлікту, а з іншого – де-факто триває процес полярного протистояння. Міжнародні структури, на кшталт ООН, хоча й роблять спроби впливати на цей процес, однак ці наміри є досить фрагментарними. Незважаючи на цілу низку рішень і резолюцій, ООН так і не запровадила дієвого міжнародно-правового

механізму, який би оптимізував кібербезпекову проблематику. Чимало документів ООН у цій сфері мають суперечливий характер та не сприймаються деякими державами-членами як фундаментальні. Хоча останнім часом ООН демонструє активізацію у сфері нормативного врегулювання світової кібербезпекової тематики. Наприклад, у червні 2015 року за підсумками засідання Групи урядових експертів ООН з міжнародної інформаційної безпеки було визнано, що до сфери використання інформаційно-комунікаційних технологій застосовується міжнародне право, однак у разі необхідності воно може бути доповнене, у тому числі за рахунок прийняття нових норм.

Модернізація політики інформаційної безпеки на рівні ООН зумовлена новими чинниками відповідальної поведінки держав, приватного сектора, наукових кіл й громадянського суспільства у кіберпросторі, яка могла б сприяти підвищенню ефективності міжнародного співробітництва [10, с. 103]. З 2019 року парадигма обговорення та схвалення тематики кібербезпеки в ООН зазнала суттєвих змін, що пов'язано із стрімким поширенням глобальних гібридних загроз міжнародного масштабу у цій площині. Останнім часом активізувалася робота на експертному рівні ООН з метою розробки міжнародних документів щодо вироблення єдиного підходу адекватного реагування на виклики сьогодення, оскільки у світі існує система незбалансованого розподілу та несправедливого управління критично важливими інтернет-ресурсами, що створює певну загрозу безпеці, пов'язану із безперебійним функціонуванням цієї інфраструктури. На цьому фоні держави повинні брати участь в управлінні та розподілі міжнародних інтернет-ресурсів на рівних та паритетних засадах. Адміністратори ключових ресурсів не повинні перебувати під контролем будь-якого уряду. Проте, основним проблемним питанням, актуальним для ООН, є застосування діючого міжнародного права у кіберпросторі.

Так, 28 грудня 2019 року Генеральна Асамблея ООН схвалила Резолюцію щодо боротьби з кіберзлочинністю. "Проти" цієї Резолюції виступили, зокрема, США, Канада, європейські держави та, передусім, Україна. Авторами документа виступили 47 держав, зокрема РФ, Білорусь, Казахстан, Азербайджан, Таджикистан, Вірменія, Китай, Індія, Сирія, Єгипет, КНДР, Іран і Венесуела. Цей документ передбачає створення міжнародного комітету для розробки міжнародної конвенції щодо протидії використанню інформаційно-комунікаційних технологій у злочинних цілях, який мав запрацювати у серпні 2020 року. У США і ЄС вважають, що запропонована ініціатива може призвести до встановлення цензури в Інтернеті та становити реальну загрозу свободі слова в глобальній мережі. Невипадково у представництві США при ООН заявили, що ухвалена резолюція може підірвати міжнародну співпрацю з метою боротьби проти кіберзлочинності. Навіть міжнародна правозахисна організація "Human Rights Watch" наголосила, що авторами Резолюції виступили держави, у першу чергу РФ, які використовують репресивні методи боротьби проти інакомислення. Україна обурена законодавчими ініціативами ООН, оскільки ця міжнародна структура певним чином підігрує державі-агресору, яка власне і запропонувала проект цієї Резолюції з метою поширення свого впливу над кіберпростором, отримання легітимного способу "блокувати інформацію" в Інтернеті та значно обмежити цифрові права громадян. Підставою для таких законодавчих пропозицій для ООН з боку держави-агресора стало набуття чинності з 1 листопада 2019 року в РФ федерального Закону про "суверенний Рунет", головним концептом якого визначено створення інфраструктури, яка дозволить Кремлю ізолювати російський сегмент Інтернету та фільтрувати як внутрішній, так і зовнішній Інтернет-трафік.

Очкується, що перспективна робота ООН, зокрема групи урядових експертів ООН з питань інформаційної безпеки буде сфокусована на чотирьох ключових аспектах:

1) правила, норми та принципи поведінки держав в інформаційному просторі;

2) заходи, спрямовані на зміцнення довіри у ньому;

3) нарощування цифрового потенціалу;

4) інституціоналізація переговорного механізму з питань міжнародної інформаційної безпеки в ООН.

Враховуючи сучасні виклики та загрози, актуальним для України є забезпечення участі України у роботі міжнародної платформи Програми дій із заохочення відповідальної поведінки держав у кіберпросторі Генеральної Асамблеї ООН та Групи урядових експертів ООН з питань інформаційної безпеки (UNGGE).

Найбільш впливовою та авторитетною міжнародною структурою, яка постійно удосконалює власну безпекову політику, є саме НАТО, яка тлумачить кіберпростір як арену протистояння та середовище інформаційного протиборства, визначаючи при цьому саме кібербезпеку як основний пріоритет своєї діяльності. Союзники підтвердили оборонний мандат НАТО й визнали кіберпростір середовищем операцій, в якому НАТО має ефективно захищатися, як це відбувається в інших фізичних середовищах протиборства. Командування НАТО з питань швидкого реагування на кіберзагрози доручило надавати допомогу союзникам щодо протидії кібератакам. Крім того, для захисту держав-членів НАТО можуть залучатися національні підрозділи кібербезпеки для проведення спеціальних операцій. Зокрема у 2019 році було схвалено рекомендації НАТО, що містять низку інструментів для: перспективного посилення спроможностей адекватного реагування на кібератаки, активізації співпраці з діловими партнерами й бізнес-середовищем у сфері розвитку кіберпромисловості; побудови можливостей використання кіберпростору союзниками на основі рекомендаційних та безпечних норм.

Для України одним із ключових пріоритетів міжнародного співробітництва у сфері забезпечення кібербезпеки залишається стратегічне партнерство з Північноатлантичним Альянсом. При цьому основними завданнями співробітництва між НАТО та державами-партнерами у сфері забезпечення кібернетичного захисту залишаються: підтримання нормальної життєдіяльності об'єктів критичних інформаційно-комунікаційних інфраструктур; розробка дієвих заходів протидії кібератакам; надання допомоги державам-членам у відновленні нормального функціонування відповідної інфраструктури внаслідок проведення зовнішніх кібернетичних атак; функціонування системи оперативного реагування на будь-які загрози в інформаційній сфері держав-членів [5, с. 52].

Головні принципи співробітництва НАТО з державами-партнерами у сфері кібернетичного захисту передбачають, що: Альянс може надавати державам-партнерам, у разі необхідності, свою експертну допомогу та, потенційно, свої спроможності для захисту проти кібернетичних атак; держави-партнери можуть звертатися з пропозицією щодо співпраці у сфері кібернетичного захисту та отримання підтримки з боку НАТО у випадках кібератак національного значення; співпраця між НАТО та державою-партнером має бути взаємовигідною у тому сенсі, що Альянс може надати інформацію та підтримку партнерам, але, у свою чергу, може отримати необхідну інформацію та підтримку від партнерів, зокрема, що стосується обміну досвідом у сфері кібербезпеки; НАТО і партнери повинні уникати дублювання заходів, що вживаються в рамках інших міжнародних організацій, які залучаються до захисту інформаційних систем від кібератак; наявність Угоди про безпеку між НАТО та державою-партнером, в якій визначатимуться обсяги допомоги та інформаційного обміну. Як переконливо доводить світовий досвід, забезпечення національної безпеки неможливо уявити без: удосконалення національної системи забезпечення кібербезпеки, яка б відповідала критеріям членства України в НАТО, підтримки міжнародних ініціатив у сфері кібербезпеки; інтенсифікації співпраці України з

ЄС та НАТО; підвищення спроможностей сектору безпеки і оборони у сфері кібербезпеки; участі у міжнародно-правових заходах щодо зміцнення довіри в кіберпросторі.

У липні 2019 року Польща та НАТО підписали першу угоду про співпрацю у сфері кібербезпеки. Комплексна взаємодія передбачає формат створення цілодобових пунктів швидкого реагування на кіберінциденти з використанням потужностей НАТО, спрямованих на ліквідацію будь-яких загроз у кіберпросторі. Ця угода стала правовим підгрунтям щодо можливого використання Альянсом команд швидкого реагування в разі поширення загроз в кіберпросторі. Завдяки угоді Польща братиме участь у розробці систем раннього попередження про загрози в кіберпросторі, також може розраховувати на поради експертів НАТО та плідну співпрацю з оборонною промисловістю. На цьому фоні ефективність міжнародного співробітництва між Україною та НАТО у кібербезпекових питаннях є очевидною.

Одним із базових аспектів безпекової політики для України залишається розвиток конструктивного партнерства з НАТО, в основі якого міститься критерій протидії сучасним викликам та загрозам, досягнення Україною провідних стандартів у сфері обороноздатності. У рамках розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки для України особливе партнерство з НАТО є невід'ємною складовою євроінтеграційного курсу, оскільки доповнює процес внутрішньодержавних перетворень необхідними реформами оборонного та безпекового секторів. Практика, що склалася в цьому форматі, передбачає щорічне схвалення на державному рівні Національної програми співробітництва Україна – НАТО.

Указом Президента України [11] було затверджено порядок розроблення, моніторингу та оцінювання результатів виконання річної національної програми під егідою Комісії Україна-НАТО. Аналіз цього програмного документа засвідчує, що взаємодія з НАТО не обмежується лише проведенням реформ у сфері безпеки. Річна національна програма під егідою Комісії Україна – НАТО являє собою ключовий інструмент досягнення Україною необхідних критеріїв членства в НАТО. Це системний документ, який містить опис реформ, визначає їхню стратегічну мету, зміст, завдання і заходи в наступних напрямках: політичні та економічні питання, оборонні і військові питання, питання ресурсів, питання безпеки, правові питання. Зокрема, Уряду доручено щорічно затверджувати перелік заходів щодо виконання річної національної програми та показників ефективності її виконання; здійснювати координацію діяльності центральних органів виконавчої влади та інших державних органів з моніторингу та оцінки результатів виконання Річної національної програми; регулярно інформувати громадськість про хід та результати виконання річної національної програми.

В сучасних умовах саме через систему діяльності Трастового фонду з кібербезпеки держави-члени НАТО надаватимуть підтримку Україні з метою розвитку її оборонних можливостей у галузі забезпечення кібернетичної безпеки, що передбачає постачання устаткування та обладнання, програмного забезпечення, надання технічної допомоги, консультативних послуг та проведення навчальних тренінгів. Додатковими контриб'юторами цього Трастового фонду виступили такі держави: Албанія, Італія, Туреччина та США. З огляду на можливості та потенціал Трастового фонду НАТО до основних заходів, реалізація яких дасть змогу посилити кібербезпеку в нашій державі, відносяться: проведення консультацій експертів з питань кіберзахисту, активізація діяльності фонду в напрямі формування базових концептів національної системи кібербезпеки.

Керівництвом НАТО Румунію як державу-члена ЄС було визнано провідною державою цього Трастового фонду, а його координаторами – Румунську спецслужбу та

Державну румунську компанію "RASIROM RA", яка спеціалізується на інтеграції та інжинірингу систем кібербезпеки. Перспективний розвиток оборонного технічного потенціалу України у сфері кібербезпеки досягається шляхом: впровадження на об'єктах критичної інфраструктури передових технічних рішень, які забезпечуватимуть належний рівень кібербезпеки; створення центральної та мережевої лабораторій комп'ютерно-технічних експертиз із фіксованими та мобільними компонентами; проведення тренінгів для персоналу, у тому числі для групи реагування на інциденти кібербезпеки (CERT) щодо експлуатації, ремонту й управління створеними інформаційними системами. Виходячи з цього, найбільш актуальним та важливим завданням діяльності Трастового фонду з питань кібербезпеки є надання допомоги Україні щодо розвитку технологічних можливостей протистояння сучасним кіберзагрозам.

У липні 2017 року в Службі безпеки України відбулася офіційна церемонія завершення першого етапу програми Трастового фонду НАТО зі сприяння Україні у зміцненні її спроможності у сфері кіберзахисту. Загальна сума відрахувань до Трастового фонду становила на першому етапі 1 млн. Євро. Крім постачання обладнання та програмного забезпечення, програма передбачала оплату проведення тренінгів та навчань персоналу. Ще у 2018 році в м. Києві відкрили перший ситуаційний центр кібербезпеки, який був створений згідно з угодою про реалізацію Трастового фонду Україна – НАТО. За результатами роботи у 2018 році Трастовий фонд кібербезпеки повністю виконав першу фазу, після чого відбувся перехід до другої фази, яка наразі триває. За таких умов, актуальним напрямом міжнародного співробітництва у сфері забезпечення кібербезпеки залишається конструктивна співпраця з НАТО, що передбачає: проведення консультацій та переговорів з питань кіберзахисту; продовження удосконалення нормативно-правової бази з питань кібербезпеки; забезпечення та сприяння розвитку під егідою Альянсу Трастового фонду з кібербезпеки. Таким чином, держава здійснює діяльність щодо консолідації зусиль, спрямованих на прискорення запровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту.

Загалом можна констатувати, що Україна реалізує конструктивний діалог з НАТО у сфері забезпечення кібербезпеки. За таких умов, Україна має розвивати міжнародне співробітництво у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України, поглиблюючи діалог України з Організацією з безпеки і співробітництва в Європі щодо зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої співпраці. У майбутньому динамічний розвиток співпраці з НАТО у сфері кібербезпеки матиме результативне продовження, якщо українське політичне керівництво буде підтримувати, у першу чергу, темпи реформ у військовій та оборонній сферах та покращить рівень міжвідомчої координації.

Російська гіперактивність в кіберпросторі є головним викликом та загрозою для України у сфері забезпечення кібербезпеки. РФ використовує кіберпростір як простір нових можливостей для здійснення не тільки розвідувально-підривної діяльності проти України, але й проведення спеціальних операцій з прихованого проникнення в кібер-мережі органів державної влади й управління, встановлення дистанційного контролю над об'єктами критичної інфраструктури з метою отримання переваг та забезпечення своїх інтересів у інформаційній, військово-політичній, фінансово-економічній, енергетичній сферах. Загальновідомо, що в РФ напрацьовані зразки кіберзброї для нейтралізації та виведення з ладу об'єктів критичної інфраструктури супротивника з метою підвищення ефективності наступного першого удару або ж максимального послаблення його спроможностей чинити опір. Адже подібна кіберзброя не може мати ніякого потенціалу стримування.

Також занепокоєння викликає і факт насичення українського ринку засобами мобільного зв'язку китайського виробництва з відповідним програмним забезпеченням. На тлі резонансних розслідувань у Європі та США щодо прихованих можливостей китайських продуктів для збору інформації для України важливою є співпраця з НАТО, спрямована на запобігання можливим негативним наслідкам їх масового використання та недопущення появи подібного обладнання і програмного забезпечення в системі державного та військового управління. Не випадково у січні 2021 року Генеральний секретар Північноатлантичного альянсу Столтенберг закликав членів Військового комітету НАТО продовжувати збільшувати витрати на оборону та інвестувати в сучасні технології через "агресивні дії РФ та підйом Китаю".

В умовах співпраці з НАТО, стратегічним завданням для України є захист від кібератак, мішенню яких неодноразово ставали об'єкти критичної інфраструктури держави. Україна зацікавлена у залученні до роботи Агентства з питань мережевої та інформаційної безпеки ЄС (далі – ENISA), Європейського центру досліджень та компетенції з кібербезпеки, а також до тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки. Посилення кібербезпеки України та поглиблення співпраці у цій сфері відповідає інтересам як ЄС так і України. На цьому тлі актуальним для України є посилення співробітництва з ENISA, зокрема з питань скоординованого розкриття уразливостей та імплементації Директиви ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive) від 6 липня 2016 року щодо заходів для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, як елементу євроінтеграції України.

У рамках перспективного розвитку співробітництва між Україною та НАТО варто, перш за все, враховувати поточні тенденції такої співпраці. Подальше співробітництво доцільно зосередити на наступних напрямках: використання передового досвіду НАТО у цій площині, поглиблювати державно-приватне партнерство; ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе Україні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері; нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду НАТО з кібербезпеки та у співпраці із Румунією; розробити механізми розподілення ризиків через використання захищених Хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади; залучати кращі практики задля посилення міжвідомчого співробітництва з виробленням конкретного дієвого механізму його практичного застосування; спільними зусиллями розробити систему мотивації для фахівців, зайнятих у сфері кібербезпеки тощо.

Міжнародний позитивний досвід у боротьбі із загрозами у сфері кібербезпеки та його здобутки є конче необхідними для України та мають бути враховані під час формування державної безпекової політики та адаптовані під час розбудови власної системи кібербезпеки. На сучасному етапі перед політичним керівництвом України постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід, разом із світовим співтовариством спільними зусиллями активізувати реалізацію дієвих заходів щодо боротьби з міжнародною кіберзлочинністю, що передбачає, передусім: побудову ефективної моделі національної системи кібербезпеки, її поступову інтеграцію до спільноти НАТО; залучення та кооперацію з європейськими інституціями, які опікуються проблематикою забезпечення кібербезпеки; концентрацію зусиль у напрямі розробки міжнародно-правового механізму гарантування кібербезпеки та його впровадження на теренах України; залучення можливостей міжнародної технічної допомоги з метою розбудови національної системи кібербезпеки, грантів міжнародних організацій у рамках

реалізації комплексних міжурядових програм розвитку міжнародної інформаційної безпеки; забезпечення поглиблення співпраці України з НАТО для підвищення стійкості та посилення спроможностей держави у сфері кібербезпеки.

Україна робить важливі поступальні кроки у сфері нарощування потенціалу у сфері кібербезпеки, активізуючи міжнародне співробітництво. Так, останнім часом, Україна та Ізраїль домовилися про поглиблення співпраці у галузі кібербезпеки. На початку 2020 року Україна та Японія визначили сфери майбутньої співпраці у галузі кібербезпеки та висловили готовність до посилення двостороннього співробітництва щодо боротьби з кіберзагрозами. Очікується, що така перспективна двостороння співпраця сприятиме розбудові та визначенню більш чіткого плану подальшого руху у напрямку покращення систем та заходів з реагування на майбутні загрози. На цьому тлі сторони домовилися про взаємодію компетентних органів двох держав щодо побудови відкритого, операційно-сумісного, надійного та безпечного кіберпростору.

На виконання Постанови Верховної Ради України від 4 лютого 2020 року [12] на 15 квітня 2020 року було заплановано проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення". Проте у зв'язку із запровадженням локдауну внаслідок поширення масштабів пандемії COVID-19 в Україні вказаний захід так і не відбувся.

Під час офіційного візиту 21 – 23 березня 2021 року Голови Верховної Ради України Д. Разумкова до Бельгії було проголошено, що саме реалізація курсу, спрямованого на прискорення реформування військової та безпекової сфери відповідно до принципів та стандартів НАТО є пріоритетом для України. А тому визнання України стратегічним партнером НАТО з розширеними можливостями є важливим етапом реалізації євроатлантичних прагнень України. Голова Верховної Ради також наголосив, що завданням Альянсу та України є відновлення формату засідань Комісії Україна – НАТО на високому рівні. За таких умов можна впевнено констатувати, що євроатлантична інтеграція залишається пріоритом зовнішньої та безпекової політики України.

Висновки.

У світових масштабах проблема забезпечення кібербезпеки з кожним роком посилюється та постійно актуалізується як перед світовою спільнотою, так і політичним керівництвом України. Таким чином, у міжнародному кіберпросторі, незважаючи на прагнення світової спільноти врегулювати питання його мирного використання та повної демілітаризації, спостерігається конфронтація та протиборство між групами держав (США, РФ, КНР), що бажають довести своє домінуюче становище та лідерство у кіберпросторі, який на сьогодні є ареною протистояння, продемонструвати силу та перевагу. З огляду на викладене, можна констатувати, що міжнародне співробітництво у сфері забезпечення кібербезпеки здійснюється переважно у організаційно-правових формах, типових і для інших сфер міжнародного регулювання – договірній та інституційній.

Україна повинна продовжувати участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна буде не лише учасником, але й ініціатором та організатором. Враховуючи викладене, Україна повинна займати більш проактивну позицію на міжнародній арені з питань забезпечення кібербезпеки. Держава має розвивати міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності і державного суверенітету, відновлення територіальної цілісності України, підтримання ініціатив учасників системи колективної безпеки НАТО.

З цією метою доцільно прискорити вжиття таких заходів, як: динамічний розвиток міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив, які відповідають національним інтересам України, поглиблюючи діалог України з Організацією Північноатлантичного договору та ЄС, особливо у питаннях зміцнення довіри при використанні кіберпростору, спільного розуміння ландшафту кіберзагроз та вдосконалення механізмів такої паритетної співпраці; визначити та затвердити перелік пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України. Іншими словами, актуальним напрямком для України залишається продовження партнерської співпраці з НАТО у кіберсфері. При цьому головним зовнішньополітичним фарватером України у сфері кібербезпеки є: поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками НАТО; вжиття інших узгоджених з іноземними партнерами заходів, спрямованих на посилення кіберстійкості України; розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Використана література

1. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право.* 2019. № 2. С. 203-207.

2. Демедюк С.В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності, *Вісник Харківського національного університету внутрішніх справ*. 2014. № 4. С. 65-75. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2014_4_10 (дата звернення: 31.03.2021).

3. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека.* 2015. № 2 (57). С. 107-113.

4. Марущак А.І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право.* № 3(26)/2018. С. 104-110.

5. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України. Серія: "Державне управління"*. 2015. № 4. С. 50-56. URL: http://nbuv. gov.ua/UJRN/Vnadu_2015_4_10 (дата звернення: 31.03.2021).

6. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право.* № 1(10)/2014. С. 93-100.

7. Шемчук В.В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Юридичні науки"*. 2018. № 2. Т. 29 (68). С. 125-130.

8. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05.10.17 р. № 163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 31.03.2021).

9. Про рішення Ради національної безпеки і оборони України від 7 грудня 2019 року "Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки": Указ Президента України від 20.12.19 р. № 923/2019 URL: https://zakon.rada.gov.ua/laws/show/923/ 2019#Text (дата звернення: 31.03.2021).

10. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 2020. № 1. С. 102-109.

11. Про затвердження Положення про Річні національні програми під егідою Комісії Україна – НАТО: Указ Президента України від 24.02.21 р. № 72/2021. URL: https://www.president.gov.ua/documents/722021-36825 (дата звернення: 31.03.2021).

12. Про проведення парламентських слухань на тему: "Кібербезпека, критична інфраструктура, електронні комунікації в Україні: стан, проблеми, шляхи їх вирішення": Постанова Верховної Ради України від 04.02.20 р. № 500. URL: https://zakon.rada.gov.ua/laws/ show/500-20#Text (дата звернення 31.03.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

СТЕЖКО С.М., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-0696-2131.
ШЕВЧЕНКО Т.О., молодший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5849-5566.

СУЧАСНИЙ ДОСВІД США У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *Розглянуто зміст та ключові аспекти Стратегії кібербезпеки США. Визначено засади державної кібербезпекової політики США. Окреслено типові загрози для США у кіберпросторі. Узагальнено державні пріоритети щодо посилення складових кіберзахисту в США. Деталізовано питання фінансування кібербезпеки у США в 2021 році. Конкретизовано засади спільної діяльності американо-українських відносин у сфері забезпечення кібербезпеки. Визначено перелік заходів, які впроваджуються в США з метою посилення спроможностей держави у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, кіберзахист, стратегічні засади кібербезпеки, кіберпростір, фінансування, США.*

Summary*. The content and key aspects of the US Cyber Security Strategy are considered. The principles of the state cyber security policy of the USA are defined. Typical threats to the United States in cyberspace are outlined. The state priorities for strengthening the components of cyber defense in the United States are summarized. The issue of financing cyber security in the United States in 2021 is detailed. The principles of joint activities of American-Ukrainian relations in the field of cyber security are specified. The list of measures implemented in the United States to strengthen the state's capabilities in the field of cyber security has been identified.*

Keywords: *cyber security, cyber attack, cyber defense, strategic principles of cyber security, cyberspace, financing, USA.*

Аннотация. *Рассмотрены содержание и ключевые аспекты Стратегии кибербезопасности США. Определены основы государственной политики кибербезопасности США. Очерчены типичные угрозы для США в киберпространстве. Обобщены государственные приоритеты касаемо усиления составляющих киберзащиты в США. Детализированы вопросы финансирования кибербезопасности в США в 2021 году. Конкретизированы основы совместной деятельности американо-украинских отношений в сфере обеспечения кибербезопасности. Определен перечень мероприятий, которые внедряются в США с целью усиления возможностей государства в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, киберзащита, стратегические основы кибербезопасности, киберпространство, финансирование, США.*

Постановка проблеми. У XXI столітті держава, суспільство та бізнес перейшли у нове середовище існування під назвою Інтернет, а інформаційно-комунікаційні технології стали основою для усіх сучасних інноваційних управлінських систем. Інтернет та цифрові інформаційно-комунікаційні технології дедалі більш інтегруються у всі сфери життєдіяльності держави та суспільства. За таких умов одним з основних завдань політичного керівництва будь-якої держави є забезпечення гарантованого функціонування

відкритого, надійного та захищеного кіберпростору. Відсутність кордонів у кіберпросторі, а також закладена в основі сучасних Інтернет-технологій відкритість та анонімність сприяють значному зростанню кількості зовнішніх кібератак та кіберзагроз, що автоматично призводить до необхідності розробки чіткої стратегічної концепції як ідейної основи формування пріоритетних засад національної політики у кіберпросторі. Тому останнім часом колосального масштабу у світі набула проблема захисту кіберпростору та елементів системи стратегічних комунікацій сектору безпеки і оборони від загроз несанкціонованого втручання.

Практично безмежні можливості використання Інтернету підкреслюють глобальну загрозу віртуальних кримінальних правопорушень, кібертероризму та кібервійни. Анонімність глобальних інформаційних мереж, швидкість передачі інформації та простота їх використання одночасно дозволяють використовувати всі ці переваги для здійснення протиправних діянь. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть реагувати на це. Адже загроза кібератак, особливо таких, що керуються чи фінансуються державами та застосовуються як інструмент примусу своїх політичних супротивників, є серйозним викликом і вимагають негайного адекватного реагування.

Реалії сучасності переконливо доводять, що важливою складовою національної безпеки виступає саме кібербезпека держави. Агресія з боку РФ проти України відбувається одночасно у багатьох площинах – військовій, політичній, інформаційній тощо, що вимагає від нашої країни комплексних дій у відповідь. Саме в умовах агресивної експансійної інформаційної політики РФ, динамічних змін у зовнішньому та внутрішньому безпековому середовищі України, посилення світових тенденцій щодо мілітаризації кіберпростору, його використання розвідувальними та спеціальними військовими структурами, хакерами та кібертерористами важливим та своєчасним завданням української держави є розбудова національної системи кібербезпеки. Тому в період сучасного глобального протистояння у сфері цифрових технологій та гонки озброєння у кіберпросторі безумовним лідером залишається США. Сфера кібербезпеки не є виключенням. Базовий ландшафт інструментарію реалізації окреслених кіберзагроз характеризується зростанням її високотехнологічної складової . Враховуючи викладене, актуальним та своєчасним є визначення стратегічних засад кібербезпеки США, а також напрямків двосторонньої співпраці між Україною та США у сфері забезпечення кібербезпеки.

