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

№ 4(39)/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

№ 4(39)/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

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. 27.5. 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 № 10 від 09.12.21 р.

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

Informative Law

Informative and National Safety

Recommended for publication by the IISL of the NALS of Ukraine, protocol № 10 dated 09.12.21

Інформаційне право

УДК 342.5(351/354)

КОРЖ І.Ф., *доктор юридичних наук, с.н.с.,* завідувач наукової лабораторії
ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-0446-5975.

АМБІВАЛЕНТНІСТЬ ФУНКЦІОНУВАННЯ ПУБЛІЧНОЇ ВЛАДИ В УКРАЇНІ

Анотація. *В даній статті досліджується питання такого феномену сьогодення, як "амбівалентність", що є сучасним негативним явищем у функціонуванні органів публічної влади і відповідною перепоною у розбудові України, як демократичної, економічно розвинутої країни, яка прагне приєднатися до когорти розвинутих країн Європи. Проаналізовані причини виникнення згаданого явища і наведені конкретні приклади у сучасному житті українського суспільства. Зроблено висновки щодо шляхів подолання цього негативного явища.*

Ключові слова: *амбівалентність, громадянське суспільство, публічна влада, Конституційний Суд України, парламент України, Президент України.*

Summary*.This article examines the issue of such a phenomenon as "ambivalence", which is a modern negative phenomenon in the functioning of public authorities, as well as a corresponding obstacle in the development of Ukraine as a democratic, economically developed country that seeks to join the cohort of developed countries in Europe. The reasons for the occurrence of this phenomenon are analyzed and specific examples are given in the modern life of the Ukrainian society. Conclusions are made about the ways to overcome this negative phenomenon.*

Keywords: *ambivalence, civil society, public authority, Constitutional Court of Ukraine, Parliament of Ukraine, The President of Ukraine.*

Аннотация. *В данной статье рассматривается вопрос такого феномена, как "амбивалентность", которое является современным негативным явлением в функционировании органов публичной власти и соответствующим препятствием в развитии Украины, как демократической, экономически развитой страны, которая стремится присоединиться к когорте развитых стран Европы. Проанализированы причины возникновения этого явления и приведены конкретные примеры в современной жизни украинского общества. Сделаны выводы о путях преодоления этого негативного явления.*

Ключевые слова: *амбивалентность, гражданское общество, публичная власть, Конституционный суд Украины, парламент Украины, Президент Украины.*

Постановка проблеми. Нинішнє суспільне життя в Україні, сучасний процес його демократизації позначений не лише складностями духовно-ідеологічного самовизначення, суперечливістю процесів "відродження" і "модернізації". Головна особливість державного будівництва, здійснення демократичних перетворень в усіх сферах соціуму полягає в тому, що вони відбуваються в гострій ситуації, на фоні незавершених реформ політичних, економічних і соціальних інститутів.

Нині в Україні ще не сформувалися впливові політичні партії, які здійснювали б політичну мобілізацію мас саме на демократичні перетворення. Енергія інтелектуальних сил, ангажованих до політичної діяльності, часто-густо використовується нераціонально: значна частина партій здебільшого кристалізує конфліктні інтереси, суспільні розбіжності та суперечності.

Внаслідок значного зубожіння основних верств населення соціальна база демократичних реформацій в Україні виглядає значно вужчою порівняно зі східноєвропейськими країнами, країнами колишнього соціалістичного табору.

На перший погляд не існує серйозних перешкод вітчизняному процесу демократизації, оскільки створена належна правова база, інтегрована до європейських демократичних принципів. Однак на практиці існують значні проблеми реалізації згаданих принципів і побудови в Україні дійсно демократичного устрою, успішної та економічно розвинутої держави, що підтверджується не лише внутрішніми різнобічними проблемами суспільного життя, які відомі українцям, а й тими проблемами, на яких акцентують увагу наші зарубіжні партнери. Найголовніша з них – це розбіжність між напрацьованою правовою базою регулювання суспільних відносин та реалізацією правових норм у практичному житті українських громадян.

Суперечністю позначене і питання демократичного узгодження принципу народовладдя з вимогами професіоналізму та компетентності у справах державного управління.

Метою статті є дослідження питання та здійснення аналізу стану сучасного етапу демократичних трансформацій в Україні; напрацювання висновків – чи потребує посилення механізмів безпосередньої участі громадян у суспільно-політичних процесах, чи неефективність функціонування основних інститутів публічної влади обумовлена недостатністю громадського контролю за їх діяльністю та обмеженням політичної участі громадян лише електоральними процесами, чи подальший розвиток форм прямої демократії в Україні обумовлює необхідність удосконалення конституційних засад реалізації механізмів безпосередньої участі громадян в управлінні державними справами.

Виклад основного матеріалу. Україна здійснює заходи щодо напрацювання відповідних умов, які забезпечать її вступ до цивілізованої, економічно розвинутої, з демократично діючими принципами сім'ї європейських народів. І головною рушійною силою реалізації зазначеного є подальше зміцнення української державності, становлення демократичних інститутів, розвитку громадянського суспільства, що мають забезпечувати високоосвічені, активні та відповідальні громадяни України. Зазначені якості, а головне – відповідальність за долю власної країни, мають закладатися й формуватися у кожного громадянина ще в дитячі і підліткові роки, а розвиватися і реалізовуватися – в період активної життєдіяльності.

Серед ключових практичних завдань у зазначений період в сучасному світі є розуміння та активна позиція громадян щодо демократичних перетворень, суспільної модернізації, інноваційного розвитку суспільства і держави. Дедалі більшої гостроти набуває проблема розуміння та активна участь у забезпеченні демократичного й мирного врегулювання соціально-політичних конфліктів та криз. Крім того, на своє вирішення очікують нові для суспільства глобальні та регіональні проблеми різного характеру. Іншими словами, світ вступив у полосу потужних політичних перетворень, які вимагають прискіпливого й вдумливого аналізу.

У сучасному глобалізованому світі демократичні процеси значною мірою впливають на формування внутрішніх складових повсякденного життя дедалі більшого кола громадян, а тому пояснення цих феноменів є нагальною потребою у формуванні їхнього світогляду. І в цьому надважливого значення набуває такий дуалізм діяльності суб'єктів забезпечення зазначеного, як поєднання активних зусиль публічної влади у цій сфері та зайняття щодо цього активної життєвої позиції з боку кожного громадянина.

Відповідно до теорії плюралістичної демократії, авторами якої є Е. Хейвуд [1] та Г. Ласк (Великобританія) [2] держава є органом, що відповідальний за нормальне

функціонування всіх секторів суспільної системи. Головна роль держави полягає в підтримці суспільної справедливості і вона є арбітром, що гарантує дотримання законів, правил гри для кожного члена суспільств, не допускаючи монополізації влади.

Відповідно до теорії партиципаторної демократії, представниками якої є К. Пейтман (автор терміну "демократія участі"), К. Макферсон та Б. Барбер [3], громадяни повинні активно брати участь не тільки у виборі своїх представників, і, навіть, не тільки в прийнятті рішень на референдумах, але й безпосередньо – в підготовці, прийнятті і здійсненні рішень, а також в контролі за їх реалізацією.

Представницька теорія демократії має концепцію розуміння демократії як компетентного і відповідального перед народом представницького правління. Реально репрезентативна демократія зазвичай втілюється в парламентаризмі, головний принцип якого – обмеження безпосередньої участі мас в управлінні. Головним носієм демократичних цінностей є не маса рядових громадян, котра часто є некомпетентною, легко піддається ідеологічним впливам, а так звана "еліта", котра здатна більш ефективно управляти суспільством, і захищати цінності ліберальних демократів. Маса ж повинна мати право періодично контролювати згадану "еліту" за допомогою виборів, впливати на її склад. Інші існуючі теорії демократії більш строкаті і не представляють широкого інтересу.

Таким чином, відповідно до численних наукових визначень терміну "демократія", можна виділити її наступні основні критерії:

– безпосереднє або/та представницьке (через вибраних представників) управління країною самими людьми;

– форма держави, країни, суспільства, що мають демократичний уряд;

– правління більшості;

– сприйняття і реалізація принципу рівності, прав і свобод громадян, а також їх можливостей.

Доцільним є згадка про основні принципи, на яких базується демократія. Такими принципами є:

– поділ влади, за якої кожна з гілок (законодавча, виконавча і судова) володіє власними специфічними функціями;

– виборність основних органів публічної влади, що передбачає відповідальність владних структур перед виборцями і періодичність переобрання через вільні вибори;

– плюралізм, що передбачає законність існування різних соціально-політичних сил; виключення монополії на владу з боку будь-кого; проголошення ідеї самого широкого вибору в усіх сферах суспільного життя; наявність опозиції; різнобічність думок;

– гласність, що передбачає доступ преси і громадськості до інформації про діяльність органів публічної влади, установ і організацій, донесення такої інформації до широкого загалу;

– рівність, тобто політична рівність усіх перед законом;

– більшість, за яким рішення приймаються на основі думи більшості, але з урахуванням і дотриманням інтересів і прав меншості;

– належний контроль, який здійснюється громадськими об'єднаннями, самими громадянами самостійно або з органами державного контролю за діяльністю державних структур. Основним методом контролю є перевірка діяльності та виконання ухвалених рішень, дотримання вимог чинного законодавства. За результатами перевірок громадськість та відповідні державні органи інформуються про виявлені порушення, пропонуються пропозиції щодо притягнення правопорушників до відповідальності.

Зазначимо, що серед головних критеріїв демократичності суспільства є наявність і дотримання основоположних прав і свобод людини. Розуміння людини як абсолютної цінності, пріоритет прав та інтересів людини над будь-якими іншими (класовими, партійними, національними та ін.) правами.

Дуже важливим та актуальним для розвитку демократії в Україні є впровадження механізмів самоврядування, яке є частиною системи державного управління і проявом функціонування громадянського суспільства. У зв'язку з цим, особливої ваги набуває потреба підвищення статусу і розширення повноважень місцевих органів влади, а також активна участь у житті місцевих громад насамперед тих громадян, які займають активну життєву позицію.

Основний Закон України [4], а саме ст. 5 зазначає, що "Носієм суверенітету і єдиним джерелом влади в Україні є народ. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування. Право визначати і змінювати конституційний лад в Україні належить виключно народові і не може бути узурповане державою, її органами або посадовими особами. Ніхто не може узурпувати державну владу".

Зазначеним положенням надано визначення Конституційним Судом України у відповідних рішеннях [5]. Так, щодо єдиного джерела влади зазначено, що це треба розуміти так, що в Україні вся влада належить народові. Влада народу є первинною, єдиною і невідчужуваною та здійснюється народом шляхом вільного волевиявлення через вибори, референдум, інші форми безпосередньої демократії у порядку, визначеному Конституцією та законами України, через органи державної влади та органи місцевого самоврядування, сформовані відповідно до Конституції та законів України.

Що ж до зміни конституційного ладу, то тільки народ має право безпосередньо шляхом всеукраїнського референдуму визначати конституційний лад в Україні, який закріплюється Конституцією України, а також змінювати конституційний лад внесенням змін до Основного Закону України в порядку, встановленому його Розділом XIII.

Щодо того, що ніхто не може узурпувати державну владу, то це треба розуміти як заборону захоплення державної влади шляхом насилля або в інший неконституційний чи незаконний спосіб органами державної влади та органами місцевого самоврядування, їх посадовими особами, громадянами чи їх об'єднаннями. А як назвати, наприклад, дії Президента України у його протистоянні із судовою гілкою державної влади, насамперед з Конституційним Судом, діяльність якого фактично паралізована?

До такого стану призвели неконституційні дії гаранта Конституції (ст. 102), що є своєрідним парадоксом! Повноваження Президента України визначаються Конституцією України (ст. 106), а у відповідних законах вони можуть лише дублюватися, а не збільшуватися і розширюватися. Однак гарант Конституції у своїх діях щодо скасування актів разової дії, якими є Укази Президента України про призначення у 2013 році суддів Конституційного Суду України (О.М. Тупицького і О.В. Касмініна), і які не можуть апріорі бути скасованими, вийшов за межі своїх повноважень і можливостей здійснювати відповідні дії. Зазначені акти є ненормативними актами, передбачають конкретні приписи, звернені до окремого суб'єкта чи юридичної особи, застосовуються одноразово і після реалізації вичерпують свою дію [6], а тому не можуть бути скасовані. На відміну від зазначених ненормативних актів, нормативним актам притаманна невизначеність дії у часі та неодноразовість їх застосування, такі акти стосуються не індивідуально визначених суб'єктів, а охоплюють їх широке коло і розраховані на неодноразовість застосування, а тому можуть бути скасовані.

Такі амбівалентні дії (сутність амбівалентності розкривається нижче) гаранта Конституції не підтверджують принцип дотримання права у державі і не слугують прикладом дотримання правової культури, боротьби з правовим нігілізмом, підривають віру громадян в справедливість.

Окрім зазначеного, до форм безпосередньої демократії відноситься право кожного брати участь в управлінні своєю державою як безпосередньо, так і через вільно обраних представників, направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування. Зазначене цілком відповідає вимогам ст. 21 Загальної декларації прав людини, яка проголошує право кожного брати участь в управлінні своєю державою як безпосередньо, так і через вільно обраних представників [7].

Конституція України також закріплює право громадян мирно збиратися та проводити мітинги і демонстрації. Така форма безпосередньої участі передбачає обговорення під час громадських зборів важливих суспільно-політичних проблем в різних сферах, а також питань, пов'язаних із виборами, законодавчими актами та окремих державних рішень. І в цьому насамперед полягає створення в державі громадянського суспільства.

Зазначимо, що формування громадянського суспільства є однією з найважливіших умов у подальшому розвитку України, що здійснюється шляхом проведення економічних, політичних і правових реформ, які, передусім, спрямовуватимуться на демократизацію громадського життя, лібералізацію економіки, захист прав і свобод людини і громадянина, становлення правової демократичної держави. Саме про необхідність взаємодії органів державної влади, органів місцевого самоврядування з громадськістю йдеться у Національній стратегії сприяння розвитку громадянського суспільства на 2016 – 2020 роки [8], а також в Національній стратегії на 2021 – 2026 роки [9].

Як зазначено в документах, ураховуючи підвищення ролі громадянського суспільства в різних сферах діяльності органів державної влади та органів місцевого самоврядування, зокрема щодо впровадження реформ, на підтримку ініціативи громадськості, а також з метою налагодження ефективного діалогу та партнерських відносин органів державної влади, органів місцевого самоврядування з організаціями громадянського суспільства, передусім з питань забезпечення прав і свобод людини і громадянина, відповідно до частини другої статті 102 Конституції України та відповідно до пункту 28 частини першої статті 106 Конституції України, зазначені документи прийняті з метою створення сприятливих умов для формування та діяльності інститутів громадянського суспільства. Ознакою сталості громадянського суспільства є саме функціонування інститутів громадянського суспільства, через які громадяни та суспільні групи забезпечують самоорганізацію, представництво, реалізацію і захист прав та інтересів.

Партнерство між державою та громадянським суспільством є вагомим чинником реалізації демократичних цінностей, закріплених у положеннях Конституції України, зокрема щодо свободи та особистої недоторканності громадян, свободи слова і думки, свободи вираження поглядів і переконань, свободи світогляду і віросповідання, свободи об'єднання, участі громадян в управлінні державними справами тощо.

Громадянське суспільство є виразником та захисником інтересів і прагнень різноманітних суспільних груп та громадян. Громадянське суспільство здатне зробити значний внесок у сталий розвиток держави шляхом надання соціальних послуг, забезпечення здійснення соціального підприємництва, збільшення кількості робочих місць і самозайнятих осіб, поліпшення бізнес-середовища, протидії корупції, сприяння прозорості діяльності органів державної влади та органів місцевого самоврядування та

реалізації інших суспільно корисних проектів. Інститути громадянського суспільства в Україні також відіграють активну роль у сприянні відновленню територіальної цілісності та розбудові миру.

Ураховуючи роль громадянського суспільства у різних сферах суспільного життя, створення сприятливих умов для його розвитку та налагодження взаємодії з його інститутами є важливим завданням органів державної влади, органів місцевого самоврядування. Правові засади державної політики сприяння розвитку громадянського суспільства закладені у Конституції України [4], законах України "Про засади внутрішньої і зовнішньої політики" [10], "Про місцеве самоврядування в Україні" [11], а також законах України, що визначають правовий статус та засади діяльності інститутів громадянського суспільства, а саме у законах України "Про громадські об'єднання" [12], "Про благодійну діяльність та благодійні організації" [13], "Про професійні спілки, їх права та гарантії діяльності" [14], "Про організації роботодавців, їх об'єднання, права і гарантії їх діяльності" [15], "Про свободу совісті та релігійні організації" [16], "Про професійних творчих працівників та творчі спілки" [17], "Про органи самоорганізації населення" [18] та інших.

Однак зазначені вище принципи і критерії нині залишаються і будуть залишатися малоефективними через недостатню прозорість діяльності державних органів, насамперед виконавчої гілки влади, та забюрократизовані процедури взаємодії з громадянським суспільством, зберігаючи при цьому низький рівень взаємної довіри. Так Урядом, як свідчать численні факти, фактично продовжується недотримування (ігнорування) положень згаданих вище актів, так само як і відповідних положень Національної стратегії у сфері прав людини [19], Стратегії людського розвитку [20], а також Регламенту Уряду (його параграфу 3 "Взаємодія з громадськістю") [21] та своєї Постанови № 996 [22]. Тим самим Уряд свідомо чи несвідомо фактично саботує подальший розвиток в Україні громадянського суспільства.

При цьому доцільно зазначити конкретні міжнародні акти у даній сфері, положення яких, незважаючи на взяті на себе Україною зобов'язання щодо їх безумного виконання, порушуються публічною владою України – Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (ІІІ) Генеральної Асамблеї ООН від 10 грудня 1948 р.; Міжнародний пакт про громадянські й політичні права від 16 грудня 1966 р.; Резолюція 53/31 Генеральної Асамблеї ООН від 23 листопада 1998 р. "Підтримка системою Організації Об'єднаних Націй зусиль урядів з розвитку і зміцнення нових чи відроджених демократій"; Про захист прав людини і основоположних свобод: Європейська Конвенція від 04 листопада 1950 р.; Європейська соціальна хартія від 18 жовтня 1961 р.; Копенгагенська нарада Конференції з людського виміру ОБСЄ від 29 червня 1990 р. тощо.

Засади громадянської участі в управлінні державними справами, які закладені в Резолюціях та інших актах Парламентської Асамблеї Ради Європи (далі – ПАРЄ), положення яких має виконуватися владою України, теж часто фактично ігноруються державною виконавчою владою. Так, у Резолюції 980 (1992) "Про участь громадян у політиці" ПАРЄ підтверджує: "демократія атрофується без широкої участі громадян, з якими повинні, де це можливо, консультуватися з питань, що їх безпосередньо стосуються, за допомогою відповідних механізмів" (п. 2). На виконання цієї Резолюції була прийнята Рекомендація ПАРЄ 1180 (1992) "Про участь громадян у політиці", яка наголошує на важливій ролі неурядових організацій (асоціацій, фондів, рухів або груп, незалежних від уряду, заснованих на некомерційній основі для захисту певних інтересів) у розвитку участі громадян у політичному житті. Інші акти, такі як Резолюція

ПАРЄ 1121 (1997) “Про інструменти участі громадян у представницькій демократії” та Резолюція ПАРЄ 1154 (1998) “Демократичне функціонування національних парламентів” наголошують, що дієвість демократії залежить від активного внеску всіх громадян. Їх участь у політичному житті та співробітництво в межах політичних інституцій є вирішальним фактором налагодженого функціонування демократичних інституцій (установ). Тому ПАРЄ звернула увагу на необхідність більш широкої участі громадян у прийнятті політичних рішень.

Необхідно зазначити, що нормотворча (законотворча) формалізація зазначених вище вимог, критеріїв і принципів в діяльності публічної влади України є лише півкроком до їх належного виконання та застосування, що, у свою чергу, реалізується шляхом нормозастосування та підзаконної нормотворчої діяльності. Значні порушення, недотримання згаданих вище зобов’язань відбуваються саме в нормозастосовній практиці влади – органів виконавчої влади, судової влади та органів місцевого самоврядування.

Тобто, в умовах потреби належної законодавчої нормотворчої діяльності органів публічної влади, існує розбіжність у нормозастосовній практиці щодо застосування та дотримання положень формалізованих зазначених вище вимог, критеріїв і принципів, а також у підзаконній нормотворчій діяльності, можна назвати ***амбівалентністю*** (від. лат. *ambo* – “обидва” і лат. *valere* – “володіти, діяти”) [23]. За узагальненням, *амбівалентність* – це *стан роздвоєності у діяльності; у співіснуванні протилежностей у відносинах, в станах тощо, за наявності існування одночасно позитивного і негативного факторів*.

Водночас, необхідно зазначити, що в Україні і законотворчій діяльності притаманні певні факти амбівалентності. Для прикладу можна навести положення статті 62 і 64 Конституції України [4] щодо “невинуватості особи у вчиненні злочину і не можливості бути підданою кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду”; що “конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. В умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. Не можуть бути обмежені права і свободи, передбачені статтями 24, 25, 27 – 29, 40, 47, 51, 52, 55 – 63 цієї Конституції”.

І от Верховна Рада України, “з метою захисту та утвердження демократичних цінностей, верховенства права та прав людини в Україні”, “примудрилася” прийняти Закон України “Про очищення влади” [24], який є наочним прикладом грубого і зухвалого (з правової точки зору) порушення зазначених прав людини. Десятки, якщо не сотні тисяч українських громадян, без суду і слідства були визнані правопорушниками лише за сферою відповідної діяльності та навчання (у відповідних ВУЗах) і позбавлені конституційних прав на різні періоди часу.

У зв’язку із зазначеним, доцільно навести короткий зміст проміжного висновку Європейської Комісії за демократію через право (далі – Венеціанська Комісія) щодо згаданого Закону, який був схвалений на 10-й її Пленарній сесії [25].

Венеціанська Комісія оцінила Закон “Про люстрацію” у світлі чотирьох основних принципів, що випливають з відповідних міжнародних стандартів, а саме, що:

– провина повинна бути доведена в кожному конкретному випадку;

– право на захист, презумпція невинності і право на оскарження в суді мають бути гарантовані;

– повинні бути дотримані різні функції і цілі з однієї сторони люстрації, а саме захист нової демократії, та з іншої сторони кримінальне право, тобто покарання осіб провину яких доведено;

– люстрація повинна відповідати суворим часовим рамкам як в період її виконання, так і в період перевірки.

Комісія дійшла наступних основних висновків:

a) Застосування люстраційних заходів до періоду правління радянської комуністичної влади через стільки років після закінчення цього режиму і вступ в силу демократичної конституції в Україні потребують переконливих причин, щоб обґрунтувати наявність конкретної загрози для демократії, яку колишні комуністи становлять на даний час. Комісія вважає, що важко виправдати таку пізню люстрацію.

b) Застосування люстраційних заходів стосовно недавнього періоду, протягом якого пан Янукович був Президентом України, в кінцевому рахунку поставить під сумнів реальне функціонування конституційних і правових рамок України як демократичної держави, заснованої на верховенстві права.

c) Закон "Про люстрацію" містить кілька серйозних недоліків і потребує перегляду, принаймні, наступних положень:

– Люстрація повинна стосуватися тільки посад, які можуть дійсно становити значну загрозу для прав людини та демократії; перелік посад, які підлягають люстрації, повинен бути переглянутий;

– Провина повинна бути доведена в кожному конкретному випадку і не може припускатися на підставі лише приналежності до категорії державних установ; критерії для люстрації повинні бути переглянуті;

– Відповідальність за проведення процесу люстрації повинна бути знята з Міністерства юстиції та покладена на спеціально створену незалежну комісію, за активної участі громадянського суспільства;

– Процедура люстрації повинна поважати гарантії справедливого судового розгляду (право на адвоката, рівність сторін, право бути вислуханим особисто); судові розгляди повинні призупинити адміністративне рішення про люстрацію до ухвалення остаточного рішення; Закон "Про люстрацію" повинен конкретно передбачати ці гарантії;

– Люстрація суддів повинна регулюватися лише одним законом а не тими, які перекриваються і здійснюватися тільки при повній повазі конституційних положень, що гарантують їх незалежність, і тільки Вища рада юстиції повинна нести відповідальність за будь-яке звільнення судді;

– Інформація про осіб, що підлягають люстраційним заходам, повинна оприлюднюватися тільки після остаточного рішення суду.