Результати аналізу наукових публікацій. Питання стратегічного забезпечення кібербезпеки у США певним чином досліджували у своїх працях такі фахівці, як: Ю. Геращенко [1], Н. Литвиненко [2], В. Шемчук [3], та інші. Проте розгляд останніх законодавчих ініціатив, направлених на посилення стану кібербезпеки в США, та висвітлення здобутків у рамках партнерства у цій площині між Америкою та Україною жоден із фахівців детально не розглядав, що посилює тематичну спрямованість цієї наукової статті.

Метою статті є узагальнення здобутків США у сфері забезпечення кібербезпеки, визначення сучасних засад побудови конструктивного діалогу між Україною та США у кібербезпекових питаннях.

Виклад основного матеріалу. 20 вересня 2018 року Міністерство оборони США оприлюднило Стратегію з кібербезпеки адміністрації Президента Д. Трампа [4]. Сучасний документ має значно спростити процес узгодження кібербезпекових питань між силовими й оборонними відомствами цієї країни. У стратегічних положеннях задекларовано, що американці стають більш залежними від сучасних цифрових

технологій, більш вразливими до таких загроз, як: корпоративні порушення безпеки, фішинг та шахрайство в соціальних мережах, кібератаки тощо. Додаткові можливості кібербезпеки і правозастосування мають вирішальне значення для забезпечення захисту у кіберпросторі. У Стратегії кібербезпеки США викладені нові інструкції щодо дотримання безпеки в кіберпросторі для усіх федеральних відомств. Крім того, положення стратегії декларують наступальний характер США у глобальному кіберпросторі. У її положеннях викладені пріоритети уряду США щодо захисту держави та приватних даних її громадян від іноземних хакерів та спецслужб іноземних держав, передусім КНР, РФ, Ірану, Північної Кореї. За логікою документа, США матимуть більше свободи у протидії кібератакам і здійсненні наступальних кібероперацій. У стратегії деталізується ціла низка пріоритетних напрямів забезпечення політики кібербезпеки США. Серед таких пріоритетів – розробка міжнародної Інтернет-політики і комплектування державних структур та відомств компетентними співробітниками, які мають досвід роботи в ІТ-сфері та розуміються в питаннях кібербезпеки. Кінцевою метою цієї стратегії визначено налагодження дієвого кіберзахисту, запобігання поширенню ризиків, пов'язаних із кібербезпекою, забезпечення безпеки національних інформаційних систем та мереж.

Відповідно до базових положень Стратегії кібербезпеки США [4] кібербезпека – це комплекс заходів, спрямованих на захист комп'ютерних систем (включаючи апаратні засоби, програмне забезпечення та дані) від несанкціонованого доступу або атак через мережу Інтернет. Відповідно до положень цього документа Міноборони США визнало Китай та Росію основними загрозами у кіберпросторі. У документі йдеться про те, що загрозливі дії з боку КНР у кіберпросторі, зокрема викрадення конфіденційної інформації, розмивають військове панування та економічну безпеку США у глобальному вимірі. РФ, на думку авторів стратегії, проводить інформаційні операції, щоб маніпулювати свідомістю, посягаючи на демократичні цінності та права людини в мережі Інтернет. Щоб протидіяти РФ, Ірану, Китаю і КНДР у кіберпросторі, США планує збільшити свій наступальний потенціал, а у разі війни – "боротися з супротивником за допомогою повітряних, сухопутних, морських і космічних сил". Стратегія також передбачає регулювання ринку систем і засобів захисту інформації, зокрема уніфікацію устаткування та відбір дистриб'юторів. Документ закріплює право вимагати фінансового відшкодування від виконавців та організаторів проведення кібератак.

Адміністрація США докладатиме всіх зусиль щодо екстрадиції обвинувачених у хакерстві іноземних громадян, а також посилить для них покарання за скоєні кіберзлочини. Аналіз положень зазначеної стратегії дає змогу констатувати, що з метою підвищення рівня захищеності урядові структури будуть передавати в режимі онлайн виробникам мережевого обладнання інформацію щодо ймовірних ризиків та загроз. Вірогідно, що після цього компанії виготовлятимуть дві версії устаткування: для США і для решти країн світу. Отже, російські, китайські чи іранські обчислювальні системи, що використовують американське мережеве обладнання, вже не зможуть стримувати деякі комп'ютерні атаки. Найбільш вразливими у контексті гарантування кібербезпеки в США залишаються космічна і транспортна галузі, зокрема морські вантажні перевезення, особливо – газу і нафтопродуктів. Щоб зберегти кіберпростір в якості рушійної сили динамічної цифрової економіки, США взаємодіють з іноземними партнерами та іншими групами зацікавлених сторін, включаючи громадянське суспільство і приватний сектор, для просування передового досвіду і політики, які сприяють інноваціям, відкритості та ефективності. Серед запроваджених новацій стратегії США – розробка міжнародної політики кіберстримування; спрощення

регламентних правил, що регулюють наступальні операції в мережі; масштабніші наслідки від операцій для держав-супротивників, якщо вони відбуватимуться у складі коаліції; здійснення наступальних кібер- та військових дій США в рамках реагування на кібератаку. Сучасна стратегія кібербезпеки є першим за 15 років чітко сформульованим документом США у цій сфері. Як свого часу заявив радник президента США з національної безпеки Джон Болтон, нова стратегія "розв'язує руки" в тому числі, для проведення "наступальних" операцій у відповідь на кібератаки, а не тільки для пасивної оборони від кіберзагроз. Головними джерелами кіберзагроз для США все ще залишаються Китай, Іран, Північна Корея і Росія.

Враховуючи важливість та актуальність питань забезпечення кібербезпеки та її складових, Уряд США планує у 2021 році витратити у цьому сегменті $5,4 млрд. Відповідно до інформації, оприлюдненої на сайті Міністерства оборони США у рубриці "DOD Releases Fiscal Year 2021 Budget Proposal", ці кошти планують витратити як на забезпечення кібербезпеки, так і на проведення наступальних операцій у кіберпросторі, проведення розробок у сфері штучного інтелекту, хмарні технології тощо – загалом $9,6 млрд. Також важливим напрямом залишається посилення міждоменних рішень (*cross-domain solution, CDS*) та рішень у сфері шифрування, що сприятиме зниженню ризиків кібератак на урядові мережі. $3,8 млрд. – обсяг фінансування операцій як наступальних так і оборонного характеру на виконання положень кіберстратегії.

Наприкінці березня 2021 року стало відомо, що Адміністрація Д. Байдена готує новий указ Президента США з метою посилення кібербезпеки в сучасних реаліях. Проектом цього указу визначено 12 стратегічних кроків, якими будуть впроваджені заходи щодо мінімізації кількості кіберінцидентів, напрямки посилення захисту усіх об'єктів критичної інфраструктури. У квітні 2021 року США оголосили про 100-денний план з метою посилення кібербезпеки електроенергетичної інфраструктури країни. Передбачається плідна співпраця міністерства енергетики, приватних компаній й Агентства з кібербезпеки та інфраструктурної безпеки. Причинами для цього стали останні уразливості об'єктів енергосистеми США, які неодноразово страждали від кібератак. Вашингтон вважає, що за деякими з цих атак стоять російські хакери. З метою симетричної відповіді США у квітні 2021 року запроваджено санкції проти шести російських технологічних компаній у відповідь на "ймовірні неправомірні дії", пов'язані з кібератакою на IT-компанію "SolarWinds" та зломом систем низки американських відомств, зокрема Міненерго.

США підтримують прагнення України розвивати власну кібербезпеку та здійснювати системні заходи з метою її забезпечення. У лютому 2018 року Палата представників Конгресу США підтримала законопроект "Ukraine Cybersecurity Cooperation Act of 2017", яким було окреслено засади співробітництва між Україною та США, включаючи такі ключові напрями: вдосконалення систем безпеки урядових систем, передусім тих, які захищають критичну інфраструктуру України; зменшення залежності від російських інформаційно-комунікаційних технологій; нарощування потенціалу, розширення обміну інформацією щодо кібербезпеки; співробітництво в кіберпросторі. Передбачається, що сумарний бюджет його проектів становитиме майже $500 млн. у 2019 – 2022 роках.

У 2020 році США схвалили рішення про виділення Україні $38 млн. міжнародної технічної допомоги. Цьому передував активний діалог між США та Україною з кібербезпекових питань. Так, 3 березня 2020 року Сполучені Штати Америки та Україна провели третій діалог з питань кібербезпеки у Києві з метою визначення подальших кроків у напрямку паритетної взаємодії та закріплення нашої спільної відданості

політиці забезпечення відкритого, взаємосумісного, надійного і безпечного кіберпростору, в якому всі держави поводяться відповідально на партнерських засадах. Також у фокусі уваги сторін були такі питання, як: технологічне забезпечення зв'язку п'ятого покоління 5G, розбудова кіберпотенціалу, засад міжнародної політики стосовно забезпечення цифрового інформаційного простору, у тому числі перспективна участь у багатосторонніх заходах (форумах, конференціях, самітах), питання публічної відповідальності за наслідками кібератак.

Демонструючи свою постійну прихильність до підтримки кібербезпеки, США оголосили, що надають ще $8 млн. на кібербезпеку від Державного департаменту, у додаток до $10 млн., які були виділені у 2017 році. Частина цього фінансування буде спрямована на підтримку нового проекту з кібербезпеки Агентства США з міжнародного розвитку, за яким планується інвестувати загалом до $38 млн. протягом чотирьох років у розбудову потенціалу кібербезпеки України шляхом підтримки правової та регуляторної реформи, розвитку робочої сили у галузі інформаційних технологій, залучення приватного сектору. Очікується, що фінансування буде спрямовано на практичну реалізацію таких проектів: посилення кібербезпеки критичної інфраструктури; розробка та реалізація оновленої кіберстратегії; підвищення рівня кіберзахисту, реагування на інциденти, засоби обміну інформацією; підвищення обізнаності щодо кібербезпеки для всіх зацікавлених сторін; підготовка кадрів із надійного захисту систем промислового управління і цифрової криміналістики. Ці проекти доповнюють американо-українське співробітництво з інших питань кібербезпеки.

Важливим здобутком для України стала підготовка у березні 2021 року закону США про безпекове партнерство з нашою країною. Очікується, що з набуттям чинності цим законом безпекове партнерство з Україною буде значно активізовано та авторизовано багаторічну безпекову допомогу, визначено напрямки заохочення прискорення реформування сектору безпеки і оборони України. Нормативне забезпечення процесів стратегічного партнерства сприятиме наданню додаткового фінансування оборонної сфери України та допоможе покращити підготовку, озброєння та матеріально-технічне забезпечення військових, дозволить пришвидшити перехід на стандарти НАТО. Наприкінці квітня 2021 року Комітет Сенату США підтримав законопроект з "Безпекового партнерства з Україною". Зокрема, законодавчо задекларовано, що попри кричуще ігнорування Росією міжнародних законів і зобов'язань, Україна залишається надійним партнером США і активно протидіє масштабам зловмисного впливу держави – агресора.

Останнім часом США занепокоєні прогресивними досягненнями КНР у сфері цифрових технологій та відчувають загрозу з боку Китаю у сфері кібербезпеки. Враховуючи загрози та виклики у цій площині, Сенат США приступив до розробки законопроекту про державну підтримку виробництва чипів (напівпровідників) та готується до його розгляду у травні 2021 року. Очікується, що на створення національного технологічного виробництва напівпровідників буде виділено не менш $30 млдр. Таким чином, для політичної влади США останнім часом питання забезпечення кібербезпеки набула не аби якої актуальності на фоні збільшення кількості кібератак та чисельних й масштабних випадків несанкціонованого витоку та викрадення конфіденційної інформації. У переважних випадках відповідальність за ці спроби та таку протиправну діяльність Вашингтон покладає на китайських та російських хакерів, які цілеспрямовано діють під егідою тієї чи іншої держави.

Висновки.

Між Україною та Сполученими Штатами Америки існує стратегічне партнерство, яке треба постійно розвивати. Першочерговим аспектом залишаються фінансова підтримка та технічна допомога для України з боку США. Аналіз викладених матеріалів дозволяє констатувати, що США й надалі готові відігравати важливу роль у забезпеченні кібербезпеки України. Досвід США у цій площині переконливо демонструє, що в сучасному світі кіберпростір стає ареною як наступальних так і оборонних операцій, вимагає концентрації зусиль військового та цивільного секторів у фокусі цієї проблеми, що є наслідком чіткого визначення супротивників та союзників. Засади державної кібербезпекової політики США демонструють, що ця країна визначає кібербезпеку як важливу складову національної безпеки та докладає кардинальних зусиль з метою її посилення та забезпечення, у зв'язку з чим на законодавчому рівні схвалюються нормативні акти, які є своєрідною реакцією на поширення новітніх загроз у кіберпросторі.

Використана література

1. Геращенко Ю.В. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: "Державне управління"*. 2019. Т. 30 (69). С. 140-145.

2. Литвиненко Н.П., Погоріла Н.О. Концептуальне забезпечення політики глобального лідерства США постбіполярної доби. *Актуальні проблеми міжнародних відносин.* 2017. Вип. 132. С. 44-51.

3. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4. С. 119-124.

4. National Cyber Strategy of the United States of America. (2018). (n.d.). URL: https://www. whitehouse.gov/wp - content/uploads/2018/09/National - Cyber-Strategy.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-1408-2145.

ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ В УМОВАХ ГЕОПОЛІТИЧНОГО ПРОТИБОРСТВА: КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *Розглянуто зміст та особливості цифрового суверенітету. Визначено сучасні тенденції забезпечення цифрового суверенітету в умовах геополітичного протиборства. Висвітлено кращі практики зарубіжного досвіду у сфері забезпечення цифрового суверенітету. Окреслено загрози діяльності соціальних мереж та онлайн-платформ в контексті необхідності розробок вірогідних моделей захисту національного сегменту кіберпростору. Узагальнено питання щодо блокування та видалення деструктивного контенту соціальними мережами. Акцентована увага на питаннях посилення відповідальності глобальних ІТ-корпорацій. Деталізовано шляхи удосконалення вітчизняного законодавства щодо посилення цифрового суверенітету, захисту цифрових прав та свобод громадян. Визначено напрямки унормування діяльності та оподаткування соціальних мереж в Україні.*

Ключові слова: *цифрові технології, національний суверенітет, цифровий суверенітет, кібербезпека, кіберпростір, репост, деструктивний контент, загроза, медіарегулятор, аккаунт, ІТ-корпорація, онлайн-платформа, технологічні трансформації, геополітичне протиборство.*

Summary. *The content and features of digital sovereignty are considered. The modern trends of ensuring digital sovereignty in the conditions of geopolitical confrontation are determined. The best practices of foreign experience in the field of digital sovereignty are highlighted. The threats to the activities of social networks and online platforms in the context of the need to develop plausible models for the protection of the national segment of cyberspace are outlined. The issue of blocking and removing destructive content by social networks is covered. Emphasis is placed on strengthening the responsibility of global IT-corporations. The directions of improvement of domestic legislation on strengthening digital sovereignty, protection of digital rights and freedoms of citizens are detailed. The directions of standardization of activity and taxation of social networks in Ukraine are determined.*

Keywords: *digital technologies, national sovereignty, digital sovereignty, cyber security, cyberspace, repost, destructive content, threat, media regulator, account, IT-corporation, online platform, technological transformations, geopolitical confrontation.*

Аннотация. *Рассмотрены содержание и особенности цифрового суверенитета. Определены современные тенденции обеспечения цифрового суверенитета в условиях геополитического противоборства. Освещены лучшие практики зарубежного опыта в сфере обеспечения цифрового суверенитета. Очерчены угрозы деятельности социальных сетей и онлайн площадок в контексте необходимости разработок возможных моделей защиты национального сегмента киберпространства. Обобщены вопросы блокирования и удаления деструктивного контента социальными сетями. Акцентировано внимание на вопросах усиления ответственности глобальных ИТ-корпораций. Детализированы направления усовершенствования отечественного законодательства в части усиления цифрового суверенитета, защиты цифровых прав и свобод граждан. Определены направления нормирования деятельности и налогообложения социальных сетей в Украине.*

Ключевые слова: *цифровые технологии, национальный суверенитет, цифровой суверенитет, кибербезопасность, киберпространство, репост, деструктивный контент, угроза, медиарегулятор, аккаунт, ИТ-корпорация, онлайн-площадка, технологические трансформации, геополитическое противостояние.*

Постановка проблеми. В умовах інтенсивного та динамічного розвитку цифрових технологій, які характеризуються екстериторіальним характером, останнім часом актуалізуються ризики, загрози та виклики, пов'язані із глобалізацією ключових сфер життєдіяльності сучасних держав та світової спільноти. Не виключається, що екстериторіальний потенціал сучасних цифрових технологій може бути реалізовано зовнішніми гравцями у різноманітних сферах, включаючи такі галузі, як політика та економіка, у зв'язку з чим традиційне уявлення про національний суверенітет перестає адекватно відповідати сучасним умовам технологічного розвитку людства, що, у свою чергу, формує нагальну потребу перегляду класичних підходів до визначення змісту, структури та функцій такого феномену як державний суверенітет.

Суверенітет держави – політико-юридична властивість державної влади, яка означає її верховенство і повноту всередині країни, незалежність і рівноправність у зовнішньополітичній сфері. Правовою основою державного суверенітету є конституції країн, декларації, загальновизнані принципи міжнародного права, які фіксують суверенну рівність держав, їхню територіальну цілісність, невтручання у внутрішні та зовнішні справи, право націй на самовизначення. 16 липня 1990 року Верховна Рада тоді ще Української РСР схвалила фундаментальний акт – Декларацію про державний суверенітет України [1]. Цей акт, який має понад 30-річну історію свого існування, на жаль, питання цифрового суверенітету жодним чином не регламентує. Більш того, за таких умов виникає необхідність визначення й дослідження такого феномену як цифровий суверенітет та його складових.

Аналіз сучасних тенденцій розвитку політичного та соціально-економічного життя надає підстави констатувати, що існує низка нагальних проблем, пов'язаних із встановленням та визнанням цифрового суверенітету у конгломераті формування потреб держав та суспільства. У сфері глобального геополітичного протиборства між технологічно розвиненими державами світу спостерігаються перманентні процеси інформаційного втручання в національні сегменти Інтернет-простору, що надає можливість у віддаленому режимі впливати на функціонування національних політичних режимів, створюючи завдяки інформаційно-комунікаційному впливу на свідомість населення країн-мішеней вигідні моделі масової політичної реальності, що особливо важливо у сучасних умовах. Крім того, завдяки застосуванню цифрових комунікаційних технологій держава-агресор (РФ) та її сателіти можуть здійснювати цілеспрямований підрив соціально-політичної стабільності будь-яких держав світу, які виступають у якості геополітичних опонентів. Тобто на національному рівні РФ залишається супротивником, яка здійснює відкриту збройну агресію проти України, системно застосовуючи політичні, воєнні, економічні, інформаційно-психологічні та кібернетичний потенціал, які загрожують незалежності, державному суверенітету і територіальній цілісності України.

На цьому фоні провідні технологічні платформи ("Google", "Facebook", "Twitter", "YouTube", "Instagram") фактично здійснюють монополізацію цифрового простору, пропонуючи мільярдам користувачів, незалежно від географічного розташування країн у світовому масштабі, достатньо обмежений набір моделей соціально-політичної реальності, здійснюючи при цьому блокування альтернатив, наприклад аккаунти політиків, засобів масової інформації, каналів на відеохостінгу "YouTube" тощо на своїх

сервісах. Таким чином, сучасні процеси зовнішнього інформаційно-комунікаційного втручання у суверенні національні інформаційні простори розглядаються як один із напрямків підриву цифрового суверенітету відносно потенційних держав-мішеней.

В економічній сфері також спостерігаються активні спроби та прагнення вжиття заходів з метою цифрової десуверенізації. Так, цифрова валюта "Bitcoin" та подібні до неї альтернативні криптовалюти створені з метою заміни національних фіантних валют, надають сприятливу можливість їх власникам здійснювати неконтрольовану з боку державних органів будь-яку фінансово-економічну діяльність.

У сфері національної безпеки також відбуваються активні трансформації, які призводять до появи нових сучасних інструментів та сервісів, за допомогою яких інформація зберігається у зашифрованому вигляді на пристроях Інтернет-користувачів та формуються відповідні бази даних, які перебувають у розпорядженні власників соціальних мереж. Це дозволяє обійти контроль та регулятивні правила профільних та спеціальних служб, відповідальних за забезпечення безпеки національних сегментів цифрового простору тієї чи іншої держави. За таких умов, держава втрачає свої монопольні права та традиційні можливості у сфері забезпечення та підтримання національного суверенітету.

Зазначені обставини актуалізують важливість та необхідність висвітлення феномену цифрового суверенітету та загрозливих тенденцій його забезпечення в умовах сучасних глобальних технологічних трансформацій та геополітичного протиборства.

Результати аналізу наукових публікацій. Дослідження правової природи інформаційного суверенітету та його складових здійснювали у своїх наукових працях такі фахівці, як М. Дмитренко [2], О. Довгань [3], І. Доронін [4], О. Ніщименко [5], О. Солодка [6] та інші. Аналіз праць цитованих авторів надає змогу узагальнити загальне розуміння змісту поняття "інформаційний суверенітет" що являє собою невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку і здійсненні національної інформаційної політики. Науковцями констатовано, що це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі. Проте жоден із вказаних науковців не здійснював висвітлення кращих практик зарубіжного досвіду, присвячених проблемам забезпечення цифрового суверенітету, що посилює актуальність обраного тематичного напряму дослідження. Оскільки цифровий суверенітет є різновидом інформаційного суверенітету, то завданням автора є розкриття особливостей його забезпечення у національних сегментах кіберпростору шляхом проведення порівняльно-правового аналізу деяких актів зарубіжного законодавства, необхідність окреслити сучасні загрози у цьому контексті.

Метою статті є висвітлення та узагальнення спроможностей деяких держав світу у сфері забезпечення цифрового суверенітету в умовах глобального геополітичного протиборства.

Виклад основного матеріалу. XXI століття беззаперечно вважається епохою розвитку цифрових технологій. Кардинальну трансформацію проходять традиційні галузі діяльності держави, суспільства, бізнесу. Створюються принципово нові можливості та спроможності для розвитку економіки, соціальної сфери, сектору безпеки і оборони, державного управління тощо. Разом з тим нові технологічні рішення, окрім благополуччя держав та їх населення, породжують нові ризики та загрози. Невипадково в сучасну епоху тотальної діджіталізації актуальним завданням політичного керівництва

багатьох держав світу залишається розробка та схвалення законодавчих ініціатив з метою захисту цифрового суверенітету.

У першу чергу, проголошення та забезпечення цифрового суверенітету або суверенізація Інтернету є правом будь-якої держави світу. Одним з перших визначив поняття цифрового суверенітету французький бізнесмен П'єр Беланжер у 2012 році. На його переконання, "цифровий суверенітет" (*souveraineté numérique*) являє собою "контроль над сьогоднішнім днем", який формується шляхом застосування технологій та комп'ютерних мереж. Одночасно П. Беланжер тлумачить це поняття та його зміст в контексті захисту приватного життя громадян європейських держав у кіберпросторі, зокрема, робить акцент на доцільності прискорення створення власних європейських систем у технологіях Хмарних обчислень та зберігання даних громадян. З цієї позиції Беланжер підтримує запровадження державного контролю даних та систем зв'язку, підкреслюючи необхідність зниження контролю з боку іноземних ІТ-корпорацій.

На цьому фоні уряди багатьох держав світу намагалися підвищити захищеність інтересів держави та громадян шляхом підтримки розвитку національних технологій схваленням відповідних законів. Так, Президент Бразилії Д. Русеф (2011 – 2016 рр.) запропонувала план виходу бразильського сегменту мережі Інтернет з під індустріального впливу США та американських ІТ-корпорацій, що можна вважати реалізацією спроби забезпечення власного цифрового суверенітету. Німеччина з 2015 року ініціювала процес створення власної системи обміну електронними повідомленнями, прокладання нових підводних кабелів та розпочала просування політики локалізації даних з метою протидії американському та російському впливу, особливо після скандалу із зламом особистої електронної пошти канцлера А. Меркель. Після зламу даних французького уряду під час виборчої кампанії у 2017 році Франція спрямувала значні фінанси на розробку власного зашифрованого урядового месенджера з відкритим кодом, що також є спробою встановлення певним чином цифрового суверенітету.

Таким чином, майже усі високорозвинені країни світу визначають доцільність коригування засад національного законодавства з метою гарантування цифрових прав та свобод громадян, забезпечення національного цифрового суверенітету. Хоча існують й радикальні приклади діяльності держави у цьому напрямку. Так держава-агресор (РФ) з 2011 по 2018 роки запровадила практику адміністративного та кримінального переслідування користувачів Інтернету та соціальних мереж за "деструктивні" та "екстремістські" лайки, пости та коментарі. Одночасно з 1 січня 2017 року в РФ був введений податок, який зобов'язав нерезидентів сплачувати податок на додану вартість з продажу на її території електронних послуг: цифрового контенту, послуг зберігання та обробки інформації, реєстрації доменів і хостингу тощо, при цьому вони повинні стати на податковий облік. Серед технологічних гігантів у контролюючому органі зареєструвалися "Apple Distribution International", "Google Commerce","Microsoft Ireland", "Netflix International B.V.", "Wargaming Group", "Bloomberg", "Alibaba", "Booking.com" та ін. Загалом з моменту впровадження податку на податковий облік стало 1580 компаній. Аналогічні податкові правила були введені і в Республіці Білорусь у 2018 році.

Адже у світі щодо цифрового суверенітету склалася біполярна ситуація.

З одного боку, держави прагнуть забезпечити цифровий суверенітет, захистити цифрові права та свободи громадян, гарантувати захист даних, а з іншого – намагаються контролювати дії своїх громадян у кіберпросторі та у соціальних мережах, особливо у питаннях поширення фейків та деструктивного контенту. Щодо останнього, то слід зауважити, що у державах схвалюються законодавчі акти з метою блокування та нівелювання небезпечних проявів у мережі Інтернет або у соціальних мережах. З цього

приводу у Німеччині в 2017 році було прийнято спеціальний законодавчий акт під назвою “The Network Enforcement Act” (NetzDG), який зобов’язує соціальні мережі та інші Інтернет-платформи співпрацювати з державними структурами з метою контролю поширюваного користувачами контенту та запобігання розповсюдженню протиправного або забороненого контенту. Вказаний закон охоплює перелік понад двох десятків різноманітних правопорушень у сфері соціальних мереж, розпочинаючи від закликів до насильницьких висловлювань до поширення фейкових матеріалів. З моменту набуття чинності цим законом інформаційно-комп’ютерні платформи у тому числі й інтернаціональні (“Facebook”, “YouTube”, “Twitter” тощо), зобов’язані блокувати протиправний контент.

У 2020 році Уряд Великобританії поставив перед собою одіозне завдання – створити найбезпечніший у світі онлайн-простір для спілкування користувачів. Очікується, що захист користувачів мають забезпечити саме онлайн-платформи та соціальні мережі. У випадку, якщо користувачі стануть жертвами протиправного контенту, то відповідальність будуть нести саме соціальні мережі, включаючи особисту відповідальність співробітників ресурсу. Запропоновано спеціальний механізм під назвою “Safety by Design”, який надасть змогу впроваджувати в нові продукти під час їх розробки з метою забезпечення безпеки онлайн. Під дію нових ініціатив підпадають усі платформи, які пропонують обмін даними серед користувачів. Перелік загроз, зафіксований у спеціальному документі під назвою “Online Harms White Paper”, поділяється на три категорії: 1) деструктивна інформація, яка має юридичне визначення (пропаганда агресії, заохочення самогубств тощо); 2) шкідлива інформація, яка не має юридичного статусу (тролінг, залякування); 3) легальний контент, не призначений для дітей (ненормативна лексика, додатки сайтів знайомств тощо). У лютому 2020 року Уряд Великобританії вирішив надати національному медіарегулятору “Ofcom” право боротися з шкідливим та протиправним контентом, у тому числі на форумах, відеохостингах та в соціальних мережах. Тобто ця державна структура отримала повноваження з метою кардинальної боротьби за чистоту Інтернету. За таких умов приклад Сполученого Королівства є показовим. Саме соціальні мережі зобов’язані максимально відповідально ставитися до контенту та творчості користувачів. При цьому, як переконливо засвідчує іноземний та міжнародний досвід, ІТ-гіганти, з одного боку, блокують пости та аккаунти за власним баченням (оскаржити таке рішення практично неможливо), а з іншого боку – досить часто ігнорують вимоги користувачів або представників влади тієї чи іншої держави.

Останнім часом у світі спостерігається загрозлива тенденція, за якої свою волю урядам держав нав’язують та диктують гігантські ІТ-корпорації, переважно американські, абсолютно ігноруючи закони та нормативно-правові акти цих країн. У зв’язку з чим у багатьох країнах світу – Італії, Австралії, Індії тощо активно розроблюються пропозиції та впроваджуються заходи з метою боротьби із свавіллям глобальних приватних ІТ-компаній, постачальників соціальних мереж, включаючи заходи з посилення відповідальності. Проблема функціонування соціальних мереж у глобальному вимірі тісно пов’язана із національною безпекою та державним суверенітетом, оскільки саме соціальні мережі останнім часом стали інструментом для проведення так званих “кольорових революцій”. Свого часу після подій, які увійшли в історію людства як “Арабська весна” або “твітер-революція”, кожна країна опікується питаннями планомірного захисту власного сегменту кіберпростору, особливо щодо діяльності соціальних медіа. Саме соціальні мережі виступають одночасно сучасною організаційною зброєю та привабливим бізнес-продуктом. Гігантом серед соціальних

мереж виступає американська транснаціональна корпорація “Facebook”, у якій зареєстровано понад 1,4 млрд. користувачів. Як переконливо демонструє досвід останніх років, американські соціальні мережі роками ігнорують закони інших країн світу. Тому на сьогодні в багатьох країнах світу розроблюються законодавчі ініціативи з метою забезпечення цифрового суверенітету та протидії свавіллю глобальних ІТ-компаній, включаючи запровадження серйозних санкцій.

Досить радикально підійшли до питання правової регламентації діяльності соціальних мереж у Туреччині. В цій країні вперше в історії людства було схвалено Закон “Про соціальні мережі” № 7253 [7], який набув чинності з 1 жовтня 2020 року. На виконання цього законодавчого акта великі Інтернет-платформи, представлені у цій країні, на кшалт “Facebook”, “Twitter“, “Periscope”, “YouTube” и “TikTok”, “Instagram” та інші, які мають аудиторію користувачів понад 1 млн. осіб, зобов’язані відкривати офіційні представництва своїх компаній та призначати уповноважених осіб для взаємодії з органами державної влади та судовими інстанціями Туреччини. Нормативно встановлено, що головою представництва має бути громадянин саме Туреччини. Також законом запроваджена обов’язкова вимога щодо видалення “образливого” контенту протягом 48 годин та зберігання даних турецьких користувачів в соціальних мережах виключно на території Турецької республіки. Таким чином, ресурси зобов’язані видаляти заборонений контент, як тільки його помітить місцевий регулятор – управління телекомунікацій та зв’язку. У листопаді 2020 року великі соціальні компанії “Facebook”, “Twitter”, “Periscope”, “YouTube” и “TikTok” були оштрафовані за невиконання вимог вказаного законодавчого акта на загальну суму 10 млн. турецьких лір. Таким чином, в Туреччині у цьому році з’являться офіційні представництва (локальні офіси) соціальних мереж “Facebook” та “Instagram”. Якщо вимоги закону будуть проігноровані, то соціальна мережа знов може бути оштрафована та запроваджено зменшення або гальмування її трафіку. Локальні офіси соціальних мереж в Туреччині наділені правом призупиняти роботу соціальних мереж та медіа. У Туреччині відкриття представництв “Facebook” та “Instagram” вважають значною перемогою, оскільки такий крок дозволить владі вимагати дотримання місцевого законодавства соціальними мережами. Тоді як відсутність таких представництв сприяє ігноруванню ІТ-компаніями правил ринку та дозволяє ухилятися від податків й штрафів за порушення законодавчих вимог. Іншими словами, турецький прецедент надасть змогу вирішити питання побудови унормованих відносин з американськими цифровим компаніями й в інших країнах світу.

Цікавим у цій площині є досвід Індії – держави, де знаходиться найбільший ринок месенджера “WhatsApp”. Так у 2020 році було розпочато антимонопольне розслідування у зв’язку з обов’язковим оновленням політики конфіденційності “WhatsApp”. На переконання Комісії з конкуренції Індії (Competition Commission of India, CCI) “WhatsApp” порушив місцеві закони про конкуренцію своїми вимогами. Однією із запроваджених новацій стала обов’язковість передачі даних усіх користувачів “WhatsApp” до мережі “Facebook”, що значно обурило багатьох користувачів та як наслідок призвело до збільшення навантаження на конкурентів, зокрема месенджера “Telegram”.

Австралія має намір прийняти закон, який зобов’яже Інтернет-гігантів (таких як “Google” та “Facebook”) сплачувати австралійським виданням гонорари за розміщення новинного контенту на своїх платформах. Новий законопроект про медіаринок став фактичною відповіддю на становище, яке австралійські ЗМІ вважають “несправедливим”. Вони піддають критиці Інтернет-гігантів за те, що ті отримують прибуток з демонстрації новинного контенту і при цьому ніяк не стимулюють фінансово самі видання.

ЄС також опікується питаннями забезпечення цифрового суверенітету. З цією метою Євросоюз прагне нормативно врегулювати діяльність світових ІТ-корпорацій, оскільки останні 5 років керівні органи Євросоюзу демонтують занепокоєння та активно обговорюють проблему безмежного поширення на ринку європейського континенту американських Інтернет-компаній. Ще у 2018 році Єврокомісія надала поради власникам Інтернет-платформ щодо активізації протидії поширенню незаконного контенту. Заборона поширювалася на: дитячу порнографію, ворожі висловлювання, прояви ксенофобії, пропаганду агресії, інформацію терористичного характеру тощо. За останні 3 роки ЄС вже тричі штрафував "Google" на суму понад 8 млрд. Євро за просування операційної системи "Android" через використання власного пошукового ресурсу, "Apple" підпала під розслідування за нав'язування користувачам iPhone-сервісу "Apple Music", а "Facebook" та "Amazon" були покарані за використання особистих даних користувачів з метою просування власних товарів та послуг. Однак, європейські штрафи та інші санкції фактично не вплинули на американських монополістів.

На початку 2021 року антимонопольні органи ЄС запросили у рекламодавців інформацію про практику "Google" у сфері надання рекламних технологій. На даний час ця транснаціональна компанія стикається з двома розслідуваннями, проведеними ЄС щодо своєї рекламної практики, зосередженими на технологіях і даних. Загальновідомо, що "Google" і "Facebook" разом захоплюють більше половини світового ринку продажів Інтернет-реклами. Обидві компанії в даний час є об'єктом позову США по їх угоді 2018 року, завдяки якій "Facebook" надає клієнтам можливість розмістити рекламу в мережі видавничих партнерів "Google". ЄС також хоче знати, чи отримують рекламодавці знижки при використанні посередників "Google", які дозволяють рекламодавцям або медіа-агентствам купувати рекламу у багатьох джерел.

У грудні 2020 року європейські урядовці обговорили законопроекти ЄС про цифрові послуги та цифрові ринки, які регламентують не лише продаж товарів у мережі Інтернет-онлайн, а й нормативно зачіпають процедури швидкого видалення протиправного контенту – протягом години після отримання такої вимоги. У випадку бездіяльності компанія може отримати колосальний штраф та понести відповідальність. Цими актами передбачається встановлення правил для онлайн-платформ, які зобов'язані розуміти свою роль та значення в європейській онлайн-екосистемі. Законопроектами передбачається штрафувати європейськими регуляторами ІТ-компанії на суму до 10 % глобальної виручки, а у випадку масштабних порушень – примусово її конфіскувати. Зокрема, проект закону про цифрові ринки регулюватиме антимонопольні порушення ІТ-компаній, а інший законопроект присвячений встановленню покарань за публікацію забороненого та деструктивного контенту.

Законопроект про цифрові ринки ЄС запроваджує поняття "страж" (*gatekeeper*) – компанія, статус якої дозволить контролювати платформу, тобто сервіси. Таким чином, передбачається створення природних монополій у сфері цифрової економіки. Типові приклади – магазини додатків "Apple" та "Google". Останнім часом у якості негативних прикладів у документах ЄС фігурували саме "Apple", "Google", "Amazon". Встановлюються вимоги для так званих "стражів": прибуток має складати не менш 6,5 млрд. Євро, а капіталізація – мінімум 65 млрд. Євро. Обов'язки "стража" – забезпечувати усім своїм клієнтам рівні умови роботи, заборона на створення будь-яких преференцій для власних сервісів та використання даних своїх клієнтів. "Стражі" мають узгоджувати з владою навіть дрібні угоди щодо злиття або поглинання, а також у сфері інвестування. Звідси випливає, що запрацюють антимонопольні обмеження. Передбачаються й штрафи щодо ІТ-корпорацій: 6 % від прибутку треба буде заплатити у випадку відмови компанії видаляти контент, який

визнано в ЄС неприпустимим. Акцент зроблено на посиленні податкового законодавства, особливо щодо компаній “Apple”, “Google”, “Facebook”, “Amazon”, які акумулюють великі прибутки, надаючи свої послуги у державах ЄС, хоча сплачують податки за мінімальними ставками, відкриваючи свої штаб-квартири в Ірландії або в Нідерландах. Тому в ЄС для транснаціональних ІТ-компаній обговорюється питання про перехід до сплати ПДВ на територіях надання своїх послуг.

Таким чином, ЄС взяв курс на посилення та зміцнення свого цифрового суверенітету на фоні загострення протистояння між КНР та США. ЄС має намір інвестувати мільярди Євро у власний ІТ-сектор в рамках посилення свого технологічного суверенітету. Тобто європейські лідери планують зменшити залежність від розробок, які надходять з КНР та США, а також значно послабити зарубіжні ІТ-корпорації на власному цифровому ринку. Європейський цифровий суверенітет має бути спрямований на динамічний розвиток власних цифрових навичок, принаймні ключових технологій, не виключаючи присутність інших постачальників. Проте, на переконання провідних експертів, на даний час домінує позиція, згідно з якою ІТ-індустрія є сферою, у якій Європа значно поступається не тільки США, але й Китаю, Японії та навіть Південній Кореї.

За таких умов можна підсумувати, що у ЄС дедалі частіше говорять про цифровий суверенітет, але, швидше, в контексті цифрової безпеки. Загальною потребою для політикума ЄС є необхідність вдосконалити своє законодавство та виробити норми для технологічних компаній і транснаціональних корпорацій, що оперують у діджитал-сфері й активно впливають на повсякденне життя європейських громадян. Таким чином, європейці наголошують на виробленні правил і контролі за доброчесністю з боку засобів масової комунікації як можливих засобів або ж суб’єктів недоброчесних дій стосовно не тільки держави, а й пересічних громадян. На цьому фоні не останнім питанням залишається забезпечення цифрового суверенітету, який включає забезпечення цифрових прав громадян при використанні засобів масової комунікації, зміст якого охоплює не тільки захист персональних даних, а й право розпоряджатися своїми даними.

Ще одним перспективним напрямком захисту цифрового суверенітету вбачається створення вітчизняної операційної системи програмного забезпечення, відмова від використання китайської продукції та відповідних розробок. Так, наприклад, останнім часом відбувалося лобіювання з боку США бойкоту китайській компанії “Huawei” та її продукції, внесення до чорного списку сотні інших китайських технологічних компаній.

Висновки.

В сучасних реаліях контекст пандемії коронавірусу призвів до потреби глобального переосмислення ролі та значення цифрових технологій та практики їх застосування. Довгострокова тенденція загального зростання ринку електронної комерції була підтримана режимом карантину, в умовах масової самоізоляції та чисельного використання соціальних мереж та різноманітних онлайн-платформ. Ще 10 років тому втручання у внутрішні справи держави передбачало агресію та перетинання кордонів. Зараз спричинити шкоду іншій державі реально за допомогою Інтернет-технологій, у зв’язку з чим парламенти держав світу мають забезпечити цифровий суверенітет своїх країн. При цьому з запровадженням цифрових технологій парламенти мають працювати над законами, норми яких спрямовані не тільки на побудову нової економіки, але й врегулювати питання, пов’язані із кібербезпекою та забезпеченням цифрового суверенітету, захисту персональних даних, національного сегменту кіберпростору. Тобто передові держави світу шляхом схвалення відповідного законодавства вживають заходів з метою побудови власної моделі цифрового суверенітету. Підставами для цього

також є тиск на гравців світового ринку з боку зарубіжних ІТ-гігантів, зокрема “Google” та “Facebook”, які отримують колосальні прибутки від своєї діяльності у тій чи іншій державі, хоча не підпадають під національну юрисдикцію та сплачують мінімальні податки.

Набувають неабияких масштабів численні випадки порушення цифрових прав громадян зарубіжними ІТ-компаніями, які демонстративно ігнорують вимоги національного законодавства. Актуальним є збереження цифрового суверенітету, оскільки вже стало практикою соціальних мереж втручатися у справи електронних ЗМІ та блогерів шляхом видалення контенту або блокування цілих каналів. Також збір даних користувачів соціальних мереж має відбуватися тільки за їх згоди, щонайменше користувачі повинні бути поінформовані про те, що дані збираються та акумулюються. Наприклад, мережі “Facebook” та “Twitter” порушують права громадян, оскільки не переносять до національних юрисдикцій держав сервери з даними користувачів. Також “Instagram”, який належить мережі “Facebook”, без пояснень практикує знищення аккаунтів користувачів, порушуючи права на свободу самовираження, на свободу слова, захист персональних даних тощо. У зв’язку із викладеним, обов’язком держави є забезпечення захисту цифрових прав громадян, впровадження заходів з метою входження зарубіжних компаній у правове поле держави та здійснення своєї діяльності виключно у його рамках.

Достатня увага повинна приділятися питанням видалення деструктивного контенту соціальними мережами. На законодавчому рівні доцільно запровадити такі вимоги. Держави мають об’єднатися з метою примусу ІТ-корпорацій встановити прозорі та відкриті правила поведінки соціальних мереж, які у свою чергу, повинні показати свої стандарти модерації, оскільки кожен повинен розуміти – за що його можуть заблокувати, перелік існуючих стоп-слів тощо.

Ефективним механізмом може стати заборона будь-яких угод між державними органами та державних компаній з “Google”, “Facebook” та іншими від розміщення реклами, включаючи закупівлю товарів та послуг. Проте жодне цифрове законодавство не є універсальним засобом від усіх загроз та ризиків, оскільки кордони між реальним та віртуальним життям стерлися, а системна робота над створенням безпечного та відкритого Інтернет-середовища є справою не тільки держави, але й соціальних платформ, які надають відповідні послуги. Сучасне світове законодавство та прискіплива увага до цифрової грамотності населення це переконливо доводять та підтверджують.

Досить перспективним та корисним вбачається турецький досвід, який кардинально змінив ставлення світової спільноти до соціальних мереж, підвищив їхню відповідальність. У світовій практиці достатньо прикладів регулювання Інтернет-сфери, забезпечення цифрового суверенітету, проте для України доцільно враховувати здобутки міжнародного досвіду та нормативно деталізувати власне розуміння цієї проблематики, спрямувати зусилля на розвиток та захист українського сегменту мережі Інтернет. У сучасному глобальному вимірі домінує позиція, що діяльність соціальних мереж становить чималу загрозу національному цифровому суверенітету в будь-якій країні світу. Передумовами для цього стала діяльність транснаціональних гігантів ІТ-індустрії у національних сегментах кіберпростору, яка здійснюється поза межами національної юрисдикції та з порушенням вимог законодавства тієї чи іншої держави. З метою унормування функціонування соціальних мереж, глобальних ІТ-платформ кожна держава розробляє та встановлює законодавчий алгоритм моніторингу та контролю за їх діяльністю, включаючи механізми впливу у вигляді штрафів та санкцій, збільшення податкового навантаження на цих суб’єктів тощо.

Враховуючи викладене, для України є актуальним посилення захисту цифрових прав громадян, одночасно зі створенням передумов для адміністрування податку на додану вартість при оподаткуванні електронних послуг фізичним особам, що постачаються нерезидентами в мережі Інтернет. В Україні результатом тривалих дискусій з приводу запозичення кращих практик європейського та міжнародного досвіду у сфері забезпечення цифрового суверенітету стала підготовка законопроекту "Про внесення змін до Податкового кодексу України щодо оподаткування податком на додану вартість електронних послуг, що постачаються нерезидентами фізичним особам, місце постачання яких розташовано на митній території України" від 19.12.19 р. № 2634 (так званий "податок на "Google") [8]. Ще наприкінці 2020 року депутати обговорювали можливість оподаткування доходів "Google", "Netflix", та "Amazon", а також компаній, що продають відео, музику, рекламу, ігри та доступ до Хмарних сервісів.

17 лютого 2021 року Верховна Рада України прийняла за основу відповідний законопроект, а 8 квітня 2021 року він був схвалений. Положеннями законопроекта передбачено: механізм оподаткування податку на додану вартість нерезидентами; можливість сплачувати податок у валюті, фактично не перебуваючи на території України. Завдяки цьому закону буде запроваджений дієвий механізм, який зобов'яже світових гігантів ("Google", "Facebook" тощо), які працюють в Україні, сплачувати податки до бюджету, що дозволить урівняти в правах український бізнес і бізнес транснаціональний, який чомусь сьогодні є пільговим. Також доцільно у вітчизняному законодавстві визначити поняття "іноземна соціальна мережа", її правове становище, податковий режим тощо.

Використана література

1. Декларація про Державний суверенітет України від 16 липня 1990 року. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text (дата звернення: 02.04.2021).

2. Дмитренко М. Проблемні питання інформаційної безпеки України 2018. URL: https://journals.iir.kiev.ua/index.php/pol_n/article/download/3318/2997 (дата звернення: 02.04.2021).

3. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право*. № 3(12)/2014. С. 102-112.

4. Доронін І.М. Правові проблеми суверенізації Інтернету. *Інформація і право.* № 2(29)/2019. С. 74-81.

5. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право.* 2016. № 1. С. 17-23.

6. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право.* № 1(32)/2020. С. 80-87.

7. Internet ortaminda yapilan yayinlarin düzenlenmesi ve bu yayinlar yoluyla işlenen suçlarla mücadele edilmeSİ Kabul Tarihi: 29.07.2020. URL: http://www.lebibyalkin.com.tr/mevzuat/mevzuattaki-son-degisiklikler/2020-mevzuattaki-son-degisiklikler_temp_temp-000_/2020-temmuz_temp_temp-000_2020_07 (дата звернення: 02.04.2021).

8. Щодо оподаткування податком на додану вартість електронних послуг, що постачаються нерезидентами фізичним особам, місце постачання яких розташовано на митній території України: проект закону про внесення змін до Податкового кодексу України від 19.12.19 р. № 2634. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67703 (дата звернення: 02.04.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.951

ГРИГОРЕНКО В.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-0511-3402.

НАЙКРАЩІ ЗАРУБІЖНІ ПРАКТИКИ РОЗБУДОВИ МЕХАНІЗМІВ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Анотація. *Визначено роль та місце державно-приватного партнерства у сфері забезпечення кібербезпеки в сучасних умовах. Деталізовано моделі розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки через призму набутого досвіду окремих передових країн світу (Ізраїль, Німеччина, США, Великобританія). Узагальнено позитивні здобутки зарубіжного досвіду державно-приватного партнерства у сфері забезпечення кібербезпеки. Сформульовано проблемні питання врегулювання державно-приватного партнерства як складової національної системи кібербезпеки. Запропоновано шляхи удосконалення державно-приватного партнерства у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кіберзахист, кібератака, кіберзагроза, кіберпростір, стартап, державно-приватне партнерство, ІТ-ринок, цивільний сектор безпеки.*

Summary. *The role and place of public-private partnership in the field of cybersecurity in modern conditions are determined. Models of building public-private partnerships in the field of cybersecurity through the prism of the experience of some advanced countries (Israel, Germany, USA, GB) are detailed. The positive achievements of foreign experience of public-private partnership in the field of cybersecurity are summarized. Problematic issues of public-private partnership development as a component of the national cybersecurity system are formulated. The directions of improvement of public-private partnership in the field of cybersecurity are proposed.*

Keywords: *cybersecurity, cyberdefense, cyberattack, cyberthreat, cyberspace, startup, public-private partnership, IT- market, civil security sector.*

Аннотация. *Определены роль и место государственно-частного партнерства в сфере обеспечения кибербезопасности в современных условиях. Детализированы модели развития государственно-частного партнерства в сфере обеспечения кибербезопасности через призму приобретенного опыта отдельных передовых стран мира (Израиль, Германия, США, Великобритания). Обобщены позитивные достижения зарубежного опыта государственно-частного партнерства в сфере обеспечения кибербезопасности. Сформулированы проблемные вопросы государственно-частного партнерства как составляющей национальной системы кибербезопасности. Предложены направления усовершенствования государственно-частного партнерства в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, киберзащита, кибератака, киберугроза, киберпространство, стартап, государственно-частное партнерство, ИТ-рынок, гражданский сектор безопасности.*

Постановка проблеми. Проблема забезпечення безпеки у кіберпросторі не має кордонів. Кожна держава розробляє та впроваджує механізми забезпечення кібербезпеки, використовуючи досягнення світової практики. Важливою складовою та прерогативою цих процесів є залучення приватних гравців, які також активно використовують кіберпростір та його потенційні можливості. У наш час спостерігається підвищена активність приватного сектору та інституцій громадянського суспільства у заходах, спрямованих на забезпечення кібербезпеки як на національному, так і на міжнародному рівнях.

З метою реалізації сучасних завдань у сфері забезпечення кібербезпеки держава повинна активніше: покладатися на підтримку та допомогу підприємств ІКТ-галузі, волонтерських організацій, наукових установ, закладів освіти та громадських організацій; впроваджувати дієві механізми громадського контролю в питаннях забезпечення кібербезпеки; налагоджувати оперативний обмін у режимі реального часу інформацією між державними органами, приватним сектором і громадянами стосовно кіберзагроз, кібератак та кіберінцидентів; залучати представників експертного середовища наукових установ, професійних об'єднань та громадських організацій до підготовки галузевих індикаторів стану кібербезпеки, проектів відповідних нормативних актів у цій сфері. За таких умов висвітлення кращих практик зарубіжного досвіду у сфері розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки є актуальним та своєчасним, особливо в умовах тенденційного поширення гібридних загроз та агресивної експансіоністської політики РФ проти України, у тому числі й у кіберпросторі.

Результати аналізу наукових публікацій. Питанням державно-приватного партнерства у сфері забезпечення кібербезпеки певним чином приділяли увагу у своїх наукових працях такі вчені, як: М. Гребенюк, Б. Леонов [1], Д. Дубов [2], В. Круглов [3], Р. Прав [4], В. Шеломенцев [5] та інші. Проте висвітлення кращих практик зарубіжного досвіду у сфері розбудови державно-приватного партнерства забезпечення кібербезпеки жоден із вказаних авторів не здійснював, що посилює тематичну актуальність цієї наукової публікації.

Метою статті є деталізація заходів, які вживаються для розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки у провідних зарубіжних країнах світу, та на їх підставі узагальнення і визначення дієвих кроків щодо удосконалення національної системи кібербезпеки з урахуванням спроможності цивільного сектору безпеки.

Виклад основного матеріалу. Важливим компонентом посилення спроможностей держави у сфері забезпечення кібербезпеки є саме побудова конструктивного діалогу у форматі державно-приватного партнерства. Набутий міжнародний досвід переконливо доводить, що без комплексної взаємодії держави та приватного сектору неможливо побудувати ефективний та надійний кіберзахист. Державно-приватне партнерство передбачає таку форму співпраці, за якої досягаються цілі та завдання, що сприятимуть забезпеченню національної безпеки, економічного розвитку та побудові безпечного кіберсередовища для усіх громадян. Тобто модель державно-приватного партнерства можливо охарактеризувати як динамічну взаємодію між державними та приватними інституціями, які здійснюють спільну реалізацію функцій з метою забезпечення безпеки у кіберпросторі.

Держава Ізраїль залишається першою країною у світі з найбільшими інвестиціями у кібербезпеку та рекордною кількістю стартап-компаній. Динамічний розвиток цієї сфери залишається першочерговим пріоритетом держави. Так, наприклад, у Ізраїлі на виконання політики Уряду дедалі активніше залучаються до співпраці у сфері забезпечення кібербезпеки компанії приватного сектору. У цій країні в 2017 році в секторі кібербезпеки було задіяне 420 підприємств, а на кіберіндустрію витрачено понад $815 млн. Невипадково держава Ізраїль зарекомендувала себе як світовий лідер у сфері інноваційних кібертехнологій. На ізраїльські передові підприємства, які співпрацюють із міжнародними корпораціями та стартапами, покладаються завдання щодо розробки сучасних та інноваційних систем захисту від кібератак з метою адекватного реагування на ситуативну динаміку та загрози в кіберпросторі. Приватні компанії з кіберзахисту

активно використовують штучний інтелект для розпізнавання шкідливого програмного забезпечення та виявлення агресивної поведінки в Інтернеті [1, с. 48-49].