Українська влада погодилася, що Закон "Про люстрацію" вимагає вдосконалення з метою відповідності міжнародним стандартам і звернулася за допомогою до Венеціанської комісії. Комісія вітає прихильність української влади і готова надати свою підтримку у внесенні поправок до Закону "Про люстрацію".

Однак, як показала українська реальність, парламент не прислухався до зауважень Комісії, внаслідок чого українські суди "завалені" судовими позовами постраждалих громадян, так само як і Європейський суд з прав людини (далі – ЄСПЛ). Саме ЄСПЛ, рішенням Великої палати відмовилась задовольнити апеляцію української влади у справі "Полях та інші проти України". Таким чином, суд підтвердив, що закон про люстрацію в Україні порушує права людини. В підтвердження зазначеного, Міністр юстиції України Денис Малюська, коментуючи рішення великої палати ЄСПЛ, наголосив, що Мінюст зробить усе, "щоб забезпечити права громадян та збереження механізму люстрації, хоч і в обмеженому вигляді". У своєму повідомленні у соцмережі Facebook він зауважив, що ЄСПЛ "не визнавав неправомірною люстрацію цілком, а лише її надмірний обсяг.

…Окремі категорії громадян, на думку суду, були автоматично люстровані, хоча нічого поганого не вчиняли", зазначив український чиновник [26].

Подібна амбівалентність у нормотворчій діяльності притаманна і українським судам. Для прикладу наведемо наступне [27]: відповідно до ст.ст. 263 і 263-1 Кримінального кодексу України (далі – КК України) передбачена кримінальна відповідальність за "Незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами" та за "Незаконне виготовлення, переробка чи ремонт вогнепальної зброї або фальсифікація, незаконне видалення чи зміна її маркування, або незаконне виготовлення бойових припасів, вибухових речовин чи вибухових пристроїв".

За різними даними за 2007 – 2016 рр. В Україні до кримінальної відповідальності лише за ст. 263 КК України було притягнуто 52011 осіб. В державі має функціонувати закон, положенням якого регулювалися б згадані питання і за порушення яких, громадяни несли б зазначену відповідальність відповідно до КК України. Однак, до цього часу такий закон в Україні відсутній, хоча робилися неодноразові спроби щодо його розробки і прийняття. Цілком логічно постає питання: за яких правових підстав, за відсутності відповідного закону, громадян притягують до кримінальної відповідальності?

Ще зовсім недавно (вирок від 19 лютого 2018 р.) Печерський районний суд, виправдовуючи підсудного у справі № 757/7651/16-к, зазначив, що держава не має права застосовувати до особи процесуальний примус у вигляді кримінальної відповідальності за відсутність дозволу, передбаченого законом, поки немає закону, який передбачає отримання цього дозволу. І зазначене, на наше переконання, є цілковитою правовою позицією суду, оскільки відповідає загальновизнаній правовій засаді *"nullum crimen sine lege"* (немає злочину і покарання без наперед установленого закону). Зазначимо, що зазначений принцип закріплений в статті 7 Міжнародної Конвенції про захист прав людини і основоположних свобод від 04.11.1950 р.: "Нікого не може бути визнано винним у вчиненні будь-якого кримінального правопорушення на підставі будь-якої дії чи бездіяльності, яка на час її вчинення не становила кримінального правопорушення згідно з національним законом або міжнародним правом…".

Однак, 31 травня 2018 року колегія суддів Другої судової палати Касаційного кримінального суду Верховного Суду у своїй постанові (справа № 127/27182/15-к, провадження № 51-3305км18) зазначила, що поняття "закон", вжите законодавцем у ст. 263 КК України**,** має розширене тлумачення і включає в себе законодавство у цілому, в тому числі нормативні акти, що регулюють відповідні правовідносини, порушення яких утворює об'єктивну сторону складу злочину, передбаченого цією статтею кримінального закону. Під розширеним поняттям "закон" Верховний Суд має на увазі відповідний наказ Міністерства внутрішніх справ України**,** прийнятий на підставі Закону України "Про міліцію", який, до речі, втратив чинність 2 липня 2015 р.

На нашу думку, хибність даної позиції Суду полягає у наступному:

По-перше, об'єктивна сторона злочину за статтями 263 і 263-1 КК України полягає у незаконному поводженні зі зброєю, бойовими припасами або вибуховими речовинами та у незаконному виготовленні, переробці чи ремонті вогнепальної зброї або фальсифікації, незаконному видаленні чи зміні її маркування, або незаконному виготовленні бойових припасів, вибухових речовин чи вибухових пристроїв. Таким чином, законодавець визначив функціонування (наявність) закону, предметом регулювання якого є регулювання суспільних відносин, пов'язаних із зазначеним вище, і яким передбачено отримання дозволу на зазначене. Тобто, призначення згаданого закону полягає у здійсненні регулятивної функції. У свою чергу, відповідно до частини другої ст. 178 Цивільного кодексу України "Види об'єктів цивільних прав, перебування яких у

цивільному обороті не допускається (об'єкти, вилучені з цивільного обороту), мають бути прямо встановлені у законі. Види об'єктів цивільних прав, які можуть належати лише певним учасникам обороту або перебування яких у цивільному обороті допускається за спеціальним дозволом (об'єкти, обмежено оборотоздатні), встановлюються законом".

Основна ж функція кримінального права – це охоронна функція. Саме кримінальне право через застосування КК України покликано стояти на сторожі найважливіших суспільних відносин від їх порушення, застосовувати до винних найсуворіші заходи примусу – покарання. Як зазначає відомий науковець П. Фріс – кримінальне право, охороняючи нормами Особливої частини КК України суспільні відносини, не регулює їх, а для визначення факту порушення в ряді випадків відсилає через банкетну норму до регуляторних актів інших галузей права, у даному випадку до закону, якого не існує. У свою чергу, Конституційний Суд України зазначає, що бланкетна диспозиція кримінально-правової норми лише називає або описує злочин, а для повного визначення його ознак відсилає до інших галузей права.

По-друге, тлумачення Судом терміну "закон" в широкому сенсі, що включає в себе усі нормативно-правові акти публічної влади, не відповідає положенням загальної теорії держави і права і національному законодавству. Закон є творінням законодавчої влади.

В Україні використовується в широкому сенсі термін "законодавство", але не "закон", оскільки в країні не запроваджено делеговане законодавство, як це передбачено в конституціях багатьох європейських країн. Як зазначає суддя Конституційного суду України В. Кампо – в Конституції Італії з 1947 року передбачено здійснення законодавчих функцій парламенту може бути делеговано уряду. Аналогічні конституційні положення є в конституціях Іспанії 1978 року, Франції 1958 року, а також у Великобританії.

В Україні досвід застосування такого інституту був у Президента України Л. Кучми у 1990-х роках. Лише в окремих федеративних державах (Австрія, Бельгія, Федеративна республіка Німеччина, Швейцарія, Російська Федерація...) поряд з "федеральним законом" використовується вираз "закони учасника федерації", які мають назви, такі як "декрети" або "постанови". Федеральний закон та закон учасника федерації мають однаковий статус. Однак, в деяких федеративних державах "федеральний закон має перевагу над кантональним правом".

Таким чином, вищезазначене дає підстави констатувати факт відсутності на сьогодні в Україні закону, що здійснює регуляцію суспільних відносин в сфері обігу зброї, боєприпасів та вибухових речовин, що у свою чергу не дає можливості визначати законність чи незаконність тих чи інших дій із зазначеними предметами. Тим не менш органи досудового розслідування продовжують реєструвати кримінальні провадження та здійснювати попереднє розслідування, а суди виносити обвинувальні вироки за ст.ст. 263 і 263-1 КК України. При цьому вони посилаються на порушення особами порядку обігу цих предметів, врегульованого підзаконними актами.

Викликає, м'яко кажучи, подив твердження Суду, що законодавець, використовуючи термін "закон", мав на увазі його розширене тлумачення – "законодавство" у цілому. Зазначене є перекручуванням термінологічного змісту з певним умислом (можливо в будь-який спосіб заповнити існуючий вакуум правового регулювання даної сфери), оскільки законодавець чітко знає свої повноваження щодо врегулювання суспільних відносин шляхом прийняття ним законів, як це і передбачено Конституцією України.

Таким чином, притягнення особи до кримінальної відповідальності у згаданих випадках грубо порушує Конституцію України, і влада не має права застосовувати до особи процесуальний примус у вигляді кримінальної відповідальності.

Крім того, термінологічні маніпуляції з метою надання вироку певного вигляду законності це – прийняття завідомо неправосудного рішення і створення великої загрози правовій безпеці суспільства. Зазначена амбівалентність у діяльності публічної влади України викликає у наших європейських партнерів ознаки недовіри і сумніви в оперативному подоланні цього негативного фактору на шляху інтеграції нашої держави до Євросоюзу.

Висновки.

Підсумовуючи викладене вище, необхідно зазначити, що нинішня політична ситуація в державі яскраво демонструє хиткість і вразливість молодої української демократії перед викликами авторитаризму. Дії публічної влади, чи то в нормотворчій, чи нормозастосовній практиці, свідчать про наявні проблеми в житті українського суспільства, як то:

– посилення протистояння владних інститутів і конфліктність у політичній системі держави;

– відособленість органів публічної влади та їх посадових осіб від представників громадянського суспільства, наслідком чого є відірваність державної влади від потреб суспільного розвитку;

– відхід політичних структур, які знаходяться у владі, від положень передвиборчих програм;

– непрозорість процесів підготовки та ухвалення рішень органами публічної влади;

– низька довіра до органів публічної влади з боку громадян тощо.

Зазначене викликано насамперед таким негативом, як амбівалентність дій публічної влади, коли слова/обіцянки розходяться з практичними діями. Тому важливим для українського суспільства у його поступу до когорти демократичних і розвинутих країн Європи є поширення у суспільних колах запиту на наявність та ефективність дії демократичних процедур з метою впливу на органи публічної влади задля налагодження рівноправного та взаємовигідного діалогу між владою та суспільством. Така стратегія зі зміцнення системи суспільних зв'язків дозволить кожній громадській інституції посилити власну спроможність у відстоюванні інтересів відповідної соціальної групи та суспільства в цілому.

Використана література

1. Хейвуд Эндрю. Политология: учебник для студентов вузов ; пер. с англ. под ред. Г.Г. Водолазова, В.Ю. Вельского. Москва: ЮНИТИ-ДАНА, 2005. 544 с.

2. Теория плюралистической демократии Г. Ласки. URL: https://studme.org/82774/politekonomiya/teoriya_plyuralisticheskoy_demokratii_laski (дата звернення: 10.10.2021).

3. Теория политики: учебное пособие. Серия 2 ; под ред. Б.А. Исаева. СПб.: Питер, 2008. 464 с. ил. URL: http://politics.ellib.org.ua/pages-cat-70.html (дата звернення: 10.10.2021).

4. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

5. Рішення Конституційного Суду України у справі за конституційним поданням 60 народних депутатів України про офіційне тлумачення положень частини першої статті 103 Конституції України в контексті положень її статей 5 та 156 за конституційним зверненням громадян Галайчука Вадима Сергійовича, Подгорної Вікторії Валентинівни, Кислої Тетяни Володимирівни про офіційне тлумачення положень частин другої, третьої, четвертої статті 5 Конституції України (справа про здійснення влади народом) від 5 жовтня 2005 року № 6-рп/2005. URL: https://zakon.rada.gov.ua/laws/show/v006p710-05#Text (дата звернення: 13.10.2021).

6. Рішення Конституційного Суду України від 16 квітня 2009 року № 7-рп/2009, у справі за конституційним поданням Харківської міської ради щодо офіційного тлумачення положень частини другої статті 19, статті 114 Конституції України, статті 25, частини чотирнадцятої статті 46, частини першої, десятої статті 59 Закону України "Про місцеве самоврядування в Україні" (справа про скасування актів органів місцевого самоврядування). URL: https://zakon.rada.gov.ua/laws/show/v007p710-09#Text (дата звернення: 07.11.2021).

7. Загальна декларація прав людини від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 13.10.2021).

8. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26.02.16 р. № 68/2016. URL: https://zakon.rada.gov.ua/laws/show/68/2016#Text (дата звернення: 14.10.2021).

9. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021 – 2026 роки: Указ Президента України від 07.09.21 р. № 487/2021. URL: https://zakon.rada.gov.ua/laws/show/487/2021#n17 (дата звернення: 14.10.2021).

10. Про засади внутрішньої і зовнішньої політики: Закон України від 01.07.10 р. № 2411-VI. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text (дата звернення: 14.10.2021).

11. Про місцеве самоврядування в Україні: Закон України від 21.05.97 р. № 280/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text (дата звернення: 14.10.2021).

12. Про громадські об'єднання: Закон України від 22.03.12 р. № 4572-VI. URL: https://zakon.rada.gov.ua/laws/show/4572-17#Text (дата звернення: 14.10.2021).

13. Про благодійну діяльність та благодійні організації: Закон України від 05.07.12 р. № 5073-VI. URL: https://zakon.rada.gov.ua/laws/show/5073-17#Text (дата звернення: 14.10.2021).

14. Про професійні спілки, їх права та гарантії діяльності: Закон України від 15.09.99 р. № 1045-XIV. URL: https://zakon.rada.gov.ua/laws/show/1045-14#Text (дата звернення: 14.10.2021).

15. Про організації роботодавців, їх об'єднання, права і гарантії їх діяльності: Закон України від 22.06.12 р. № 5026-VI. URL: https://zakon.rada.gov.ua/laws/show/5026-17#Text (дата звернення: 14.10.2021).

16. Про свободу совісті та релігійні організації: Закон України від 22.06.12 р. № 5026-VI. URL: https://zakon.rada.gov.ua/laws/show/987-12#Text (дата звернення: 14.10.2021).

17. Про професійних творчих працівників та творчі спілки: Закон України від 07.10.97 р. № 554/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/554/97-%D0%B2%D1%80#Text (дата звернення: 14.10.2021).

18. Про органи самоорганізації населення: Закон України від 11.07.01 р. № 2625-III. URL: https://zakon.rada.gov.ua/laws/show/2625-14#Text (дата звернення: 14.10.2021).

19. Про Національну стратегію у сфері прав людини: Указ Президента України від 24.03.21 р. № 119/2021. URL: https://zakon.rada.gov.ua/ laws/show/119/2021#Text (дата звернення: 14.10.2021).

20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію людського розвитку": Указ Президента України від 02.06.21 р. № 225/221. URL: https://zakon.rada.gov.ua/laws/show/225/2021#Text (дата звернення: 14.10.2021).

21. Про затвердження Регламенту Кабінету Міністрів України: Постанова Кабінету Міністрів України від 18.07.07 р. № 950. URL: https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF#Text (дата звернення: 22.10.2021).

22. Про забезпечення участі громадськості у формуванні та реалізації державної політики: Постанова Кабінету Міністрів України від 03.11.10 р. № 996. URL: https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text (дата звернення: 22.10.2021).

23. Ambivalence. The Free Dictionary. URL: https://www.thefreedictionary.com/ambivalence (дата звернення: 26.10.2021).

24. Про очищення влади: Закон України від 16.09.14 р. № 1682-VII. URL: https://zakon.rada.gov.ua/laws/show/1682-18/ed20140916#Text (дата звернення: 26.10.2021).

25. Проміжний висновок щодо Закону “Про очищення влади” (Закон “Про люстрацію”) в Україні, схвалений Венеціанською Комісією на її 101-й Пленарній сесії, Венеція, 12 – 13 грудня 2014 року. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2014)044-ukr (дата звернення: 03.11.2021).

26. Закон про люстрацію порушує права людини: Київ програв апеляцію в ЄСПЛ. URL: https://www.dw.com/uk/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD-%D0%BF%D1%80%D0%BE-%D0%BB%D1%8E%D1%81%D1%82%D1%80%D0%B0%D1%86%D1%96%D1%8E-%D0%BF%D0%BE%D1%80%D1%83%D1%88%D1%83%D1%94-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8-%D0%BA%D0%B8%D1%97%D0%B2-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%B2-%D0%B0%D0%BF%D0%B5%D0%BB%D1%8F%D1%86%D1%96%D1%8E-%D0%B2-%D1%94%D1%81%D0%BF%D0%BB/a-52530321 (дата звернення: 03.11.2021).

27. Modern achievements of EU countries and Ukraine in the area of law: collective monograph. Riga: Izdevnieciba “Baltija Publishing”, 2020. P. 2. Корж І.Ф. Виклики правовій безпеці суспільства в Україні. 311-330 p. (632 p.).

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

УДК 316 (477)

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,* головний науковий співробітник ДНУ ІІБП НАПрН України.
ORCID: http://orcid.org/0000-0002-2075-7508.
ЖДАНЕНКО С.Б., *кандидат філософських наук, доцент*, доцент кафедри філософії Національного юридичного університету імені Ярослава Мудрого.
ORCID: https://orcid.org/0000-0003-4335-8224.

ІНФОРМАЦІЙНА РЕВОЛЮЦІЯ: СОЦІОАНТРОПОЛОГІЧНІ ТА СВІТОГЛЯДНІ ТРАНСФОРМАЦІЇ

Анотація. *Показано, що в сучасній дійсності критично важливою є не тільки поява нового інформаційно-комунікаційного поля, що радикально перетворює звичну інфраструктуру соціального життя, але й вибухове зростання швидкості змін, викликаних бурхливим розвитком цифрових технологій. Звертається увага на якісний скачок швидкості розвитку, під яким розуміється перехід у реальність, де докорінні зміни технологічної інфраструктури та обумовлені ними зміни у житті соціуму стали відбуватися багаторазово протягом одного людського життя, в режимі реального часу. Обґрунтовується, що в результаті інформаційної революції виникла невизначеність нового порядку, яка вимагає від людини нового способу мислення. Проаналізовано проблему мінімально коректного прогнозування в основних сферах буття соціального.*

Ключові слова: *інформаційне суспільство, інформаційна революція, інформаційно-комунікаційні технології, скачок швидкості розвитку, інфраструктурні трансформації.*

Summary. *It is shown that the critical factor in the modern reality is not only the emergence of a new information and communication field, radically transforming the usual infrastructure of social life, but also the explosive growth of the speed of change caused by the rapid development of digital technology. Attention is drawn to the qualitative leap in the speed of development, which refers to the transition to a reality where radical changes in technological infrastructure and the resulting changes in the life of society began to occur repeatedly in the course of a single human life, in real time. It is argued that as a result of the information revolution a new order of uncertainty has arisen, which requires a new way of thinking on the part of man. The problem of minimally correct forecasting in the main spheres of social being is analyzed.*

Keywords: *information society, information revolution, information and communication technologies, speed of development, infrastructural transformations.*

Аннотация. *Показано, что в современной действительности критически важным является не только появление нового информационно-коммуникационного поля, радикально преобразовавшего привычную инфраструктуру социальной жизни, но и взрывной рост скорости перемен, вызванных бурным развитием цифровых технологий. Обращается внимание на качественный скачок скорости развития, под которым понимается переход в реальность, где коренные изменения технологической инфраструктуры и обусловленные ими перемены в жизни социума стали происходить многократно в течение одной человеческой жизни, в режиме реального времени. Обосновывается, что в результате информационной революции возникла неопределенность нового порядка, которая требует от человека нового образа мышления. Проанализирована проблема минимально корректного прогнозирования в основных сферах бытия социального.*

Ключевые слова: *информационное общество, информационная революция, информационно-коммуникационные технологии, скачок скорости развития, инфраструктурные трансформации.*

Постановка проблеми. На всіх рівнях життя сучасної людини від глобальної політики до побутової повсякденності, за останні кілька десятиліть відбулися кардинальні зміни. У цій новій дійсності критично важливим є не лише факт появи нового інформаційно-комунікаційного поля, яке радикально перетворило звичну інфраструктуру соціального життя, але й вибухове зростання швидкості змін, викликаних проривним розвитком цифрових технологій.

Унікальність пережитого історичного моменту полягає у тому, що докорінні зміни відбуваються в режимі реального часу, створюючи при цьому як небувалі можливості, так і проблеми, з якими людство досі ніколи ще не стикалося у своїй історії.

Як перехід до цифрової інформації всіх сторін економічного й соціального життя цифровізація з простого методу поліпшення різних приватних сторін життя перетворюється на драйвер світового суспільного розвитку, що забезпечує підвищення ефективності економіки та якості життя.

Цифровізація (цифрова трансформація) дедалі повніше відповідає таким вимогам, як охоплення виробництва, бізнесу, науки, соціальної сфери та звичайного життя громадян; супроводження лише ефективним використанням її результатів, які доступні користувачам перетвореної інформації; використання її результатів не тільки фахівцями, але й пересічними громадянами; наявність у користувачів цифрової інформації навиків роботи з нею, тому у широкому сенсі її цілком доцільно розглядати як тренд ефективного світового розвитку [1, с. 23].

Важливо відзначити, що феномен надшвидкого розвитку виникає одночасно з приходом цифрових технологій, особливість яких полягає у тому, що при колосальному впливі на всю технологічну та соціальну інфраструктуру самі вони вимагають мінімального залучення матеріальних ресурсів і мінімальних змін навколишнього середовища.

Таким чином, надшвидкий розвиток – це властивість саме домінуючого прогресу цифрових, інформаційно-комунікаційних технологій і, відповідно, обидва ці феномени – одномоментний в історичному масштабі прихід цифрової цивілізації і практично скачкоподібне збільшення швидкості змін, що нерозривно взаємопов’язані.

Іншою найважливішою особливістю сучасного етапу розвитку є те, що вперше в історії його визначальним напрямком є прогрес в інформаційних комунікаціях і когнітивних технологіях [2 – 3]. Технологія вступила у Sancta Sanctorum, у ту сферу, яка робить людину людиною розумною, а людський соціум виділяє з будь-яких інших біологічних спільнот. Відповідно, надшвидкий розвиток цифрових технологій зумовлює і неминучість докорінних соціальних зрушень, які відбуваються на наших очах і втілюються у таких поки що нових поняттях, як “інформаційне (цифрове) суспільство”, “цифрова цивілізація”, “цифровий світ”, “інформаційна (цифрова) епоха”; 3-тя, а тепер вже й 4-та промислові революції, “інформаційна (цифрова) революція”.

У кінці ХХ ст. стає очевидним, що технології інформаційних комунікацій виявляються “стрижнем сучасної економічного й соціального життя”, що і проголошують Комісія європейських країн [4] і Окінавська хартія глобального інформаційного суспільства [5].

Результати аналізу наукових джерел. Поява в середині ХХ ст. обчислювальних машин породжує наукові дискусії про специфічну роль інтелектуальних машин, їх можливе суперництво з людиною, проблеми майбутнього, обумовлені цим напрямком розвитку технології (Н. Вінер, Дж. Ліклайдер). У другій половині ХХ ст. спостерігається сплеск інтересу до осмислення трансформації суспільства у зв’язку з прогресом інформаційних комунікацій (зокрема, книгодрукування, телебачення і перших

комп'ютерів). Детальний аналіз цих явищ міститься у доробках Ж. Фурастьє, Н. Вінера, Д. Белла, М. Хайдеггера, М. Кастельса, К. Ясперса, Е. Тоффлера, М. Маклюена, Н. Лумана, Ю. Хабермаса та ін. У цей же час з'являється і скепсис щодо "кібернетичної революції", яка, на думку Д. Белла, виявилася "ілюзорною". Вплив технологічного розвитку (передусім інформаційно-комунікаційного) на суспільство розглядається в різних аспектах. Зміни, що відбуваються, відображаються у появі нових концепцій, понять і термінів. Проривний розвиток технологій інформаційних комунікацій привносить у наше життя нові поняття: "інформаційна революція", "інформаційна епоха" або "інформаційне суспільство", що розробляються у працях Й. Масуди і П. Друкера. Практично найбільший внесок у вивчення інформаційного суспільства здійснив М. Кастельс, створивши теорію "інформаціонального способу розвитку" – поки що єдину цілісну модель, що відповідає всім критеріям наукової теорії.

Проблеми швидкості і прискорення розвитку технологій торкаються у своїх роботах Г. Адамс, Б. Андерсен, М. Форд, тема збільшення темпів науково-технічного прогресу спрямувала дослідження Ф. Лінна, Е. Тоффлера, П. Вірильо, З. Баумана. У деяких працях робиться спроба виміряти швидкість технологічного прогресу, а десь тема прискорення розвитку технологій трансформується у проблему сингулярності (В. Віндж, Н. Бострем, Р. Курцвейл, М. Шанахан).

На початку XXI ст. відбувається прорив в інформаційних технологіях, що супроводжується їх розповсюдженням у планетарних масштабах і перетворенням різних сторін соціального та індивідуального життя. Ця тема стає предметом широкої дискусії у суспільстві, звучить на численних форумах, у мас-медіа, у промовах політиків і фінансистів. Вплив технологічного розвитку (передусім інформаційно-комунікаційного) на суспільство розглядається у різних аспектах.

Таким чином, у багатовимірній проблематиці непізнаного цифрового світу виникла необхідність сфокусувати увагу на проблемі існування людини й соціуму в умовах іманентно властивих цьому цифровому світові надшвидких змін.

Мета статті – акцентувати увагу на характерних рисах суспільних явищ і соціальних трансформацій, породжених якісною зміною темпів науково-технічного розвитку, обумовленого проривом в інформаційно-комунікаційних технологіях, які революційно перетворюють практично усі сегменти соціальної інфраструктури та здійснюють специфічний вплив на людину.

Виклад основного матеріалу. Розуміння того, що "все тече, все змінюється", притаманне ще античним мислителям. Тут доречно згадати вислів "O tempora! O mores!", поняття "тепер" у Аристотеля, для якого "у часі нічого не можна схопити крім тепер" [6, с. 224], а також про вічну проблему батьків і дітей. Але то був час плавних, поступових і тому передбачуваних змін. Вони не суперечили прогнозуванню майбутнього як у короткостроковій, так і в довгостроковій перспективі. Це все входить у стійку усталену картину світу.

Зміни відбуваються, коли у цю картину, повну звичних, рутинних змін, привноситься щось принципово нове, чого взагалі ніколи раніше не було; такою технологічною новацією стало, наприклад, відкриття заліза. При цьому, переможний тріумф заліза у різних культурах представляв собою плавний тривалий історичний процес зміни бронзового століття залізним. Радикальні модифікації привнесли винахід ткацького і друкованого верстатів, відкриття електрики, але й ці зміни впроваджувалися в життя людини плавно, протягом численних поколінь. Відтак, незважаючи на важливі технологічні прориви, у цю епоху можна було передбачати, як жити і розвиватися, як виховувати наступне покоління, знаючи, які поняття будуть йому необхідні, як буде

будуватися його життя. Все це можна було витягти з власного досвіду. За допомогою екстраполяції минулого досвіду будувалося і бачення майбутнього, на цьому засновували свої прогнози навіть найбільш прозорливі пророки.

Унікальність пережитого нами історичного моменту полягає в тому, що стався якісний перехід від відносно плавного розвитку у передцифрову епоху до шокуючої швидкості розвитку цифрової цивілізації. Стався так званий якісний скачок швидкості розвитку [7] (далі – СШР), що означає перехід у реальність, де докорінні зміни технологічної інфраструктури та обумовлені ними зміни у житті соціуму стали відбуватися багато разів протягом одного людського життя, в режимі реального часу, створюючи при цьому як небувалі можливості, так і проблеми, з якими людство ніколи раніше ще не стикалося. Співвіднесення частоти появи критичних інновацій і обумовленого ними темпу соціально-економічних та інфраструктурних трансформацій з тривалістю людського життя дозволяє констатувати реальність цього історичного переходу.

Ефект такого якісного скачка посилюється тим, що драйвером надшвидкого розвитку, який ми спостерігаємо, є прогрес у сфері інформаційних комунікацій, який має особливе значення для людини і соціуму, оскільки, з одного боку, становить основу людської природи, представляючи її найбільш чутливу й делікатну сферу, а з іншого – критично впливає на всі сегменти технологічної цивілізації і суспільного життя.

Якісний СШР призвів до того, що підґрунтя, на яке можна було спертися, прогнозуючи майбутнє, стає хитким. Людині (як окремому індивіду, так і людським спільнотам) доводиться перебудовуватися, розуміючи, що фундамент життєвого досвіду предків, на який вона спиралася всю історію свого існування, більше не справляється зі своєю функцією, зазнаючи нескінченних трансформацій. Спиратися більше немає на що, горизонт передбачення радикально наблизився, схеми прийняття рішень доводиться виробляти в ситуації повної невизначеності. Побудувати своє життя і навіть завтрашній день неможливо, а отже, неможливо обрати вірні дії вже сьогодні.

Коли в епоху до СШР ми зустрічалися з ситуацією складного вибору, то це означало, що потрібно вибирати з декількох можливих альтернатив. Але в разі, коли ми бачимо низку альтернатив, ми все ж можемо застосувати певні інструменти аналізу. Сучасна ж ситуація характеризується тим, що ми не бачимо навіть можливих альтернатив, ми тільки знаємо, що дуже скоро все так чи інакше зміниться. Це, за висловом Зіґмунда Баумана, як "робити "раціональний вибір" в еру миттєвості" [8, с. 140].

Люди тисячоліттями жили у світі, де характер буття не змінювався скільки-небудь помітно протягом життя принаймні декількох поколінь. У цих умовах люди відчували визначеність і прогнозованість своїх реалій, сталість існування людства. Звичайно, життя людей на окремих територіях могло змінюватися радикально: війни, зникнення племен, мов тощо, але при повній непередбачуваності історичної долі даної обмеженої спільноти існувала прогнозованість технологічна: та ж зброя, житло, способи виробництва продовольства, взагалі спосіб і стиль життя; відповідно, завдання подібного прогнозування для того часу були коректними. Зокрема, навіть в індустріальну епоху (XIX – XX ст.) можна було робити досить достовірні довгострокові прогнози технологічного розвитку і на їх основі будувати промисловість, оборону, фінансові інститути тощо.

Спостерігалися періоди стабільності і процвітання, але були й випадковості. Всі такі форс-мажорні ситуації були практично відомі, тому і їх можна було передбачити і підготуватися до них. Невизначеність попередніх історичних епох з їх турбулентністю була зрозуміла, і, отже, у першому наближенні зрозумілими були можливі дії. Не

вимагалося перегляду картини світу, ментальної революції зі зміною базових світоглядних установок, що лежать в основі сприйняття світу і уявлень про роль і місце людини у цьому світі, про його призначення.

Зараз же значення подібних негативних факторів зведено до мінімуму. Але виникла невизначеність іншого порядку, яка вимагає від людини нового способу мислення.

Якісний СШР – це, по суті, перехід у нову дійсність, де істотними є не тільки поява нового інформаційно-комунікаційного поля, яке радикально перетворює звичну інфраструктуру життєдіяльності, а й гігантська швидкість змін, викликаних проривним розвитком інформаційно-комунікаційних технологій, а отже, наближення горизонтів планування.

Шокуюча швидкість розвитку цифрової цивілізації – це реальність, до якої має звикнути людство, прийнявши її за нову парадигму існування. Попередня його парадигма, на якій будувалося все людське існування, ґрунтувалася на розумінні того, що ми з високим ступенем ймовірності можемо прогнозувати майбутнє, і якщо не всі деталі картини, то засадничі речі, на які можна спиратися у виборі дій сьогодні. У новій реальності руйнується вся аксіоматика, з якої логічно випливав процес прийняття рішень. Користуючись категоріальним апаратом, введеним Томасом Куном [9], можна припустити, що людство, здійснивши перехід у нову реальність, стоїть на порозі революційного трансформування парадигми мислення. Сьогодні відбувається руйнування ментальності, оскільки ми знаємо, що ми увійшли в епоху перманентних змін і епохи стабільності практично більше не буде ніколи.

Елвін Тоффлер, перебуваючи ще на самому початку цифрової цивілізації, вже передбачив “шок майбутнього”, викликаний проблемами адаптації [10]. В іншій своїй роботі він дає пом’якшене порівняння подібного розвитку з хвилями океану, які на своєму шляху втягують у процес трансформації всіх людей як учасників [11]. Ці хвилі набули формату цунамі. І якщо активні учасники цього процесу самі розкрутили і продовжують розкручувати маховик прогресу, не знаходячи в собі сил зупинитися, володіючи нестримною творчою енергією, яка змушує їх працювати, відкривати, крокувати далі, то основна маса мимовільних свідків, які не бажали б нічого змінювати, випадково опинилася в цій невигідній для неї ситуації. Точніше, вони побічно задіяні, оскільки створюють запит на комфорт, про що говорить поширене висловлювання “лінь – двигун прогресу”. Для них ідея прогресу – це рух до комфорту, але він дивним чином викликав і зворотну ситуацію дискомфорту, за якої доводиться безперервно у собі щось змінювати, ситуацію, яка вимагає надлюдських швидкостей адаптації.

А сучасна людина (людина інформаційна), щоб продовжувати свою кар’єру, а значить, залишатися соціально необхідною, затребуваною, має безперервно розвиватися, як велосипедист повинен крутити педалі, оскільки припинення цієї дії означає зупинку або падіння, внаслідок якого його обженуть інші. Крім необхідності безперервного руху зі швидкістю, що не знижується, головним завданням виявляється визначення напрямку руху, оскільки куди бігти – незрозуміло, оскільки нічого не видно за найближчим горизонтом. Людина потрапила під лавину, де “швидкість змін має значення більш важливе, аніж напрямок змін” [10, с. 157].

Це схоже на стан безвиході, коли ясно, що потрібен швидкий рух, але куди прагнути – незрозуміло. Тут ключове слово – “швидко” і у цій гонці напрямок змін стає незбагненним. Зрозумілим є одне: зміни неминучі і настануть дуже скоро. У цю епоху людина опиняється в полі дії якоїсь нової, невідомої раніше сили. Описуючи об’єкт у полі дії сили, свого часу Павло Флоренський ввів поняття “активної пасивності”, що

означає відповідність об'єкта впливу силі, яка на нього діє. Ніщо не здатне сприймати причину, не маючи у собі тих чи інших умов сприйняття, співвідносних з природою діючої сили. Сила заподіює зміни [12].

Щоб усвідомити весь драматизм ситуації, вважається доцільним навести гіпотетичне припущення щодо можливості появи квантового комп'ютера, основне завдання якого, на думку професора університету Калгарі Олександра Львівського, забезпечення безсмертя людини [13]. Можливість людства вже у найближчому майбутньому продовжувати своє життя – не така вже й фантастика. Згідно з деякими прогнозами, до 2050 року кілька людей вже будуть безсмертними [14]. Поява такої можливості спричинить руйнування усталених уявлень людини про себе, про свою роль у суспільних відносинах, про сенс життя, мораль, право.

Сучасна ситуація за масштабом можливої трансформації способу мислення близька до наведеного гіпотетичного прикладу. Зокрема, це демонструє експеримент по введенню безумовного базового доходу для всіх громадян, що проводиться в розвинених країнах. Дана революційна ідея набирає популярності по всьому світу, від Кремнієвої долини до Індії [15]. Якщо експеримент вдасться, то це фактично означатиме побудову утопії, а саме комунізму. За цим простежуються радикальні наслідки. Наприклад, у такій країні не буде громадян, які спонукаються до роботи необхідністю вижити, а це вже інший соціум, з новими мотиваціями, з новою картиною світу, де зміниться розуміння кар'єри, соціального статусу, положення і всього життєвого шляху.

Іншим втілюваним у реальність прикладом, який тісно переплітається у причинно-наслідковому зв'язку з першим, є витіснення людини з трудової діяльності. У багажі життєвого досвіду людства основним призначенням людини є праця, і людей з дитинства готували до цього. У праці відбувалася і соціалізація, і позиціонування себе. При позитивному розвитку сучасної ситуації платформа самореалізації через працю пропадає. Це ускладнюється тим, що досягнутий у результаті якісного СШР темп науково-технічного прогресу і трансформації соціально-економічної інфраструктури не дозволяє не те що перебудувати ментальність людини, але навіть припустити, до яких подій готуватися.

Тим більше непередбачуваним стає майбутнє після появи штучного інтелекту, який є, на думку авторитетного американського фахівця у галузі штучного інтелекту, що досліджує проблеми технологічної сингулярності й виступає за створення "дружнього штучного інтелекту" Еліезера Юдківського, просто назвою для нескінченного "простору можливостей поза крихітною людською точкою", а отже, побудова будь-яких прогнозів розвитку ситуації після його появи є "абсолютно дивною", адже штучний інтелект є потужнішим за людський і "руйнує всі ваші прогнози" [16].

У результаті якісного СШР здійснився "перехід Рубікону" у двох реальностях. Ми опинилися у новій реальності, де все багаторазово зазнає змін протягом життя, в реальності, де нічого не можна передбачити, оскільки осмисленню і, відповідно, плануванню піддається існування в межах горизонту, але він невблаганно наближається. Відмінність нової реальності полягає в тому, що у доцифрову епоху радикальні зміни технологічного середовища і зумовлені ними трансформації в житті суспільства або зовсім не відбувалися, або були розтягнуті на декілька поколінь, надаючи можливість відносно комфортної адаптації. Коли ж траплялися винятки, це призводило до суспільних потрясінь. Тепер же, на очах нинішнього покоління, темп розвитку збільшився таким чином, що радикальні зміни технологічної та, як наслідок, соціально-економічної інфраструктури, призводячи до зміни "життєвого світу" (Lebenswelt за Гуссерлем [17]), стали за час одного людського життя траплятися багаторазово, що

виключає можливість поступової адаптації. Цей феномен німецький філософ Герман Люббе позначає як "скорочення справжнього", позначаючи ним стан справ у "динамічній цивілізації". Відповідно до цієї концепції "зі зростанням кількості інновацій в одиницю часу зменшується хронологічна відстань до того минулого, яке в багатьох життєвих відносинах вже застаріло, в якому ми не можемо вже розпізнати звичної структури сьогоднішнього життєвого світу і яке тому представляється нам чужим і навіть незрозумілим" [18, с. 379]. І якщо у мистецтві фотографії швидкість сприяє, "головним чином, баченню і більш-менш ясному розумінню" [19, с. 129], то в новій реальності вона затьмарює всі перспективи. Чилійський вчений Даріо Салас Соммер про такий стан говорить, що це все одно що рухатися в густому тумані, коли дорогу начебто видно, а начебто й ні, і немає глибокого розуміння того, що відбувається [20]. У новій реальності швидкість отримала "панування над часом і простором" (Вірильо [19, с. 131]), швидкість забезпечує відтепер бачення, оцінку і, отже, осмислення реальності [19, с. 136], де немає навіть надії на гальмо у вигляді Камперовського "стоп-крана" [21].

Якісний СШР критично впливає на низку найважливіших аспектів життя суспільства й індивіда і особливо на уявлення про майбутнє, що визначають побудову життєвої траєкторії будь-яким відповідальним індивідом або корпорацією. Ми, потрапивши в нову реальність, розуміємо, що процес іде, нам його не зупинити, рухатися і йти потрібно в ньому, але куди? Виходить, що ми йдемо кудись, але бачимо тільки те, що відбувається "тут і зараз". Картина майбутнього навіть не розмита, її зовсім не видно. Навіть у непередбачуваності погоди є імовірнісні факти, але у прогнозуванні майбутнього ми нічого не можемо закласти в розрахунок ймовірного передбачення, оскільки не знаємо, що буде винайдено "завтра" і які будуть наслідки. Наприклад, як вже було сказано, винахід безсмертя спричинить повну зміну парадигми буття. При цьому лінію поведінки у таких умовах потрібно виробити вже зараз, а для того, щоб це зробити, необхідно усвідомити, до якої мети ми йдемо.

Усвідомлення настання "епохи технологічної непередбачуваності" [7, с. 70-84] на сьогоднішній день вже починає формуватися і оформлятися концептуально. Однак важливо не тільки усвідомлення, але й можлива реакція, оскільки неможливо продовжувати будувати траєкторію подальшого розвитку виходячи із трендів сьогодення, як це, по суті, і роблять усі провісники. Подібні прогнози, як у випадку передбачення погоди, виходячи з поточного стану, розумні і правильні, але на короткому відрізку часу. Гідрометцентр дає немислимо точні прогнози зміни погоди по годинах за багатьма параметрами. Це можливо, причому з такою точністю, досягти якої дозволяють наявне глибоке розуміння процесу і інформація – глобальна й детальна (за параметрами у всіх зрізах простору і часу), а також потужний комп'ютер для обробки даних як інструмент потужної аналітики. І навіть у цьому випадку горизонт передбачення з певною мірою достовірності – кілька днів. У даному контексті горизонт передбачення визначається межами обчислювальної потужності ком'пютера. Там діють різні фактори, але якщо врахувати їх усі, то передбачення в принципі є можливими і в тому числі на досить тривалий термін. Сучасна наука передбачає навіть еволюцію планети Земля, всієї Сонячної системи, а також Всесвіту на мільярди років вперед [22].

На відміну від цього розвиток науки є непередбачуваним у принципі. Однак в попередні епохи (до СШР) відповідно до їх темпоральності планування соціотехнологічного розвитку на покоління вперед представлялося можливим. І в цьому сенсі принципова різниця полягає в тому, що стався якісний скачок швидкості розвитку. "Короткий термін" замінив "тривалий термін" і зробив миттєвість своїм "вищим ідеалом" [8, с. 136]. Тому колосальна швидкість і майже повна непередбачуваність

соціотехнологічного розвитку наближають горизонт передбачення перетворень технологічної інфраструктури та соціального середовища і відтинають можливість хоч якогось коректного передбачення навіть на середньострокову перспективу, не кажучи вже про довгострокові прогнози.

Таким чином, проблема прогнозування та планування у попередні епохи була нормальним, коректним завданням; вона ставилася і з деяким ступенем ймовірності вирішувалася. Якісний СШР привів нас до ситуації, коли горизонт скільки-небудь надійного прогнозування очевидним чином звужується, де сама постановка завдання довгострокового прогнозу розвитку є некоректною. Однак саме ця непередбачуваність робить особливо затребуваними скільки-небудь достовірні прогнози, тому саме в цій новій ситуації навіть мінімально коректне прогнозування стає критично актуальним.

Зокрема, ця проблема безпосередньо стосується сфери освіти. Як розвивати людський капітал і якою має бути освіта? Що робити у першу чергу: модернізувати існуючу систему освіти (які рішення слід приймати для цього вже сьогодні) або будувати нову (і яку)? Чи актуальна існуюча система освіти і яка модель ринку освітніх послуг є найбільш перспективною? Які професійні навички необхідно отримувати людині, коли багато класичних професій зникають, з'являються нові, яким сьогодні не вчать в університетах або тільки приступають до навчання? Прискорювані темпи розвитку сучасної науки, техніки і технологій призводять до того, що навчання у вищих навчальних закладах відстає від реального життя.

Ситуація, звичайно ж, починає усвідомлювати на різних рівнях. Звідси й безперервні спроби з боку системи освіти щось модернізувати, виробити програму, адекватну новій реальності, нових запитів суспільства, що варіюються від розвитку гуманітарної складової або концентрації на загальнофундаментальній освіті до повного перемикання на плекання когорти інженерних кадрів. Реакцією на ситуацію є, наприклад, міркування, що потрібно "учити вчитися" і ідея повністю прибрати класичний формат лекцій. Проблема полягає в тому, що освіта, будучи системою, яка повинна бути локомотивом, мчить, орієнтуючись на передові тренди, і тягне розвиток інших сфер, в реальності виявляється абсолютно консервативною системою, і щоб її розгойдати, потрібні десятиліття. Це протиріччя між швидкістю розвитку реального життя і відставанням системи освіти автор концепції "організації, що навчається" професор Пітер Сенге називає "невимовно іронічною пасткою" [23]. Крім того, одним із викликів у даному контексті є ускладнена можливість системи освіти захистити культурні основи, коди національної ідентичності в умовах інформаційної глобалізації.

Разом з тим, зазначені вище та інші заходи (акредитація в Україні наявних освітніх ресурсів чи створення так званого "парасолькового агрегатора освітніх ресурсів"), з-поміж іншого, не можуть гарантувати рівного доступу до освіти, забезпечувати належну якість та єдність навчання, забезпечувати захист персональних даних та сприяти керованості системи освіти [24].

Досить проблематичним стає прогнозування і у сфері політики і влади. Темпи розвитку цифрової цивілізації і багаторазова тотальна трансформація соціально-економічної інфраструктури за останні кілька років кидають виклик у тому числі й інститутам влади, однією з першорядних завдань яких є вибудовування програми розвитку держави та її окремих інститутів, а також планування бюджету. Це завдання надзвичайно ускладнюється, коли мова йде про планування на середньострокову перспективу, і шанси її коректного вирішення практично дорівнюють нулю при довгостроковому плануванні.

Найважливішим інструментом політики є засоби масової інформації, які виконують функції управління і контролю суспільством, створення політичного порядку в суспільній думці, способі реалізації влади, які стрімко переходять у віртуальний простір, де вони погано контролюються і мимовільно розвиваються у непередбачуваних напрямках. Одним із наслідків такого неконтрольованого розвитку Інтернету і соціальних мереж є створення горизонтальних (не вертикально-пірамідальних) структурованих спільнот [25 – 27].

Гігантська швидкість розвитку технологічної інфраструктури вимагає адекватного темпу розвитку правових відносин, включення зароджуваних і вже функціонуючих процесів у правові рамки і, що не менш актуально, але у багато разів складніше, вимагає адекватного описання цього в термінах етики й моралі.

Новою проблемою, викликаною темпом розвитку технологій, з'явилася проблема браку кваліфікованих кадрів у сфері кібербезпеки, яка відчувається в усьому світі. "З розвитком технологій підключається все, обсяги даних, що генеруються, зростають по експоненті і це зростання не припиняється. У новому світі дані стають найголовнішим активом будь-якої організації, і необхідно думати про те, що вони означатимуть для нашого майбутнього. Дані неймовірно важливі, і завдання їх захисту є актуальним як ніколи" [28].

Перманентна і тотальна трансформація інфраструктури економіки ставить питання, в які напрямки розвитку інвестувати. Особливо це питання є важливим, коли мова йде про інвестиції в довгостроковій перспективі, наприклад для пенсійних фондів, державних фондів розвитку тощо. Саме для України очевидну важливість має диверсифікація економіки, тобто переорієнтація переважно сировинної економіки на розвиток інноваційних технологій і виробництво високотехнологічних продуктів. Тут знову виникають питання: яких технологій і яких продуктів? Питання полягає у тому, що будь-який такий розвиток – це процес, що вимагає планування на період часу не менше 5 років, а як правило і більше (це час проходження винаходу від стадії науково-технічної розробки до промислового виробництва).

Концепції містобудування, розвитку транспорту і розподілу трудових ресурсів повинні враховувати, стрімко впроваджувані й важкопередбачувані за наслідками можливості (пов'язані з розвитком ІТ і робототехніки) повноцінної участі у робочому процесі без безпосереднього перебування працівників на робочому місці. Дійсно, як, наприклад, зробити прогноз розвитку транспортної інфраструктури на 20 років наперед (з огляду на далекий горизонт окупності в машинобудуванні – кілька десятків років), якщо завдяки розвитку інформаційних комунікацій і робототехніки може виявитися, що вже через 5 – 10 років значна частина населення буде виконувати свої службові обов'язки, не виходячи з дому?