Згідно із даними дослідницького центру "Cyber Security Ventures", дев'ять ізраїльських компаній входять у топ – 100 найбільш успішних та прибуткових світових компаній у сфері кібербезпеки. Наприклад, Check Point Software посідає у цьому рейтингу четверте місце з ринковою вартістю $15 млрд. Останнім часом, за Ізраїлем закріпився бренд іміджу під назвою "Startup Nation", оскільки у цій державі за сприяння Уряду активно процвітає стартап-індустрія. Венчурний фонд "Flint Capital" інвестував $3 млн. в ізраїльський стартап "CyberX", який спеціалізується на виробництві програмного забезпечення у сфері кібербезпеки для промислових потреб Інтернету речей. Стартап "Checkmarx", який надає сервісні послуги з метою аналізу вихідного коду програмного забезпечення та виявлення кіберзагроз на ранніх стадіях, залучив $ 84 млн. інвестицій. Стартап "Saferide Technologies" представляє на ринку власно розроблений багаторівневий програмний пакет з метою захисту систем кібербезпеки під назвою "vSentry Core", який дозволяє виявляти та ліквідовувати усі потенційні загрози, захищатися від хакерів та різноманітних шкідливих атак.

Тобто сфера підтримки стартапів за тематикою кібербезпеки не залишається поза увагою великих інвесторів. У сучасних умовах інфраструктура сфери кібербезпеки включає у цій країні понад 150 компаній, серед яких представлені стартапи, венчурні фонди, науково-дослідницькі проекти, які реалізують співпрацю між високотехнологічними компаніями та академічними й науковими колами. Спостерігається тенденція перетворення держави Ізраїль на міжнародний центр високих технологій та світового лідера у сфері кібербезпеки. Ізраїль одним із перших почав налагоджувати співпрацю у сфері кібербезпеки між заінтересованими суб'єктами, науковими установами та організаціями приватного сектора.

Одна із провідних ініціатив Ізраїлю в цій царині – проект "CyberSpark Innovation Initiative143", започаткований 2014 року як спільне підприємство INCB муніципалітету Беершеба, університету Бена Гуріона, та бізнес-партнерів: EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs та Elbit.IDF та CERT-IL також беруть участь в ініціативах CyberSpark, серед яких – робота зі спільнотою дипломатів та проведення семінарів для фахівців із кібербезпеки з усього світу. З моменту запуску, CyberSpark створив "екосистему" для багатьох заінтересованих сторін – уряду, наукових кіл, бізнесу, місцевого самоврядування та громадянського суспільства. Уряд потужно підтримує ізраїльську галузь кібербезпеки та відповідний бізнес через декілька джерел. Так, Офіс головного вченого в Міністерстві економіки (зараз Національне агентство з технологічних інновацій) надав різноманітні науково-дослідні та інвестиційні інструменти через свій фонд досліджень і розробок, програми Kidma, Magnetta Meimad з підтримки досліджень у царині кібербезпеки та розробок подвійного призначення.

Крім CyberSpark, близько 20 науково-дослідних центрів у галузі кібербезпеки, що працюють над рішеннями безпеки для світового ринку, створені в Ізраїлі транснаціональними корпораціями, серед яких – PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee та Ciscom. Наразі корпорації також створюють в Ізраїлі кіберцентри. Так в Ізраїлі працюють дев'ять науково-дослідних університетів, два з яких 2016 року увійшли до сотні найкращих наукових установ у світі й мають кафедри інформатики (Єврейський університет та "Техніон"). У рамках національних програм у середніх школах Ізраїлю проводяться дослідження й тренінги з кібербезпеки. Загалом на сьогодні серед пріоритетів Ізраїлю в галузі кібербезпеки слід виділити забезпечення прозорості дій у цій царині для громадськості, інституційні інновації та державні

інвестиції як короткострокового (субсидії для компаній, що працюють у галузі кібербезпеки), так і довгострокового характеру. Таким чином, можна констатувати, що протягом останніх десятиліть Ізраїль перебуває у світовому авангарді інновацій та науково-технологічних напрацювань у галузі кібербезпеки, яка безпосередньо залежить від обсягу залучених інвестицій та інновацій. Культура інновацій Ізраїлю, його унікальний людський капітал та зусилля з національної безпеки створюють ідеальне середовище, задовольняючи цю потребу як на місцевому, так і на глобальному рівні.

Німеччина є однією із ключових країн, форми державно-приватного партнерства якої є ефективним інструментом у системі забезпечення кіберзахисту країни в цілому. Сфера державно-приватного партнерства у галузі кібербезпеки між операторами критично важливої інфраструктури та відповідними державними органами регулюється в Німеччині планом реалізації "UP KRITIS", який розроблений і фінансується урядом цієї країни. З одного боку, платформа "UP KRITIS" регулярно інформує національних партнерів про відповідні заходи щодо захисту критичної інфраструктури; з іншого – рішення, прийняті членами "UP KRITIS", представляються на розгляд європейських структур, впливаючи тим самим на європейський порядок денний на ранніх стадіях запобігання кіберзагроз, посилюючи інтереси Німеччини в даному секторі безпеки. Також кожен громадянин має доступ до веб-сайту *//www.bsi-fuer-buerger.de* та телефонної гарячої лінії для передачі та отримання інформації чи рекомендацій щодо дій у випадку скоєння кібератаки. Тобто одним із напрямів державно-приватного партнерства, ініційованих Німеччиною, є заохочення співпраці між державними структурами та приватними організаціями, громадськими структурами на ранніх етапах дослідницького та інноваційного процесу як у країні, так і в ЄС в цілому. Зазначене сприятиме синхронізації доступу до інноваційних та надійних європейських рішень – продуктів, послуг та програмного забезпечення для ІКТ.

Цікавим видається досвід США у цій площині. Позитивним прикладом сучасних моделей паритетної взаємодії державного та приватного секторів у сфері забезпечення кібербезпеки є створення на базі Департаменту внутрішньої безпеки США автоматизованої програми відстеження кіберзагроз, яка надає змогу забезпечити автоматизований обмін інформацією між державним і приватним секторами. Аналогічні приклади існують і в європейських країнах (Великобританія, Нідерланди). Також у США з метою прогнозного супроводження діяльності державних інституцій та приватного сектору у сфері забезпечення кібербезпеки створено некомерційний дослідний центр "TechAmerica Foundation", який об'єднує фахівців та експертів 1200 компаній з метою визначення орієнтовно-планових обсягів щорічного фінансування кібероборони, при цьому акценти діяльності постійно передбачають значне збільшення витрат виходячи із потенційних та реальних кіберзагроз. Також у США успішно функціонує некомерційна організація як приватний інститут "SANS" (SysAdmin, Audit, Network and Security) [6], який займається дослідженнями, тренінгами та сертифікацією в галузі комп'ютерної безпеки. На сьогодні "SANS" являє собою один із найбільших сертифікаційних центрів у цій галузі, де окрім традиційного навчання, здійснюється експериментальна діяльність. З метою збільшення аудиторії слухачів використовуються різноманітні формати – навчання он-лайн, проведення науково-практичних заходів, конференцій тощо. Щорічно по усьому світу 12 тис. осіб проходять курс навчання в "SANS". Періодично ця інституція проводить змагання між своїми інструкторами, а також здійснює пошук нових тренерів.

1 листопада 2016 року була представлена Стратегія кібербезпеки Великобританії на 2016 – 2021 роки [7]. У цьому документі підкреслюється важливість трансформацій, що сприятимуть впровадженню цифрових технологій як публічними, так і приватними

підприємствами, але наголошено на значній ролі бізнесу та приватних організацій у реагуванні на кіберзагрози. При цьому акцентована увага на важливості партнерства між урядом та приватним сектором у розробці стандартів кібербезпеки. Згідно із цим документом у цій країні був створений Інститут досліджень питань кібербезпеки, який об'єднав зусилля дослідників, котрі займаються цією темою в різних університетах по всій країні. Інститут фінансується за рахунок гранту 3,8 млн. фунтів. Він став частиною програми Уряду Великобританії, направленої на розширення можливостей академічної науки у сфері кібербезпеки.

Очікується, що діяльність цієї структури надасть методичну допомогу компаніям, приватним особам та державним організаціям, допоможе схвалювати обґрунтовані рішення щодо використання заходів з метою забезпечення безпеки кіберпростору та кардинально вирішувати складні завдання у державному та приватному секторах, об'єднавши їх зусилля. Структурно ця інституція є віртуальною та об'єднує сім університетів, партнерство семи британських науково-дослідницьких рад, серед яких виділяється "Research Councils UK" (RCUK), Дослідницька Рада інженерних та фізичних наук (EPSRC), Департамент бізнесу та навичок (BIS). Таким чином, діяльність цієї організації сприятиме залученню провідних вчених у сфері кібербезпеки, у тому числі соціологів, математиків, програмістів з усіх куточків Сполученого Королівства. Актуалізовано, що ця країна є однією із найбільших Інтернет-економік світу та має гігантський сектор послуг у сфері кібербезпеки, у зв'язку з чим діяльність інституту зарекомендувала себе на правах досвідченого центру вироблення стратегічних рішень у сфері блокування та ліквідації кіберзагроз та їх масштабів. Слід вказати, що на вітчизняному ринку кібербезпеки Великобританії функціонує достатня кількість авторитетних ІТ-компаній, які мають значний досвід у цій сфері, вдало впроваджують новітні технології та надають послуги щодо виявлення кіберінцидентів, виконують комплексні комп'ютерні експертизи тощо.

Невипадково у стратегічних документах ЄС з кібербезпеки неодноразово наголошується на важливості розбудови державно-приватного партнерства в боротьбі з кібератаками і кіберзлочинністю. Слід зазначити, що при вирішенні завдань у сфері забезпечення кібербезпеки держава та її правоохоронні органи відчувають потребу в залученні кваліфікованих спеціалістів з приватного ІТ-сектору, які мають знання, навички та вміння щодо розробок, впровадження та обслуговування сучасного програмного забезпечення. Також важливим питанням залишається впровадження ефективного проектного менеджменту з питань забезпечення кібербезпеки, у тому числі, у питаннях управління науково-технічними проектами з використанням механізмів державно-приватного партнерства. Організація постійної взаємодії у рамках державно-приватного партнерства також може використовуватися з метою скоординованого управління кіберризиками на національному рівні.

Таким чином, на основі узагальнення здобутків зарубіжного досвіду державно-приватного партнерства у сфері забезпечення кібербезпеки можна виділити такі його складові: основною його метою є побудова конструктивного діалогу та плідної співпраці, реальна довіра між приватним сектором та державними інституціями; заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу. Державно-приватні інвестиції активно спрямовуються на дослідницькі програми щодо розробки інструментів та прототипів у сфері посилення кіберзахисту та його складових. Серед перспективних спільних заходів у сфері посилення кібербезпеки виділяються: залучення стартапів та науковців щодо проведення комп'ютерно-технічних експертиз; розробки і впровадження сучасного програмного

забезпечення для виявлення і запобігання кіберзагрозам на ранніх стадіях; постійний моніторинг кіберпростору; підготовка галузевих фахівців, розробка та сприяння реалізації освітніх онлайн-платформ тощо.

Висновки.

Як переконливо засвідчує статистика, станом на 2020 рік 25 % компаній – світових лідерів у сфері розробки програмного забезпечення для мобільних платформ мали свої офіси або представництва в Україні. Також в Україні працює понад чотирьох тисяч IT-компаній і понад 110 R&D центрів всесвітньо відомих міжнародних компаній. У 2019 році частка IT-індустрії в українській економіці становила 4 % ВВП, а у цій сфері було задіяне понад 150 тисяч осіб. У той самий час, важливо розуміти, що на цьому етапі розвитку галузі вітчизняний IT-ринок переважно працює на аутсорсі. Тобто надає послуги іноземним компаніям і не надто поспішає у створенні власних технологічних компаній. Саме через нерозвиненість в Україні компаній, які програмують для власних продуктів, та відсутність технологічних дослідницьких центрів оцінка вітчизняного IT-ринку досить низька, порівнюючи із світовими.

На цьому фоні в рамках розбудови державно-приватного партнерства актуальним завданням залишається консолідація зусиль та посилення спроможностей складових сектору безпеки і оборони України та недержавного сектору, особливо під егідою Національного координаційного центру кібербезпеки при РНБО України, який відіграє провідну роль у питаннях розбудови державно-приватного партнерства.

В Україні на ринку кібербезпеки діє досить багато асоціацій, IT-компаній, структур громадянського суспільства, які мають значний досвід і техніко-технологічні напрацювання в зазначеній сфері, надають послуги з виявлення комп'ютерних атак, розслідування обставин виявлених інцидентів, формування доказів при виконанні обстеження комп'ютерних систем і проведенні комп'ютерних експертиз. Чимало вітчизняних IT-компаній, які посіли міцні позиції в зазначеній сфері, не тільки демонструють високу ефективність, напрацювали багаторічний досвід, мають значний штат компетентних фахівців та експертів необхідної кваліфікації, але й проявляють зацікавленість у розширенні своєї діяльності, опануванні нових сегментів ринку послуг кібербезпеки. Серед них можна виділити такі: Українська міжбанківська асоціація членів платіжних систем "ЄМА", Інтернет Асоціація України, Українська Антипіратська Асоціація, Всеукраїнська асоціація "Інформаційна безпека та інформаційні технології", громадська організація ISACA, Об'єднання підприємств "Український мережевий інформаційний центр", Платформи громадянського суспільства "Україна – ЄС", Центр реагування на комп'ютерні надзвичайні події "CERT", IT-компанія "Linkos Group", IT-компанія "Eset", Експертно-правова консалтингова компанія "ЮрЕкс", Київський експертно-дослідний центр тощо. Тому ще одним перспективним напрямом у зазначеному контексті видається залучення спеціалістів та експертів комерційних IT-структур з метою використання сучасного обладнання та програмного забезпечення щодо збору цифрових доказів і проведення комп'ютерно-технічних експертиз, що дасть змогу спільно з правоохоронними органами створювати потужні спеціалізовані криміналістичні лабораторії з метою виконання експертиз будь-якої складності.

Враховуючи сучасні засади та перспективні тенденції реформування цивільного сектору безпеки, на сьогодні важливим завданням держави є врегулювання питання державно-приватного партнерства у сфері кібербезпеки на законодавчому рівні. Тому актуалізується важливість питань кібербезпеки при розгляді системних дій держави у секторі безпеки за сучасних умов. Тобто доцільно розвивати державно-приватне партнерство у сфері забезпечення кібербезпеки, зміцнювати правову основу такої

співпраці. Необхідно прискорити діяльність за такими напрямами: врегулювати на законодавчому рівні питання щодо: посилення державно-приватного партнерства у сфері кібербезпеки, визначення форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері, залучення на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення нормативно-правових актів, нормативних документів та стандартів у цій сфері; стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури; співпраці всіх суб'єктів забезпечення кібербезпеки, зокрема в рамках державно-приватного партнерства, задля досягнення стратегічних цілей, заснування ініціатив, вироблення узгоджених планів та проектів у сфері кібербезпеки.

Розбудова державно-приватного партнерства у сфері забезпечення кібербезпеки має відбуватися за такими перспективними напрямами: укладання та забезпечення виконання партнерських угод за участю держави та провідних вітчизняних ІТ-компаній, у тому числі й зарубіжних; формування відповідного профільного законодавства, що передбачає розробку вітчизняних правових норм, якими повинні регулюватися процедурні питання участі недержавних структур у зборі цифрових даних та доступу до електронних доказів, порядок та умови державної атестації й сертифікацій таких компаній тощо.

Актуальним питанням залишається необхідність узгодження між державою та інституціями громадянського суспільства питань активізації залучення інвестицій у цивільний сектор кібербезпеки, покращення фахової підготовки спеціалістів у цій сфері, спільної діяльності щодо організації дієвого кіберзахисту, сприяння держави розвитку краудсорсингу в Україні, підвищення довіри та досягнення порозуміння у відносинах державно-приватного партнерства. Держава має проводити постійний моніторинг громадської думки в питаннях забезпечення кібербезпеки, зокрема за допомогою прогнозів-опитувань, соціологічних досліджень та технологій контент-аналізу.

Використана література

1. Гребенюк М.В., Леонов Б.Д. Досвід Їзраілю у сфері забезпечення кібербезпеки *Інформація і право*. № 2(25)/2018. С. 45-50.

2. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

3. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки ТНУ ім. В.І. Вернадського. Серія: "Державне управління"*. 2018. № 3. Т. 29(68). С. 57-61.

4. Прав Р.Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. *Інвестиції: практика та досвід.* 2019. № 21. С. 143-150.

5. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/ boz_2014_2_44

6. The SANS (SysAdmin, Audit, Network and Security). URL: https://www.sans.org/about

7. National Cyber Security 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 342.951

ШЕВЧЕНКО В.П., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/ 0000-0001-5095-1160.

ІМПОРТОЗАМІЩЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ВАЖЛИВА СКЛАДОВА ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Анотація. *Досліджено загрози поширення діяльності китайської корпорації Huawei на американському та європейському цифровому ринках. Деталізовано перспективи глобального впровадження технологій нового покоління 5G. Проаналізовано законодавство окремих держав світу щодо запровадження імпортозаміщення програмного забезпечення та технологічної продукції, особливо для потреб державного сектору. Визначено загальносвітові тенденції посилення кібербезпеки за напрямом ліквідації технологічної залежності від іноземних виробників інформаційно-комунікаційних технологій. Узагальнено засади вітчизняної державної політики у сфері імпортозаміщення програмного забезпечення та технологічного розвитку. Окреслено шляхи удосконалення вітчизняного ІТ-ринку та визначено його внесок у справу забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, інформаційно-комунікаційні технології, софт, імпортозалежність, програмне забезпечення, критична інфраструктура, технології 5G, ІТ-аутсорсинг.*

Summary. *The threats of Chinese Huawei's activity in the American and European digital markets have been studied. Prospects for the global implementation of new generation 5G technologies are detailed. The legislation of some countries on the introduction of import substitution programs for software and technological products, especially for the needs of the public sector, is analyzed. Global trends in strengthening cyber security in the direction of eliminating technological dependence on foreign manufacturers of information and communication technologies have been identified. The principles of domestic state policy in the field of software import substitution and technological development are generalized. The directions of improvement of the domestic IT-market and its contribution to cyber security are outlined.*

Keywords: *cybersecurity, cyberattack, information and communication technologies, software, import dependence, software, critical infrastructure, 5G technology, IT-outsourcing.*

Аннотация. *Исследованы угрозы распространения деятельности китайской корпорации Huawei на американском и европейском цифровых рынках. Детализированы перспективы глобального внедрения технологий нового поколения 5G. Проанализировано законодательство отдельных государств мира в отношении внедрения импортозамещения программного обеспечения и технологической продукции, особенно для нужд государственного сектора. Определены общемировые тенденции усиления кибербезопасности по направлению ликвидации технологической зависимости от иностранных производителей информационно-коммуникационных технологий. Обобщены основы отечественной государственной политики в сфере импортозамещения программного обеспечения и технологического развития. Очерчены направления усовершенствования отечественного ИТ-рынка и определен его вклад в дело обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, информационно-коммуникационные технологии, софт, импортозамещение, программное обеспечение, критическая инфраструктура, технологии 5G, ИТ-аутсорсинг.*

Постановка проблеми. Цифрова трансформація, яка є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури, які призначені для забезпечення задоволення життєво важливих потреб громадянина, особи, суспільства і держави, є недостатньо захищеними від кібератак. На цьому фоні, останнім часом спостерігається висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і не задекларованих функцій у такому обладнанні та значно звужують вітчизняні спроможності протидії кіберзагрозам. Також значна частина підприємств, установ та організацій усіх форм власності не забезпечують надійний кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі.

У сучасному світі безперервно збільшується кількість кібератак, спрямованих на викрадення персональних та інших конфіденційних даних громадян та організацій із використанням методів соціальної інженерії. Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних, у першу чергу, країні-агресору та іншим країнам. Збільшення інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах створило глобальний ринок для розвитку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет. Усе частіше спрямовані кібератаки не здійснюються безпосередньо на уряди країн та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до значної кількості їх клієнтів та завдання масштабної шкоди. Популярні веб-сайти, соціальні мережі збирають велику кількість різноманітних персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

Зазначене провокує прискорення розробки та впровадження на державному рівні програмних документів, які б визначали умови та порядок здійснення імпортозаміщення у вітчизняній галузі ІТ-технологій. Проте основна проблема – відсутність чіткої стратегії розвитку високотехнологічних галузей на державному рівні, що визначає пріоритети держави у даній сфері. Окрім того, законодавство України також потребує вдосконалення на основі вивчення кращих світових та європейських практик у цій площині. За таких умов актуальним та доцільним є розгляд проблемних питань імпортозаміщення програмного забезпечення у сфері інформаційних технологій з метою визначення дієвих кроків, практична реалізація яких сприятиме посиленню стану кібербезпеки держави.

Результати аналізу наукових публікацій. Сучасний стан, особливості та тенденції розвитку вітчизняного ринку високих технологій досліджували у наукових працях: Р. Винничук [1], О. Журавльов [2], І. Кораблінова [3], І. Новаківський [4], М. Чайковська [5] та інші. Окремі питання правового забезпечення безпеки у кіберпросторі вивчали такі

фахівці, як: О. Баранов [6], М. Гребенюк [7], І. Доронін [8], В. Шеломенцев [9] тощо. Проте висвітлення передового іноземного досвіду та сучасних зарубіжних законодавчих практик у сфері подолання технологічної залежності від імпортної продукції ІКТ та програмного забезпечення, пошуку ефективних й оптимальних моделей уникнення імпортної залежності, особливо в умовах масштабного впровадження системи рухомого (мобільного) зв'язку п'ятого покоління – 5G, як важливої складової забезпечення кібербезпеки держави, жоден із вказаних авторів не здійснював, що посилює актуальність обраної теми цієї наукової публікації.

Метою статті є визначення заходів, які вживаються державами світу для уникнення та подолання імпортозалежності програмного забезпечення та цифрових технологій щодо посилення спроможностей у сфері кібербезпеки, особливо в умовах світової пандемії COVID-19.

Виклад основного матеріалу. Якщо раніше держави світу конкурували за право володіти природними ресурсами та землями, то в сучасному геополітичному просторі усі країни прагнуть отримати доступ та домінувати у сфері передових цифрових технологій, оскільки революційна технологічна перевага – це гарантія прориву у всіх інших сферах, від освіти до безпеки і оборони, від охорони здоров'я до запуску космічних об'єктів. На фоні глобального поширення пандемії COVID-19, світовий цифровий ринок зіткнувся із необхідністю перебудовувати технологічні та бізнес-процеси у відповідності до нових санітарних норм й стандартів. При цьому, у пріоритеті залишаються рішення, які сприятимуть швидкому, безпечному та ефективному процесу організації дистанційної роботи.

Важливим комбінованим показником, який характеризує досягнення країн світу з позиції розвитку інформаційно-комунікаційних технологій (далі – ІКТ) є "Індекс інформаційно-комунікаційних технологій" (ICT Development Index), який було запроваджено ще у 2007 році. У 2017 році перше місце у цьому рейтингу посідала Ісландія, 5-е місце Великобританія, 15-е місце Франція, 16-е США. За прогнозами експертів, до 2025 року глобальна ІТ-індустрія буде біполярною: американські та деякі європейські гіганти протистоятимуть компаніям з КНР, Південно-Східної Азії, Індії та РФ. Китай мріє про світове лідерство у сфері цифрових технологій, у зв'язку з чим активно залучає інвестиції у власне виробництво процесорів, власних операційних систем, мікрочипів, розробляє та запускає власні месенджери та є державою закритою від зовнішнього технологічного впливу. На сьогодні, одним із прикладів такого суперництва є запуск бездротових мереж формату 5G. Беззаперечно, новий стандарт не просто покращить роботу стільникового зв'язку, але й відкриває безпрецедентні можливості для розвитку Інтернету речей. Це дозволить оперативно управляти інфраструктурою, енергетикою, здійснити прорив у сфері штучного інтелекту, безпілотного транспорту та машинного навчання. Очікується, що до 2025 року кількість користувачів 5G досягне 1,2 млрд. осіб, при цьому третина з них буде знаходитися саме у Китаї. Китайська компанія "Huawei" найбільш просунулася на ринку високих технологій у цьому сегменті, виступає основним постачальником обладнання для забезпечення роботи нового стандарту навколо світу. Жодна інша компанія у світі не може продемонструвати такі колосальні успіхи. Тобто промислова політика Пекіну виводить КНР на роль світового лідера у сфері високих технологій, що провокує занепокоєння з боку інших великих держав світу (США, РФ, Великобританія).

У США політикум неодноразово повідомляв, що діяльність "Huawei" представляє суттєву загрозу усьому світу. Навіть у 2018 році президент США Д. Трамп підписав указ, яким заборонив використання урядовими відомствами продукції цієї компанії. У

подальшому адміністрація Д. Трампа неодноразово виступала за недопущення “Huawei” до запуску 5G через побоювання щодо використання цією китайською компанією у своїх продуктах бекдорів (“уразливостей”), які можуть сприяти відстеженню трафіка, який проходить по мережам. Тобто, на випадок глобальної кібервійни компанія зможе відключити своє обладнання, таким чином, заблокувавши роботу усієї критичної інфраструктури. Навіть у травні 2019 року китайська компанія “Huawei” була внесена Міністерством торгівлі США у чорний список. Американським підприємствам було заборонено здійснювати реалізацію бізнес-проектів з китайським IT-гігантом, а щоб продавати йому продукцію вимагалися особливі ліцензії. Тобто вже понад два роки компанія Huawei бойкотується в США та перебуває у “чорному списку” завдяки звинуваченням у можливій співпраці зі спецслужбами КНР. Запроваджені Вашингтоном санкції фактично спрямовані на обмеження доступу цієї компанії до напівпровідників, які є конче необхідними для виробництва телекомунікаційного обладнання та відповідного програмного забезпечення, включаючи мережі 5G. У рамках посилення інституційних спроможностей забезпечення кібербезпеки на початку 2019 року керівники трьох американських спецслужб ЦРУ, АНБ і ФБР офіційно заявили, що смартфони “Huawei” та “ZTE” можуть стежити за користувачами. У зв’язку із оприлюдненням цієї інформації, розвідувальна служба Нової Зеландії відхилила запит постачальника телекомунікацій щодо використання обладнання “Huawei” 5G, а Австралія заборонила “Huawei” постачати обладнання для платформи 5G. Обидві країни назвали підставами для таких заходів наявні загрози національній безпеці.