Невизначеність майбутнього яскраво простежується й у сфері охорони здоров'я. Чи збережеться медицина як професія, з поточними вимогами до представника цієї професії? Тенденції такі, що стандартизація в медицині вже є загальноприйнятою світовою практикою [29 – 30]. Далі – один крок до того, щоб ця професія піддалася знищенню. У цьому випадку не потрібні будуть лікарі, які мають лише знання стандартів, оскільки на це будуть здатні програми. Необхідним буде лікар, що перевершує робота, що володіє (понад банальної здатності до запам'ятовування) особливими талантами, здатний бачити людину, як певну систему, але систему унікальну, яку можна усвідомити лише якимось незбагненним чином. Це означає сумніви у затребуваності на ринку професій "нормальних" лікарів, які "нормально" лікують, тобто так, як написано в інструкції. Можливо, їх замінять розумні програми, а свої ніші в людських професіях знайдуть і

будуть затребуваними, якщо на це не буде заборони на державному рівні, лише лікарі, які мають свою специфіку.

Міжнародне безпекове середовище та природа конфліктів швидко змінюються, значною мірою через розвиток науки і технологій. Новітні та проривні технології створюють як нові можливості, так і загрози не лише у сфері безпеки і оборони, але й в інших галузях. У воєнній сфері такі технології спрямовані на розширення здатності сил та засобів діяти в оперативній обстановці, що швидко змінюється: у космосі, кіберпросторі, районах міської забудови. У той же час постає питання щодо забезпечення належного контролю за їх поширенням і використанням, а також урахування правових, політичних, економічних та організаційних обмежень на самому початку їх розробки [31].

Як свідчить світовий досвід, ефективні системи забезпечення національної стійкості є достатньо децентралізованими, рішення щодо реагування на загрози приймаються на найнижчому можливому рівні [32]. У той же час координація відповідної діяльності, яка має надзвичайно важливе значення у цій сфері, визначення єдиних і зрозумілих для всіх учасників правил, стандартів і порядку дій на різних етапах циклу забезпечення стійкості, суттєво ускладнюється завдяки швидкоплинним соціальним і технологічним процесам.

В оборонній промисловості актуальним є питання, як вибудовувати концепцію розвитку оборонно-промислового комплексу в реаліях перманентної науково-технічної революції, обумовленої у даний час стрімким розвитком засобів інформаційних комунікацій і робототехніки. Наближення горизонтів планування робить особливо уразливими довгострокові проекти, які, як видається, повинні бути реалізовані для підтримки належної обороноздатності держави. Наочним прикладом є розвиток флоту, що вимагає для будівництва (без урахування дослідно-конструкторські розробки) масштабу часу близько десяти років.

Однак найгострішим у всьому цьому переліку питань є питання про розвиток людини. Як зазначалося раніше, віртуалізація життєвого часу у просторово-часовому континуумі характеризує принципово новий тип символічного існування людини у соціумі, культурі [33]. Цифрова цивілізація, що стрімко увірвалася в наше життя, зі швидким знеціненням розумової праці поставила питання про нагальну необхідність переосмислення (перегляду) уявлень про працю як головне покликання людини, і реалізації людини у професії як бази для побудови життєвої траєкторії. Отже, ми приходимо до необхідності перегляду самих основ розуміння сенсу життя людини, її мотивації, що включає відповіді на питання про те, що означає відбутися у цьому житті, не дарма його прожити. У цьому буде виражатися турбота про саму людину, і саме кожному окремому індивіду це потрібно у першу чергу. Цілком імовірно, що нова реальність вимагає нової людини з іншим (усередненим) архетипом, з іншим набором базових установок, можливо, іншим психотипом: більш відкритим і толерантним до змін. Подібне висловлювання не є новим, але розуміння цього факту у сучасних умовах має особливу глибину, оскільки для людини “звичка – друга натура”. Усе її буття знаходиться у світі уподобань, традицій, спирається на чуттєву, емоційну сферу, яка у своїй основі має базові установки. У новій реальності значущими є не просто нові смисли і призначення людини, ревізії вимагає саме її ставлення до реальності. Нова картина буття потребує людини з новим баченням світу і себе в ньому. Особистість, що загубилася у 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 [33].

Висловлювання “людина, створи себе сама” і аналогічні є концентрованим уявленням про траєкторію вірного шляху, свого роду “Дао” західної людини. Вони були

хорошими і працювали до сьогодні, але виявилося, що вони можуть увійти в конфлікт з новою реальністю. Навіть якщо ми дотримуємося традиційного способу життя, все ж незрозуміло, у чому реалізовуватися, якщо немає можливості приносити користь своєю працею. Невизначеність породжує розгубленість, страх, дискомфорт.

У міру роботизації, що включає заміну розумової праці, дедалі більша частина людства буде з виробників перетворюватися на чистих споживачів, а оскільки це відбувається і буде відбуватися все інтенсивніше, то вже завтра (а свідчення цьому ми бачимо вже сьогодні) суспільство зіткнеться з питанням про призначення такої людини. З огляду на масштаби явища (воно має тенденцію охопити більшість людства) і його непередбачувані наслідки для збереження гармонії у суспільстві і позитивного соціального розвитку, робота у цьому напрямку вбачається надактуальною: її результати повинні якомога швидше стати предметом суспільної дискусії, увійти у концепції виховання та освіти, знайти своє відображення у культурному процесі. Можна сказати, що це питання масштабу "бути чи не бути?". При цьому нова картина буття з усіма її деталями, а також усі концепції формування людини, адекватної новій реальності, повинні формуватися з урахуванням вкрай обмеженої передбачуваності навіть найближчого майбутнього.

Цифровий світ дав людству безліч нових можливостей вибудовування особистої і державної безпеки. Стрімке впровадження цифрових технологій породжує й низку системних соціально-економічних та соціально-політичних проблем, у тому числі – кардинальне переформатування світового ринку праці та поширення масового безробіття; зміну експортної спеціалізації країн, що розвиваються, зокрема, остаточне закріплення за ними експортної сировинної орієнтації; розриви традиційних, існуючих ще з кінця XX ст. промислових виробничих "ланцюгів створення доданої вартості"; розрив традиційних виробничих коопераційних зв'язків між країнами світу та формування нових, на основі цифрової економіки, "Індустрії 4.0", ІКТ, "Індустріального Інтернету", "Промислового Інтернету" [34, с. 53]. Все це увійшло в протиріччя з особистою свободою людини.

Процеси цифровізації обумовлюють практично усі соціально-економічні та політичні наслідки кардинальної структурної перебудови сфер суспільного буття.

Висновки.

Майбутнє не можна передбачити у його конкретиці, у тому, які саме відбудуться соціальні трансформації, які потрібно виробляти озброєння, що зміниться у системі освіти й економіки, які нові девайси будуть нас оточувати. Такі пророцтва особливо важкі в умовах сучасної нам швидкості змін. При цьому можна прогнозувати, що зміни будуть ще більш радикальними й відбудуться у найближчому майбутньому. Прогноз на майбутнє вказує лише на тренд, який спрямований до великих швидкостей розвитку. Однак ми не можемо стверджувати, що він спрямований до щасливого майбутнього. Це суперечка між оптимістами, віруючими у прогрес, і технологічними песимістами.

У минулій історії людства наукове прогнозування здійснювалося методом екстраполяції тих трендів, які вже вгадувалися у сьогоденні (Мальтус, Маркс, Римський клуб). Як свідчить історичний досвід, цей метод виявився неспроможним навіть у "повільному" минулому, коли це стосувалося більш довгострокових прогнозів. У сучасних умовах передбачення технологічного майбутнього цим єдино поки що відомим способом стає очевидно некоректним вже у середньостроковій перспективі (наприклад, на 20 років), і вельми сумнівним навіть у короткостроковій (5 – 10 років). У результаті виникає дефіцит бачення майбутнього.

Для індивіда проблемою стає усвідомлений вибір життєвого шляху (а також і взагалі розуміння свого призначення у стрімко мінливому цифровому світі).

Для людських спільнот і корпорацій виникають проблеми в таких основоположних аспектах суспільного життя, як планування, інвестиції, розвиток людського капіталу, безпека. Розмивання картини соціотехнологічного майбутнього – дуже серйозний виклик інформаційної революції і навряд чи чисто технократичний підхід здатний дати тут адекватну відповідь. Парадоксально, але у світі інтелектуальних машин зростає роль людської думки, яка одна тільки здатна прозріти і прокласти шляхи у створеній нею ж самою новій темпоральній реальності.

Використана література

1. Чмерук Г.Г. Цифровізація – тренд світового розвитку, який визначає розвиток економіки і суспільства. *Економічний простір*. 2020. № 153. С. 18-24.
2. Дзьобань О.П. Філософія інформаційних комунікацій: монографія. Харків: Майдан, 2012. 224 с.
3. Дзьобань О.П., Мелякова Ю.В. Комунікаційна природа інформаційного простору. *Інформація і право*. № 2(5)/2012. С. 81-88.
4. Green Paper on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernization (presented by the Commission). URL: https://op.europa.eu/en/publication-detail/-/publication/d60386fe-69d4-4846-bf01-b1d23b20e134 (дата звернення: 25.08.2021).
5. Окінавська хартія глобального інформаційного суспільства. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text (дата звернення: 25.08.2021).
6. Аристотель. Физика. Соч. в 4 т. Т. 3. Москва: Мысль, 1981. С. 58-262.
7. Шестакова И.Г. Человек и социум в темпоральности цифрового мира: дис. ...д-ра филос. наук. Санкт-Петербург, 2020. 430 с.
8. Бауман З.Б. Текучая современность ; пер. с англ. под ред. Ю.В. Асочакова. Санкт-Петербург: Питер, 2008. 240 с.
9. Кун Т. Структура научных революций ; пер. с англ. И. Налётова. Москва: АСТ, 2015. 317 с.
10. Тоффлер Э. Шок будущего ; пер. с англ. Е. Руднева и др. Москва: АСТ, 2008. 557 с.
11. Тоффлер Э. Третья волна ; пер. с англ. К.Ю. Бурмистрова и др. Москва: АСТ, 2009. 795 с.
12. Флоренский П.А. Исследования по теории искусства. Статьи и исследования по истории и философии искусства и археологии. Москва: Мысль, 2000. С. 350-400.
13. Что может дать нам бессмертие. URL: https://tvrain.ru/teleshow/interview/chto_mozhet_dat_ nam_bessmertie-391220 (дата звернення: 26.08.2021).
14. Harari Y.N. Sapiens: a brief history of humankind. UK: Penguin Random House, 2011. 498 p.
15. Копленд С. Гарантированный доход для всех граждан: польза или вред? URL: https://www.bbc.com/russian/vert-fut-38982423 (дата звернення: 23.08.2021).
16. Horgan J. AI Visionary Eliezer Yudkowsky on the Singularity, Bayesian Brains and Closet Goblins. URL: https://blogs.scientificamerican.com/cross-check/ai-visionary-eliezer-yudkowsky-on-the-singularity-bayesian-brains-and-closet-goblins (дата звернення: 10.07.2021).
17. Гуссерль Э. Логические исследования. Картезианские размышления. Кризис европейских наук и трансцендентальная феноменология. Кризис европейского человечества и философии. Философия как строгая наука. Минск-Харвест. Москва: АСТ, 2000. 752 с.
18. Люббе Г. В ногу со временем: сокращенное пребывание в настоящем ; пер. с нем. под науч. ред. В.А. Куренного. Москва: НИУ ВШЭ, 2016. 456 с.
19. Вирильо П. Машина зрения ; пер. с фр. А.В. Шестакова / под ред. В.Ю. Быстрова. Санкт-Петербург: Наука, 2004. 141 с.
20. Соммэр Д.С. Мораль XXI века. Москва: Кодекс, 2014. 600 с.

21. Кампер Д. Схватиться за стоп-кран. Искусство в головокружении скоростей. *Художественный журнал.* 2000. № 30/31. С. 27-28.

22. James P., Peebles E., Schramm D., Turner Ed., Kron R. The Evolution of the Universe. *Scientific American.* 1994. Vol. 271. P. 29-33; Foundations of Big Bang Cosmology. URL: https://map.gsfc.nasa.gov/universe/bb_concepts.html (дата звернення: 20.08.2021).

23. Global Education Futures. URL: https://futuref.org/educationfutures (дата звернення: 05.07.2021).

24. Іщенко А.Ю. Національна платформа цифрової освіти як пріоритетний інструмент оновлення вітчизняної освітньої системи. URL: https://niss.gov.ua/sites/default/files/2020-05/cyfrova-osvita.pdf (дата звернення: 25.08.2021).

25. Афанасьєв Д.М. До питання формування соціального потенціалу Інтернет-спільнот. *Соціальні технології: актуальні проблеми теорії та практики*. 2016. Вип. 69-70. С. 41-47.

26. Кокарча Ю.А. Інтернет-спільноти в системі суспільно-політичних відносин. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін*. 2014. Спец. вип. С. 451-456.

27. Олійник О.В. Інтернет-спільноти як суб'єкт взаємодії "суспільство – влада": проблеми та перспективи. *Вісник Львівського університету. Серія соціологічна*. 2014. Вип. 8. С. 202-207.

28. 4-я промышленная революция: что будет с рабочими местами? URL: https://www.cisco.com/c/ru_ru/about/press/press-releases/2016/01-25.html (дата звернення: 25.08.2021).

29. The American Telemedicine Association. URL: http://www.americantelemed.org (дата звернення: 25.08.2021).

30. Телемедицина в Украине и мире: текущие воможности и перспективы развития. URL: https://alfaic.ua/ru/blog/telemedicina-v-ukraine-i-mire-tekushchie-vomozhnosti-i-perspektivy-razvitiya (дата звернення: 25.10.2020).

31. Войтовський К.Є. Глобальні тренди розвитку науки і технологій: нові виклики і можливості. URL: https://niss.gov.ua/sites/default/files/2020-05/nauka-i-tehnologii.pdf (дата звернення: 25.08.2021).

32. Щодо координації діяльності з розбудови національної стійкості (стратегічний рівень): аналітична записка. URL: https://niss.gov.ua/sites/default/files/2020-02/analit-resnikova-national-secu rity-9-2020-1.pdf (дата звернення: 25.08.2021).

33. Дзьобань О.П. Цифрова людина як філософська проблема. *Інформація і право*. № 2(37)/2021. С. 9-21.

34. Біла С.О. Стратегічні пріоритети цифровізації суспільного виробництва: світовий досвід. *Економічний вісник університету*. 2021. Вип. 48. С. 40-55.

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

УДК 342.22:004.8

РАДУТНИЙ О.Е., *доктор філософії (Ph.D.) з юридичних наук, доцент*,
доцент кафедри кримінального права № 1
Національного юридичного університету ім. Ярослава Мудрого.

ПРАВОВИЙ СТАТУС ТА ХАРАКТЕРИСТИКА ЦИФРОВОЇ ЛЮДИНИ

Анотація. *В статті окреслено шлях, яким розвивається людство від Homo sapiens до цифрової людини за трьома основними напрямками. Доведено, що новітні високотехнологічні пристрої забезпечують щільний інтерактивний зв'язок з користувачем, тим самим поступово стають невід'ємними частинами біологічного тіла та свідомості людини, своєрідними органами або ланцюжками для передачі нервових сигналів. Можливість поєднання вуглецевої технології (людини) з кремнієвою технологією (штучний інтелект, імплантати, об'єкти робототехніки) створює новий потужний виклик для правової доктрини, одним з основних завдань якої стає опис правових характеристик цифрової людини, визначення її правового статусу в системі правовідносин. Для узагальнення понять "перехідна людина" (transhuman) та постлюдина (posthuman), якими оперує трансгуманізм, автор пропонує використовувати термін цифрова людина (digital human being). Аргументовано необхідність спрямування державного регулювання на обмеження або запобігання асоціальному використанню цифровою людиною своїх покращених фізичних та когнітивних властивостей. Розглянуто можливість квантового безсмертя. Висловлено припущення про появу нових прав, обов'язків і свобод, які зараз існують лише у теорії або навіть знаходяться за межами уяви і обговорення. Вони можуть стати предметом надприродного права як правонаступника права природного. Проаналізовано можливість переходу процесу прийняття рішень від цифрової людини до штучного інтелекту в її імплант, коли мозок буде продовжувати одержувати сигнали, які утворюватимуть ілюзію свободи волі. Доведено, що цифрова людина має бути визнана спеціальним суб'єктом правовідносин, спеціальною правовою персоною.*

***Ключові слова*:** *цифрова людина, перехідна людина, постлюдина, кіборг, трансгуманізм, інтелект, штучний інтелект, імплант, нейронна мережа, нейромедіатор, блокчейн, Великі Дані, інформація, Всеосяжний Інтернет, сингулярність, когнітивні функції, моторошна долина, правова персона, юридична відповідальність, природне право, надприродне право, гуманізм, постгуманізм.*

Summary. *The article outlines the path that humanity is developing from Homo sapiens to digital human being in three main vectors. The latest high-tech devices have been proven to provide a tight interactive connection with the user, thus gradually becoming an integral part of the biological body and human consciousness, a kind of organs or chains for transmitting nerve signals. The possibility of combining carbon technology (human) with silicon technology (artificial intelligence, implants, robotics) creates a powerful new challenge for legal doctrine, one of the main tasks of which is to describe the legal characteristics of digital human being, determine his or her legal status in the law system. To generalize the concepts of transhuman and posthuman, which operates on transhumanism, the author proposes to use the common term of digital human being. The necessity of directing state regulation to limit or prevent the antisocial use of improved physical and cognitive properties by digital human being is argued. The possibility of quantum immortality is considered. It has been suggested that new rights, responsibilities, and freedoms may emerge that now exist only in theory or even beyond imagination and discussion. They can become the subject of supernatural law as the successor of natural law. The possibility of the transition of the decision-making process from a digital human being to artificial intelligence in its implant, when the brain will continue to receive signals that will form the illusion of free will, is analysed. It is proved that a digital human being must be recognized as a special persona of legal relations.*

Keywords: *digital human being, transhuman, posthuman, cyborg, transhumanism, intelligence, artificial intelligence, implant, neural network, neurotransmitter, blockchain, Big Data, information, Internet of Everythings, singularity, cognitive functions, uncanny valley, legal persona, legal responsibility, natural law, supernatural law, humanism, posthumanism.*

Аннотация. *В статье рассмотрен путь, которым развивается человечество от Homo sapiens к цифровому человеку по трем основным направлениям. Доказано, что новейшие высокотехнологичные устройства обеспечивают плотную интерактивную связь с пользователем, тем самым постепенно становятся неотъемлемой частью биологического тела и сознания человека, своеобразными органами или цепочками для передачи нервных сигналов. Возможность сочетания углеродной технологии (человека) с кремниевой технологией (искусственный интеллект, имплантаты, объекты робототехники) создает новый мощный вызов для правовой доктрины, одной из основных задач которой становится описание правовых характеристик цифрового человека, определение его правового статуса в системе правоотношений. Для обобщения понятий "переходный человек" (transhuman) и постчеловек (posthuman), которыми оперирует трансгуманизм, автор предлагает использовать термин цифровой человек. Аргументированно необходимость направления государственного регулирования на ограничение или предотвращение асоциального использования цифровым человеком своих улучшенных физических и когнитивных свойств. Рассмотрена возможность квантового бессмертия. Высказано предположение о возможности появления новых прав, обязанностей и свобод, которые сейчас существуют только в теории или даже находятся за пределами воображения и обсуждения. Они могут стать предметом надприродного права как правопреемника естественного права. Проанализирована возможность перехода процесса принятия решений от цифрового человека к искусственному интеллекту, размещенному в имплантате, когда мозг будет продолжать получать сигналы, создающие иллюзию свободы воли и выбора. Доказано, что цифровой человек должен быть признан специальным субъектом правоотношений, специальной правовой персоной.*

Ключевые слова: *цифровой человек, переходный человек, постчеловек, киборг, трансгуманизм, интеллект, искусственный интеллект, имплантат, нейронная сеть, нейромедиатор, блокчейн, Большие Данные, информация, Всеобъемлющий Интернет, сингулярность, когнитивные функции, зловещая долина, правовая персона, юридическая ответственность, естественное право, надприродное право, гуманизм, постгуманизм.*

Постановка проблеми. Як стверджують Р. Шіллер (Robert Shiller) та Дж. Акерлоф (George Akerlof), людина мислить наративами, тобто за допомогою розповіді, в якій розвиток подій має внутрішню логіку та динаміку, що справляє враження одного цілого [31, с. 75]. Тож, перші оповіді про співіснування людини і технологій можливо відшукати в найдавніших пам'ятках, зокрема, Епосі про Гільгамеша, Старому Завіті, давньогрецьких міфах тощо. Більш пізніми роздумами є ідея симбіозу людини з машиною Дж. Ліклайдера (J.C.R. Licklider), за яку людина та комп'ютер співіснують сумісно, коли машинному інтелекту відводиться істотна роль у розширенні та інтенсифікації розуму людини [18], або концепція кіборга (кібернетичного організму, від англ. – cybernetic organism, скорочено – cyborg) на підґрунті осмислення М. Клайнсом (Manfred E. Clynes) та Н. Клайном (Nathan S. Kline) можливостей виживання людини поза Землею впродовж тривалих космічних польотів [5].

Той шлях, яким розвивається людство за останні 100 років з 200 тисяч років свого існування, іменують генно(біо)-культурною коеволюцією Кевін Лаланд (Kevin Laland), технологічно-психологічною еволюцією Роберт Фогель (Rober Fogel), або метабіологічною еволюцією Джонас Солк (Jonas Edward Salk). На ньому спостерігається відчутна зміна способу та тривалості життя, основних характеристик організму (зріст, обсяг, вага,

сила), патоморфозу[1], рівня IQ тощо. Крім того, у значних обсягах зменшено природній відбір та інші регулятори (голод, хвороби, широкомасштабна внутрішньовидова агресія), відшукано можливість втручатися в генетичний код, клонувати органи, синтезувати штучну бактерію тощо. Так, нещодавно в Ізраїлі розробили та успішно випробували імплант в серце людини у формі трубки [6], який працює під керуванням штучного інтелекту. Набирає оберти наукова програма з розшифрування конектому (повного опису структури зв'язків у нервовій системі) людського мозку, яка дозволить транспонувати особистість у "хмару", жити там вічно та позбутися соматичного та психологічного страждання.

Тож, сучасна еволюція *Homo sapiens* у цифрову людину [39, с. 57-63; 40, с. 202-213; 41, с. 41-43] є у своїй переважній більшості штучною та відбувається у декількох основних напрямках, зокрема: 1) біоінженерія (втручання в організм людини на клітинному та атомному рівнях; розробка гібридних нанороботів на основі синтетичних білків; імплантація реконструйованої ДНК; вирощування органів на замовлення або їх 3D-друк тощо); 2) створення живої істоти, що поєднує органіку з неорганікою, або формування кібернетичного організму (кіборга) – біологічного організму, який містить механічні та(або) електронні компоненти – за двома піднапрямками, зокрема, *а)* відновлення органу або його функцій (кардіостимулятори, серцеві клапани, кохлеарні імплантати для оновлення слуху, iBrain Neurointerface для тонкого моторного контролю, штучна рука i-LIMB Pulse, колінний протез RheoKnee, протез сітківки ока Retina Implant у вигляді мікрочіпу, окуляри EnChroma для сприйняття кольорів тощо) та *б)* доповнення існуючих натуральних можливостей новими більш ефективними штучними (пам'ять без прогалин, GPS навігація, кохлеарні імплантати для виведення слуху на новий рівень, імплант у сітківку ока, який дозволяє сприймати сигнали в іншому спектрі тощо); 3) створення неорганічної форми життя (копіювання або повне перенесення свідомості, інтелекту та особистості людини в цифровий або інший носій; сканування мозку людини та його відновлення у вигляді електронної копії, набуття цифрового безсмертя з можливістю передачі ідентичності людини до "хмари" цифрового сервера або шляхом розпорошення у мережі за технологією блокчейн) [42, с. 158-171]. У зв'язку з цим Ю. Мартинюк обґрунтовано прогнозує появу неіснуючих раніше біологічних форм [37, с. 155].