Проте у сучасному світі є держави, які більш-менш лояльно ставляться до імпортозаміщення у сфері телекомунікацій та цифрових технологій. Так, політична влада Франції не запровадила повної заборони на використання обладнання китайської компанії Huawei з метою розгортання мереж 5G. Наприклад, на переконання британської розвідки, існують серйозні ризики використання китайського обладнання та програмного забезпечення, особливо на військових об’єктах, атомних електростанціях та в інших стратегічних галузях, хоча британські спеціалісти здатні проконтролювати Huawei та запобігти встановленню шпигунського обладнання. Проте фінальне рішення, яке було схвалено на засіданні британської ради безпеки, надало цій китайській компанії доступ у розмірі квоти 35 % усього ринку телекомунікацій. Хоча компанію “Huawei” не допускатимуть до таких ключових об’єктів британської національної інфраструктури, а також на особливі військові та ядерні об’єкти. Будь-яке обладнання компанії має бути сумісними з розробками інших учасників проекту, такими як шведський “Ericsson” або фінський “Nokia”. У 2019 році 5G розпочав функціонувати у Великобританії, проте покриття мережі залишається досить низьким.

На переконання провідних експертів світу, техніка виробництва компанії “Huawei” нібито має “чорні двері”, які дають китайським спецслужбам доступ до зашифрованих даних пристроїв, хоча Пекін це заперечує. Таким чином, низка держав, зокрема: США, Канада, Австралія, Великобританія та Японія, наклали значні обмеження на сфери впливу компанії “Huawei” через побоювання, що використання продукції компаній зробить їхні мережі вразливими для проникнення та шпигунства ззовні. У Пекіні вбачають у такому вибірковому ставленні в ЄС до “Huawei” прояв недобросовісної конкуренції, оскільки після запровадження масштабних санкцій проти цієї китайської корпорації з боку США, багато країн Євросоюзу почали з побоюванням сприймати діяльність китайців в Європі.

Викладене дає підстави констатувати, що у 2020 році технологічний суверенітет став питанням номер один у глобальному порядку денному на фоні різкого

технологічного протистояння між США та КНР, а європейські держави вкладають €10 млрд. у розробку власної інфраструктури Хмарних технологій та програмного забезпечення. Хоча деякі держави світу активно розвивають та впроваджують політику імпортозаміщення іноземного програмного забезпечення та технологічного оснащення на вітчизняний софт, особливо для потреб державного сектору, оскільки задоволення внутрішнього попиту безальтернативно роками відбувалося виключно за рахунок імпортних поставок. При цьому, імпортозаміщення у сфері ІТ зростає переважно на фоні запроваджених регуляторних та стимулюючих заходів з боку держави.

Так, у РФ сфера інформаційних технологій вважається однією із найбільш залежних від імпорту та уразливих, оскільки відбувається масштабне користування комп'ютерами та сервісами, які вироблені виключно на імпортних компонентах, системному та прикладному програмному забезпеченні переважно іноземного походження. Уряд РФ заборонив державним органам та установам купувати зарубіжне програмне забезпечення при наявності вітчизняних аналогів. У зв'язку з цим держава-агресор планувала до кінця 2021 року в ІТ-інфраструктурі для усіх федеральних та регіональних органів влади запровадити на 80 % вітчизняне програмне забезпечення. Причинами для цього стали ініціативи уряду РФ ще у 2015 році, спрямовані на поступову заборону закупівлі зарубіжного програмного забезпечення для органів влади та адаптацію плану поступового переходу органів державного управління та державних корпорацій на вітчизняний софт. Оскільки софт розроблено компанією, яка відноситься до юрисдикції іншої країни світу, то завжди є вірогідність того, що масив даних, який проходить через відповідне програмне забезпечення можуть потенційно перейти у розпорядження "третіх осіб", що для державних компаній є неприйнятим. У грудні 2020 році була встановлена вимога у розмірі 50 % комп'ютерної техніки та програмного забезпечення вітчизняного виробництва, які мають працювати у державному секторі, а з 2023 року цей показник має зрости до 70 %.

Російське походження програмного забезпечення та софту підтверджується його включенням до Єдиного реєстру радіоелектронної продукції РФ. Очікується, що у перспективі політика, направлена на розвиток вітчизняного виробництва ІТ-продукції сприятиме нарощуванню темпів у цій площині, а державні підприємства мають придбати технологічну продукцію саме внесену до цього реєстру. Оскільки основна проблема інформатизації обумовлена низьким рівнем впровадження вітчизняних розробок програмного забезпечення, це певним чином впливає на загальний рівень цифровізації. Тому держава-агресор активно впроваджує політику імпортозаміщення інформаційних технологій на власне ПЗ як цілеспрямований системний курс з метою створення перспективних вітчизняних цифрових рішень до 2025 року. На переконання політичного керівництва РФ, перехід органів державної влади та державних компаній на вітчизняні програмні продукти відкриває нові можливості, зміцнює економіку та створює фундамент для створення цифрового майбутнього.

Розробка та впровадження засад державної політики імпортозаміщення програмного забезпечення також актуальна і для Казахстану. Метою її реалізації є стимулювання вітчизняної ІТ-галузі шляхом надання доступу до фінансових інструментів, які відповідають специфічним умовам її розвитку [10]. В сучасних умовах сфера інформаційно-комунікаційних технологій залишається однією із найбільш динамічно розвинутих галузей казахської економіки. У 2021 році заплановано внесення змін до законодавчої бази цієї країни у сфері закупівлі та розробки програм імпортозаміщення та відповідного фінансування за такими напрямками: заміна раніше придбаного зарубіжного програмного забезпечення та вітчизняне; проведення аналізу усіх програмних продуктів,

іноземного походження, що використовуються в органах державної влади та управління. Також у 2020 році було розроблено та схвалено спрощений механізм списання іноземного програмного забезпечення. На його виконання було вирішено провести аналіз усіх програмних продуктів, які використовуються в державних компаніях, та визначити детальний план поетапної їх заміни з урахуванням показників економічного ефекту. Отже, Казахстан робить поступальні кроки у напрямку зниження технологічної залежності від іноземного програмного забезпечення.

Для України питання імпортозаміщення програмного забезпечення також є одним із пріоритетних. Указом Президента України від 30 вересня 2019 року [11] з метою забезпечення національних інтересів України щодо сталого розвитку економіки, громадянського суспільства і держави визначено Цілі сталого розвитку України на період до 2030 року. Одним із пріоритетів визначено створення стійкої інфраструктури, сприяння всеохоплюючій і сталій індустріалізації та інноваціям. За таких умов, держава має поступово запроваджувати ефективні інституціональні механізми для розвитку високотехнологічних галузей, створювати сучасну інформаційно-комунікаційну інфраструктуру, стимулювати розвиток новітніх перспективних та випереджальних технологій та забезпечити суттєве зменшення імпортної залежності вітчизняного високотехнологічного сектору.

11 листопада 2020 року Уряд України ухвалив Розпорядження, яким затвердив план заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління 5G [12]. Документ встановлює перелік необхідних заходів для забезпечення впровадження в Україні системи 5G та забезпечує їх проведення. Основними функціональними особливостями мереж 5G є вдосконалений мобільний широкосмуговий доступ до Інтернету та наднадійні комунікації з низькою затримкою, на основі яких будується все різноманіття послуг і можливостей нових мереж 5G.

До таких послуг і можливостей належать: висока швидкість передачі даних, промислова автоматизація, зв'язок при надзвичайних ситуаціях тощо. Технологія 5G дозволяє використовувати мережу Інтернет, швидкість якого перевищує 4G у 10-20 разів, а в деяких випадках швидкість 5G може бути більшою навіть у 100 разів. У провідних технологічних компаніях світу – в США, Японії, Південній Кореї та КНР – сподіваються, що технологія 5G значно прискорить розвиток інших технологій, таких як "розумне місто", безпілотні автомобілі тощо.

Для України велике значення має розвиток ринку IT-аутсорсингу. Україна є лідером серед країн – аутсорсерів в Європі. Проте вітчизняна IT-галузь України – це не тільки аутсорсинг. Вітчизняні технологічні стартапи створюють продукти міжнародного рівня, які визнають у всьому світі. Наприклад, український стартап "Reface" потрапив в список рекомендованих від "Google". Проте такі випадки поодинокі. На переконання вітчизняних експертів, 90 % наших IT-спеціалістів працюють саме на засадах аутсорсингу, а не як розробники власних IT-продуктів. Розвитку IT-технологій в нашій країні сприятиме здійснення комплексу заходів, спрямованих на використання у всіх сферах діяльності не лише ліцензійного програмного забезпечення, але і переважно вітчизняного, що, у свою чергу, потребує активізації зусиль у напрямку розробки власних напрацювань та їх запровадження, перш за все, в органах державної влади та на державних стратегічних підприємствах.

Проте останнім часом, пріоритети вітчизняної політики щодо розвитку ІКТ в Україні певним чином стали незрозумілими для наших стратегічних партнерів, особливо США. Так 15 жовтня 2020 року стався резонансний випадок. Проблема полягає у тому, що Держспецзв'язку України підписав меморандум про співпрацю з китайською

компанією “Huawei”, ігноруючи побоювання та відкриту позицію політичного керівництва США щодо глобальної загрозливої діяльності цієї корпорації. На своє виправдання Держспецзв’язку офіційно повідомив, що цей меморандум сприятиме розбудові відповідної платформи з метою впровадження ефективних механізмів державно-приватного партнерства з будь-якими компаніями, які представлені на вітчизняному ринку, у тому числі й компанією “Huawei”. Таким чином, Державна служба спеціального зв’язку порушила законодавство України, підписавши меморандум про співпрацю з компанією “Huawei” без координації та узгодження із зовнішньополітичним відомством України. Укладання вказаного меморандуму стало наслідком негативної реакції з боку міжнародних партнерів, з якими наша країна працює над зміцненням кібербезпеки, що у свою чергу, викликало обурення представників світової спільноти, спричинило потужний удар по іміджу України на міжнародній арені.

Висновки.

Останні світові тенденції демонструють посилення конкуренції між країнами за збереження існуючого ІТ-бізнесу та залучення нових іноземних та локальних інвесторів в цифрову економіку. Держави шукають оптимальні шляхи збереження та підвищення своєї конкурентоздатності на світовому ринку. На цьому фоні у сучасному світі відбувається геополітичне протистояння у кіберпросторі між великими гравцями (США, КНР, РФ) у боротьбі за світове домінування та лідерство. На цьому фоні ситуація, що склалася у вітчизняній ІТ-сфері є досить непростою. На жаль, вітчизняні програмні продукти нездатні замінити зарубіжні аналоги, хоча поступальні кроки у цьому напрямку активно здійснюються. Чимало держав світу законодавчо обмежують використання імпортного програмного забезпечення, особливо у державному секторі, стимулюючи активізацію власних ІТ-розробок та продуктів у цьому сегменті.

Українська ІТ-індустрія все ще перебуває на стадії зародження та розвитку і має потенціал необмеженого зростання в майбутньому. Вітчизняний ІТ-ринок характеризується позитивною тенденцією до зростання показників його прибутковості: у 2019 році вона дорівнювала за обсягами $5 млрд. Хоча сфера інформаційних технологій вважається однією із найбільш залежних від імпорту, оскільки в сучасних умовах досить часто використовуються комп’ютери та сервіси, вироблені виключно за рахунок імпортних компонентів, системного та прикладного програмного забезпечення іноземного походження. Враховуючи викладене, для України в сучасних умовах актуальним залишається визначення концептів державної політики імпортозаміщення, особливо в умовах поширення масштабів пандемії та зростання ролі та значення цифрових технологій для держави, суспільства та пересічених громадян.

Тому доцільним є прискорення розробки та формування правових основ щодо визначення пріоритетних засад імпортозаміщення програмного та технологічного забезпечення власними аналогами на фоні загального розвитку цифрової економіки та зростання частки високотехнологічних продуктів та послуг власного виробництва, що передбачає, зокрема, прискорення прийняття законопроекту “Про стимулювання розвитку цифрової економіки в Україні” від 02.11.20 р. № 4303 [13]. Цей законопроект спрямований на формування важелів щодо стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих передумов для ведення інноваційного бізнесу, залучення інвестицій, розбудови вітчизняної цифрової інфраструктури. Очікується, що у випадку схвалення цього законопроекту українська ІТ-індустрія до 2025 року становитиме 10 % загального ВВП країни, яка генеруватиме у сукупності $11,8 млрд. Очевидно, що при зростанні вітчизняної ІТ-індустрії та кількості зайнятих у цій сфері фахівців, податкові надходження до державного бюджету також активно зростатимуть,

відбудеться посилення забезпечення кібербезпеки, відбудеться модельний перехід на абсолютне задоволення потреб державного сектору власними технологічними продуктами та відповідним програмним забезпеченням з метою уникнення імпортної залежності.

Використана література

1. Винничук Р.О., Склярук Т.В. Особливості розвитку ІТ-ринку в Україні: стан та тенденції. *Вісник Національного університету "Львівська політехніка". Серія: "Логістика"*. 2015. № 833. С. 3-8. URL: http://nbuv.gov.ua/UJRN/VNULPL_2015_833_3

2. Журавльов О.В., Сімачов О.А. Статистичне дослідження ринку ІТ-послуг в Україні. *Статистика України*. 2018. № 4. С. 25-33.

3. Кораблінова І.А., Кульбацька Н.М. Актуальні проблеми дослідження ІТ-ринку України. *Ефективна економіка.* 2017. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5997

4. Новаківський І.І. Розвиток вітчизняної ІТ-галузі як основа формування конкуретноздатної національної економіки. *Соціально-економічні проблеми сучасного періоду України*. 2015. Вип. 3. С. 14-18. URL: http://nbuv.gov.ua/UJRN/sepspu_2015_3_5

5. Чайковська М.П. Стратегії розвитку ІТ-ринку України в умовах фінансової кризи. *Вісник соціально-економічних досліджень*: зб. наук. праць. Вип. № 35. Одеса: ОДЕУ, 2009. С. 132-138.

6. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Інформація і право.* № 2(42)/2014. С. 54-62.

7. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право*. 2019. № 2. С. 203-207.

8. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* № 1(20)/2017. С. 104-111.

9. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_44

10. Отчет по развитию отрасли информационно-коммуникационных технологий в Республике Казахстан в 2019 году. URL: https://zerde.gov.kz/upload/Отчет%20ИКТ%20отрасли%202019.pdf

11. Про Цілі сталого розвитку України на період до 2030 року: Указ Президента України від 30.09.19 р. № 722/2019. URL: https://zakon.rada.gov.ua/laws/show/722/2019#Text

12. Про затвердження плану заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління: Розпорядження Кабінету Міністрів України від 11.11.20 р. № 1409. URL: https://zakon.rada.gov.ua/laws/show/1409-2020-р#Text

13. Про стимулювання розвитку сфери інформаційних технологій в Україні: проект закону України від 18.11.20 р. № 4303-2. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70474

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 338.246.8

ПРАВДЮК А.Л., *кандидат юридичних наук,* доцент кафедри права
Вінницького національного аграрного університету.
ORCID: https://orcid.org/0000-0002-5248-8111.

ОСОБЛИВОСТІ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджуються трансформаційні процеси, які відбуваються у сфері законодавчого забезпечення економічної безпеки України. Робиться наголос на потребі кардинального перегляду державної політики та системи управління. Проаналізовано досвід держав-членів ЄС і НАТО у сфері законодавчого забезпечення економічної безпеки, а також виявлено недоліки нормативно-правового регулювання забезпечення економічної безпеки України та запропоновано шляхи та напрямки її покращення.*

Ключові слова: *економічна безпека, забезпечення економічної безпеки, законодавство у сфері економічної безпеки.*

Summary. *The article examines the transformation processes taking place in the field of legislative support of economic security of Ukraine. Emphasis is placed on the need for a radical overhaul of public policy and governance. Such a system should be built based on the goals and principles of economic security by creating a modern regulatory framework. Taking into account Ukraine's European integration, the article also analyzes the experience of EU and NATO member states in the field of economic security, as well as identifies shortcomings in the regulation of Ukraine's economic security and suggests ways and directions to improve it.*

Keywords: *economic security, ensuring economic security, legislation in the field of economic security.*

Аннотация. *В статье исследуются трансформационные процессы, происходящие в сфере законодательного обеспечения экономической безопасности Украины. Определяется необходимость кардинального пересмотра государственной политики и системы управления. Анализируется опыт государств-членов ЕС и НАТО в сфере законодательного обеспечения экономической безопасности, а также выявлены недостатки нормативно-правового регулирования обеспечения экономической безопасности Украины и предложены пути и направления ее улучшения.*

Ключевые слова: *экономическая безопасность, обеспечение экономической безопасности, законодательство в сфере экономической безопасности.*

Постановка проблеми. Економіка України протягом останніх 10 років не забезпечувала досягнення національних економічних інтересів. Упродовж 2010-2019 років стан економічної безпеки оцінювався як незадовільний із погіршенням показників практично за усіма складовими до небезпечного рівня. Середнє значення рівня економічної безпеки за цей період становило 40 % (зона рівня незадовільного стану). У 2019 році рівень економічної безпеки України склав 43 %, а за підсумками першого півріччя 2020 року – 41 % відповідно. Тобто рівень всіх основних складових економічної безпеки залишався низькими, що зберігає високі ризики масштабних явищ дестабілізації у розвитку економіки у довгостроковій перспективі [1; 2]*.

Негативний вплив на рівень економічної безпеки України чинять: тіньова економіка, яка складає 50 % від реального ВВП країни, що пов’язана зі скороченням надходжень до

* За розрахунками, відповідно до Методичних рекомендацій щодо розрахунку рівня економічної безпеки України, затверджених наказом Мінекономіки від 29.10.13 р. № 1277.

бюджету внаслідок несплати податків; високий рівень бідності працюючого населення; низький рівень дотримання чинного законодавства і, як наслідок, втрата довіри населення до правоохоронної та судової систем держави; низький рівень соціальної захищеності громадян; погіршення зовнішньоторговельного балансу; низькі обсяги іноземних інвестицій; проблема зайнятості населення; залежність від забезпечення країни енергоносіями; незаконний вивіз капіталу з України; погіршення демографічної ситуації; експорт товарів з низькою часткою доданої вартості тощо [3, с. 302-304]. Наразі внутрішній та зовнішній борг України (на лютий 2021 року) складає 2.552.963,1 млн. грн., при цьому 1.490.55,0 млн. грн. – зовнішній борг, а 1.063.908,1 млн. грн. – внутрішній борг [4].

Сучасний стан економіки в цілому та її галузей, нові виклики вимагають пошуку неординарних і негайних рішень, зокрема потребує проектування новітніх систем забезпечення економічної безпеки з урахуванням історичних основ та сучасних тенденцій розвитку економічних відносин.

Результати аналізу наукових публікацій. У науковій літературі є чимало робіт, присвячених вивченню проблем економічної безпеки, що так чи інакше торкаються досліджуваної теми статті. Це праці З. Варналій, В. Васенко, Т. Воронкової, В. Геєць, В. Зализко, О. Кириченко, О. Линник, В. Ляшенко, І. Матвєєва, В. Малишко, Л. Малюти, В. Прозорової, О. Рудої, Т. Сак, А. Ульянченко, Ю. Харазішвілі, О. Чубукової та інших.

Істотно поглиблюється розуміння процесів, що відбуваються навколо проблеми забезпечення економічної безпеки країн-членів ЄС і НАТО завдяки працям З. Гбур та М. Денисенко, які узагальнили зарубіжний досвід, виявили проблеми та окреслили перспективи розвитку у досліджуваній сфері.

Проте слід зазначити, що у останніх роках практично не було праць, які стосуються вирішення проблем якісного законодавчого забезпечення економічної безпеки України.

Метою статті є виявлення особливостей, проблем та окреслення перспектив розвитку законодавчого забезпечення економічної безпеки України.

Виклад основного матеріалу. У системі національної безпеки України економічна безпека є її фундаментом і матеріальною основою, а забезпечення економічної безпеки є винятковою прерогативою держави. У практичному плані забезпечити економічну безпеку країни означає створити певну систему її самозбереження, що автоматично приводила б у рух її механізми захисту від тієї або іншої загрози [5, с. 130].

Механізм забезпечення економічної безпеки держави, за Ставицьким О.В., має складатися з виявлення загроз економічній безпеці в сучасних умовах; визначення об’єктів захисту; прогнозування та аналізу механізмів реалізації загроз; визначення компетенції і відносин суб’єктів, які здійснюють діяльність по захисту; формування системи правових, організаційно-економічних та інших заходів; протидія загрозам економічної безпеки і локалізація їх негативних наслідків. Всі наявні проблеми і ті, які можуть виникнути у перспективі, повинні бути ув’язані в єдиний системний процес, спрямований на досягнення не розрізнених, а взаємопов’язаних основних цілей, на конкретні шляхи розвитку і інтенсифікації економіки у державі [6].

Сак Т.В. вважає, що задля економічної безпеки має бути досягнуто таких показників: “1. Економічна незалежність (фінансова, сировинно-ресурсна, інноваційна тощо); 2. Економічна стабільність (рівень розвитку, що гарантує відчуття безпеки сьогодні та в майбутньому); 3. Економічний розвиток (інноваційно-інвестиційна активність, реструктуризація, фінансове оздоровлення)” [7]. Пріоритетним при цьому має бути збалансована політика держави щодо структурної перебудови економіки, стимулювання інноваційно-інвестиційної активності, розвитку підприємництва, пришвидшення

інтеграційних процесів тощо. Саме тому економічну безпеку варто розглядати не лише як стан захищеності національних інтересів, але і наявність й можливість застосування інструментів впливу на економічні процеси для гарантування добробуту в довгостроковому періоді [8].

Узагальнюючи праці багатьох дослідників [9] слід зазначити, що деякі з них або дуже вузько розглядають функціональну предметну область системи економічної безпеки, або надмірно широко. Немає серед авторів абсолютної згоди у баченні окремих складових економічної безпеки. Так, до внутрішніх компонентів системи економічної безпеки вони відносять: сировинно-ресурсну, енергетичну, фінансову, воєнно-економічну, технологічну, продовольчу, соціальну, демографічну, екологічну, інформаційну, інноваційно-технологічну, інвестиційну, науково-технологічну, виробничу, тіньову економіку, політичну, військову і правоохоронну, кримінальну, безпеку підприємництва, безпеку підприємства, прісноводну, медичну, трудоресурсну, транспортну, промислову, інституційну, макроекономічну, зовнішньоекономічну.

Феноменом економічної безпеки як поліскладної системи з багаторівневою і багатоаспектною структурою Чубукова О.Ю. та Воронкова Т.Є. виділяють сукупність взаємопов'язаних структурних підсистем – вертикальних (економічна безпека індивідууму (базовий рівень); корпоративна економічна безпека підприємств, організацій, установ, господарств (мікрорівень); економічна безпека регіонів в тому числі транскордонна економічна безпека (мезорівень); національна економічна безпека (макрорівень); міжнародна і глобальна економічна безпека (мегарівень), а також – горизонтальних (функціональних) підсистем і елементів (виробнича, фінансова, інвестиційна, інноваційно-технологічна, енергетична, науково-технічна, продовольча, соціальна та зовнішньоекономічна) [10].

Харазішвілі Ю.М. та Ляшенко В. І. пропонують концепцію економічної безпеки України розглядати як шлях до сталого промислового розвитку країни на основі збалансованого розвитку за трьома складовими: соціальна, економічна та екологічна безпека держави. Варто погодитись із думкою фахівців, що якщо країни не будуть робити кроків за всіма трьома напрямками – підтримувати економічне зростання, сприяти соціальному розвитку та прагнути до екологічної стійкості – і по досягненню компромісних рішень між ними, то малоймовірно, що такі країни далеко просунуться на шляху до сталого промислового розвитку, незалежно від рівня їх розвитку. Концепція сталого розвитку економіки, по кожному зазначеному складовому, на їх думку, має включати 7 компонентів визначення структури сталого розвитку: визначення меж безпечного існування; ідентифікація рівня сталого розвитку; визначення дисбалансу сталого розвитку; визначення впливу загроз; обґрунтування стратегічних орієнтирів; інституціональні заходи [11, с. 234].

Відповідно до Методичних рекомендацій щодо розрахунку рівня економічної безпеки України, затверджених Міністерством економічного розвитку і торгівлі України у 2013 р. до складових економічної безпеки України віднесено: макроекономічну, зовнішньоекономічну, виробничу, енергетичну, науково-технологічну, соціальну, продовольчу, фінансову, демографічну, інвестиційну. В свою чергу найважливіша підсистема економічної безпеки – фінансова безпека включає такі елементи безпеки: бюджетну, валютну, грошово-кредитну, боргову, безпеку страхового та фондового ринку [1].

Основною умовою ефективності реалізації завдань захисту економіки від реальних і потенційних загроз є прискорене реформування системи безпеки та підвищення ефективності функціонування всіх, без винятку, суб'єктів забезпечення економічної безпеки.

Відповідно до статті 17 Конституції України забезпечення економічної безпеки є найважливішими функціями держави, справою всього українського народу, а на інститути влади покладається завдання щодо забезпечення економічної безпеки держави. Отже основними суб'єктами забезпечення економічної безпеки України є функціональні і галузеві міністерства, відомства, податкові та митні служби, біржі, фонди і страхові кампанії.

Складність законодавчого забезпечення економічної безпеки України вбачається перш за все у визначенні кола реальних та потенційних загроз економічній безпеці країни. Тільки після цього можна вести мову про-успішність застосування тих чи інших шляхів реформ, оскільки без цього реалізація заходів її забезпечення неможлива.

Для формування комплексу заходів щодо боротьби з загрозами має бути економічна концепція, що осмислює ці загрози. В Україні окремі складові доктрини економічної безпеки є в Конституції України, відповідних законах, Указах Президента України тощо. Зокрема 30.09.19 р. Президентом України підписано Указ про "Цілі сталого розвитку України на період до 2030 року", серед яких: подолання бідності, голоду, досягнення продовольчої безпеки, поліпшення харчування і сприяння сталому розвитку сільського господарства; забезпечення здорового способу життя та сприяння благополуччю для всіх у будь-якому віці; забезпечення всеохоплюючої і справедливої якісної освіти та заохочення можливості навчання впродовж усього життя для всіх; забезпечення гендерної рівності, розширення прав і можливостей усіх жінок та дівчат; забезпечення доступності та сталого управління водними ресурсами та санітарією; забезпечення доступу до недорогих, надійних, стійких і сучасних джерел енергії для всіх; сприяння поступальному, всеохоплюючому та сталому економічному зростанню, повній і продуктивній зайнятості та гідній праці для всіх; створення стійкої інфраструктури, сприяння всеохоплюючій і сталій індустріалізації та інноваціям; скорочення нерівності; забезпечення відкритості, безпеки, життєстійкості й екологічної стійкості міст, інших населених пунктів; забезпечення переходу до раціональних моделей споживання і виробництва; вжиття невідкладних заходів щодо боротьби зі зміною клімату та її наслідками; збереження та раціональне використання океанів, морів і морських ресурсів в інтересах сталого розвитку; захист та відновлення екосистем суші та сприяння їх раціональному використанню, раціональне лісокористування, боротьба з опустелюванням, припинення і повернення назад (розвертання) процесу деградації земель та зупинка процесу втрати біорізноманіття; сприяння побудові миролюбного и відкритого суспільства в інтересах сталого розвитку, забезпечення доступу до правосуддя для всіх і створення ефективних, підзвітних та заснованих на широкій участі інституцій на всіх рівнях; зміцнення засобів здійснення й активізація роботи в рамках глобального партнерства в інтересах сталого розвитку [12].