Понятійний апарат суспільних наук починає збагачуватися і предметно оперувати таким поняттями, як постлюдина (розумна істота, модифікована до ступеню, що вже не є звичайною людиною), надрозум (будь-який розум, що значно перевершує будь-які досягнення людства), віртуальна реальність (оточення, яке відчувають, не знаходячись у ньому фізично) тощо [33, с. 4].

Поява та подальше використання будь-якого генетичного матеріалу спочатку у вигляді бінарного комп'ютерного коду з наступним його перетворенням на певну послідовність ДНК реального біологічного організму відкриває перед людством нечувані можливості. Прорив у розшифруванні геному став можливим завдяки зростаючий доступності обладнання та технологій. Позитивний ефект від цього вбачається у більш точній і менш інвазійній діагностиці, ефективному лікуванні завдяки персоналізованій медицині, зниженні кількості генетичних захворювань тощо, негативний – у протиправному використанні результатів поєднання біології з інформаційними технологіями, маніпуляції речовинами в атомному або молекулярному масштабі за

[1] Патоморфоз (від давньогрец. πάθος – "страждання", μορφή – "вид, форма") – зміна ознак окремої хвороби, захворюваності та причин смертності під впливом біологічних та соціальних факторів.

допомогою нанотехнологій, розробленні та використанні персоналізованої біологічної зброї, що спирається на унікальну біологічну, в тому числі генетичну, інформацію конкретної людини або певної людської групи, штучному підробленні зразків крові, слини або інших біологічних матеріалів з ДНК-профілю конкретної людини або певної людської групи, генетичній дискримінації тощо.

Завдяки кооперації між другим та третім напрямками (нейротехнології, імпланти, сканування мозку людини та його відновлення у вигляді електронної копії тощо) незрячі люди можуть отримати вперше або відновити здатність бачити, люди з обмеженими можливостями – контролювати протезні кінцівки, комп'ютерні маніпулятори або інвалідні коляски за допомогою сили думки, в той час як нейронний зворотний зв'язок (можливість здійснювати моніторинг мозкової діяльності в режимі реального часу) пропонує величезну кількість неоднозначних з точки зору права та етики можливостей для координації поведінки. Своєчасне збирання, обробка, зберігання та аналіз великих обсягів даних про мозкову діяльність конкретної людини дозволяють підвищити ефективність діагностики і вирішення психічних проблем [7]. Але так само не виключається ризик прийняття рішень суто на основі одержаних мозкових даних без урахування інших чинників [25], небезпеки читання думок, снів, бажань тощо, маючи своїм наслідком поступове зникнення приватності життя, ризик загрози повільної втрати творчих здібностей, появи неочікуваних типів нової поведінки через використання нових розширених фізичних або когнітивних можливостей.

Завдяки технологіям дедалі більше розширюються межі усвідомленого сприйняття людиною свого власного біологічного тіла. Зсув цієї межі раніше фіксувався за прикладами відчуття досвідченим воїном кінцівки своєї холодної зброї, водієм – габаритів транспортного засобу як свого власного тіла тощо, тож з прискорення поточної технологічної революції цей процес продовжує розгортатися далі, в тому числі, захоплюючи додану реальність. Новітні засоби комунікації пропонують щільний інтерактивний зв'язок з користувачем, тим самим поступово стають невід'ємними частинами біологічного тіла та свідомості людини, своєрідними органами або ланцюжками для передачі нервових сигналів. Новації спокушають і після нетривалого звикання унеможливлюють подальше життя без них. Спроби їх ігнорувати є такими ж марними, як і намагання позбавитися та жити без них.

Тож не є дивним, що разом з поколінням нових приладів з'являється нове покоління людей з ознаками стійкої технологічної залежності. Інформаційно, програмно та апаратно розвинуті індивіди з гібридними формами надбаної ідентичності починають формувати і закріплювати нові форми соціальних зв'язків. Разом вони створюють, за Г. Рейнгольдом (Howard Rheingold), "розумні натовпи" (*smart mob*) [27, с. 103], які взаємодіють у новий спосіб, поєднуючи між собою різні особистості, матеріальні об'єкти та географічні координати у загальну мережу.

Можливості поєднання вуглецевої технології (людини) з кремнієвою технологією (штучний інтелект, імплантати, об'єкти робототехніки), як її формулює М. Кайку (Michio Kaku) [15, с. 233], а також перенесення структури і зв'язків мозку людини один нейрон за іншим на неорганічний або напіворганічний носій, створюють новий потужний виклик для правової доктрини. Одним з актуальних завдань останньої стає опис правових характеристик цифрової людини, визначення її правового статусу в системі правовідносин.

Результати аналізу наукових публікацій. Вагомі внески у дослідження пов'язаного з цифровою людиною феномену штучного інтелекту здійснені Д. Барратом (James Barrat), Е. Вайценбок (Emily M. Weitzenboeck), Л. Вайт (L. White), Е. Хорвіцем (Eric Horvitz), Н. Бостромом (Niklas Boström), І. Маском (Elon Musk), Д. Дайсоном (George

Dyson), К. Келлі (Kevin Kelly), Р. Кало (Ryan Calo), П. Асаро (Peter M. Asaro), В. Вінджем (Vernor Steffen Vinge), К. Хернесом (Christoffer Hernæs), П. Черкою (P. Čerka), С. Чопрою (S. Chopra) та багатьма іншими, у галузі вітчизняного права – О.А. Барановим, В.М. Брижко, М.В. Карчевським, В.А. Мисливим, В.І. Павликівським, В.Г. Пилипчуком, Н.А. Савіновою, Є.О. Харитоновим, О.І. Харитоновою, К.В. Юртаєвою та багатьма іншими. Інші публіканти (Л.А. Улашкевич, В. Муренко під кураторством В.В. Мачуського) використовують ідеї і тексти, презентуючи їх як свої власні або не вказуючи на авторство, чим певною мірою підкреслюють їх цінність та популяризують запозичене.

Прихильниками ідей трансгуманізму[2] як напрямку створення надлюдини з покращеними фізичними та когнітивними здібностями, завдяки чому вид *Homo sapiens* отримав новий еволюційний поштовх, є професор Оксфордського університету Н. Бостром (Niklas Boström), футуролог Г. Моравець (Hans Moravec), винахідник та футуролог Р. Курцвейл (Raymond Kurzweil), "батько" кріоніки Р. Еттінгер (Robert Chester Wilson Ettinger), біолог і політик Дж. Гакслі (Sir Julian Sorell Huxley) тощо.

На думку їх опонентів будь-який винахід або технологія являють собою самоампутацію частини фізичного тіла або свідомості, що вимагає пошуку нових пропорцій та рівноваги між іншими органами та мозковими процесами [36, с. 54], звісно, якщо не будуть реалізовані сценарії за твором Ф. Герберта "Дюна" (Dune, Frank Herbert), кінофільму "Матриця" (The Matrix) братів (зараз сестер) Вачовскі (Lana Wachowski раніше Laurence Wachowski, Lilly Wachowski раніше Andrew Paul Wachowski), комп'ютерної гри "Горизонт: Світанок з нуля" (Horizon: Zero Dawn) студії Guerrilla Games тощо. Основним дороговказом при цьому має виступати запобігання сингулярності (В. Віндж, Р. Курцвейл), яка є не лише невизначеністю [43, с. 449-451], але незворотною точкою неможливості стримувати під належним контролем надрозум машин, що Дж. Ланьє (Jaron Zepel Lanier) дорівнює до Апокаліпсису [17, с. 152].

Натомість, для трансгуманістів технологічна сингулярність виступає точкою відліку нової історії людства, де людина є попереднім етапом по відношенню до "перехідної людини" (*transhuman*) та її наступника "постлюдини" (*posthuman*), основні здібності якої настільки радикально перевищують аналогічні у сьогоднішніх людей, що вона більше вже не є людиною відповідно до звичайних стандартів [1].

При цьому важливою складовою процесу перетворення виступає зростаюча взаємодія з віртуальними світами та віртуальними персонами. Втім, правники і так є звиклими до них, адже юридична особа насправді є віртуальною правовою персоною, суб'єктом правовідносин, яку ніхто ніколи не бачив і про існування якої дізнаємося лише з паперів або через маніфестації уповноважених фізичних осіб. Тож, вбачається можливим об'єднати "перехідну людину" та "постлюдину" загальним поняттям "цифрова людина" (*digital human being*).

І якщо теорія інформаційного суспільства (Daniel Bell, Laszlo Karvalics, Manuel Castells Oliván, Pekka Himanen та інші) приділяє більшу увагу позитивним аспектам технологічного майбутнього, то з протилежного боку її врівноважує жанр "кіберпанку" (*cyberpunk*), представниками якого є Gardner Raymond Dozois, William Gibson, Bruce Sterling та інші), що висвітлює темний бік високих технологій, без якого не є можливим жодне явище.

[2] Трансгуманізм (від лат. *trans* – "крізь, через", *humanitas* – "людяність", *humanus* – "людяний", *homo* – "людина") – світогляд, заснований на осмисленні досягнень та перспектив науки, що визнає можливість і бажаність докорінних змін у становищі людини, за допомогою передових технологій задля позбавлення їх від страждання, старіння та смерті, а також значного посилення фізичних, розумових і психологічних можливостей людини.

Інші дослідники [32] вказують на можливі значні ризики при переході до "швидкого світу" при наближені до "бар'єру Лема" (на думку Станіслава Лема такий бар'єр має місце під час переходу до систем управління та виконання стратегічних завдань на прискорених і недоступних для людей швидкостях, коли адекватна реакція вимагає виключення людини із кола прийняття рішень). Примітною є та обставина, що цифрова людина може бути оснащена такими системами.

Т. Копечек (Tomáš Kopečeк) [16, с. 30] зазначає, що штучний інтелект і всі похідні від нього є суто людським проектом з усіма притаманними цьому здобутками і недоліками. В той час як на думку А. Малапі-Нельсон (Alcibiades Malapi-Nelson) [19] проект *Homo sapiens* взагалі існує в системі дарвінівської еволюції виключно завдяки випадковості. У природі не існує особливого місця для нього, ми прийшли, і оскільки жоден вид не є вічним, також зникнемо. Але трансгуманізм відкидає цю точку зору як морально, так і метафізично, стверджуючи, що існує можливість дедалі більше знаходити себе когнітивно поза природною еволюцією, тож не просто бути її частиною, але керувати нею, щоб захистити своє виживання на противагу теорії Чарльза Дарвіна.

Таким чином, окреслена правова проблема цифрової людини продовжує залишатися дискусійною, а так само відкритою для дослідження та обговорення. Важливо поряд з технологіями розвивати право та інші способи соціальної взаємодії.

Метою статті є оцінка окремих правових характеристик цифрової людини, визначення її правового статусу в системі правовідносин.

Виклад основного матеріалу. На думку М.М. Чурсіна [48, с. 290] людство поступово стає більш залежним від ступеню прив'язаності до зовнішньої пам'яті (сховища тексту), обладнання та програмного забезпечення для її обробки, ніж від спілкування з подібними істотами. В результаті всі інформаційні процеси, включаючи прийняття рішень, залишають біологічне лоно і переходять у кремнієвий світ. Цитуючи Метта Хейга (Matt Haig) [13, с. 89], ми поступово занурюємось у світ, в якому очікуємо більше від технологій і менше один від одного.

Втім, це проблема сучасного покоління людей, але не наступного. У останнього можуть з'явитися більш складні і непередбачувані виклики. Життя розвивається і одержує нові будівничі елементи. Так, дослідниками з Scripps [30] вдалося створити першу в історії напівсинтетичну бактерію з двох нових нуклеїнових основ на додаток до існуючих базових (зокрема, adenine (A), cytosine (C), guanine (G), thymine (T) та uracil (U), що складають ДНК будь-якого біологічного організму.

Поступово і неухильно підтверджуються прогнози Клауса Шваба (Klaus Martin Schwab) з посиланням на Звіт Міжнародної експертної ради Всесвітнього економічного форуму "Глибинні зміни – технологічно переломні моменти та соціальний вплив" за 2015 р. [49, с. 190] щодо зростання числа людей, підключених до пристроїв, які в більшій мірі стають приєднаними до їх тіл. Пристрої не тільки переносяться (*wearable electronic*), але вони також імплантуються в організм людини, виконуючи функції зв'язку, оздоровчі функції, визначення місця розташування і моніторингу поведінки тощо. "Розумні" цифрові татуювання не тільки виглядають привабливо, але можуть виконувати корисні функції (ідентифікація, визначення місцезнаходження, розблокування автомобіля, проведення фінансових транзакцій, введення кодів мобільного телефону за допомогою вказівки пальцем або дотику до тіла тощо). "Розумний" пил (масиви повністю укомплектованих комп'ютерів з антенами, кожний з яких менше піщинки) організовуються всередині тіла людини у певні мережі для підтримки цілого ряду складних внутрішніх процесів (атакують хворобу на ранній стадії, полегшують біль, зберігають важливу інформацію в зашифрованому вигляді). "Розумна" пігулка від

компаній Proteus Biomedical та Novartis має прикріплений цифровий пристрій, який повністю біологічно розкладається через певний час, але до того передає на телефон або інший визначений пристрій дані про те, як організм реагує на введені ліки [22]. Позитивний ефект від цього вбачається в зростанні ефективності лікування, підвищенні самодостатності, поліпшенні процесу прийняття рішень тощо, негативний – у потенційному спостереженні, зниженні рівня безпеки даних, напрацюванні залежності, підвищенні рівня нервово-психічного збудження (синдрому дефіциту уваги) тощо.

Імпланти, які покращують окремі фізичні властивості тіла людини (сила, спритність, гнучкість, витривалість, швидкість реакції тощо) здатні позбавити її тяжкої, небезпечної або нудної фізичної праці, а так само розширити еволюційні горизонти (краще чути, бачити, сприймати без обмежень всі сигнали оточуючого світу тощо). Імпланти, які покращують окремі когнітивні властивості людини (пам'ять, аналітичні здібності, обробка значних обсягів інформації, можливість відрізняти головне від несуттєвого, рухливість розуму, вміння аргументувати та знаходити взаємозв’язки, приходити до висновку завдяки ланцюжку роздумів, критичність, широта мислення тощо) здатні звільнити розум від рутинної роботи та(або) суттєво покращити її результати. Це передбачає, в тому числі, можливість обробляти та архівувати величезні обсяги інформації, включаючи Big Data. Тоді в окремих напрямках людство може знову претендувати на повернення перемоги над неорганічним штучним інтелектом, наприклад, у грі в шахи після 1997 р. (коли сталася перемога над чинним чемпіоном Гарі Каспаровим, після якої жодна людина вже не претендувала на вищість), або в стародавній китайській грі го після 2016 р. (аналогічна історія з Лі Седолем), якщо цифрова людина як спадкоємець *Homo sapiens* буде здатною збільшити ефективність своїх мозкових процесів, аналізуючи величезну бібліотеку дебютів, стандартних завершень та зіграних партій, конкурувати з нейронними мережами штучного інтелекту у розробці нестандартних рішень тощо, адже можлива кількість комбінацій на дошці складає для шахів 10^{53} варіантів та для “Го” 10^{123} варіантів, що на 40 порядків перевищує можливу кількість атомів у Всесвіті.

Істотне покращення біологічних та когнітивних властивостей у дійсності має теж саме призначення, що й вживання допінгу, яке на їх фоні виглядає вже доволі примітивним. Але якщо останній у більшості випадків викликає негативну реакцію з боку суспільства (Антидопінгова Конвенція ETS № 135 від 16.11.1989 р., ратифікована Законом України від 15.03.01 р. № 2295-III, Міжнародна конвенція про боротьбу з допінгом у спорті, ратифікована Законом України від 03.08.06 р. № 68-V, Закон України “Про антидопінговий контроль у спорті” від 07.02.17 р. № 1835-VIII, ст. 323 КК України тощо), то вказані біологічні та когнітивні зміни мають бути так само враховані правом. У випадку асоціального використання таких властивостей державне регулювання може бути спрямоване на їх обмеження або запобігання настанню негативних наслідків.

Прояви цифровою людиною своїх змінених здібностей (надзвичайна сила, спритність, гнучкість, розумові здібності тощо) на рівні соціальної взаємодії здатні спровокувати ефект “моторошної долини” (*uncanny valley*), гіпотеза якої була сформульована в галузі робототехніки та трьохвимірної комп’ютерної анімації з приводу можливої реакції людини на людиноподібного робота. Оригінальна ідея Масахіро Морі (Masahiro Mori) [21] передбачає, що зі збільшенням людиноподібності робота збільшується позитивне враження та емпатія до нього з боку людини аж до того моменту, коли враження різко стає відразливим, страшним або огидним (напр., у випадку демонстрації нутрощів або неприродних здатностей, які людина мати не може). Ця область негативного враження між виглядом “трохи людським” і “цілком людським” одержала назву “моторошної, неприродної долини”. Вона виражає ідею про те, що майже ідеально людиноподібні роботи

(у розглядуваному випадку – цифрова людина) виглядають “дивно” і “неприродньо” для людини, викликаючи відразу або страх, тож не зможуть викликати належну емпатію. Однак, у подальшому не виключається збільшення позитивності враження (термін долина пов’язаний з відповідною частиною на графіку між сприйняттям та огидою).

Ще більше очікувань існує відносно взаємодії нейронної системи мозку людини з нейронними мережами штучного інтелекту. Останні планується наділили такими властивостями як повна обізнаність у принципах своєї побудови і роботи, самонавчання, саморозвиток, самоперебудова, самовдосконалення (перша версія утворює вдосконалену версію самої себе і так переписує програму до нескінченності), автономність від людини, самостійність прийняття рішень і самостійне їх виконання тощо. Можливо, при цьому нейронні системи мозку людини та нейронні мережі штучного інтелекту навчаться певним чином доповнювати та тренувати одна одну.

Втім, доволі значною проблемою залишається неможливість розпізнавання алгоритму дій штучного інтелекту, який здатний до самонавчання (*self-learning Artificial Intelligence*), або цифрової людини з відповідним імплантом, під час прийняття ними рішень. Вже сьогодні у значній кількості випадків це є чорною скринькою без будь-якого зворотного зв’язку, коли одержується результат, але не є відомим, які саме аргументи або критерії було покладено в його основу. У значній кількості випадків розробники алгоритму не можуть повною мірою дати звіт про те, що відбувається у “первісному бульйоні” (primordial soup)[3] штучних нейронних мереж.

Для права це має принципове значення не тільки відносно несправедливого рейтингування, позбавлення прав або покладання додаткових обов’язків. Якщо у подальшому буде складно визначитися з тим, чи дійсно певний акт поведінки цифрової людини є її вільним волевиявленням, або навпаки рішення було прийняте за неї алгоритмами штучного інтелекту, що вбудований у її імплант, то основи правової доктрини зазнають істотного виклику на рівні фундаментального підґрунтя. За певних обставин (необхідність обробки значного обсягу даних, ризикована ситуація, яка потребує миттєвих рішень, або виконання стратегічних завдань на прискорених і недоступних для людей швидкостях, коли адекватна реакція вимагає виключення людини із кола прийняття рішень) керування може переходити від людини до алгоритму, але цифрова людина продовжуватиме вважати, що приймає такі рішення самостійно. Мозок цифрової людини навіть може отримувати відповідні сигнали, які утворюватимуть ілюзію свободи волі. Зазначені контроль та керування можуть спиратися як на програмне забезпечення (software) певного високотехнологічного імпланту (hardware) у поєднанні з нейронними мережами мозку, так і на контрольовані біохімічні процеси за допомогою нейромедіаторів та гормонів (адреналін, ацетилхолін, норепінефрин, дофамін, серотонін, окситоцин, ендорфін тощо).

Між тим, принцип відносної, але достатньої свободи волі індивіда є наріжним каменем обґрунтування будь-якого виду юридичної відповідальності, в тому числі цивільної, адміністративної, фінансової або кримінальної тощо. Схибленість волі індивіду (цифрової людини) може поставити під сумнів наявність фактичної підстави юридичної відповідальності. Так само не виключаються випадки безсвідомого використання цифрової людини для вчинення правопорушення або небажаних для неї дій у зв’язку з протиправним втручанням або одержанням контролю над її імплантом під керуванням штучного інтелекту.

[3] Первинний суп, або пребіотичний суп (пребіотичний бульйон) – гіпотетичний набір умов, що існують на Землі приблизно з 4,0-3,7 мільярда років тому. Фундаментальний аспект гетеротрофної теорії походження життя, вперше запропонованої Олександром Опаріним у 1924 р. та Дж. Халденом (John Burdon Sanderson Haldane) у 1929 році [24; 14].

Втім, на сьогодні відсутні підстави виключати цифрову людину з кола суб'єктів правовідносин. Вона є еволюційним наступником *Homo sapiens* та правонаступником фізичної особи як правової персони. Тривалий час можливе їх співіснування. Натомість цифровій людині можливо надати окремий правовий статус (спеціальний суб'єкт правовідносин, спеціальна правова персона) та врахувати випадки посередньої винності, коли, наприклад, правопорушення вчинюється "… шляхом використання інших осіб, що відповідно до закону не підлягають кримінальній відповідальності за скоєне…" (ч. 2 ст. 27 КК України), якщо певного рівня маніпулювання цифровою особою буде визнане обставиною, яка виключає винність та волимість її діяння.

Досліджуючи соціальні аспекти, К.В. Райхерт [45, с. 98-104] прогнозує наступні різновиди ставлення до кіборгізованої людини: 1) кіборгізована людина більше не сприймається як людина, до неї ставляться як до робота; 2) кіборгізована людина сприймається як людина, до неї ставляться як до людини; 3) кіборгізована людина сприймається як людина, до неї ставляться як до людини, але при цьому вважається, що на фізичному рівні між людиною та роботом не має жодної відмінності. Останній варіант ілюструється висловом Дж. Маркоффа (John Markoff) [20, с. 10] про те, що технології, які розширюють інтелектуальні можливості людини, можуть її також повністю замінити, потенційно стираючи різницю між людиною та машиною зі штучним інтелектом не лише на фізичному, але й на інших рівнях, наприклад, юридичному (машини зі штучним інтелектом можуть мати права, свободи й обов'язки) чи етичному (чи можна знищувати машини зі штучними інтелектом). Крім того, К.В. Райхерт [46, с. 86] пропонує до обговорення ще одне слушне питання про те, як кібернетичний організм, наділений свідомістю (психікою, особистістю) померлої людини, або перенесена на інший носій особистість упорається з переживанням смерті в якості психічної травми.

Між тим, можливість квантового безсмертя обговорюється фізиками та іншими представниками природознавчих наук з моменту появи у 1957 р. теорії "Множинності світів" (Many-Worlds theory) Х. Еверета (Hugh Everett III) [9], відповідно до якої життя являє собою нескінченну множину ймовірних подій, з якої мозок людини відображає лише ті варіанти ситуацій, в яких вона залишається живою до повного вичерпування таких можливостей. Втім, відповідно до принципу невизначеності В.К. Гейзенберга (Werner Karl Heisenberg) ми не є нейтральними спостерігачами, але активно впливаємо на об'єкт спостерігання, в тому числі якщо в якості останнього обрати життя людини (спостерігаючи за квантовою системою ми впливаємо на неї, змінюючи на величину, яка не перевищує половину зведеного кванта дії [12]). Але поки що не є вирішеним питання, про чиє життя йдеться – своє власне чи інших осіб з будь-якого близького або віддаленого оточення.