Бізнесменами-практиками, власниками та топ-менеджерами провідних українських компаній, а також експертами з метою створення комплексного документу, що визначає інституційну здатність на системному рівні підтримувати послідовну реалізацію національно-державних інтересів в економічній сфері, наявні та потенційно можливі загрози їх реалізації, напрями і пріоритети державної політики в економічній сфері, шляхи подолання загроз економічного характеру у 2019 році була розроблена доктрина економічної безпеки України як складова національної безпеки і оборони. Документ зареєстровано у Верховній Раді України від 05.05.20 р. за № 3433 як проект закону про внесення змін до Закону України "Про національну безпеку України" [13]. Однак, законопроект було відхилено, оскільки визнано, що "доктрина" – документ більш загального характеру у порівнянні зі стратегією, а тому її прийняття на основі Стратегії

національної безпеки визначено недоцільним. Крім того членами Ради національної безпеки і оборони України підтримано проект нової Стратегії національної безпеки України, якою передбачено розроблення Стратегії економічної безпеки, а 10 березня 2021 року на черговому засіданні Кабінету Міністрів України схвалено проект Стратегії економічної безпеки України на період до 2025 року [14]. Проект розроблений на виконання п. 66 Стратегії національної безпеки України "Безпека людини – безпека країни", затвердженої Указом Президента України від 14.11.20 р. № 392, та п. 3 рішення Ради національної безпеки і оборони України від 14.11.20 р. "Про Стратегію національної безпеки України".

У проекті Стратегії економічної безпеки вперше законодавчо визначено взаємоузгоджені поняття "економічна безпека", "національні економічні інтереси", "економічна стійкість" та "економічний суверенітет", а також основні виклики й загрози для економічної безпеки України та шляхи їх подолання. Проведено детальну оцінку стану економічної безпеки та ідентифіковано загрози за основними її складовими – фінансовою, виробничою, інвестиційно-інноваційною, зовнішньоекономічною, макроекономічною. Важливе місце займають виклики, пов'язані зі збройною агресією Російської Федерації та тимчасовою окупацією частини території України.

На виконання Стратегії в Україні проводяться такі заходи:

- створено Бюро економічної безпеки [15] (Закон України "Про бюро економічної безпеки України" від 28.01.21 р. № 1150-IX), який створює інституційні умови для захисту економічних процесів від тиску силових органів. Цей пункт є також одним з основоположних у векторі "верховенство права" Національної економічної стратегії. Йдеться про створення належного захисту приватної власності та рівних умов перед законом, що зрештою має призвести до підвищення кредитних рейтингів та інвестиційної привабливості нашої держави;

- ухвалено парламентом проект закону (№ 4543) про внесення зміни до розділу V "Прикінцеві та перехідні положення" Закону України "Про приватизацію державного і комунального майна" [16] щодо приватизації об'єктів великої приватизації, що має усунути певні перешкоди для відновлення приватизації великих державних підприємств. Але, слід зазначити, що ВР України за поданням КМ України не затверджено перелік об'єктів державної власності, що не підлягають приватизації, відповідно до такої ознаки як об'єкти, що забезпечують національну безпеку України або приватизація яких створює істотні ризики для безпеки держави. Наразі такий перелік не затверджено і за цих обставин надання фактично дозволу на проведення аукціонів з продажу об'єктів великої приватизації в умовах дії карантину та обмежувальних заходів щодо запобігання виникненню та поширенню коронавірусної хвороби (COVID-19) до затвердження вказаного переліку може призвести до втрати державою контролю за об'єктами, що забезпечують національну безпеку України, і приватизація яких створює істотні ризики для безпеки держави;

- вводяться податкові стимули для інвестиційних проектів зі значними інвестиціями;

- згідно із Законом України від 02.03.21 р. № 1294-IX "Про внесення зміни до пункту 4 розділу XXI "Прикінцеві та перехідні положення" Митного кодексу України щодо звільнення від оподаткування ввізним митом нового устаткування (обладнання) та комплектуючих виробів до нього, що ввозяться для реалізації інвестиційного проекту із значними інвестиціями на виконання спеціального інвестиційного договору" [17], до 1 січня 2035 року від оподаткування ввізним митом звільняється устаткування та обладнання, що ввозитиметься в Україну для реалізації інвестиційних проектів. Маємо

надію, що податкові стимули сприятимуть модернізації основних засобів на підприємствах й посиленню конкурентоспроможності виробленої в Україні продукції;

- створюються податкові умови для ведення ІТ-бізнесу в Україні. 15.04.21 р. ухвалено у першому читанні доопрацьований проект закону № 4303 "Про стимулювання розвитку цифрової економіки в Україні" який закладає основи для запровадження в країні спеціального правового режиму для ІТ-галузі, що визначає засади функціонування правового режиму "Дія City" [18], який запроваджується з метою стимулювання розвитку України як цифрової держави. Завдяки його запровадженню ІТ-індустрія має досягти 10 % у ВВП країни, а кількість робочих місць в галузі – збільшитись з нинішніх 200 тисяч до 450 тисяч до 2025 року. Вступ до "Дія City" буде добровільним. Він не обмежуватиметься територіально, а діятиме по всій країні. Основними засадами проекту закону є: свобода діяльності; невтручання держави; презумпція правомірності діяльності резидентів; стабільність (режим запроваджується мінімум на 15 років); формальний характер процедури набуття статусу резидента. Документ передбачає запровадження нової форми співпраці між компаніями та фахівцями (GIG-контракти), а також додаткові механізми захисту прав на інтелектуальну власність та інвестицій.

Україна обрала шлях до розвитку цифрової трансформації. Завдяки цьому держава не лише має підвищити продуктивність економіки, але й безпосередньо вплинути на якість життя громадян. Парламент проголосував за проект закону про внесення змін до Закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус" (№ 4355), який мав би прирівняти статус електронних паспортів до їх фізичних аналогів. Проте за висновком Головного юридичного управління Апарату Верховної Ради України законопроект не містить достатніх та завершених механізмів правового регулювання, а тому не забезпечує дотримання принципу правової визначеності як елементу конституційного принципу верховенства права. Серед недоліків, у законопроекті фактично здійснюється підміна поняття "документ, що посвідчує особу" на "засіб, за допомогою якого надається інформація про особу та підтверджується її достовірність", а також неврегульованим залишається питання щодо встановлення таких механізмів захисту персональних даних особи як: забезпечення зчитування з "е-паспортів" лише того обсягу інформації, що передбачена для них законом або згодою суб'єкта персональних даних; унеможливлення доступу до інформації про особу, яка не є його користувачем; унеможливлення зберігання інформації про особу в мобільному пристрої; використання такої інформації лише з метою, передбаченою законом; інших механізмів захисту персональних даних від несанкціонованого доступу [19].

Крім зазначеного, ухвалено пакет законопроектів щодо "податкової амністії", задля можливості активізувати капітал, що до цього не був задекларований або перебував у тіньовому секторі. Мінфін та Держмитслужба розпочали впровадження інституту авторизованих економічних операторів, а також проводиться робота над спрощенням митних процедур, що надасть можливості полегшити міжнародну торгівлю та дозволить Україні бути більш інтегрованою в європейські ринки.

З огляду на обрання Україною шляху до євроінтеграції позитивним стане досвід ряду держав-членів ЄС і НАТО у сфері законодавчого забезпечення економічної безпеки [20]. Так, у країнах Західної Європи (Німеччина, Франція, Великобританія, Італія) спеціальна законодавча база щодо забезпечення економічної безпеки відсутня, проте забезпечення економічної безпеки у цих країнах спрямоване на підтримку цивілізованих ринкових відносин, забезпечення економічного і соціального прогресу, недопущення монополізму в окремих галузях, створення умов для справедливої

конкуренції та стабільності національної валюти, захист від економічного шантажу; зниження вразливості господарської системи країни, збереження самостійності зовнішньої політики, усунення диспропорцій у рівні економічного розвитку суб'єктів господарювання; недопущення надмірної зовнішньої залежності в найважливіших секторах економіки, мінімізацію ризиків, пов’язаних із залежністю від зовнішнього світу; прогнозування і запобігання найбільш небезпечним зовнішнім і внутрішнім ризикам. При виробленні та реалізації рішень, що відносяться до забезпечення економічної безпеки, акцент робиться на спеціалізовані організації, що представляють інтереси промисловців і підприємців та на захист інтересів національних виробників на внутрішньому і зовнішньому ринках.

В Іспанії законодавча база щодо забезпечення економічної безпеки існує, в ній чітко визначено функції органів управління та організацій у цій сфері, якими розробляються спеціальні програми економічного розвитку. Нормативно-правові акти безпосередньо пов'язані з відповідним законодавством ЄС. Методи щодо забезпечення економічної безпеки захищають інтереси пріоритетних галузей промисловості, а також спрямовані на стимулювання інвестицій, забезпечення валютного контролю, на розробку законодавства про акціонерні товариства тощо.

У країнах Центральної Європи (Чехія, Болгарія, Угорщина, Польща, Словакія) немає спеціальної законодавчої бази щодо забезпечення економічної безпеки. Однак при виборі методів країни враховують геополітичну ситуацію, вектор і стратегію розвитку економіки відповідно до тенденцій регіонального та світового еволюційного процесу, напрям економічних реформ.

Серед країн Центральної Європи в Румунії питання забезпечення економічної безпеки містяться в Стратегії національної безпеки. Основними напрямами забезпечення є: здійснення ефективних заходів макроекономічної стабілізації, прискорення структурних реформ в економіці, створення приватного сектора, залучення іноземних інвестицій та підтримка малого і середнього бізнесу; узгодження фінансово-економічного законодавства, фінансової, економічної і митної політики із законодавством ЄС тощо.

В Латвії, Литві, Естонії на кшталт західних країн спеціальна законодавча база щодо забезпечення економічної безпеки відсутня. Забезпечення орієнтується на відповідні нормативно-правові акти ЄС. Методи забезпечення економічної безпеки спрямовані насамперед на реалізацію фінансово-економічної безпеки країн.

У Російської Федерації забезпечення економічної безпеки регулює Концепція національної безпеки, Державна стратегія економічної безпеки РФ, Закон РФ “Про безпеку”. Відмінною рисою законодавства є наявність регіонального аспекту щодо формування критеріїв і показників оцінки стану економічної безпеки. Методи забезпечення зорієнтовані на реалізацію економічних реформ на найближчу перспективу, зменшення небезпеки зростання нерівномірності соціально-економічного розвитку регіонів.

В Республіці Білорусь законодавчо економічна безпека відображається у Концепції національної безпеки Білорусі. До пріоритетних напрямів забезпечення економічної безпеки відносяться: розвиток системи економічних відносин, створення механізмів розв’язання виникаючих у суспільстві протиріч та скасування передумов їх виникнення; розробка стратегії забезпечення реалізації життєво важливих економічних інтересів у країні; формування довгострокової програми економічних перетворень; забезпечення сталого соціально-економічного розвитку; використання не інфляційних методів фінансування дефіциту бюджету та ефективний перерозподіл фінансових ресурсів; удосконалення зовнішньоекономічної політики; створення сприятливих умов для підприємницької діяльності та ін.

В США проблеми економічної безпеки вирішуються за допомогою дієвих методів для підтримки економічної безпеки шляхом створення ефективної законодавчої бази: Національної стратегії внутрішньої безпеки, Стратегії національної безпеки США, законами "Про економічну безпеку", "Про економічну безпеку та відтворення", "Про створення робочих місць і економічну безпеку". Крім цього діє Закон США "Про освіту для економічної безпеки" [21, с. 15-19].

Враховуючи викладене, можна зробити висновок, що в країнах з високим рівнем розвитку економіки, оцінювання рівня економічної безпеки держави не проводиться, зокрема не використовуються індикатори економічної безпеки та їх порогові значення, натомість рівень економічної безпеки визначається за показником ВВП на душу населення. Зокрема у державах-членах ЄС, США, Японії, де система забезпечення економічної безпеки держави передбачає упередження загроз, зокрема зовнішніх, які визнаються пріоритетними, оскільки негативний вплив від них значно більший ніж від внутрішніх загроз. У зазначених країнах внутрішні загрози нівелюються в зв'язку з тим, що фундаментом економічної безпеки цих країн є сильна національна економіка, здатна через ринкові механізми, а також державні інституції, механізми та важелі протистояти негативному впливу змінам ринкової кон'юнктури. Особливості забезпечення економічної безпеки держав-членів ЄС полягають в усуненні системних загроз та упередженні потенційних через підвищення макроекономічної стабілізації й підтримки внутрішньої та зовнішньої стабільності, прискорення структурних реформ в економіці, залучення іноземних інвестицій та підтримці малого і середнього бізнесу.

Натомість в Україні, як і у пострадянських країнах, застосовується інтегральна оцінка економічної безпеки держави, що вперше була запропонована російськими вченими. Проте в Росії, на відміну від України, офіційно не затверджено переліку індикаторів економічної безпеки держави та їх порогових значень, а також методики оцінювання рівня економічної безпеки. Система забезпечення економічної безпеки Росії ґрунтується на ліквідації загроз та негативних наслідків від них.

Виявлення реальних та потенційних загроз економічній безпеці держави потребує системного моніторингу макроекономічних явищ та аналізу їх впливу на рівень економічної безпеки держави. У цьому контексті, як засвідчує зарубіжний досвід, значну роль відіграють так звані "незалежні мозкові центри" (*think tank*). Зокрема, у США даними питаннями у значній мірі займається корпорація "RAND", у Нідерландах – Гаазький центр стратегічних досліджень, у Великій Британії – аналітичний центр "DEMOS". Такі мозкові центри, які існують в країнах з розвиненою економікою, на запит відповідних урядових структур, які приймають управлінські рішення, направлені на забезпечення економічної безпеки держави, на початковому етапі аналізують та про водять моніторинг ситуації, що склалася в окремому секторі безпеки, і надають попередні рекомендації. На наступному етапі створюються робочі групи із розробки сценаріїв загроз та генерування управлінських рішень. Можливість ефективної протидії зовнішнім загрозам економічній безпеці держави виникає лише за умови внутрішньої збалансованості національних економічних інтересів та здатності вчасно упереджувати внутрішні загрози економічній безпеці держави [22, с. 43-46].

Слід звернути увагу на те, що недосконале правове поле, що стосується убезпечення від загроз економічній безпеці України здатне сприяти виникненню та поширенню економічної злочинності в Україні. Серед найпоширеніших злочинів в економічній сфері на сьогодні слід назвати незаконне привласнення майна, шахрайство у сферах закупівель та управління персоналом, кіберзлочини, а також приховування величини прибутків та несплата податків; шахрайство з фінансовими ресурсами,

детермінантами виникнення яких є задуми приватних банків отримати прибутки мегарозмірів на основі маніпуляцій недосконалими правовими нормами держави; у сфері валютного ринку – приховування та зменшення продажу іноземної валюти з метою різкого збільшення ціни на іноземну валюту; штучне підвищення і утримання високих цін на товари, медикаменти і послуги та виготовлення неякісних, шкідливих для здоров'я товарів споживання тощо.

Протиправна діяльність спроможна створювати загрози економічній безпеці України. Задля виявлення і розслідування економічних злочинів має значення формування відповідного законодавства. У сучасному світі фактично сформувалася система глобалізму як специфічна форма інтеграції держав, що породжує нові закономірності розвитку економіки, культури і науки на планеті. У XXI ст. відбуваються глибинні трансформації, пов'язані з руйнуванням або виродженням традиційних соціальних структур та формування нових, глобальних. Такі трансформації змушують не просто зрозуміти їх логіку, але й вирішувати питання про можливість нашої держави впливати на їх розгортання та усувати причини криміналізації економки [23, с. 299].

З огляду на зазначене, прийняття 28.01.2021 р. Закону України "Про Бюро економічної безпеки України" [24], беззаперечно, є важливим кроком. На Бюро покладено правоохоронну, аналітичну, економічну, інформаційну та інші функції. Відповідно до статті 4 Закону визначено завдання Бюро економічної безпеки України, серед яких виявлення зон ризиків у сфері економіки шляхом аналізу структурованих і неструктурованих даних; оцінювання ризиків і загроз економічній безпеці держави, напрацювання способів їх мінімізації та усунення; надання пропозицій щодо внесення змін до нормативно-правових актів з питань усунення передумов створення схем протиправної діяльності у сфері економіки; забезпечення економічної безпеки держави шляхом запобігання, виявлення, припинення, розслідування кримінальних правопорушень, що посягають на функціонування економіки держави; збирання та аналіз інформації про правопорушення, що впливають на економічну безпеку держави, та визначення способів запобігання їх виникненню в майбутньому; планування заходів у сфері протидії кримінальним правопорушенням, віднесеним законом до його підслідності; виявлення та розслідування правопорушень, пов'язаних з отриманням та використанням міжнародної технічної допомоги; складання аналітичних висновків і рекомендацій для державних органів з метою підвищення ефективності прийняття ними управлінських рішень щодо регулювання відносин у сфері економіки.

Створення Бюро економічної безпеки України, яке має запрацювати з вересня 2021 року, в цілому покликано усунути дублювання функцій усіма правоохоронними органами щодо розслідування злочинів у сфері економіки. Головною метою є суттєве зменшення тиску на бізнес, адже сьогодні правоохоронна система в Україні працює таким чином, що стосовно одного і того ж суб'єкта господарювання та навіть з приводу претензій щодо проведення одних і тих же господарських операцій кримінальні провадження відкривають підрозділи і Національної поліції, і Служби безпеки України, і Державної фіскальної служби України (податкова міліція), і Державного бюро розслідування, і прокуратури. А інколи, як свідчить практика, у разі "особливих заслуг" суб'єкта господарювання – й усіма цими правоохоронними відомствами водночас. Чи спроможне новостворене Бюро економічної безпеки України забезпечити усунення дублювання таких функцій іншими правоохоронними органами покаже час.

На нашу думку прийнятий Закон України "Про Бюро економічної безпеки України" лише декларує створення нового правоохоронного органу, але не вносить змін до чинних законів (кодексів), які мали б забезпечити усунення дублювання.

Нині, у провідних країнах світу відбуваються процеси, пов’язані з підготовкою та впровадженням технологічного устрою, що передбачає розвиток наноелектроніки, наноматеріалів, біотехнології, штучного інтелекту тощо. Слід зазначити, що шостий технологічний устрій – це можливість мільярдних інвестицій та великого потенціалу росту, при цьому без прив'язки до географічних, політичних, економічних чинників країни чи регіону. За оцінками низки вітчизняних та іноземних експертів шостий технологічний рівень буде включати складові двох рівнів:

- перший – новітні технології промислового виробництва, нова інфраструктура та система управління (на глобальному, регіональному (субрегіональному) і національному рівнях);

- другий – цифрова економіка.

Відповідно, за наявними прогнозними оцінками, країни світу за цих умов можуть поділитися на три групи:

– країни, які будуть володіти складовими обох рівнів шостого технологічного устрою, у тому числі системою управління;

– країни, що будуть мати лише цифрову економіку;

– країни, які не будуть мати жодної складової вказаного технологічного устрою.

За цих умов відповідно постане й питання щодо визначення майбутнього України та її місця в сучасному глобалізованому світі.

За статистичними даними, складеними протягом останніх п’яти років, Україна в глобальному рейтингу за рівнем розвитку інновацій має непогані показники. У порівнянні з найвищою оцінкою, яку займає Швеція – 66,08 з 100 можливих балів, бал України становить 36,32. Найнижчу оцінку у рейтингу займає Ємен – 13,56. З цього можна зробити висновок, що економіка України за рівнем розвитку інновацій працює краще, ніж можна було б очікувати за рівнем вкладень та випереджає такі країни як Росія, Індія, Туреччина, Бразилія, Вірменія, Грузія та інші [25].

Проте слід звернути особливу увагу на те, що застосування новітніх технологій промислового виробництва та цифрової економіки сприятиме не лише створенню нових продуктів і послуг та розширенню можливостей людини, а також може призвести до низки негативних соціально-економічних наслідків, зокрема, зростання безробіття, соціального розшарування населення, посилення кризових процесів тощо.

Узагальнюючи бачення вітчизняних вчених [26], які до головних факторів забезпечення економічної безпеки відносять пристосування до мінливих зовнішніх умов й адекватне реагування на виклики зовнішнього середовища; створення сприятливих умов для забезпечення реалізації національних інтересів; проведення самостійної й ефективної економічної політики з метою захисту національних інтересів; забезпечення ефективного захисту економічних інтересів особи, суспільства, держави; забезпечення стійкості до зовнішніх і внутрішніх загроз та здатність ефективно захищати національні інтереси в усіх сферах функціонування держави; вчасне виявлення загрози національним економічним інтересам і запобігати заподіянню збитків соціально-економічній системі в цілому.

За нашими оцінками до зазначеного переліку слід додати криміналізацію нових, раніше невідомих національному правовому полю суспільно небезпечних діянь за результатами їх всебічного вивчення й аналізу та розробка відповідних заходів протидії таким видам злочинності, а також здійснення модернізації чинного законодавства та практики боротьби згідно із потребами часу.

Отже, рівень стану економічної безпеки залежить від ефективності державного управління, його орієнтованості на захист національних інтересів в економічній і

соціальній сферах, послідовність та системність у здійсненні економічних реформ, досконаліть національного законодавства щодо забезпечення економічної безпеки та ефективного управління економікою, а також належний рівень кваліфікації державних службовців з питань забезпечення національної безпеки та недопустимість корупції в управлінських структурах.

Висновки.

Складність законодавчого забезпечення економічної безпеки України вбачається перш за все у визначенні кола реальних та потенційних загроз економічній безпеці країни, оскільки в сучасному світі з розвитком інформаційних технологій виникають все нові виклики і загрози. Виявлення і прогнозування реальних небезпек від цих загроз має бути покладено перш за все на наукову спільноту.

Прийняття Стратегії економічної безпеки України стало основою для формування державної політики у сфері забезпечення економічної безпеки. Реалізація Стратегії має запровадити прозору систему постійного моніторингу економічної стійкості та щорічну оцінку стану економічної безпеки, що має на меті сприяти підвищенню ефективності реалізації державної політики у сфері забезпечення економічної безпеки і політичної відповідальності за її результати. Створення Бюро економічної безпеки України має сприяти усуненню дублювання функцій усіма правоохоронними органами щодо розслідування злочинів у сфері економіки.

В сучасній Україні відбуваються процеси формування законодавства у сфері забезпечення економічної безпеки країни, але якість законопроектів залишається низькою. В ряді законопроектів не враховуються норми інших, пов’язаних законів, що призводить до неузгодженості та затримки прийняття важливих законодавчих актів.

З урахуванням досвіду держав-членів ЄС і НАТО у сфері законодавчого забезпечення економічної безпеки країни, слід зазначити, що у країнах з високим рівнем розвитку економіки, оцінювання рівня економічної безпеки держави не проводиться, не використовуються індикатори економічної безпеки та їх порогові значення, натомість рівень економічної безпеки визначається за показником ВВП на душу населення. Особливості забезпечення економічної безпеки країн-членів ЄС полягають в усуненні системних загроз та упередженні потенційних через підвищення макроекономічної стабілізації й підтримки внутрішньої та зовнішньої стабільності, прискорення структурних реформ в економіці, залучення іноземних інвестицій та підтримці малого і середнього бізнесу та забезпеченні постійного динамічного розвитку економіки та міжнародного співробітництва.

У країнах з розвиненою економікою значну роль у виявленні реальних та потенційних загроз економічній безпеці відіграють так звані “незалежні мозкові центри” (*think tank*), які існують на запит відповідних урядових структур, які приймають управлінські рішення, направлені на забезпечення економічної безпеки держави, на початковому етапі аналізують та про водять моніторинг ситуації, що склалася в окремому секторі безпеки, і надають попередні рекомендації. На наступному етапі створюються робочі групи із розробки сценаріїв загроз та генерування управлінських рішень.

За експертними оцінками економіка України за рівнем розвитку інновацій працює краще, ніж очікувалося за рівнем вкладень. Прогнозовано Україна зможе з’явитися на світовій мапі ВВП та увійти в ТОП лідерів світової економіки до 2030 р. тільки у разі, якщо зробить інноваційній технологічній стрибок. Для цього необхідно створити умови для впровадження інновацій, залучити інвестиції в цифрові технології та інфраструктуру. У випадку, якщо не відбудеться перехід української економіки до

інноваційної, то Україна залишиться на задвірках цивілізації. Слід також враховувати, що застосування новітніх технологій промислового виробництва та цифрової економіки сприятиме не лише створенню нових продуктів і послуг та розширенню можливостей людини, а також може призвести до низки негативних соціально-економічних наслідків, зокрема, зростання безробіття, соціального розшарування населення, посилення кризових процесів тощо.

Використана література

1. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України: наказ Мінекономрозвитку України від 29.10.13 р. № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#n9 (дата звернення: 18.03.2021).
2. Питання Міністерства розвитку економіки, торгівлі та сільського господарства. URL: https://zakon.rada.gov.ua/laws/show/459-2014-%D0%BF#Text (дата звернення: 11.04.2021).
3. Линник О.І., Матвєєв І.А.. Проблеми економічної безпеки України: матеріали 8 наук.-практ. конф. *Дослідження та оптимізація економічних процесів*, м. Харків, 5 – 7 груд. 2012 р. Харків: НТУ "ХПІ", 2012. С. 302-304.
4. Державний борг України. URL: https://index.minfin.com.ua/ua/finance/debtgov (дата звернення: 11.05.2021).
5. Малишко В.М. Актуальні проблеми економічної безпеки в системі національної безпеки України. *Юридичний вісник*. № 4 (37) 2015. С. 130.
6. Ставицький О.В. Формування моделі економічної безпеки. URL: https://ela.kpi.ua/bitstream/123456789/23882/1/S.71-77.pdf (дата звернення: 13.04.2021).
7. Сак Т.В. Економічна безпека України: поняття, структура, основні тенденції. URL: https://core.ac.uk/download/pdf/153578704.pdf (дата звернення: 13.04.2021).
8. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 19.03.2021).
9. Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення: монографія. Київ: НІСД, 1997. 144 с.; Мунтіян В.І. Економічна безпека України: навч. посібник. Київ: Лібра, 1999. 462 с.; Геєць В.М. Економіка України: ключові проблеми і перспективи. *Економіка і прогнозування*. 2016. № 1. С. 7-22.; Економічна безпека: навч. посіб. / Варналій З.С. та ін. Київ: Знання, 2009. 647 с.; Руда О., Малюта Л. Організація економічної безпеки в контексті активізації розвитку товаровиробництва. *Галицький економічний вісник*. 2012. № 3(36). С. 35-42.
10. Чубукова О.Ю., Воронкова Т. Є. Система економічної безпеки (екосестейт): сутність, структура. URL: http://www.economy.nayka.com.ua/?op=1&z=3169 (дата звернення: 12.03.2021).
11. Харазішвілі Ю.М., Ляшенко В.І. Сучасна концепція сталого розвитку з позицій економічної безпеки: матеріали Міжнар. наук.-практ. конф. *Економічна та інформаційна безпека: проблеми та перспективи,* м. Дніпро, 27 квіт. 2018 р. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 276 с. С. 243.
12. Президент України Володимир Зеленський підписав указ про Цілі сталого розвитку України на період до 2030 року. URL: https://www.ukrinform.ua/rubric-polytics/2790358-zelenskij-shvaliv-cili-stalogo-rozvitku-ukraini-do-2030-roku.html (дата звернення: 14.04.2021).
13. Про внесення змін до Закону України "Про національну безпеку України": проект закону. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68754 (дата звернення: 14.04.2021).
14. Уряд схвалив проект Стратегії економічної безпеки України на період до 2025 року. URL: https://www.kmu.gov.ua/news/uryad-shvaliv-proekt-strategiyi-ekonomichnoyi-bezpeki-ukrayini-na-period-do-2025-roku (дата звернення: 15.05.2021).
15. Про Бюро економічної безпеки України: Закон України від 28.01.21 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text (дата звернення: 25.05.2021).