На думку В.П. Казначеєва та групи вчених Новосибірського університету [34, с. 41, 43] людина, як планетарно-астральне утворення, формуючи свій інтелект, спочатку входить в узгодження, а потім у поступову розкоординацію з власним тілом, у якому виникає і співіснує протягом певного часу. Її мозок, як суб'єкт, що розташований у тілесній структурі, синхронізується з тілом у вітальному циклі з відтворення і зберігання поколінь, запобігаючи зникненню виду живої істоти. Однак з віком мозок дедалі більш співвідноситься із хвильовим простором космосу, стає дедалі більш самостійним суб'єктом, якому вже недостатньо енергетичного матеріалу у вигляді окисних процесів. Поступово він входить у протиріччя зі своїм носієм – тілом і змінює численні гомеостатичні процеси в організмі, що викликає хвороби та руйнування тіла. Мозок при цьому виживає, з віком його диктатура стає більш жорсткою, спрямованою в живий космічний простір. Тіло поступово відстрілюється, як запущена в космос ракета відстрілює

першу, другу або третю ступінь. Із затуханням окисно-відновлювальних процесів існування в організмі білково-нуклеїнової форми завершується природною смертю, а його хвильова форма поступово нарощує термодинамічні властивості, віддаляється й на останок залишає кліткові утворення тіла, повертаючись, скоріш за все, в геокосмічний простір живих інтелектуальних потоків. Іншими словами, життя відділяє свою хвильову (соліторно-голографічну) форму і зливається у безсмерті з безмежно живим простором космосу.

Такий підхід не є поодиноким і його певною мірою сповідують інші дослідники, зокрема, Д. Кларк (Josh Clark) [4], С. Хамерофф (Stuart R. Hameroff) та Р. Пенроуз (Roger Penrose) [28]. Крім того, він не суперечить вищезгаданому принципу невизначеності В.К. Гейзенберга (Werner Karl Heisenberg) та відповідає на питання теорії "Множинності світів" (Many-Worlds theory) Х. Еверета (Hugh Everett III) про те, куди після закінчення всієї множини ймовірнісних подій зникає свідомість.

Тож, на думку окремих фізиків, нейробіологів та правників, щодо яких складно сформулювати підозру в езотериці, квантове безсмертя окремо обраної свідомості є цілком реальним, адже згідно з законом збереження енергії остання не виникає ні з чого і не зникає без сліду, вона лише перетворюється з одного виду в інший та переходить з одного стану в інший. Таким чином, свідомість не є тлінною субстанцією, речовиною або іншим об'єктивним феноменом, тож навіть після фізичної смерті біологічного тіла як певної оболонки квантова інформація може зберігатися у Всесвіті вічно і здійснювати тим самим вплив на нього. Отже, на розвиток цього теоретичного підґрунтя залишається відкритим лише питання практичної реалізації третього напрямку еволюції *Homo sapiens* у цифрову людину, а саме – створення неорганічної форми життя, копіювання або повне перенесення свідомості, інтелекту та особистості людини в цифровий або інший носій, відновлення мозку людини у вигляді електронної копії, надбання цифрового безсмертя з можливістю передачі ідентичності людини до "хмари" цифрового сервера або через розпорошення у мережі за технологією блокчейн тощо.

Таку практичну реалізацію вже сьогодні пропонує невролог з Йєльського університету (Yale University) Стівен Новела (Steven Novella) [23]. Так само Стівен Хокінг (Stephen William Hawking) не заперечував теоретичної можливості скопіювати мозок людини у комп'ютер та забезпечити таким чином життя після смерті біологічного тіла [3]. І хоча він об'єктивно скаржився на відсутність ефективних технологій, але сам був прикладом можливості життя в активний спосіб за допомогою досягнень науково-технічного прогресу, не зважаючи на істотні фізичні обмеження свого тіла.

Ще однією примітною властивістю цифрової людини є наступна. Вона може бути здатною враховувати більше ніж традиційних 5 – 7 факторів під час прийняття рішення, або ефективно взаємодіяти більше ніж з 5 – 7 іншими людьми, або взаємодіяти більше ніж з 120 – 150 особами, що значно перевищуватиме число Данбара (Dunbar`s number) [8] – граничну межу кількості комунікаційних одиниць, з якими окрема людина здатна підтримувати стабільні соціальні відносини, в яких вона знає, ким хто кому доводиться і як з кожним слід поводитися. Спілкування, опрацювання інформації та прийняття рішень для цифрової людини можуть перейти у раніше згадану фазу "швидкого часу", в системі якого мозкові процеси звичайної людини можуть виглядати як принизливо повільні. Це саме може стосуватися й інших властивостей і здібностей. Вказані порівняння здатні спровокувати зверхнє ставлення цифрової людини до всього іншого людства, появу нового прошарку або нової касти вдосконалених людей, право і мораль яких можуть відрізнятися від поширених сьогодні [44, с. 78-96]. Такий зверхній погляд підживлює антропоцентризм на користь людини, але все може принципово змінитися з появою цифрової людини та утворенням впливової альтернативи. Скажімо, замість природного

права засадничою базою для цифрової людини може стати право *надприродне*. Тонкий культурний шар, який миттєво зникає у випадку необхідності боротьби за виживання, може бути замінений надкультурним. Гуманізм, який сповідує цінність кожного людського життя, може бути переглянутий для цифрової людини у напрямку *постгуманізму*, що неодмінно потягне за собою переосмислення основних прав та обов'язків людини та цифрової людини. Логічною виглядає поява нових прав, свобод та обов'язків, які зараз існують лише у теорії або навіть знаходяться за межами уяви і обговорення.

Свого часу розум, хитрість, здатність до кооперації та інші корисні навички стали для *Homo sapiens* підґрунтям для перевершення та знищення всіх найближчих конкурентів (*Homo habilis, rudolfensis, ergaster, erectus, floresiensis, antecessor, heidelbergensis, neanderthalensis, rhodesiensis, cepranensis, georgicus* etc.). Тож є підстави побоюватися та очікувати подібної поведінки і від цифрової людини, яка здатна буде продовжити ескалацію чистого інтелекту у всіх сферах економічного, політичного, корпоративного, інформаційного та військового протистояння як всередині свого виду, так і по відношенню до *Homo sapiens*.

Так само, як штучному інтелекту зовсім не потрібно намагатися стати людиною, так і цифровій людині не потрібно вирішувати, яку частку свого попереднього буття обов'язково залишити, яку частину себе та своїх поглядів замінити на щось нове, відходячи все далі від традиційного зразка.

У можливому протистоянні між людиною та штучним інтелектом навряд чи матиме місце відкрита агресія. Скоріш за все це будуть методи м'якої сили. Штучний інтелект може спочатку усунути для людини необхідність думати, а потім взагалі усунути здатність робити це. В той же час складно передбачити, як це буде по відношенню до цифрової людини. Але вона може просто не помітити цього, так само як і *Homo sapiens*. Здатність до мислення була і поки залишається переможною еволюційною навичкою людини, але за відсутність потреби будь-яку навичку легко втратити через брак відповідного тренування.

Крім того, як зазначав Станіслав Лем [35, с. 276], нечувано швидкі машини можуть помилятися нечувано швидко. Сьогодні приклади таких помилок спостерігаються в системах алгоритмічного трейдінгу на фондових біржах [10] та в багатьох інших сферах, в тому числі об'єктів критичної інфраструктури (енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації, продовольство, охорона здоров'я, комунальне господарство тощо). Тому перехід до "швидкого світу" може як збільшувати безпеку шляхом зменшення негативного впливу з боку людського фактору, так і створювати нове підґрунтя для невизначеності.

Кожна з наведених властивостей або функцій може вказувати на наявність у цифрової людини певних переваг у порівнянні з звичайною людиною та особливого правового статусу спеціального суб'єкта правовідносин. Тому такий стан речей викликає необхідність перегляду багатьох основних доктринальних положень, зокрема, щодо заборони євгенічної практики, спрямованої на селекцію людини (п. 2 ч. 2 ст. 3 Хартії основних прав Європейського Союзу [47]), прав, свобод та обов'язків представників нового покоління.

Такі ознаки мають бути прямо закріплені в законі, наприклад, у формулюваннях "фізична особа з штучно покращеними фізичними або когнітивними властивостями" з відповідною конкретизацією щодо кожної з них – сила, спритність, гнучкість, витривалість, швидкість реакції, покращена властивість до сприйняття певних сигналів електромагнітного спектру будь-яких діапазонів (інфрачервоне, гамма, рентгенівське,

ультрафіолетове, оптичне, електромагнітне терагерцове випромінювання, мікро- та радіохвилі тощо), здатність сприймати звук в діапазоні до 16 Гц (інфразвук), понад 20 кГц (ультразвук), або на частоті 10^9 – 10^{13} Гц (гіперзвук), коли звичайний діапазон для людини становить від 16 Гц до 20 кГц, штучна пам'ять, аналітичні здібності на базі імплантованого програмного та апаратного забезпечення, можливість обробки значних обсягів інформації Big Data тощо.

Поява, закріплення та поширення виду (класу, роду) цифрової людини знаменують собою початок нової цивілізації. Вона може бути ворожою, дружньою або нейтральною до попередньої, але вона точно буде іншою.

На доповнення до роздумів про нову правову, соціальну та технологічну культуру цифрової людини слід також врахувати ще один важливий аспект. Колись за задумкою Карла Ліннея (Carl Linnaeus, Carl Linné, Carolus Linnaeus, Carl von Linné, 1707 – 1778) слово *sapiens* у словосполученні *Homo sapiens* повинне було підкреслити наявність інтелекту тільки у людини. Ця унікальна властивість мала виокремити останню серед всіх інших істот на планеті. Така теза не виглядає безспірною не тільки з точки зору Кембриджської декларації про свідомість (The Cambridge Declaration on Consciousness, July 7, 2012) [29], але й у зв'язку з появою у *Homo sapiens* нового потужного еволюційного конкурента, на що вже було звернуто увагу у попередніх публікаціях [26; 39, с. 57-63]. Ним поряд зі штучним інтелектом є цифрова людина (*digital human being, Homo digital, Homo numeralis, Homo digitalis, Homo Horologium*) [40, с. 202-213; 41, с. 41-43]. Так сталося, що будь-яка істота, яка не має можливості користуватися людськими засобами комунікації, через цю обставину автоматично стає позбавленою змоги переконливо та у повному обсязі продемонструвати представнику цивілізації людей наявність свого власного досвіду або почуттів, пояснити прийняті рішення та їх аргументацію, довести існування усвідомленості, власну суб'єктивність, кваліа (qualia)[4, почуття гідності та систему виконавчого контролю розуму [11, с. 60]. Заперечення факту наявності свідомості у будь-якої іншої істоти, крім людини, має наслідком висновок про моральність і допустимості спричинення їй шкоди, адже життя та інші інтереси такої істоти не являють собою цінностей, подібних до людських. Втім, якщо сучасне людство не стане у спромозі налагодити комунікацію з іншою цивілізацією (внутрішньою – інші розумні істоти, цифрова людина, штучний інтелект, який не матиме перешкод у комунікації з людиною, успішно долаючи тест Тьюрінга, або зовнішньою – позаземний інтелект) та довести їй свою фундаментальну цінність, воно може опинитися у доволі незручному для себе становищі, якщо продовжуватиме спиратися виключно на переможний до цього часу антропоцентризм та сповідувати власну вищість. Вельми необачним стає розташовувати інших істот на щаблях нижче за людину, а так само відносити інші інтелекти до "другої природи" (або природи другого сорту, напр., штучний інтелект є продуктом людини, отже не може бути розумнішим і впливовішим за свого творця).

Якщо розгадку таємниці людської свідомості пропонується шукати не через окремо обрану людину, натомість в інтелектуальній діяльності всього людства, то феномен штучної свідомості може повною мірою розкритися через поєднання будь-який різновидів штучного інтелекту у мережі блокчейну або Всеосяжного Інтернету (Internet of Everything). Таке злиття здатне проілюструвати дію діалектичного принципу переходу кількості в якість шляхом перетворення слабкого, вузького, прикладного або обмеженого штучного інтелекту (Weak Artificial Intelligence, Artificial Narrow Intelligence, Applied

[4] Кваліа (від лат. *qualia* – "властивості, якості") – філософський термін для позначення сенсорних, чуттєвих явищ будь-якого роду, або властивостей чуттєвого досвіду. Введений у науковий обіг Кларенсом Ірвінгом Льюїсом (Clarence Irving Lewis, 1883 – 1964) у 1929 р. [2, с. 400-405].

Artificial Intelligence, AAI) у найпотужніший штучний суперінтелект (Artificial Superintelligence, ASI) [38, с. 13-29]. Цифрова людина може стати органічною частиною цього Всеосяжного Інтернету (Internet of Everything) разом зі штучним інтелектом.

Висновки та пропозиції.

Перші згадки про співіснування людини і технологій мають багатовимірні витоки, серед яких Епос про Гільгамеша, Старий Завіт, давньогрецькі міфи, ідея симбіозу людини з машиною Дж. Ліклайдера, концепція кіборга (кібернетичного організму) М. Клайнса та Н. Клайна тощо. Шлях, яким розвивається людство від *Homo sapiens* до *Цифрової людини* за трьома основними напрямками, іменують генно(біо)-культурною коеволюцією, технологічно-психологічною або метабіологічною еволюцією.

Новітні високотехнологічні пристрої забезпечують щільний інтерактивний зв'язок з користувачем, тим самим поступово стають невід'ємними частинами біологічного тіла та свідомості людини, своєрідними органами або ланцюжками для передачі нервових сигналів. Можливість поєднання вуглецевої технології (людини) з кремнієвою технологією (штучний інтелект, імплантати, об'єкти робототехніки) створюють новий потужний виклик для правової доктрини, одним з основних завдань якої стає опис правових характеристик цифрової людини, визначення її правового статусу в системі правовідносин.

Представники трансгуманізму не ототожнюють технологічну сингулярність з незворотною точкою неможливості стримувати під належним контролем надрозум машин, натомість, для них вона виступає точкою відліку нової історії людства, де людина є попереднім етапом по відношенню до "перехідної людини" (*transhuman*) та її наступника "постлюдини" (*posthuman*), основні здібності якої настільки радикально перевищують аналогічні у сьогоднішніх людей, що вона більше вже не є людиною відповідно до звичайних стандартів. Вбачається можливим об'єднати "перехідну людину" та її наступника "постлюдину" загальним поняттям "цифрова людина" (*digital human being*).

Важливою складовою процесу перетворення виступає зростаюча взаємодія з віртуальними світами та віртуальними персонами, з окремими з останніх (юридична особа) право має справу доволі значний час. Імпланти, які покращують фізичні властивості тіла людини (сила, спритність, гнучкість, витривалість, швидкість реакції тощо) здатні позбавити тяжкої, небезпечної або нудної фізичної праці, або запропонувати нові здібності (краще чути, бачити, сприймати всі сигнали оточуючого світу тощо). Імпланти, які покращують когнітивні властивості людини (пам'ять, аналітичні функції, обробка значних обсягів інформації, рухливість розуму, вміння аргументувати та знаходити взаємозв'язки, широта мислення тощо) здатні звільнити розум від рутинної роботи та(або) суттєво покращити її результати. У випадку асоціального використання таких властивостей державне регулювання може бути спрямоване на обмеження або запобігання.

Прояви цифровою людиною своїх змінених здібностей здатні на рівні соціальної взаємодії спровокувати ефект "моторошної долини" (*uncanny valley*), концепція якої передбачає, що зі збільшенням людиноподібності робота або кіборгізації звичайної людини збільшується позитивне враження та емпатія до них аж до того моменту, коли враження різко стає відразливим, страшним або огидним.

Симбіоз нейронних систем мозку людини з нейронними мережами штучного інтелекту планується наділили такими властивостями як повна обізнаність у принципах своєї побудови і роботи, самонавчання, саморозвиток, самоперебудова, самовдосконалення (перша версія утворює вдосконалену версію самої себе і так переписує програму до нескінченності), автономність від людини, самостійність прийняття рішень і самостійне їх

виконання тощо. Істотною проблемою залишається відсутність зворотного зв'язку та неможливість розпізнавання алгоритму їх дій під час прийняття рішень.

За певних обставин (необхідність обробки Big Data, ризикована ситуація, або виконання завдань на прискорених і недоступних для людей швидкостях) керування може переходити від людини до алгоритму, але цифрова людина продовжуватиме вважати, що приймає такі рішення самостійно. Мозок цифрової людини може одержувати відповідні сигнали, які утворюватимуть ілюзію свободи волі. Контроль та керування цифровою людиною можуть бути побудовані на базі використання імпланту, програмного забезпечення у взаємодії з нейронними мережами мозку, або як контрольовані біохімічні процеси за допомогою нейромедіаторів та гормонів (адреналін, ацетилхолін, норепінефрин, дофамін, серотонін, окситоцин, ендорфін тощо). Складність у визначенні того, чи дійсно певний акт поведінки цифрової людини є її вільним волевиявленням, може поставити під сумнів наявність фактичної підстави юридичної відповідальності. Не виключаються випадки безсвідомого використання цифрової людини для вчинення правопорушення або небажаних для неї дій у зв'язку з протиправним втручанням або одержанням контролю над її імплантом під керуванням штучного інтелекту.

Відсутні підстави виключати цифрову людину з кола суб'єктів правовідносин. Натомість їй можливо надати окремий правовий статус (спеціальний суб'єкт правовідносин, спеціальна правова персона) та врахувати випадки посередньої винності, коли, наприклад, правопорушення вчинюється "…шляхом використання інших осіб, що відповідно до закону не підлягають кримінальній відповідальності за скоєне…" (ч. 2 ст. 27 КК України), якщо певного рівня маніпулювання цифровою особою буде визнане обставиною, яка виключає винність та волимість діяння.

Можливість квантового безсмертя є цілком реальною.

Зіставлення властивостей людини та цифрової людини здатне спровокувати зверхнє ставлення останньої до всього іншого людства, появу нового прошарку або нової касти вдосконалених людей, право і мораль яких можуть відрізнятися від поширених сьогодні. Замість природного права це може бути право *надприродне*. Гуманізм, який сповідує цінність кожного людського життя, може перейти на платформу *постгуманізму*, що неодмінно потягне за собою переосмислення основних прав і обов'язків людини та цифрової людини. Логічною виглядає поява нових прав, свобод та обов'язків, які зараз існують лише у теорії або навіть знаходяться за межами уяви і обговорення.

Кожна з властивостей або функцій цифрової людини можуть вказувати на наявність у неї певних переваг та особливого правового статусу спеціального суб'єкта правовідносин, що викликає необхідність перегляду багатьох основних доктринальних положень, зокрема, щодо заборони євгенічної практики, спрямованої на селекцію людини (п. 2 ч. 2 ст. 3 Хартії основних прав Європейського Союзу [47]), появу прав і свобод нового покоління. Такі ознаки мають бути прямо закріплені в законі, наприклад, у формулюваннях "фізична особа з штучно покращеними фізичними або когнітивними властивостями" з відповідною конкретизацією щодо кожної з них – сила, спритність, гнучкість, витривалість, швидкість реакції, покращена властивість до сприйняття певних сигналів електромагнітного спектру будь-яких діапазонів (інфрачервоне, гамма, рентгенівське, ультрафіолетове, оптичне, електромагнітне терагерцове випромінювання, мікро- та радіохвилі тощо), здатність сприймати інфразвук, ультразвук, або гіперзвук), штучна пам'ять, аналітичні здібності на базі імплантованого програмного та апаратного забезпечення, можливість обробки значних обсягів інформації тощо.

Вельми необачним стає розташовувати всіх інших істот на щаблях нижче за людину, а так само відносити інші інтелекти до "другої природи" (або природи другого сорту).

Перспективи подальших досліджень. Порушені питання та надана їм авторська оцінка є дискусійними та відкритими для конструктивної критики і широкого обговорення з огляду на їх актуальність та важливість для забезпечення подальшого розвитку інформаційного суспільства.

Використана література

1. Bostrom, Nick. (2003). The Transhumanist FAQ. A General Introduction. Version 2.1 (2003) / Oxford University, Faculty of Philosophy, 2003. 56 p.p. URL: https://web.archive.org/web/20061231225013/http://www.transhumanism.org/resources/FAQv21.pdf (дата звернення: 31.07.2021).
2. Chalmers, David J. (2002) Philosophy of Mind: Classical and Contemporary Readings, Oxford University Press. 687 p.
3. Collins, Nick. (2013). Hawking: 'in the future brains could be separated from the body'. *The Telegraph.* 20 Sep 2013. URL: https://www.telegraph.co.uk/news/science/10322521/Hawking-in-the-future-brains-could-be-separated-from-the-body.html (дата звернення: 31.07.2021).
4. Clark, Josh. (2007). How Quantum Suicide Works. *HowStuffWorks, Science.* 12 October 2007. URL: https://science.howstuffworks.com/innovation/science-questions/quantum-suicide.htm (дата звернення: 31.07.2021).
5. Clynes M., Kline N. (1960). Cyborgs and space. *Astronautics*. September 1960. URL: https://archive.nytimes.com/www.nytimes.com/library/cyber/surf/022697surf-cyborg.html (дата звернення: 31.07.2021).
6. Computer inside the heart aims to aid treatment. *BBC News, Technology.* 2 March 2020. URL: https://www.bbc.com/news/av/technology-51660393/computer-inside-the-heart-aims-to-aid-treatment (дата звернення: 31.07.2021).
7. Doraiswamy, P. Murali. (2015). 5 brain technologies that will shape our future. *World Economic Forum.* 19 Aug 2015. URL: https://agenda.weforum.org/2015/08/5-brain-technologies-future/ (дата звернення: 31.07.2021).
8. Dunbar, R.I.M. (1992) Neocortex size as a constraint on group size in primates. *Journal of Human Evolution.* Volume 22, Issue 6, June 1992, P. 469-493. URL: https://doi.org/10.1016/0047-2484(92)90081-J (дата звернення: 31.07.2021).
9. Everett III, H. (1957) "Relative State" Formulation of Quantum Mechanics. Rev. Mod. Phys. 29, 454. Published 1. July 1957 by American Physical Society. URL: https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.29.454 (дата звернення: 31.07.2021).
10. Farr, M.K. (2012). Knightmare on Wall Street – Revenge of the Machines / CNBC, 8 Aug 2012. URL: https://www.cnbc.com/id/48575707 (дата звернення: 31.07.2021).
11. Farthing, William G. (1992). The Psychology of Consciousness. Englewood Cliffs, N.J. Prentice Hall, 1992. 542 p.
12. Gefter, Amanda. (2007). Curiosity doesn't have to kill the quantum cat. *New Scientist.* 9 May 2007. URL: https://www.newscientist.com/article/mg19426031-400-curiosity-doesnt-have-to-kill-the-quantum-cat (дата звернення: 31.07.2021).
13. Haig, Matt. (2019). Notes on anervous planet. – Country Edinburgh, United Kingdom: Canongate Books, 2019. 320 pp.
14. Haldane, J.B.S. (1929). The Origin of Life. URL: https://www.uv.es/~orilife/textos/Haldane.pdf (дата звернення: 31.07.2021). (Cite: Tirard S. J. B. S. Haldane and the origin of life. J Genet. 2017 Nov; 96(5):735-739. doi: 10.1007/s12041-017-0831-6. PMID: 29237880).
15. Kaku, M. (2008). Physics of the Impossible: A Scientific Exploration Into the World of Phasers, Force Fields, Teleportation, and Time Travel. Doubleday Publishing, Duke University Libraries. 456 p. P. 233
16. Kopeček, Tomáš. (2015). Anthropomorphization of Artificial Intelligence. Bachelor thesis. Masaryk University Department of Sociology. Brno 2015. 40 p.
17. Lanier, Jaron Zepel. (2009). You Are Not a Gadget: A Manifesto. NY: Alfred A. Knopf, 2009. 221 pp.

18. Licklider J. C. R. (1960). Man-Computer Symbiosis. IRE Transactions on Human Factors in Electronics. Vol. HFE-1, no 1. Pp. 4-11. March 1960, doi: 10.1109/THFE2.1960.4503259. URL: https://ieeexplore.ieee.org/document/4503259 (дата звернення: 31.07.2021).

19. Malapi-Nelson, Alcibiades. (2018). Classical Cybernetics and Transhumanism: A Reply to Richmond's Review of The Nature of the Machine and the Collapse of Cybernetics. Sage Publishing, *Philosophy of the Social Sciences*, 2018, Volume: 49 issue: 1, page(s): 64-68. URL: https://doi.org/10.1177/0048393118811308 (дата звернення: 31.07.2021).

20. Markoff, J. (2016). Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots. Ecco, 2016. 400 p.p.

21. Mori, Masahiro (1970). Bukimi no tani The uncanny valley (K. F. MacDorman & T. Minato, Trans.). Energy, 7(4), 33-35. (Originally in Japanese). URL: https://spectrum.ieee.org/automaton/robotics/humanoids/the-uncanny-valley (дата звернення: 31.07.2021).

22. Mullin, Rick. (2012). Odd Couplings. Drug firms engage in nontraditional research partnerships in a bid to get closer to the patient. *Chemical & Engineering News.* February 13, 2012. URL: http://cen.acs.org/articles/90/i7/Odd-Couplings.html (дата звернення: 31.07.2021).

23. Novella, Steven. (2013). The Continuity Problem. *Neuroscience*. Apr 23, 2013. URL: https://theness.com/neurologicablog/index.php/the-continuity-problem (дата звернення: 31.07.2021).

24. Oparin, A.I. (1924). The Origin of Life (translation by Ann Synge of A.I. Oparin (1924) Proiskhozhdenie zhizny. Moscow. Izd. Moscovskiy Rabochiy. URL: https://breadtagsagas.com/wp-content/uploads/2015/12/AI-Oparin-The-Origin-of-Life.pdf (дата звернення: 31.07.2021).

25. Oullier, O. (2012). Clear up this fuzzy thinking on brain scans. *Nature.* 483, 7 (2012). URL: https://doi.org/10.1038/483007a (дата звернення: 31.07.2021).

26. Radutniy, O.E. (2020). Novel Criminal Delicts Related to Digital Human Being. *Herald of the Association of Criminal Law of Ukraine*. Vol 1, No 13 (2020). URL: http://vakp.nlu.edu.ua/issue/view/12594 (дата звернення: 31.07.2021).

27. Rheingold, H. (2002). Smart Mobs: The Next Social Revolution. Perseus Publishing, 2002. 288 p.

28. Stuart R. Hameroff, Roger Penrose. (2016). 14: Consciousness in the Universe an updated review of the "ORCH OR". *Theory Biophysics of Consciousness*. Pp. 517-599 (2016). URL: https://www.worldscientific.com/doi/abs/10.1142/9789814644266_0014 (дата звернення: 31.07.2021).

29. The Cambridge Declaration on Consciousness of 7 July 2012. Written by Philip Low and edited by Jaak Panksepp, Diana Reiss, David Edelman, Bruno Van Swinderen, Philip Low and Christof Koch. University of Cambridge. URL: http://fcmconference.org/img/CambridgeDeclarationOnConsciousness.pdf (дата звернення: 31.07.2021).

30. Zhang, Y., Ptacin, J., Fischer, E. et al. (2017). A semi-synthetic organism that stores and retrieves increased genetic information. *Nature*. 551, 644-647 (2017). URL: https://doi.org/10.1038/nature24659 (дата звернення: 31.07.2021).

31. Акерлоф Джордж, Шиллер Роберт. Spiritus Animalis, или Как человеческая психология управляет экономикой и почему это важно для миров. Москва: Юнайтед Пресс, 2011. 273 с. С. 75.

32. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Пределы и риски цифровой трансформации. *Цифровая трансформация*. 2020. № 2(11). С. 51-57. URL: https://doi.org/10.38086/2522-9613-2020-2-51-57 (дата звернення: 31.07.2021).

33. Вощенко В.Ю. Трансгуманізм як філософія постлюдини: матеріали міжнародної науково-практичної конференції *Сучасні наукові дослідження та розробки: теоретична цінність та практичні результати*, м. Братислава, 16-18 берез. 2016 р. Київ: ТОВ "НВП "Інтерсервіс", 2016. 208 с.

34. Казначеев В.П., Акулов А.И., Кисельников А.А. и др. Выживание населения России. Проблемы "Сфинкса XXI века". Новосибирск: Изд-во Новосиб. ун-та, 2003. С. 40-48.

35. Лем С. Системы оружия двадцать первого века. Библиотека XXI века. Москва: АСТ, 2003. 602 с.

36. Маклюэн Г.М. Понимание медиа: Внешние расширения человека ; пер. с англ. В. Николаева / закл. М. Вавилова. Москва-Жуковский: “Канон-пресс-Ц”, “Кучково поле”, 2003. 464 с.

37. Мартинюк Ю. Трансгуманізм і постгуманізм: етична проекція: збірник матеріалів Всеукраїнської науково-практичної конференції *Антропний принцип в контексті актуальних проблем філософії науки*, м. Львів, 15-16 груд. 2016 р. Львів, 2016. С. 155-161.

38. Радутний О.Е. Право та окремі аспекти світу атомів і бітів (робототехніка, штучний інтелект, цифрова людина: збирник наук. праць *Питання боротьби зі злочинністю* / ред. Б.М. Головкін та ін. Харків: Право, 2021. Вип. 41. 216 с. С. 13-29.

39. Радутний О.Е. Правові аспекти феномену цифрової людини в кібернетичному та іншому просторі: збірник тез наукових доповідей науково-практичного семінару *Забезпечення кібербезпеки: правові та технічні аспекти*, м. Харків, 8 лист. 2018 р. Харків: Нац. аерокосм. ун-т ім. М. Є. Жуковського “ХАІ”, 2018. 112 с. С. 57-63.

40. Радутний О.Е. Розвиток кримінально-правової доктрини у напрямку визнання штучного інтелекту та цифрової людини суб’єктом правовідносин та суб’єктом злочину: матер. міжнарод. наук.-практ. кругл. столу *Ефективність кримінального законодавства: доктринальні, законотворчі та правозастосовні проблеми її забезпечення*, м. Харків, 17 трав. 2019 р. / укладачі: Л.М. Демидова, К.А. Новікова, Н.В. Шульженко. Харків: Константа, 2019. 324 с. С. 202-213.

41. Радутний О.Е. Кваліфікуючі ознаки, пов’язані з досягненнями наукового прогресу (біоінженерія, штучний інтелект, неорганічна та змішана форма життя): матер. Всеукр. наук.-практ. конф. *Актуальні проблеми кримінального права, кримінології та кримінально-виконавчого права*, м. Дніпро, 25 трав. 2018 р. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 214 с. С. 41-43.

42. Радутний О.Е. Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект. *Інформація і право*. № 2(25)/2018. С. 158-171.

43. Радутний О.Е. Здогадки про сингулярність крізь оптику штучного інтелекту і цифрової людини: зб. тез доп. наук.-практ. конф., присвяч. пам’яті члена правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової, *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*, м. Харків, 16 квіт. 2021 р. – (МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України). Харків: ХНУВС, 2021. 464 с. С. 449-451.

44. Радутний О.Е. Мораль і право для штучного інтелекту та цифрової людини: закони робототехніки та “проблема вагонетки”. *Інформація і право*. № 3(30)/2019. С. 78-96.

45. Райхерт К. Кіборг як кіборгізована людина: філософський розумовий експеримент. *Схід. Філософські науки*. 2017. № 4 (150). С. 98-104.

46. Райхерт К.В. Перемещение человеческого мозга (сознания, личности) в кибернетический организм как психическая травма (в кинофильмах Vindicator, RoboCop, 8 Man, Ghost in the Shell). *Актуальні проблеми філософії та соціології.* Одеса, 2017. Вип. 17. С. 86-89.

47. Хартія основних прав Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text (дата звернення: 31.07.2021).

48. Чурсин Н.Н. Понятие тезауруса в информационной картине мира: монография. Луганск: Изд-во “Ноулидж”. 2010. 305 с. С. 290.

49. Шваб Клаус. Четвертая промышленная революция ; пер. с англ. *The Fourth Industrial Revolution by Klaus Schwab*. Изд-во Форс: 2019. 208 с.

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

УДК 316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук.*
ORCID: https://orcid.org/0000-0002-3941-1013.

МОДАЛЬНІСТЬ ПРАВОВОЇ ВИЗНАЧЕНОСТІ У СФЕРІ ЗАХИСТУ ТА БЕЗПЕКИ ПРИВАТНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. *З урахуванням результатів раніше проведених досліджень, розглянуто понятійні, термінологічні і семантичні питання приватності, захисту та безпеки персональних даних щодо визначення, тлумачення та кореляції ключових понять у зв'язку з забезпеченням прав людини на особисте життя та життєдіяльність у інформаційній сфері. Подано пропозиції з вдосконалення систематизації законодавства сфери персональних даних в Україні.*

Ключові слова: *приватність, інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних.*

Summary. *Taking into account the results of previous research, the conceptual, terminological, and semantic issues of privacy, protection and security of personal data are considered with regard to human rights to privacy and life activities in the information sphere. Proposals are given to improve the systematization of legislation on personal data in Ukraine.*

Keywords: *privacy, information privacy, privacy in communications, protection and security of privacy of personal data.*

Аннотация. *С учетом результатов прежде проведенных исследований, рассмотрены понятийные, терминологические и семантические вопросы приватности, защиты и безопасности персональных данных в контексте определения, толкования и корреляции ключевих понятий в связи с обеспечением прав человека на личную жизнь и жизнедеятельность в информационной сфере. Представлены предложения по совершенствованию систематизации законодательства сферы персональных данных в Украине.*

Ключевые слова: *приватность, информационная приватность, приватность в комуникациях, конфиденциальность приватности, защита и безопасность приватности персональных данных.*

Постановка проблеми. У 2016 році Європейський Парламент і Рада затвердили Пакет захисту персональних даних (англ. – GDPR) [1], який передбачає нові Правила та порядок захисту персональних даних для країн європейського континенту (набули чинності 25.05.18 р.). Головним документом є Регламент (ЄС) 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних…" (далі – Регламент GDPR) [2, с. 2-103]. Важливою новацією у Регламенті GDPR є те, що вперше у міжнародному документі щодо захисту персональних даних у п. 1 Преамбули офіційно констатовано: *"**Захист фізичних осіб у зв'язку з обробкою персональних даних є основоположним правом**"* (курсив – *Авт.*).

Застосування слова ***"основоположні"*** до слова ***"право"*** знаменно тим, що вказує на придання пріоритетності вихідним принципам, приписам та нормам у зв'язку з обробкою персональних даних людини, яка має здійснюватися на підставі законності та справедливості. "Справедливість" (з грец. означало лише "звичай", "уклад життя" [3]), завжди була та є важливою категорією соціально-філософської думки, моральної та правової свідомості, наявність якої передбачає встановлення та виконання у соціумі вимог, зокрема щодо рівних прав та обов'язків, а також юридичної відповідальності та захисту від правопорушень. При цьому, як пам'ятаємо, у Конвенції Ради Європи "Про захист прав людини і основоположних свобод" від 1950 р. мова йде про "основоположні свободи", а стаття 8 сформульована як "Право на повагу до приватного …життя" [4]. Зараз, згідно

рішення інституцій Європейського Союзу, права людини саме у зв'язку з захистом персональних даних віднесено до "основоположних прав". Це може бути свідченням того, що права людини у зазначеної сфері удосконалюються, розвиваються та посилюються.

Також, можна виходити з того, що права людини у сфері персональних даних, як царина морально-етичних поглядів та загальних принципів щодо "справедливості", стають однією з пріоритетних сфер правової думки, яка потребує нових юридичних конструкцій щодо удосконалення правової (юридичної) визначеності та відповідних нормативних змін, зокрема у зв'язку з розвитком новітніх технологій та цифрової трансформації.

Результати аналізу наукових публікацій. Як вважаємо, на увагу заслуговують результати робіт таких вчених, як: Пилипчук В.Г., Баранов О.А., Богуцький П.П, Брайчевський С.М., Дзьобань О.П., Корж І.Ф., Леонов Б.Д., Радутний О.Е., Серьогін В.О.

Поряд з пошуками перспектив розвитку інформаційно-комунікаційної сфери, продовжує існувати неоднозначність у термінологічному визначенні та тлумаченні різних понять та термінів, що складають основу такої, зокрема, домінантної категорії в сфері прав людини як "приватність". Вона, як "стрижень" у багатогранних процесах захисту та безпеки персональних даних, потребує не лише чіткого уявлення, але й оцінки суттєвих ознак, предметного змісту, кореляції (взаємозв'язку) та юридичного визначення таких супутніх їй словосполучень, як: інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних.

Метою статті є узагальнення семантично-понятійного тлумачення та кореляції основних понять у сфері захисту та безпеки приватності персональних даних, а також надання пропозицій вдосконалення систематизації законодавства в Україні.

Виклад основного матеріалу.

Приватність. Поняття "приватність" (англ. – *privacy)* у англомовних країнах розглядається як можливості та право людини *"на самоту", "бути залишеною у спокої", "бути наданою самої собі".* За узагальненням – *"кожна людина має право на свій "куточок" у просторі, захищений від довільних зазіхань із боку інших"* [5]. Вищевказані словосполучення можливо й прийнятні для прецедентного загального права (*common law*) разом з статутним правом, як у США та Британії [6], але не дуже сприймаються стосовно розуміння відмінностей у ознаках різних за змістом понять, як прийнято в континентальній правовій системі, що може позначатися на суб'єктивному трактуванні предмета захисту приватності. Важливість означеного полягає у тому, що коли предмет (об'єкт, явище тощо) визначається, він повинен мати *"чіткість, зрозумілість та однозначність"* змісту сенсу ознак, для встановлення його ідентичності (тотожності). В Україні про це йдеться у Рішеннях Конституційного Суду України, див. [7; 8].

Сьогодні, в аспекті уявлень про "приватність", недоторканність приватного життя, згадується у ст. 3, 12 Загальної декларації прав людини 1948 р., ст. 5, 8 Європейської Конвенції з прав людини та основоположних свобод 1950 р., ст. 6-8, 11 Хартії основних прав Європейського Союзу 2000 р., рішеннях Європейського Суду з прав людини, що уточнюють сенс окремих формулювань та продовжують прецедентну практику. Загалом, документи ЄС не мають юридичного визначення поняття "приватність", а у Регламенті GDPR "приватність" лише згадано у п. 4- 6, 19, 45 Преамбули. В Україні – це слово наведене у ст. 41 Конституції щодо майнових відносин, але у законодавстві визначення не має.

У загально-соціальному контексті поняття "приватність" може розумітися як право людини жити своїм життям при мінімальному сторонньому втручанні та як захищеність від втручання в її особисте життя та стосунки безпосередньо фізичним шляхом або через публікацію інформації про неї. Це надає можливість інтерпретації поняття "приватність" в термінах захисту персональних даних.

Якщо виходити з сенсу такого словосполучення як “особиста таємниця людини”, з юридичної точки зору можна запропонувати більш-менш точний зміст дефініції поняття “приватність” а саме: *приватність – це право людини на таємницю особистого життя та її захист від сторонніх на неї зазіхань*.

За предметно-складовими частинами “приватність” поділяють на такі види: інформаційна приватність (щодо збирання, використання, зберігання, поширення персональних даних та у зв’язку з їх обробкою, зокрема таких, як банківська, податкова, медична, маркетингова та ін. будь-яка інформація про людину), приватність у комунікаціях (недоторканність телефонних переговорів, електронної пошти та інших засобів зв’язку), фізична приватність (захист людського тіла від стороннього втручання, несанкціонованих медичних випробувань і використання внутрішніх органів) та територіальна приватність (обмеження на вторгнення в житло, робоче місце, громадські місця). Саме вони є визначальними складовими загального стану та рівня безпеки приватності в сфері захисту персональних даних людини в державі.

Інформаційна приватність. Поняття “інформаційна приватність” визначається можливостями людини щодо нерозголошення її особистого життя у інформаційній сфері, що передбачає нормативне забезпечення захисту людини щодо нецільового та несанкціонованого опрацювання відомостей (або обробки персональних даних) про неї. Під цим розуміється встановлення правил збирання, зберігання, використання та поширення відомостей про особисте життя людини, які відповідно до принципів обробки персональних даних, визначених Регламентом GDPR, передбачають такі основоположні права на інформаційну приватність [9]:

право на самітність, тобто право людини на захист від втручання в її особисте життя і родинні стосунки через поширення (публікацію) інформації (персональних даних);

право доступу, на припинення обробки, виправлення та видалення персональних даних (“право бути забутим”);

право на заперечення обробки та автоматизоване індивідуальне прийняття рішень;

право контролювати інформацію про себе, тобто знати, ким, коли, яким чином і в яких межах інформація про неї може бути або буде використовуватися іншими особами.

Застосування поняття “приватність” в термінах права контролю людини щодо використання інформації про себе вважається однією з основних тенденцій за кордоном в політичних і юридичних дискусіях про захист приватності персональних даних [10].

Зазначені вище правові позиції-приписи є визначальними у висновку того, що в юридичній галузі людина може мати особливе та специфічне для інформаційної сфери право – “право приватної власності на відомості про себе”, які у електронно-інформаційному середовищі вже мають так звану фактуру, що визначається словосполученням “персональні дані”. Про наявність матеріальної специфічності в інформаційній сфері детально йдеться, зокрема у [11], де інформація (персональні дані) розглядаються як фіктивно-юридичний об’єкт майнового права, що повністю узгоджується з юридично прийнятою у світі “фікцією власності” в сфері інтелектуальної власності; у зазначеній сфері, говорячи по сутності, немає власності, є лише право використання та ін.

До вищевказаного вважаємо важливим звернути увагу на наступне. Ще у 1689 році видатний англійський філософ, правознавець Джон Локк, якій заклав у державне управління ідеї про поділ державної влади та громадянське суспільство, в роботі “Два трактати про правління” писав, що *“держава повинна функціонувати для досягнення тієї єдиної мети, заради якої вона споконвічно й була створена, а саме для захисту життя, свободи та власності”*. При цьому, він висловив дуже важливу концептуальну думку: *“Кожна людина має деяку особливу власність, що полягає в її власній особистості, на*

яку ніхто, крім неї самої, не має ніяких прав" [12]. Іншими словами, як стверджували у своїх роботах С. Олсаретті "Свобода, вознаграждение и рынок"(2004) [13] та М. Доньева-Коєна "Опасные мысли: произведения о законе, себе и морали" (2002) [14], Д. Локк виходив з того, що *"кожна людина має право власності на свою особистість"*.

У соціальному плані інформаційну приватність можна поділити на приватність у побуті та приватність у публічності, яка пов'язана із сферою засобів масової інформації, а також з відповідною діяльністю з боку держави. Але, якщо остання має значну скритність, то першість головного порушника приватності належить саме масмедіа.

Звичайно, у будь-якій державі (навіть у автократичній чи тоталітарній) державна безпека корелюється тією або іншою мірою з загальною безпекою людей, що може визначатися владою потребами суспільства взагалі. Одночасно, у правовій державі будь-яка особа не може мати абсолютного імунітету на недоторканність приватності. У такій державі приватність має поступатися місцем публічності щодо інформації про осіб, які представляють усе (або частково) суспільство формально і неформально – керівники політичних сил та органів державної влади тощо, які здійснюють вплив на формування влади та стан справ у державі, регіонах тощо, або мають можливість визначати осіб, які в силу тих чи інших соціальних обставин або ж суб'єктивних уявлень становлять загрозу національній безпеці. Проте, тут існує межа – приватні відомості публічних осіб повинні мати захист, який надає їм можливість забезпечити особисту безпеку та членів її родини [15, 16], але лише за законом.

У той же час можна виходити з того, що якщо будь-хто добровільно виявився в сфері суспільної уваги та надав про себе відомості, то він повинен прийняти факт обмеженням своїх прав на приватність.

З юридичної точки зору можна запропонувати такий зміст дефініції, а саме: *інформаційна приватність – це право людини на недоторканність та захист відомостей (даних), які стосуються або пов'язані з особистим її життям.*

Приватність у комунікаціях. Комунікації – це засоби та шляхи забезпечення інформаційної діяльності щодо взаємодії (повідомлень, спілкування) відповідних суб'єктів, які є носіями певних правомочностей та правозобов'язань.

Приватність у комунікаціях, як процес передавання (поширення) та обміну інформації, – це стан та рівень диспозитивності законодавства щодо інформаційної приватності та умов нерозголошення відомостей про людину, які здійснюються нормативно-правовими засобами захисту її персональних даних, завдяки чому забезпечується інформаційна безпека людини, суспільства та держави.

Умови запобігання порушень приватності у комунікаціях мають передбачати, насамперед, наявність правових можливостей реальної інформаційної захищеності та безпеки людини. Приватність визначає загально-соціальну потребу у порядної діяльності в інформаційному середовищі, оскільки відображає індивідуалізацію людини, утворює підставу її унікальної суб'єктності і саме у такій якості здійснює трансформацію усіх приватно-правових характеристик статусу людини у публічні інформаційно-правові відносини. В інформаційно-правовому статусі людини приватність є внутрішньою його характеристикою, яка розкриває сутність права людини на інформаційну безпеку [15].

Приватність у комунікаціях і приватність персональних даних тісним чином пов'язані з Інтернетом. Інтернет-приватність розглядається, як джерело персональної інформації не призначеної до поширення. До цього може бути застосовано словосполучення "приватність у електронних комунікаціях" (тобто, приватність у електронно-інформаційному середовищі). Ця приватність безпосередньо пов'язана з поняттям "дані", як формалізованими знаково-кодовими комбінаціями для їх автоматичної обробки, до яких "інформація" прикріплена,

пристосована, або цифровими даними – закодованими електричними сигналами та електронними структурами, які при декодуванні надають інформацію.

У електронно-інформаційному середовищі приватність також може визначатися як "інформаційна приватність" – це все, що пов'язане з будь-якими засобами комунікацій та техніко-технологічними діями, які стосуються, зокрема, таємниці телефонних розмов, поштових, електронних повідомлень, сайтів, інстаграм, блогів, постів та багато ін.

Сьогодні в Європі, поряд з Регламентом GDPR, діє Директива 2002/58/ЄС "Про обробку персональних даних та захист таємниці ("приватності") в секторі електронних комунікацій" від 12 липня 2002 року [17]. Вона передбачає можливість держав-членів ЄС здійснювати перехоплення інформації, переданої за допомогою електронного зв'язку, або ухвалювати інші необхідні заходи для кожної із цих цілей, відповідно до Конвенції РЄ про захист прав людини і основоположних свобод, і роз'ясненнями, що визначаються в постановах Європейського суду з прав людини. Такі заходи повинні бути строго пропорційними до визначеної мети та необхідними в межах демократичного суспільства, а також бути адекватними у заходах безпеки згідно загальних приписів зазначеної Конвенції.

Стосовно Регламенту GDPR, то він не застосовується до обробки персональних даних по відношенню до питань національної безпеки, які підпадають під дію Розділу V Договору про Європейський Союз, і діяльності правоохоронних органів (для цілей попередження, розслідування), а також до обробки персональних даних державами-членами ЄС по відношенню до загальної зовнішньої політики і політики безпеки ЄС. Персональні дані, які обробляються державними органами в цілях запобігання, розслідування, виявлення або судового переслідування злочинів або виконання покарань, зокрема по запобіганню загрозам суспільній безпеці і вільного переміщення таких даних, регулюються Директивою (ЄС) 2016/680, див. [2, с. 104-156].

В США існують два рівня правової регламентації будь-яких значимих відносин: на рівні федерації й на рівні штатів, чиї повноваження в області законотворчості по Конституції США дуже широкі. Законодавство штатів США автономне у своїй правовій творчості [18]. Щодо сфери приватності чинними для федеральних органів є закони: *Privacy Act of 1974, 5 U.S.C. § 552a* ("Закон про приватність") та *The Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2510* ("Закон про приватність електронних комунікацій") [19]. При цьому, недоторканність приватного життя забезпечується також галузевим законодавством [20].