16. Про внесення зміни до розділу V “Прикінцеві та перехідні положення” Закону України “Про приватизацію державного і комунального майна” щодо приватизації об’єктів великої приватизації: проект закону. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70747 (дата звернення: 25.05.2021).

17. Про внесення зміни до пункту 4 розділу XXI “Прикінцеві та перехідні положення” Митного кодексу України щодо звільнення від оподаткування ввізним митом: Закон України від 02.03.21 р. № 1294-IX. URL: https://zakon.rada.gov.ua/laws/show/1294-20#Text (дата звернення: 25.05.2021).

18. Верховна Рада України ухвалила в першому читанні базовий законопроект про “Дія City”. URL: https://city.diia.gov.ua/news/verhovna-rada-ukrayini-uhvalila-v-pershomu-chitanni-bazovij-zakonoproyekt-pro-diya-city (дата звернення: 25.05.2021).

19. Про внесення змін до Закону України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”: проект закону від 10.11.20 р. № 4355. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70393 (дата звернення 25.05.2021).

20. Гбур З.В. Зарубіжний досвід забезпечення економічної безпеки держави. Інвестиції: практика та досвід. 2018. № 11. С. 111–115.

21. Денисенко М.П. Зарубіжний досвід регулювання економічної безпеки. *Економічна наука. Інвестиції: практика та досвід.* № 6/2017. С. 15-19.

22. Пугач О.А. Світовий досвід упередження загроз економічній безпеці національної економіки. *Науковий вісник Херсонського державного університету. Серія: “Економічні науки”.* Вип. 12. Ч. 3. 2015 С. 43-46.

23. Мочкош Я.В. Проблеми боротьби з економічною злочинністю. *Часопис Київського університету права.* 2012. № 2. С. 299.

24. Про Бюро економічної безпеки України: Закон України від 28.01.21 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text (дата звернення: 25.05.2021).

25. The Global Innovation Index. URL: https://www.globalinnovationindex.org/home (дата звернення: 02.04.2021).

26. Илларионов А. Критерии экономической безопасности. *Вопросы экономики*. 1998. № 10. С. 35-57.; Губський Б.В. Економічна безпека України: методологія виміру, стан і стратегія забезпечення: моногр. Київ: Укрархбудінформ, 2001. 122 с.; Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. Київ: КНТЕУ, 2001. 309 с., Мунтіян В.І. Економічна безпека України. Київ: КВІЦ, 1999. 462 с.; Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение. *Вопросы экономики*. 1994. № 12. С. 4-13. Жаліло Я.А. Економічна безпека держави, підприємства, особи в інтегрованому суспільстві. *Актуальні проблеми міжнародних відносин*. – (Київський ун-т: Інститут міжнародних відносин). 2001. Вип. 26. С. 24-27; Шлемко В.Т., Бінько І.Ф. Економічна безпека України: сутність і напрямки забезпечення. Київ: НІСД, 1997. 144 с.; Пастернак-Таранущенко Г.А. Економічна безпека держави. Статика процесу забезпечення: підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів економічного профілю; за ред. проф. Б. Кравченка. Київ: Кондор, 2002. 302 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

УДК 342.6:35.072.1

АНТОНЮК О.М., аспірантка НТУУ "КПІ ім. Ігоря Сікорського".

ІСТОРИКО-ПРАВОВІ ПЕРЕДУМОВИ ЗДІЙСНЕННЯ РЕФОРМИ ДЕЦЕНТРАЛІЗАЦІЇ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ

Анотація. *У статті висвітлено історико-правові передумови здійснення реформи децентралізації публічної влади в Україні. Досліджено основні історико-правові етапи розвитку ідеї децентралізації влади, які справили значний вплив на формування сучасної концепції реформи децентралізації публічної влади в Україні. Охарактеризовано історичні передумови здійснення реформи децентралізації протягом основних історичних етапів розвитку української державності. Обґрунтовано, що початковим етапом виникнення історичних передумов децентралізації публічної влади слід вважати період Київської Русі, оскільки саме у цей період закладено правові основи української державності, відбулось формування основних державних інститутів. З'ясовано здобутки основних історичних етапів на шляху до здійснення децентралізації публічної влади в Україні.*

Ключові слова: *історико-правові умови, реформа децентралізації, публічна влада, місцеве самоврядування.*

Summary*. The article highlights the historical and legal preconditions for the implementation of the reform of decentralization of public power in Ukraine. The main historical and legal stages of development of the idea of decentralization of power, which had a significant impact on the formation of the modern concept of decentralization reform of public power in Ukraine, are studied. The author describes the historical preconditions for the implementation of decentralization reform during the main historical stages of development of Ukrainian statehood. It is substantiated that the initial stage of historical preconditions for decentralization of public power should be considered the period of Kievan Rus, because it was during this period that the legal foundations of Ukrainian statehood were laid, the formation of basic state institutions took place. The author clarifies the achievements of the main historical stages on the way to the decentralization of public power in Ukraine.*

Keywords*: historical and legal conditions, decentralization reform, public authorities, local self-government.*

Аннотация. *В статье освещены историко-правовые предпосылки осуществления реформы децентрализации публичной власти в Украине. Исследованы основные историко-правовые этапы развития идеи децентрализации власти, которые оказали значительное влияние на формирование современной концепции реформы децентрализации публичной власти в Украине. Охарактеризованы исторические предпосылки осуществления реформы децентрализации в течение основных исторических этапов развития украинской государственности. Обосновано, что начальным этапом возникновения исторических предпосылок децентрализации публичной власти следует считать период Киевской Руси, поскольку именно в этот период заложены правовые основы украинской государственности, состоялось формирование основных государственных институтов. Установлены достижения основных исторических этапов на пути к осуществлению децентрализации публичной власти в Украине.*

Ключевые слова*: историко-правовые условия, реформа децентрализации, публичная власть, местное самоуправление.*

Постановка проблеми. Процес децентралізації влади, що наразі триває в Україні, має певні історичні передумови, які справили значний вплив на сучасні форми реалізації адміністративної реформи у цій сфері. Зокрема, тісний зв'язок між історичними передумовами децентралізації влади та формами здійснення відповідних реформ пояснюється, головним чином, тим, що саме особливості історико-правових, історико-соціальних та інших умов становлення та розвитку місцевої влади детермінує обрання відповідних способів реалізації реформи децентралізації. Це означає, що у сучасних умовах форма демократизації державної влади шляхом передачі значної частини владних повноважень від центральних до місцевих органів влади обумовлена особливостями історико-правових традицій, правової культури певної держави та ін.

Отже, дослідження історичних умов реалізації реформи у сфері децентралізації влади дає можливість відшукати оптимальну модель формування спроможної місцевої влади в Україні.

Результати аналізу наукових публікацій. Історичний аспект децентралізації влади в Україні досліджували такі науковці як М.М. Бедрій, Ю.П. Козаченко, О.М. Оргієць, Р.І. Панчишин, О.В. Ременяк та інші. У вказаних роботах науковцями висвітлюються, головним чином, питання становлення та розвитку місцевого самоврядування на території українських земель. Деякі наукові дослідження (Бедрій М.М. Верв у Київській Русі: самоврядування і право) присвячені певному історичному етапу розвитку місцевого самоврядування, в інших (Ременяк О.В. Децентралізація публічної влади в правовій теорії та державотворчій практиці) висвітлюється переважно історичний аспект децентралізації влади.

Разом з тим, незважаючи на значну кількість наукових досліджень, присвячених зазначеній проблематиці, у вітчизняній науці адміністративного права недостатньо комплексних наукових робіт, присвячених історико-правовим передумовам розвитку ідеї децентралізації влади, які справили значний вплив на формування сучасної концепції реформи децентралізації публічної влади в Україні, що підтверджує актуальність та своєчасність запропонованої теми статті.

Метою статті є визначення історико-правових передумов здійснення реформи децентралізації публічної влади в Україні.

Для досягнення поставленої мети передбачені завдання щодо визначення: початкових етапів виникнення історичних передумов децентралізації публічної влади; історичних передумов здійснення реформи децентралізації на різних історичних етапах розвитку української державності; з'ясування здобутків основних історичних етапів на шляху до здійснення децентралізації публічної влади в Україні.

Виклад основного матеріалу. У сучасній науковій літературі не склалося єдиної точки зору щодо історичного періоду, який можна вважати відправною точкою у процесі здійснення реформи децентралізації влади на українських землях.

Приміром, Ю.П. Козаченко, досліджуючи історичні передумови децентралізації в Україні, зазначає, що першим кроком на шляху становлення в Україні місцевого самоврядування стала ратифікація Європейської хартії місцевого самоврядування, що було прийнята Радою Європи в 1985 році. Водночас він також зауважує, що одним із яскравих символів вітчизняної державності, для яких характерні риси децентралізації, була Українська Центральна Рада під управлінням державного діяча М. Грушевського. При цьому Ю.П. Козаченко акцентує увагу на тому, що публічна громадська модель є аналогом "верств" населення за часів Київської Русі, інша адміністративна модель об'єднує в процесі децентралізації систему державного управління та громадського управління. децентралізація є передачею компетенцій та відповідальності за виконання

зобов'язань щодо державної служби від центрального уряду до місцевих або субнаціональних урядів. Децентралізація може відбуватися в політичній, адміністративній, фінансово-бюджетній та інших сферах [1, с. 214-215, 217].

Інші науковці стверджують, що в Україні процес децентралізації влади розпочався лише у 2014 – 2015 роках як реакція на фактичне існування протягом 2010 – 2013 рр., усупереч Конституції України, суперпрезидентської республіки, за якої встановлена жорстка централізація повноважень і ресурсів органів виконавчої влади (фактично знівельовано місцеве самоврядування, знищена фінансова самостійність територіальних громад, небачених масштабів сягнула корупція) [2, с. 23].

Досить ґрунтовний підхід до розроблення історичної періодизації процесу децентралізації влади знаходимо у роботі Ю.О. Буглака. Зокрема, на думку науковця, перші прояви децентралізації влади мали місце за часів Київської Русі (кінець IX ст. – середина XIV ст.) [3, с. 41-42]. Як вважаємо, можна погодитись з тим, що першим етапом становлення та розвитку місцевого самоврядування як головного інституту, який утворюється у процесі децентралізації влади, є період Київської Русі.

Деякі науковці зазначають, що система адміністративного управління Київської Русі генетично виросла з родоплемінної системи і військово-десятинної організації, але була істотно скоригована розвитком міського самоврядування (віча) і зміцненням спадкових князівських династій, регламентацією правових відносин [4, с. 7].

В обґрунтування думки про те, що перший етап становлення і розвитку інституту децентралізації влади бере свій початок від Київської Русі, О.В. Ременяк зазначає, що хоча основним інститутом державної влади у період існування Київської Русі була князівська влада, однак історичні трансформаційні зміни зумовили зміну системи публічної влади. Науковець наголошує, що на початку IX ст. децентралізація публічної влади характеризується її поділом між різними державними інституціями як-от: княжа влада, боярська рада, що була постійним дорадчим органом при князеві, князеві з'їзди (снеми), що наділені повноваженнями вирішувати питання зміни територіального устрою, ухвалення законодавчих актів, вирішення військових і політичних питань [5, с. 38].

М.М. Бедрій зазначає, що у період Київської Русі закладалися основи організованої територіальної громади та з'являлись перші форми об'єднаної громади. У якості прикладу вчений наводить таке організаційне утворення як "верв" – сільська територіальна громада, яка наділялась правом місцевого самоврядування та судовими функціями. Більшість вчених схиляються до того, що верв являв собою спілку сіл, тобто це своєрідне об'єднання сільських територіальних громад. Верв не лише здійснював самоврядування та судочинство на певній території, але й забезпечував чинність існуючих правових звичаїв, а також формував нові. Відтак у Київській Русі утворилася окрема підсистема звичаєвого права, яку називають "вервним правом", яке стало ядром звичаєвого права Київської Русі [6, с. 39-40].

Р.І. Панчишин, відстоюючи позицію стосовно того, що основи децентралізації влади були закладені ще у період Київської Русі, вказує, що саме у даний період громада демонструвала досить високу спроможність щодо вирішення найбільш важливих внутрішньодержавних питань. Причому, організаційно та функціонально вона була відокремлена від князівської влади, що свідчить передусім про наявність у неї самостійних функцій та реальних повноважень, необхідних для їх реалізації. Правовий статус верв та віче закріплювався в перших джерелах права Київської Русі – різних редакціях Руської правди та джерелах звичаєвого (вервного) права [7, с. 57].

Деякі науковці, досліджуючи історію Київської Русі, уточнюють, що реформу децентралізації земель навколо Києва розпочав князь Олег. Причому першопричиною такої реформи стала необхідність упорядкування системи збирання податей [8. с, 347]. Зазначається, що не родова община, а місто стає суб'єктом зобов'язання зі сплати відповідних платежів і саме воно гарантувало сплату коштів на її утримання. Отже, місто мало самоорганізуватись своїми силами, зібрати та заплатити князю гроші для забезпечення миру [9, с. 126].

Отже, у даному випадку йдеться про формування фінансових засад децентралізації влади, що вперше продемонстрували важливість такої складової як фінансова спроможність громади до самоорганізації.

Інші науковці, пояснюючи особливості децентралізації влади у Київській Русі, зазначають, що матриця владних відносин, яка сформувалася на Русі, відображала особливості різних форм соціально-економічного освоєння території та її членування. Зрештою її занепад став наслідком того, що регіонально-корпоративні інтереси знаті взяли гору над загальнодержавними. Саме міжусобна боротьба князів Русі стала передумовою першої зі значних біфуркацій в історії України, коли здійснювався вибір шляхів розвитку між централізованою та роздрібненою державою [10].

Таким чином, у період Київської Русі були закладені важливі основи утворення багатьох сучасних інститутів місцевого самоврядування, що має безпосереднє відношення до децентралізації влади. Зокрема, саме у цей період на законодавчому рівні розмежовано повноваження між князівською владою, боярами, віче, а також утворено верви – прототипи сучасної територіальної громади, до яких передано деякі функції по управлінню місцевими територіями.

Наступним етапом, який мав важливе значення для становлення інституту децентралізації влади, став період магдебурзького права (охоплює період Литовсько-Польської доби).

Магдебурзьке право передбачало звільнення міського населення від юрисдикції урядової адміністрації (феодалів, воєвод, намісників), вони також отримували можливість запровадження власного виборного органу магістрату на чолі з бургомістром й ратманами (радниками). Магдебурзький привілей дозволяв міщанам утворювати в місті свою громаду [11, с. 35]. До складу громади входили міщани – жителі міста, але лише ті, які мешкали поза межами земельної території, що належала єпископу чи княжому замкові [12, с. 258].

Основоположною ідеєю доби магдебурзького права було формування відносно самостійних від централізованої влади міст, наділених спеціальним документом – грамотою – правом на участь в управлінні справами відповідного міста незалежно від урядової влади.

У науковій літературі зазначається, що за магдебурзьким правом виборним органом влади міста був магістрат, який складався з двох частин: ради (управлінський орган), до якої входило три – шість радців на чолі з бургомістром, що періодично змінювався з числа радців, та лави (міський суд), до якої належало від трьох до дванадцяти лавників на чолі з війтом. У містах з повним Магдебурзьким правом останнього обирали самі городяни з наступним затвердженням королем однієї з чотирьох запропонованих кандидатур, а з неповним (ратушні міста) – це право належало главі держави [13, с. 9].

Таке самоуправління в українських містах, в яких діяло магдебурзьке право, нагадувало сучасну систему місцевого самоврядування. Однак, на відміну від останньої, система міського самоуправління на території українських земель в Литовсько-

Польську добу характеризувалась відсутністю уніфікованих правил такого самоуправління, неоднаковістю становища міст та як наслідок – різним обсягом повноважень, які надавались на підставі відповідної грамоти, а також правом князя втручатися у здійснення самоуправління містом, включаючи позбавлення наданих привілеїв.

З огляду на зазначене, можна погодитись з думкою А.В. Бортнікової, яка досліджуючи становлення місцевого самоврядування на Волині, доходить висновку, що головними принципами формування та діяльності міських урядів на магдебурзькому праві були становість, корпоративізм, поєднання власності та влади, відсутність чіткого поділу на адміністративну діяльність і суд та ін. Організація суспільного життя міст, побудована за такими принципами, неминуче створювала підґрунтя для соціальних конфліктів: між привілейованими та непривілейованими верствами населення; інститутами державної влади й самоврядуванням; правом і беззаконням; міщанами магдебурзької юрисдикції і власниками та жителями юридик; церквою і міщанською громадою на магдебурзькому праві тощо [14, с. 297].

Щодо системи утворюваних органів самоуправління міста необхідно вказати на таке оформлення: рада, до складу якої входив війт (голова сільської гміни), бургомістр чи президент міста (голова міської гміни), староста (повітовий керівник і очільник місцевого самоврядування відповідної адміністративно-територіальної одиниці) та маршалок воєводства (губернатор), його заступник та інші члени [15, с. 270]. При цьому слід зауважити, що наведена система самоуправління була запозичена із польської, оскільки дія польського законодавства була поширена на більшій території українських земель.

Зважаючи на важливе значення Литовсько-Польської доби для здійснення на українських землях реформи децентралізації, деякі науковці, досліджуючи вплив магдебурзького права на становлення інституту місцевого самоврядування в Україні, цілком справедливо виокремлюють такі наслідки упровадження магдебурзького права в українських містах: припинення дії звичаєвого права (чи то польського, чи то литовського, чи то руського, чи то будь-якого); влада воєвод, намісників або урядників відтепер не поширювалась на міщан, які потрапляли під юрисдикцію війта; запроваджувалося обрання органів міського самоврядування; в місті засновувались один або кілька ярмарків та дозволялися щотижневі торги; будівництво в центрі міста ратуші та адмінбудівель; дозволялося проводити займання незаселених ділянок у місті та поза ним, як і користування прилеглими лісами та угіддями [16, с. 7].

Отже, запровадження у деяких українських містах магдебурзького права стало поштовхом для утворення певної організаційно-оформленої системи органів місцевого самоврядування, наділення їх повноваженнями у сфері здійснення місцевого управління, вирішення питань місцевого значення, незалежно від центральної урядової влади.

Важливі історико-правові передумови для здійснення реформи децентралізації склалися у козацьку добу. Досліджуючи цей історичний період у контексті формування системи місцевого самоврядування, Ю.О. Буглак зазначає, що найважливішими здобутками цієї доби є: закріплення терміну “повноваження” у тексті Конституції Пилипа Орлика від 5 квітня 1710 року, що регламентувала повноваження гетьмана, генеральної ради та генерального суду, та формування триступеневої структури військового управління державою (генеральний, полковий і сотенний уряди), в якій повноваження органів місцевого самоврядування відігравали полкові та сотенні козацькі ради [3, с. 41-42].

Водночас, важливо зазначити, що наведені здобутки хоча й були головними та справили значний вплив на подальше здійснення реформи децентралізації на українських землях, однак, окрім цих здобутків, необхідно вказати на деякі інші перетворення, які мали не менш важливе значення у сфері оформлення сучасної системи місцевого самоврядування.

Зокрема, у цей період сформувалась досить розгалужена система органів самоуправління, на чолі якої знаходилось зібрання всіх без винятку козаків – рада (коло). При цьому особливістю організації цього органу було те, що існування ради не регламентувалося формальними правилами, традиційно коло скликалась щорічно 1 січня на Січі, для переобрання отамана та старшини, а в разі поточної потреби скликалися неординарні ради, які могли збиратися там де виникала така потреба. Рада була дорадчим органом, інструментом досягнення консенсусу, прийняття спільного рішення, яке ставало обов'язковим для спільноти, що його ухвалила. Щодо виконавчої влади в козацькій громаді, то її обіймав кошовий отаман, який обирався загальним колом на один рік та мав потужний вплив на повсякденне життя Січі. Здійснювати виконавчу владу кошовому отаману допомагала козацька старшина – суддя, осавул, писар, яка обиралася задля виконання волі громади [17, с. 58].

Деякі науковці, досліджуючи процес децентралізації у козацьку добу, виокремлюють такі ознаки децентралізації публічної влади, притаманні запорізькому козацтву: 1) максимальне наближення влади до об'єктів (функціонування органів місцевого самоврядування (загальна козацька рада); 2) забезпеченість ресурсами (кожне муніципальне утворення або автономне козацьке товариство (Запорізька Січ, курінь, полкове та сотенне місто) мали власну скарбницю, яку могли використовувати на власні потреби); 3) доступність участі у житті суспільства та контролю (активне функціонування органів прямої демократії – козацької ради); 4) існування кількох (двох або більше) вертикальних рівнів публічної влади в рамках територіальної організації єдиної держави (функціонування центральної (Річ Посполита, пізніше – Російська держава) та місцевої влади (Запорізька Січ, курінь, полкове та сотенне місто); 5) наявність внутрішньодержавних територіальних утворень із різним правовим статусом і певним ступенем автономії та самостійності (полково-сотенний устрій) [18, с. 207].

Отже, як можна побачити із наведеної системи організації запорізького самоуправління, така система значною мірою нагадувала сучасну організацію органів місцевого самоврядуванням з відповідним розподілом між органами представницької (яку виконувала козацька рада) та виконавчої функцій (які виконував старшина, спираючись на суддю, осавула, писаря).

Водночас слушною видається думка Є.О. Бутиріна, який зауважує, що від самого початку козацтво чинило супротив всім формам концентрації влади в руках окремих особистостей, намагаючись вирішувати повсякденні питання виходячи з рівності, яка поширювалася й на очільників. Проте, як наголошує науковець, цей егалітарний устрій, притаманний козацькій громаді, не можна ототожнювати з класичною демократією, бо остання передбачає передачу владних функцій окремим особам чи органам [17, с. 58].

Таким чином, у козацьку добу реформа децентралізації набула нових, більш організаційно та інституційно оформлених рис, оскільки сформувалася певна система органів козацького самоуправління, між якими розподілені представницькі та виконавчі функції. Крім того, саме у цю добу демонструється важливість фінансової спроможності козацької громади, яка дає змогу самостійно приймати рішення та втілювати їх у життя.

Наведені історичні етапи мали важливе значення для формування сучасної концепції здійснення реформи децентралізації. У період перебування українських земель під владою Російської імперії та входження до складу Радянського Союзу процес національного самовизначення на українських землях зазнав певного занепаду, а реформи влади були спрямовані, головним чином, на знищення інституту місцевого самоврядування в Україні. Відродження цього інституту придбала можливість лише після здобуття незалежності.

Висновки.

Історично процес формування інституту місцевого самоврядування та децентралізації влади у своєму розвитку пройшов декілька етапів, кожен з яких справляв певний вплив на сучасний стан організації органів місцевого самоврядування, конституційні засади децентралізації влади.

Початковим етапом можна вважати період Київської Русі, коли були закладені основи децентралізації влади, що виражались, передусім, у розмежуванні повноважень між княжою владою, боярською радою, князевими з'їздами (снемами). Крім того у цей період було утворено верви – перші подібні до сучасних сільські територіальні громади, які наділялась правом місцевого самоврядування та судовими функціями.

Важливі історичні передумови для здійснення реформи децентралізації влади склалися у період магдебурзького права (Литовсько-Польської доби), протягом якого відбулось формування відносно самостійних від централізованої влади міст, наділених правом на участь в управлінні справами відповідного міста незалежно від урядової влади. Проте, така організація міського самоуправління характеризувалась відсутністю уніфікованих правил, неоднаковістю становища міст, різним обсягом повноважень, які надавались на підставі відповідної грамоти, а також правом князя втручатися у здійснення самоуправління містом, включаючи позбавлення наданих привілеїв.

Козацька доба у сфері розвитку процесу децентралізації влади дала поштовх для оформлення багатьох сучасних засад організації місцевого самоврядування, зокрема, формування багаторівневої системи органів місцевого самоврядування, розподілом між цими органами представницької (яку виконувала козацька рада) та виконавчої функцій (які виконував старшина, спираючись на суддю, осавула, писаря), набуття органами різного організаційного рівня відносної фінансової самостійності тощо.

Використана література

1. Козаченко Ю.П. Історичні передумови децентралізації в Україні. *Держава та регіони. Серія: "Державне управління"*. 2019. № 3 (67). С. 213-118.

2. Скрипнюк О. Децентралізація влади як чинник забезпечення стабільності конституційного ладу: теорія й практика. *Віче.* 2015. № 12. С. 22-24.

3. Буглак Ю.О. Історичний генезис розмежування повноважень між органами виконавчої влади і органами місцевого самоврядування України. *Topical issues of law: theory and practice*. 2017. № 2 (34). С. 37-44.

4. Оргієць О.М. Становлення територіальної громади під час формування адміністративно-територіального поділу України: історія і сучасність: електронний зб. наукових праць *Публічне адміністрування: теорія та практика*. 2011. Вип. 2 (6). URL: http://www.dridu.dp.ua/zbirnik/2011-02(6)/11oomuis.pdf

5. Ременяк О.В. Децентралізація публічної влади в правовій теорії та державотворчій практиці: дис. …канд. юрид. наук: спец. 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. Львів, 2019. 210 с.

6. Бедрій М.М. Верв у Київській Русі: самоврядування і право. *Вісник Львів. ун-ту. Серія: "Юридичні науки"*. 2011. Вип. 54. С. 39-40.

7. Панчишин Р.І. Об'єднана територіальна громада як суб'єкт муніципально-правових відносин. Системно-онтологічний аналіз: монографія; за ред. Марцеляка О.В. Київ: Основа, 2020. 400 с.

8. Полное Собрание Русскихъ Летописей. Русский Хронографъ. Часть первая. СПб: Тип. М.А. Александрова, 1911. Т. 22. 568 с.

9. Настюк А.А., Муляр Г.В. Вплив податкової системи на децентралізаційні процеси в Київській Русі. Муніципальна реформа в контексті євроінтеграції України: позиція влади, науковців, профспілок та громадськості: матеріали Третьої щорічної всеукраїнської науково-практичної конференції. Київ: ТОВ "ВІ ЕН ЕЙ ПРЕС", 2019. 228 с.

10. Дністрянський М. Адміністративно-територіальний устрій України крізь призму геополітики. *Дзвін*. 1996. № 8. С. 93-104.

11. Мануілова К.В. Магдебурзьке право в українських містах: модель децентралізації публічної влади. *ДонДУУ*. 2016. № 1 (70). С. 33-40.

12. Ровинська К.І. Магдебурзьке право як підґрунтя формування місцевого самоврядування на території України. *Теорія та практика державного управління*. 2013. № 2. С. 257-263.

13. Реформування місцевого самоврядування та територіальної організації влади в Україні: матеріали для самопідготовки; уклад. В.М. Бойко. – (Черніг. центр перепідготовки та підвищення кваліфікації працівників органів держ. влади, місцевого самоврядування, держ. п-в, установ і орг.). Чернігів: ЦППК, 2014. 40 с.

14. Бортнікова А.В. Місцеве самоврядування на Волині: суспільнополітичні традиції і сучасний процес децентралізації: дис. …докт. політ. наук: спец. 23.00.02 – політичні інститути та процеси. Луцьк, 2018. 495 с.

15. Віліжінський В. Реформування системи місцевого самоврядування в Польщі: досвід для України. *Державне управління та місцеве самоврядування*. 2014. Вип. 2 (21). С. 265-277.

16. Бутирін Є.О. Запровадження магдебурзького права на теренах українських земель періоду Литовсько-Польської доби. *Приватне та публічне право*. 2019. № 4. С. 3-9.

17. Бутирін Є.О. Місцеве самоврядування періоду козацької доби (кінець XV ст. - першої половини XVII ст.). *Вісник Маріупольського державного університету. Серія: "Право"*. 2019. Вип. 17. С. 55-64.

18. Мануілова К.В. Засади децентралізації в публічній владі запорізьких козаків. *Вчені записки ТНУ ім. В.І. Вернадського. Серія: "Державне управління"*. 2018. Т. 29 (68). № 1. С. 205-209.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 340.12

ПІКОВСЬКА Т.В., *кандидат історичних наук*, старший викладач кафедри права
факультету менеджменту та права
Вінницького національного аграрного університету.
ORCID: https://orcid.org/0000-0003-4418-5628.

ПРАВОСВІДОМІСТЬ ЯК ОСНОВА МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ГЕНДЕРНОЇ РІВНОСТІ В УКРАЇНІ

Анотація. *В статті досліджено правосвідомість як основу механізму забезпечення гендерної рівності в Україні. Встановлено, що в Україні існує проблема як низької правосвідомості громадян в цілому, так і проблема гендерної нерівності зокрема.*

Ключові слова: *гендерна рівність, правосвідомість, суспільство, гендерна політика, правова культура.*

Summary. *The article examines legal awareness as a basis for the mechanism of ensuring gender equality in Ukraine. It is established that in Ukraine there is a problem of low legal awareness of citizens in general, and the problem of gender inequality in particular.*

Keywords: *gender equality, legal awareness, society, gender policy, legal culture.*

Аннотация. *В статье исследованы правосознание как основа механизма обеспечения гендерного равенства в Украине. Установлено, что в Украине существует проблема как низкого правосознания граждан в целом, так и проблема гендерного неравенства в частности.*

Ключевые слова: *гендерное равенство, правосознание, общество, гендерная политика, правовая культура.*

Постановка проблеми. Для побудови будь-якого міцного правового інституту необхідною є наявність достатнього підґрунтя, а саме, відкритості поглядів та орієнтованості громадян, досягнення суспільством необхідного рівня знань, широти поглядів та правильності акцентів. Це особливо важливо, коли мова йде про таку важливу соціальну проблему як досягнення гендерної рівності. Гендерна рівність вже давно визначена на декларативному рівні як рівний правовий статус жінок і чоловіків та рівні можливості для його реалізації, що дозволяє особам обох статей брати рівну участь у всіх сферах життєдіяльності суспільства. Проте визначеність даного явища у теорії, у нормативних актах, на жаль, не дає підстав стверджувати й про таку ж його прозорість у житті суспільства, у спрямованості державної політики, у розумінні пересічного громадянина.

Результати аналізу наукових публікацій. Дослідженню гендерної рівності присвячені праці таких науковців як: Федін Д.Г., Цимбалюк М.О., Клімова Г.П., Жидкова О.О., Нечипорук Л.В., Івченко Ю.В., Крочук М.І. та ін.

Метою статті є оцінка значення, стану та перспектив гендерної рівності в сучасному українському суспільстві.

Виклад основного матеріалу. У період становлення в сучасній Україні демократичного суспільства та правової держави проблеми підвищення соціальної активності правосвідомості, правової культури населення набувають надзвичайно актуального характеру. Саме тому доцільно розглянути явище безпосередньої залежності потенціалу становлення гендерної рівності від відкритості до неї свідомості громадян України.

Правосвідомість – це досить складний феномен, що має різні аспекти філософського, юридичного, соціально-політичного та морального змісту, й становить сферу суспільної свідомості і виступає елементом правового буття як механізм правового регулювання [1, с. 814].

Зрозуміло, що правосвідомість громадян, які бажають жити у демократичній державі, не може виникнути спонтанно, та потребує послідовного процесу її формування, за якого можуть виникати обставини, які впливатимуть на проходження цього процесу і позитивно, і негативно. На сучасному етапі демократизації української держави на процес формування, зміни правосвідомості громадян чималий вплив справляють такі чинники, як правова освіта, правове виховання, самовиховання та перевиховання, соціалізація та вплив соціального середовища [2, с. 14].

Серед багатьох правових цінностей правосвідомості і правової культури важливе значення мають такі, як свобода, рівність, справедливість, закон. Вони виступають в якості основних правових цінностей, оскільки безпосередньо свідчать про сутність правосвідомості і правової культури [3, с. 149].

В умовах розвитку громадянського суспільства в Україні правосвідомість громадян повинна, насамперед, відображати сучасне уявлення, яке б відповідало сьогоднішнім потребам суспільства, про сутність демократичної правової держави, усвідомлення відмінності правомірних і протиправних дій, рішень, вчинків.

Правосвідомість є одним з різновидів суспільної свідомості. Їй, як і іншим формам суспільної свідомості (філософській, релігійній, моральній, політичній, естетичній), властиво відображувати навколишній світ, однак не увесь, а лише певний його аспект – правову дійсність. Тому за всієї значущості для суспільного та державного розвитку індивідуального сприйняття кожною особою права, у контексті з'ясування правових цінностей громадянського суспільства, особливо важливою є правосвідомість масова, або ж суспільна. Це є наслідком сутності самого явища громадянського суспільства, способом формування останнього та метою його існування. Суспільна правосвідомість не тільки дає людині певну суму правових знань, але й слугує основою юридичної оцінки реальних відносин між людьми, вироблення відношення до вимог правових норм, практичної діяльності з правотворчості, реалізації правових норм тощо.

Серед передумов формування гендерної політики у нашій державі можна виділити: історичні (поява жіночих організацій, вплив феміністичного руху, міжнародні документи, спрямовані на покращення становища жінок у всіх сферах життя); культурні (культ жінки-матері в суспільстві за умов існування патріархального устрою); політичні (поступове збільшення представництва жінок у Верховній Раді, органах місцевого самоврядування); освітні (запровадження навчальних предметів з гендерної освіти в університетах, створення центрів та лабораторій з гендерних досліджень); демографічні (висока і рання смертність чоловіків, зменшення народжуваності та демографічне старіння населення); медичні (запровадження програми "Планування сім'ї" та програм профілактики зі збереження репродуктивного здоров'я); економічні (жінки мають нижчий рівень економічної активності, нижчий рівень зайнятості, вищий рівень безробіття, зарплата жінок становить 68 % заробітної плати чоловіків); соціальні (насильство в сім'ї, торгівля людьми) [4].

Першим кроком до становлення в Україні суспільства громадського суспільства, у якому головною цінністю є окрема особа, незалежно від її статі, є формування належної правової свідомості, викорінення будь-яких засад дискримінації осіб за даною приналежністю.

Очевидно, що гендерні стереотипи в Україні, так само як і в інших країнах, призвели до умовного поділу ринку праці на дві частини: для жінок (освіта, культура) і для чоловіків (будівництво, армія). Головна різниця між ними полягає у тому, що ринок праці, де більшість становлять жінки, характеризується нижчим статусом і відповідно нижчим рівнем заробітної плати [5, с. 71].

Таким чином, економічна нерівність чоловіків і жінок підтримується системою гендерної нерівності на ринку праці. Насамперед це стосується сфери професійної зайнятості, можливостей творчої діяльності, серед яких чільне місце посідає кар'єрне просування сходинками бюрократичного, професійного чи фінансового успіху.

Крім цього, наявна у суспільстві дискримінація за ознакою статі виявляється у невизнанні виробничої праці жінок у домашньому господарстві як соціально значущої. З врахуванням домашньої роботи жінки у середньому зайняті різними видами робіт майже на 25 % часу більше ніж чоловіки. Вибудовується цікавий ланцюжок соціальних ролей і прав жінок в українському суспільстві, коли для соціальної самореалізації жінка повинна мати дітей. Паралельно вона повинна робити внесок до сімейного бюджету, тобто працювати поза домом, але робота не повинна перетворитися на кар'єру. Вказана ситуація зумовлена обмеженим баченням суспільства можливості корінних змін та визнання потенціалу чоловіків та жінок у історично непритаманних їм сферах.

У різних видах політичної діяльності (участь у виборах, інтерес до політики, підтримка тих чи тих політичних партій і лідерів, участь у політичних акціях, робота в органах виконавчої та законодавчої влади) співвідношення чоловіків і жінок суттєво різниться. У суспільній свідомості за жінкою не вкоренився образ працівниці й політичного лідера, а й досі продовжує домінувати образ матері-доглядальниці, вихователькі й домогосподарки. Тому жінки, незважаючи на ряд міжнародних та національних програм, практично не беруть участі у виробленні державної політики, залишаючись пасивними спостерігачами й виконавцями, а також реципієнтами соціальної допомоги. У той час як реалізація громадянських прав передбачає повноцінну участь не тільки чоловіків, а й жінок на всіх рівнях функціонуючих у суспільстві соціальних інституцій, включаючи однаковий доступ до усіх позицій соціальної структури суспільства. [6, с. 54].

Рівноправне становище жінок в суспільстві істотно змінює традиційні уявлення про такі риси, як жіночність і мужність. Жінці-лідеру тепер більше притаманні моделі поведінки, які раніше закріплювалися за чоловіками, наприклад: незалежність, здатність приймати самостійні рішення і відстоювати свою думку. Сучасний спосіб життя вимагає поєднання різних стилів керівництва. Сучасну жінку-лідера відрізняє, насамперед, глибоке усвідомлення необхідності рівних прав з чоловіками і здатність до участі в усіх сферах суспільства. Іншою важливою рисою є визнання необхідності поєднання різних соціальних ролей – не лише активної учасниці трудового і суспільного життя, а й господині дому, матері. Жінки вибирають різні варіанти поєднання цих ролей. Конкретний вибір життєвого шляху жінка робить сама відповідно до своїх особистісних якостей, смаків, уподобань. Але можливість такого вибору залежить від того, яку економічну і моральну підтримку нададуть їй держава і суспільство на кожному з обраних нею шляхів [4].

Говорячи про проблеми гендерної рівності в суспільстві, не можна обминути проблеми чоловіків, оскільки вони також у певних випадках, а також певні категорії чоловіків, стикаються з виявами гендерної дискримінації та порушення їх прав.

Традиційне чоловіче виховання спричиняє загрозу для життя та здоров'я чоловіків, збільшує рівень каліцтва. Каліцтво чоловіків провокується традиційним вихованням хлопчиків, яке не тільки не зупиняє агресивність, а й не навчає розумній зваженості та стриманості. Хоча жінки страждають в основному від агресії чоловіків, та кількість чоловіків, які потерпають від насильства з боку тих же чоловіків, значно вища.

У законодавстві України чомусь йдеться лише про охорону материнства, при розлученні суд зазвичай присуджує дитину матері. Проте й чоловіки саме через своє специфічне гендерне виховання найчастіше, розлучаючись, розривають зв'язки з дитиною.

Гендерна дискримінація жінок і чоловіків в Україні залишила на початку третього тисячоліття нашій країні низку проблем: демографічну кризу, торгівлю людьми, насильство в сім'ї та насильство в суспільстві взагалі, гендерний дисбаланс в сільській місцевості за рахунок активного відпливу жінок з села (так званий "мовчазний жіночий бунт" внаслідок потрійного тягаря на плечах сільських жінок, тривалість робочого дня яких становить 16 годин) та інші.

Українське суспільство, яке перебуває у стані не надто динамічної і сповненої протиріч трансформації, демонструє низку специфічних умов, які заважають становленню паритетного суспільства. Чи не найважливішими з-поміж них є: відсутність політичної волі до утвердження паритетності у владних відносинах; брак настанов на гендерно-паритетні стосунки в масовій свідомості; засилля патріархальних стереотипів у суспільній свідомості і їх активний вплив на формування владних і суспільних відносин між громадянами країни; орієнтація на традиційні форми взаємовідносин в економічній сфері, коли існує усталений традиційний поділ на жіночі і чоловічі професії, заняття, форми економічної діяльності; притаманна постколоніальним суспільствам орієнтація на відновлене автентичне минуле, що у свою чергу формує орієнтовані на героїчну минувшину домінантні міфи, які не передбачають рівності й рівноправності між жінками і чоловіками; прагнення сильної влади ("сильної руки"), невід'ємної від урізання демократичних свобод, зокрема й у гендерному плані, що відсуває проблеми паритетності на маргінес суспільного розвитку; посилення свідомого опору становленню гендернопаритетного суспільства як форма посилення конкуренції між статями в соціальному просторі сучасної України [7].

Поняття дискримінації та, зокрема, дискримінації за ознакою статі міститься в ратифікованих Україною міжнародних договорах, які є частиною національного законодавства, в Конституції України та у спеціальних законах.

За визначенням, наведеним у статті 1 Конвенції про ліквідацію всіх форм дискримінації щодо жінок: "дискримінація щодо жінок" означає будь-яку різницю, виключення чи обмеження за ознакою статі, що спрямовані на ослаблення чи зведення нанівець визнання щодо жінок прав людини та основних свобод у політичній, економічній, соціальній, культурній, громадській чи будь-якій іншій галузі, користування ними жінками або здійснення їх жінками, незалежно від їх сімейного стану, на основі рівноправності чоловіків і жінок.

У статті 1 Закону України "Про забезпечення рівних прав та можливостей жінок і чоловіків" міститься визначення гендерної дискримінації як дискримінації за ознакою статі – ситуація, за якої особа та/або група осіб за ознаками статі, які були, є та можуть бути дійсними або припущеними, зазнає обмеження у визнанні, реалізації або користуванні правами і свободами або привілеями в будь-якій формі, встановленій Законом України "Про засади запобігання та протидії дискримінації в Україні", крім

випадків, коли такі обмеження або привілеї мають правомірну об'єктивно обґрунтовану мету, способи досягнення якої є належними та необхідними [8].

Законом України "Про засади запобігання та протидії дискримінації в Україні" встановлено, що дискримінацією є ситуація, за якої особа та/або група осіб за їх ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, віку, інвалідності, етнічного та соціального походження, громадянства, сімейного та майнового стану, місця проживання, мовними або іншими ознаками, які були, є та можуть бути дійсними або припущеними (далі – певні ознаки), зазнає обмеження у визнанні, реалізації або користуванні правами і свободами в будь-якій формі, встановленій цим Законом, крім випадків, коли таке обмеження має правомірну, об'єктивно обґрунтовану мету, способи досягнення якої є належними та необхідними, а непрямою дискримінацією – ситуація, за якої внаслідок реалізації чи застосування формально нейтральних правових норм, критеріїв оцінки, правил, вимог чи практики для особи та/або групи осіб за їх певними ознаками виникають менш сприятливі умови або становище порівняно з іншими особами та/або групами осіб, крім випадків, коли їх реалізація чи застосування має правомірну, об'єктивно обґрунтовану мету, способи досягнення якої є належними та необхідними [9].

Ідентифікувати дискримінацію можливо за наступними ознаками.

Пряма дискримінація – це коли: до особи ставляться у менш сприятливий спосіб, у порівнянні з тим, як ставилися чи могли б ставитися до інших осіб у подібній ситуації. Несприятливе ставлення має значення для встановлення факту дискримінації, якщо воно несприятливе для однієї особи порівняно з іншою особою, що перебуває в аналогічній ситуації. В контексті права ЄС у сфері зайнятості, є дискримінація за ознакою вагітності. Згідно з існуючою практикою ЄС, що була започаткована справою Деккер (Dekker), є чітке правило, що якщо жінка зазнає несприятливого ставлення через свою вагітність, його одразу класифікують як пряму дискримінацію за ознакою статі, без необхідності наводити зразок для порівняння), і причиною такого ставлення є наявність у особи певних характеристик, що відносяться до категорії захищених ознак.

Непряма дискримінація – нейтральне правило, норма права, критерій чи практика, що впливає на групу осіб, які мають "захищену ознаку", значно більше, ніж на інших осіб в аналогічній ситуації [10, с. 11-12].

Дискримінація проти жінок є досить розповсюдженою, зокрема, при прийомі на роботу. Не зважаючи на існування статті 17 Закону України "Про забезпечення рівних прав та можливостей чоловіків і жінок": "Роботодавцям забороняється в оголошеннях (рекламі) про вакансії пропонувати роботу лише жінкам або лише чоловікам, за винятком специфічної роботи, яка може виконуватися виключно особами певної статі, висувати різні вимоги, даючи перевагу одній із статей, вимагати від осіб, які влаштовуються на роботу, відомості про їхнє особисте життя, плани щодо народження дітей" [8], у багатьох оголошеннях щодо прийому на роботу стать респондентів вказана. Роботодавці порушують Закон України "Про забезпечення рівних прав та можливостей чоловіків і жінок", оскільки немає жодних санкцій за ці протиправні дії. У даному випадку в Україні не виконується Конвенція ООН про ліквідацію всіх форм дискримінації проти жінок в Україні, зокрема, стаття 2, де вказано, що держава зобов'язана приймати санкції, які забороняють будь-яку дискримінацію проти жінок.

Гендерна рівність належить до фундаментальних засад прав особи. Норми будь-якої галузі права повинні відповідати загальним принципам права, у тому числі принципу гендерної рівності. Таким чином, норми всіх без винятку галузей права мають певний гендерний вимір.

Категорія гендерної рівності містить множину імплікацій, а саме: рівність прав – це законодавче наділення однаковими правами осіб чоловічої та жіночої статей у всіх сферах життя; рівність можливостей – забезпечення (гарантії) на практиці рівних умов щодо рівного розподілу, використання політичних, економічних, соціальних та культурних цінностей, які виключають дискримінацію та обмеження будь-якої статі, що негативно впливають на життєдіяльність і самовираження; забезпечення рівних умов для реалізації прав та можливостей; "гендерна симетрія" – стан, при якому принцип рівних прав і можливостей для жінок і чоловіків реалізований на практиці [11, с. 466].

Окрім того, питанням позитивного впливу на формування правової свідомості громадян України і у сфері питання гендерної рівності активно займаються й українські провідні соціологи, психологи та активісти. Серед основних принципів формування гендерноуважного суспільства можливо визначити наступні: гендерна проблема не може розглядатись як виключно жіноча; справедливість ліпша за рівність; роль жінки не може применшуватись; гендерні стереотипи не повинні посилюватись ЗМІ, рекламою чи іншими шляхами; різноманіття є позитивним; використання гендерночутливої лексики; відкидання статусу жертви за статевою ознакою; поблажливість – недоречна; мають вагу факти, а не теорії; відкритість громадян – як основа змін.

Для вдосконалення політики становлення гендерної рівності в Україні перш за все необхідні зусилля щодо розширення гендерно-інформаційного простору. А це передбачає постійну серйозну увагу до проблем комунікацій, адже в добу глобалізації соціальний обмін і культурні простори, що їх формує взаємодія людей, набирають кардинально інших форм [13].

Нині Україна хоч і повільно, але просувається до гендерної рівності. Україна прагне стати повноправною частиною європейської спільноти, наблизившись до останньої за основними соціально-економічними показниками та стандартами життя. Для цього державі необхідно реалізувати свої зобов'язання щодо гендерної рівності.

Подолання традиційних гендерних стереотипів, творення нових форм і загальнолюдських стандартів для жінок і чоловіків, гендерної культури нового взірця – потреба перебудови України у контексті світової спільноти, створення нових форм міжнародного спілкування та міжнаціональних відносин.

Практика гендерних перетворень має враховувати систему потреб і критеріїв, які відображають сучасні уявлення про соціальну справедливість розподілу ролей між жінками й чоловіками в суспільному житті, соціально-трудових і сімейних взаємовідносинах, бізнесі, в інформаційній сфері.

Гендерна концепція суспільного розвитку покликана окреслити перспективи розвитку соціальної держави в контексті зміцнення гендерної демократії, що забезпечить здійснення соціально відповідальної політики і розкриття громадянського потенціалу особистості; підвищити рівень загальної і політичної культури суспільства, показниками якого є можливість самореалізації громадян і забезпечення рівноправності представників обох статей у всіх сферах життєдіяльності, включаючи суспільне виробництво, соціально-трудові та сімейні відносини.

Висновки.

Разом з зазначеними вище поглядами на оцінку значення та стану гендерної рівності необхідно визнати, що в сучасному українському суспільстві існує проблема як низької правосвідомості громадян в цілому, так і проблема статевої упередженості зокрема, що пояснюється пострадянським становищем України та тривалим перебуванням її представників у тісних рамках дозволеного й прийнятного.

Сьогодні помітним є позитивний вплив демократичних європейських тенденцій, які молодь України позитивно сприймає, перебуваючи при цьому, все ж, у певному стані дисонансу, що походить з закладеного виховання й реалій життя. Необхідними до вжиття є заходи просвітницького характеру серед молоді, та й старшого покоління, щодо визнання державою значимості не статі, а особистості, щодо можливостей розвитку кожної особи. Це вимагає подальшого вдосконалення національного законодавства відносно, зокрема, засобів реалізації механізмів упорядкування відповідних суспільних відносин.

Використана література

1. Федін Д.Г. Значення правосвідомості в системі суспільної свідомості. *Форум права.* 2011. № 9. С. 813-817.

2. Цимбалюк М.О. Формування правосвідомості громадян у процесі розбудови громадянського суспільства. Острог, 2005. 261 с.

3. Клімова Г.П. Свобода, рівність, справедливість, закон як цінності правосвідомості і правової культури українських громадян. Правосвідомість і правова культура як базові чинники державотворчого процесу в Україні: монографія. Харків: Право, 2009. 352 с.

4. Жидкова О.О. Проблеми гендерної рівності в Україні. URL: file:///C:/Users/User/Downloads/2190%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-4253-1-10-20150501.pdf (дата звернення: 24.04.2021).

5. Нечипорук Л.В. Проблеми впровадження гендерного балансу на ринку праці: матеріали наук.-практ. конф. *Впровадження гендерних підходів у діяльність правоохоронних органів України*, м. Київ, 18 – 19 трав. 2005 р.). Київ, 2005. С. 70-72.

6. Івченко Ю.В. Гендерна рівність в Україні (національні особливості). *Філософські та методологічні проблеми права.* 2013. № 1-2. С. 52-59.

7. Грабовська І. Гендерне паритетне суспільство в Україні: соціальна утопія чи реальна перспектива. URL: http://www.krona.org.ua/uk/ya-magazine (дата звернення: 01.05.2021).

8. Про забезпечення рівних прав та можливостей жінок і чоловіків: Закон України від 08.09.05 р. № 2866-IV. URL: https://zakon.rada.gov.ua/laws/show/2866-15#Text (дата звернення: 24.04.2021).

9. Про засади запобігання та протидії дискримінації в Україні: Закон України від 06.09.12 р. № 5207-VI. URL: https://zakon.rada.gov.ua/laws/show/5207-17#Text (дата звернення: 24.04.2021).

10. Гендерна дискримінація: ідентифікація та механізм надання правової допомоги: методичні рекомендації затверджені наказом Координаційного центру з надання правової допомоги від 12.03.19 р. № 33. ФОП Ковалишин, 2019. 94 с.

11. Марценюк Т. Гендерна дискримінація на ринку праці в Україні (на прикладі сексуальних домагань). *Наукові записки.* Т. 83. 2008. С. 50-55.

12. Крочук М.І. Гендерна рівність як складова загального принципу рівності. *Науковий вісник Львівського державного університету внутрішніх справ.* 2011. № 4. С. 464-471.

13. Іванченко С. Багатовимірна модель гендера. URL: https://docplayer.net/114523914-Bagatovimirna-model-gendera-s-m-ivanchenko.html (дата звернення: 01.05.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

До відома авторів

"**ІНФОРМАЦІЯ І ПРАВО**" – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   - *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   - *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   - *відстань між рядками – 1 інтервал;*
   - *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов'язкові структурні елементи:

   - УДК.
   - Ім'я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.
   - Назва статті (укр. та англ. мовами).
   - Анотація та ключові слова (укр., англ. та рос. мовами).
   - **Розв'язання проблеми,** шляхом наукового вирішення завдання:
     - **постановка проблеми** *(загальна характеристика);*
     - **результати аналізу наукових публікацій** – надаються відомості про стан вирішення проблеми та ПІБ авторів, з обов'язковим посиланням на їхні роботи (в […]), повний опис бібліографії яких вказується в підрозділі "Використана література"; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;
     - **формування мети** *(постановка завдання)* статті;
     - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
   - **Висновки** за результатами розв'язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
   - **Використана література.** Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання" або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.
   - Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- ***Актуальність теми***.
- ***Новизна та обґрунтованість одержаних результатів***.
- ***Наукова (практична) цінність результатів***.
- ***Висновок про можливість відкритої публікації***.

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України "Про затвердження порядку формування переліку наукових фахових видань України" від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов'язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту**.

Реквізити для оплати робіт:

Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України". Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 *(з приміткою – за науковий журнал).*

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада Інституту не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
  Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за додержання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:

– відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
– внесення до статті змін редакційного змісту у зв'язку з обмеженням обсягу загального матеріалу.

*** * * * * * * * * ***

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 2(37)/2021

Засновники журналу:	- Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"; - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини "Україна".
Видавець:	© ДНУ ІІБП НАПрН України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України". Тел.: 234-94-56; e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	URL: //www.ippi.org.ua – ДНУ ІІБП НАПрН України; URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.

Founders of journal:	- State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; - Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine; - Open International University of Human Development "Ukraine"
Publisher:	© IISL of the NALS of Ukraine.
Address of release:	01032, Kyiv, Saksaganskogo str., 110-V. State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine". Phone: 234-94-56; e-mail: bvm777@ ukr.net
Web-pages of journal in the network Internet:	URL: //www.ippi.org.ua – IISL of the NALS of Ukraine; URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.