В державі одночасно існують дві моделі щодо сфери приватності. Перша передбачає необхідність забезпечення захисту шляхом використання різних форм саморегулювання, при якій провайдер може переглядати особисте електронне листування, зокрема, у випадку підозри про наявність збитку або з добровільної згоди відповідної людини. Інша – обмеження прав на приватність шляхом розширення повноважень поліції й спецслужб з прослуховування персональних розмов. Ця модель має дві складові. Перша передбачає – усі цифрові засоби, телефонні, стільникові і супутникові системи, а також комунікаційні технології, які удосконалюються, у тому числі Інтернет, повинні мати можливості контролю ззовні. Друга – спрямована на обмеження поширення криптографічних програм, які дозволяють громадянам самостійно шифрувати свої повідомлення.

Про "право бути наданим самому собі", зокрема й у контексті комунікацій, в США вперше заговорили в 1890 році, коли американський юрист Луїс Брэндейс і журналіст Сэмюэль Уоррен опублікували в журналі "Harvard Law Review" статтю "The Right to Privacy" (буквально – "право на приватність") [21]. Вони стверджували, що право на особисте життя не можна ставити в залежність від способу, яким здійснюється одержання інформації. Ця ідея була прийнята американською юстицією лише у 1934 р. (Л. Брэндейс

був тоді вже членом Верховного Суду), коли Конгрес США проголосував за Федеральний закон, який визнав за громадянами право на таємницю у комунікаціях у повному обсязі[1]. Поштовхом цьому слугував розвиток технічних та соціальних умов індустріалізації й, що важливо для розуміння процесів щодо нашого часу стосовно інформатизації, на тій же підставі, на якій вона зараз актуалізується: вторгнення вже новітніх технологій (раніше це стосувалося комерції з комплектування картотек щодо збирання та продажу адрес та ПІБ, відомостей з медичних книжок, переписки з поштових карток, розмов по телефону та ін.) в особисте життя й несанкціонований та комерційний продаж інформації про людину.

Комерціалізація інформації про людину отримала початок у США у 1886 році, коли шовкоторговець Л'юіс Тепен із Нью-Йорка створив агентство збору та аналізу інформації про кредитоспроможність підприємців, які зверталися до нього за позикою. Накопичивши декількох томів кредитних звітів, він став продавати інформацію. Клієнти платили від 100 до 200 дол. у рік [22].

За деякими результатами досліджень цього "феномена", світовий ринок персональних даних на початку 2000 рр. досягав більш як $3 млрд.: відомості про людину, її матеріальний стан, особисте життя "відбираються" з різноманітних баз даних та реалізуються завдяки Інтернет. У ті часи коштувала така БД від $10 (дрібний продаж) – до $1500 (продаж через Інтернет). Інформація мобільного зв'язку також потрапляла та потрапляє на чорний ринок (номер коштує $50, прослуховування – $150 за рік.) [23].

Вся ця, звичайно, несанкціонована діяльність значно поширилась у всьому світі та здійснюється не лише завдяки активності окремих фігурантів, а й комерційних структур, зокрема, за допомогою програм типу "cookies", збирання анкет для маркетингу, електронних та IP-адрес, примусу надавати ПІБ, особисті телефонні номери (існує можливість крадіжки коштів завдяки е-банкінгу), надавати про себе всю інформацію для отримання входу на сайт, анонімним пропозиціям з матеріальними обіцянками та багато ін. Ті, хто займається маркетингом постійно вишукують нові шляхи для збору різноманітних відомостей про потенційних покупців та своїх конкурентів: їх інтереси, характер діяльності, погляди, оточення, стосунки та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що з допомогою засобів електронно-інформаційного середовища набагато легше збирати величезні обсяги різної інформації (ніж займатися звичайним промисловим шпигунством), а аналіз і взаємне ув'язування відомостей ("профілювання") забезпечує істотні прибутки в бізнесі [24]. При цьому активно працюють колекторські агентства, яким відомості про клієнтів несанкціоноване та масово передають (або отримують) не тільки банки, а й будь-які зацікавлені особи.

Таким чином, хоча інформація про людину (у електронних комунікаціях – персональні дані) й є предметом ототожнення та права конкретної людини на саму себе, а в реальних умовах життєдіяльності давно є товаром, який має грошово-мінову вартість та використовується з метою задоволення матеріального або ін. інтересу, вона (інформація) не розглядається як об'єкт власності відповідної людини.

Підсумовуючи, у будь-якому разі людина має розраховувати на приватність у комунікаціях та на реальні умови захисту та безпеки відомостей про її особисте життя.

---

[1] На сьогодні право на недоторканність приватного життя розглядається як одне з конституційних прав особи, хоча воно спеціально й не згадується в американській Конституції. На підставі цієї аргументації Верховний суд США у 1985 р. визнав його існування в обмеженому обсязі. На думку прибічників прайвесі, це право логічно випливає зі змісту 1-ої, 3-ої, 4-ої та 5-ої поправок до Конституції США, якщо тлумачити їх системно [20]. У загальному плані, в США немає єдності щодо тлумачення правової природи "права на приватність".

З юридичної точки зору можна запропонувати такий зміст дефініції, а саме: *приватність у комунікаціях – це право людини на таємницю особистого життя та захист недоторканності від сторонніх на неї зазіхань у сфері інформаційної взаємодії, незалежно від засобів якими здійснюється одержання відомостей (даних) про людину*.

Конфіденційність приватності. У загальному розумінні, конфіденційність (*confidentia* – від лат. "довіра", "прихованість", "секрет" або "таємниця") передбачає наявність властивості об'єкта (предмета) на обмежений доступ, зокрема інформації, що обумовлює умови правоспроможності фізичних або юридичних осіб у ознайомленні та можливостями використання.

Конфіденційність інформації стосується усіх відомостей з обмеженим доступом, які є складовою відповідного виду таємниці: особиста (приватна), професійна, комерційна.

Чіткої класифікації видів конфіденційної інформації немає. Налічується більше 30 її різновидності, одну з яких засновано на суб'єктності права власності на інформацію.

У сфері приватності "конфіденційність" – це форма захисту відомостей про особисте життя людини, тобто захисту та безпеки приватності персональних даних.

Поняття "конфіденційність" згадується у Регламенті GDPR у пп. 39, 49, 75, 83, 85, 163 Преамбули та у ст. 14, 28, 32, 38, 54, 76 Регламенту, але юридичного його визначення та суттєвих ознак не наведене.

В Україні, згідно ст. 21 Закону України "Про інформацію", "конфіденційна інформація" віднесена до інформації з обмеженим доступом (одночасно з "таємною" та "службовою"). У Законі зазначено – "*конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень*".

Згідно ст. 7 Закону України "Про доступ до публічної інформації", також маємо визначення: "*конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов*".

Незважаючи на деяку відмінність у визначеннях, загальним їх недоліком є те, що вони не надають ознак сутності самого предмета поняття "конфіденційність", тобто не зрозуміло про що йде мова (крім діяльності з нею), та сприяють різним особисто-суб'єктивним уявленням. Це відноситься до всього законодавства, див. [25, с. 38-40].

Іншою інформацією з обмеженим доступом, яка може бути пов'язана з конфіденційністю, є "службова інформація". Її визначення у законодавстві немаємо. Ст. 9 Закону України "Про доступ до публічної інформації" обмежується посиланням на переліки відомостей, що становлять службову інформацію, які складаються органами державної влади, органами місцевого самоврядування, ін. суб'єктами владних повноважень[2].

Хоча "службова інформація" за Законом України "Про інформацію" є окремою категорією обмеженого доступу, вона, як і "конфіденційна інформація", не має чітких предметно-суттєвих ознак, за якими може визначатися. Й це, до прикладу, при тому, що персональні дані людини можуть становити службову таємницю для судді, якій є державною посадовою особою, і професійну таємницю для працівника кадрової служби комерційної фірми.

Вважаємо, якщо службова інформація стосується сфери приватності та у зв'язку з потребою захисту відомостей про особисте життя людини, вона може визначатися як

[2] *Прим.* До прикладу, стосується відомостей щодо спеціального режиму збирання, зберігання, обробки, поширення та їх використання згідно Переліку відомостей, що становлять службову інформацію в системі Міністерства внутрішніх справ: наказ МВС України від 27.05.16 р. № 432.

“конфіденційна”. Однак навряд це реально практикується та приймається до уваги в умовах відсутності на сьогоднішній день чіткого, безперечного правового поділу між різними видами таємниць. Проте головне у іншому – законодавство України має значну кількість актів, які надають лише переліки інформації про особу з посиланням на її “конфіденційність”, у відсутності предметно-суттєвих ознак, за якими її можна визначати.

У той же час існує Державний стандарт України “Технічний захист інформації. Терміни та визначення” (ДСТУ 3396.2-97) [26], якій віднесено до угруповання 01.040.35 “Інформаційні технології” згідно п. 42. Переліку державних стандартів України. Він юридично та предметно визначає поняття “конфіденційність”, надає суттєві її ознаки крізь тріаду повноважень права власності: користування, володіння та розпорядження. Але практично цей чинний стандарт не згадують та не застосовують. Хоча добре відомо, що лише інститут права власності, як жоден інший є найбільш потужним з юридичних засобів забезпечення прав людини, у стані вирішувати проблеми в сфері приватності та захисту персональних даних на якісному рівні. Тим більше, з одного боку, придання у ЄС вихідним принципам щодо обробки персональних даних людини категорії “основоположне право”, а з іншого, наявність проблем цифрової трансформації, можуть визначати потребу у нових, нетрадиційних поглядах на упорядкування та регулювання суспільних відносин.

Виходячи з юридичних поглядів та загальноприйнятих підходів по відношенню до трактування поняття “конфіденційність”, можна запропонувати такий зміст дефініції, а саме: *конфіденційність приватності у інформаційній сфері – це форма захисту відомостей (даних) про особисте життя людини, яка визначається домовленістю та зобов’язанням будь-яких суб’єктів не розголошувати їх третій стороні*.

Захист приватності персональних даних. У загальному розумінні поняття “персональні дані” охоплює об’єктивні та суб’єктивні відомості про особисте, сімейне чи публічне життя фізичної особи, що виражені у формі літер, чисел, графіки, фото, звуку чи відео символів, якщо вони дозволяють ідентифікувати таку особу. Для визнання відомостей персональними даними обов’язковою є наявність зв’язку між такими відомостями та конкретною особою.

Початок досліджень у вирішенні проблеми створення в Україні системи захисту персональних даних було покладено у 1995 р. у Національному агентстві з питань інформатизації при Президенті України. На той час, у більшості європейських країн вже було запроваджені відповідні закони, а ще у 1981 році вступила в дію перша угода світового рівня – Конвенції Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних”. В Україні питання прийняття закону для регулювання відносин у сфері захисту персональних даних дискутувалось впродовж 15 років, див. у [27].

Потрібен час, щоб прийти до думки про те, що поняття “захист персональні дані” – це не просто “захист даних або відомостей” про людину, яке визначає лише “форму-оболонку” цільової спрямованості їх внутрішнього змісту, завдяки прийнятій умовності розуміння букв, знаків, інших символів, сигналів тощо для відображення значеннєвого наповнення. У “формі” міститься основа реального змісту їх “сенсу”, а саме – бажання людини жити своїм життям при мінімальному сторонньому втручанні та у захисті особистого життя у відносинах з іншими людьми та державою, що й визначає соціально-правову потребу у практичному вирішенні проблем “приватності” та створення умов реального захисту прав людини.

Забезпечення приватності у сфері персональних даних є вкрай складною проблемою у зв’язку з тим, що вона стосується багатогранних та багатоаспектних питань життя та життєдіяльності людини, які слабко піддаються регламентації, та,

одночасно, необхідності створення збалансованості забезпечення прав людини та інтересів безпеки держави. Це вимагає однозначного трактування понять та їх юридичного визначення у чітких термінах, інше – неприпустимо для нормативного акта.

Виходячи з приписів багатьох міжнародно-правових актів, головний сенс яких полягає у тому, що *право на життя, свободу і власність є найважливішими природними правами людини*, а також – Конституції України – *людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю,* ще у 1998 році, у першій моделі законопроекту про захист персональних даних, було запропоновано запровадити у сферу захисту персональних даних України спеціальний інститут права власності людини на свої персональні дані [28][3]. Головна ідея виходила з того, що численність різноманітних актів щодо сфери персональних даних, нерідка невизначеність і важкість у сприйнятті норм та нормативна складність взагалі, будь-які адміністративні і організаційні заходи[4], обмеження, умовності та багато ін. не дуже надають захист людині так, як це може єдино потужний інститут власності.

Надалі дослідження з питань сфери персональних даних були продовжені, а їх результати представлено в ряді наукових праць в контексті стану, тенденцій і подальших перспектив у захисті та безпеці персональних даних [1; 7; 25; 27], зокрема в умовах цифрової трансформації та пов'язаних з нею проблем правового регулювання нових суспільних відносин у цій сфері, а також досліджено новий погляд на власність людини в сфері персональних даних у контексті словосполучення *"право приватної власності людини на свої персональні дані"* [29].

До вказаного можна додати, що за неофіційним повідомленням, питання власності на персональні дані було предметом розгляду інституцій ЄС, але єдності щодо правової природи "власності на персональні дані" так і не отримало.

Сьогодні чи навряд хто не згодний з тим, що світ рухається шляхом активного, малопередбачуваного розвитку процесів в електронно-інформаційному середовищі. Уже предметно обговорюється питання щодо "*цифрової людини, яка має бути визнана спеціальним суб'єктом правовідносин, спеціальною правовою персоною*" [30], штучним інтелектом, який вже почав здобувати здатність, що вважалася винятково людською прерогативою, – здатністю до навчання [31], у тому числі й у правотворчої діяльності [32]. Видання MIT Technology Review повідомляло [33] про успіхи по створенню штучного інтелекту для проектування інших систем штучного інтелекту, тобто про факти його самовдосконалення, у Массачусетському технологічному інституті, Каліфорнійському університеті в Берклі та у компанії Google.

У квітні 2021 р. Єврокомісія представила проект рекомендацій з регулювання штучного інтелекту [34], а у червні 2021 р. на саміті США-ЄС ухвалене рішення про

[3] Проект закону був внесений у 2003 р. народними депутатами України Родіоновим М., Ніколаєнко С., Юхновським І., Толочко П., Ситником К., прийнятий 13.03.2006 р. у 2-му читанні в цілому як Закон, але далі був скасований. На підставі проекту, у червні 2010 р., Верховна Рада України ухвалила інший проект закону України "Про захист персональних даних". У Законі було визначено – суб'єкт персональних даних має *особисті немайнові права* (тобто, не має економічного змісту) на персональні дані. Поняття "особисті немайнові права" було залучено з Цивільного кодексу України і застосовується лише у нашій державі. У міжнародному праві, праві ЄС, а також у законодавствах інших країн його не існує.

[4] Європейські правові стандарти визначають обов'язковість у виконанні приписів законодавства ЄС щодо створення незалежного, контролюючого органу з захисту персональних даних. На жаль, в Україні не створено відповідної та ефективної системи організації захисту прав людини у вказаній сфері (це сталося після внесення змін до законодавства у 2011 – 2013 рр.). Функції контролю стану справ було покладено на Уповноваженого Верховної Ради України з прав людини, що не відповідає нормам Конституції України.

розробку загальних підходів у використанні штучного інтелекту, керуванню даними та політиці щодо технологічних платформ [35]. За думками експертів – етичні проблеми штучного інтелекту в найближчі роки будуть ставати серйознішими й складнішими. Одна з них стосується приватності при застосуванні технологій штучного інтелекту [36].

Алгоритми штучного інтелекту, в основі яких лежать нейромережі зі зворотним зв'язком, вже здатні збирати багато персональних даних завдяки технологій "Хмарних обчислень" та "Великих Даних". Вони стали створювати умови фундаменту загальної конвергентно-аналітичної інтеграції в інформаційній сфері, завдяки можливостей швидко, більш предметно і повніше проводити автоматизований збір, фільтрацію, сортування, структуризацію і аналіз величезних обсягів даних та отримувати надсумарно-якісний ефект [37]. Терміном "Великі Дані" (*Big Data*) прийнято описувати обробку великих масивів різноманітної інформації з складною, неоднорідною або невизначеною структурою, що спрямована на параметри, які скорочено позначають як "3V"(по перших буквах англ. слів): *volume* – "обсяг", *velocity* – "швидкість" і *variety* – "різноманіття" [38]. Збираючи дедалі більше відомостей про конкретну людину, володілець алгоритму штучного інтелекту – державна або правоохоронна структура, компанія або будь-яка окрема особа, може одержати інформацію про різноманітні аспекти приватності людини, зокрема до прикладу щодо виборчих компаній, – які заходи буде відвідувати й коли, що прагне почути, за кого схильна (або ні) голосувати й багато ін. При цьому, будь-які відомості про приватність можуть дозволити не лише маніпулювати людиною, а й використовувати її у групових, корпоративних тощо інтересах.

Людство вже не повернеться назад і не відмовиться від технологій штучного інтелекту. Це отримало, навіть, назву – "технологічна сингулярність", зі смутною перспективою для людини, на що вказував, зокрема, М. Хайдеггер [39]. Про поглиблення проблем у співіснуванні людини й техніки ще у часи індустріалізації говорив, у своєму стилі, навіть В. Маяковський – *Насувається навала техніки. І якщо на неї не надягти естетичний намордник, вона всіх покусає* [28, с. 55]. Висновок з вказаного може полягати у тому, що сучасній світ стоїть на грані грандіозних змін. Головна причина – бурхливе вдосконалення й розвиток техніки та технологій приводить до того, що вони стають усе більш витонченими та розумними, а техніко-технологічний прогрес у майбутньому буде тільки більше, ширше й активніше використовуватися в самих різних сферах життєдіяльності.

Як вважаємо, може й не дуже ефективний засіб вирішення зазначених проблем, але є потреба задати хоча б рамки етичного кодексу "поведінки" штучного інтелекту з умовами захисту та безпеки приватності персональних даних (не відомо, як буде "переробляти" вказане штучний інтелект). Взагалі ж відомо, що у GDPR, проекті ЄС про "e-Privacy Regulation" [40] та "NIS Directive" [41] проблема "штучний інтелект – захист та безпека персональних даних" не розглядається або поки не має чіткого предметного вирішення.

Сучасна юриспруденція продовжує дуже повільно сприймати потребу у змінах підходів та засобів в упорядкуванні відносин у інформаційній сфері. Як деякий підсумок – законодавство про приватність та захист персональних даних в жодній країні світу не отримало своєї зрілості, насамперед на понятійно-термінологічному рівні. Повної адекватності національних законодавств не досягнуто. Основною дилемою нормативно-правового упорядкування відносин у сфері персональних даних є суперечність між прагненням максимального їх використання у корпоративних, державних та ін. інтересах, й, одночасно, бажання та спроби кожної окремої людини захистити свої особисті права від несанкціонованих дій з її персональними даними.

Щодо визначення, з юридичної точки зору можна запропонувати такий зміст дефініції, а саме: з*ахист приватності персональних даних – це нормативно-правові та*

соціальні умови, процес та результат забезпечення інформаційної недоторканності особистого життя та життєдіяльності людини, яка ідентифікована або може бути ідентифікованою.

Безпека приватності персональних даних. Безпека приватності персональних даних є складовою частиною інформаційної безпеки людини, суспільства та держави, яка безпосередньо пов'язана з негативними інформаційно-психологічними впливами через, зокрема, несанкціонований виток персональних даних, інформаційне насильство, інформаційний тероризм, маніпуляції свідомістю громадян та багато ін., про що йдеться у [42]. Це дає підстави запровадження у науковий та юридичний обіг визначення поняття "безпека приватності персональних даних".

В законодавстві України немає словосполучення "безпека приватності персональних даних" (або "безпека персональних даних"). У Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 09.01.07 р. № 537-V [43] закріплено лише термін "інформаційна безпека". Згідно п. 13 Закону "інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації".

У вищезазначеному про "процес захищеності" прямо не ідеться.

Щодо розуміння сенсу слів (тобто, внутрішнього змісту предмета) "цілісність", "конфіденційність" та "доступність", то у законодавстві це залишається без предметно-ознакового визначення. Так, до прикладу, у досить компактній роботі [44], зазначається: *"До суттєвих ознак* (курсів – *Авт.*) поняття *інформаційної безпеки* відносять *конфіденційність* (стан інформації, при якому доступ до неї отримують тільки суб'єкти, які мають на це право), *цілісність* (запобігання несанкціонованій або незаконній модифікації інформації) та *доступність* (запобігання тимчасового або постійного приховування інформації від користувачів, які отримала право на доступ)".

Вважаємо, по-перше, мова у вищенаведеному йде не про "суттєві ознаки" (показники, за якими визначається предмет) інформаційної безпеки, а про "складові дій" (частини, які входять до єдиного утворення, цілого). По-друге, "конфіденційність" це не "стан інформації", а "форма її представлення", на певний час.

Враховуючи запроваджене у законодавство поняття "інформаційна безпека", можна запропонувати такий зміст дефініції: *безпека приватності персональних даних – це стан та процес забезпечення захищеності у недоторканності відомостей (даних) про особу від нецільового та несанкціонованого збирання, зберігання, використання та поширення у зв'язку з їх опрацюванням (обробкою)*.

Схематично, перелік та кореляція ключових понять у зв'язку з захистом та безпекою приватності персональних даних, див. на Рис.

Висновки.

Не претендуючи на семантично-понятійну завершеність та однозначність сприйняття, приведемо тлумачення поняття "приватність" та супутніх йому словосполучень.

1. ***Приватність*** (англ. – privacy), у англо-сакському розумінні, – це можливості та право "людини на самоту", "бути залишеною у спокої", "бути наданою самої собі". З юридичної точки зору, *приватність – право людини на таємницю особистого життя і захист від сторонніх на неї зазіхань*.

“Приватність”, як семантично-домінантне поняття, у інформаційній сфері пов’язано з такими основними словосполученнями-термінами: інформаційна приватність, приватність у комунікаціях, конфіденційність приватності, захист та безпека приватності персональних даних людини.

Інформаційна приватність передбачає наявність нормативно-правового захисту прав людини в інформаційній сфері, згідно її особистих уявлень, інтересів та намагань у житті. З юридичної точки зору, *інформаційна приватність – право людини на недоторканність та захист відомостей (даних), які стосуються або пов’язані з особистим її життям.* Інформаційна приватність безпосередньо пов’язана с такими поняттями, як: “приватність у комунікаціях”, зокрема з Інтернет-приватністю; в контексті забезпечення таємниці відомостей про особисте життя – з “конфіденційністю приватності”; в контексті запобігання несанкціонованим зазіханням на відомості про особисте життя – захистом та безпекою приватності персональних даних.

Рис.

Приватність у комунікаціях *– право людини на таємницю особистого життя та захист недоторканності від сторонніх на неї зазіхань у сфері інформаційної взаємодії, незалежно від засобів якими здійснюється одержання відомостей (даних) про людину.*

Конфіденційність приватності *– форма захисту відомостей (даних) про особисте життя людини, яка визначається домовленістю та зобов'язанням будь-яких суб'єктів не розголошувати їх третій стороні.*

Захист приватності персональних даних *– нормативно-правові та соціальні умови, процес та результат забезпечення інформаційної недоторканності особистого життя та життєдіяльності людини, яка ідентифікована або може бути ідентифікованою.*

Якщо розглядати захист приватності в контексті власності людини на свої персональні дані, то оцінка ознак предмета захисту може виходити з такої формули: *право приватної власності людини (фізичної особи) на персональні дані* – це сукупність приписів та норм, які регулюють право володіння, користування та розпорядження персональними даними людини про свою особу, за умов збалансованості та узгодженості цього права з правами інших громадян та потребами суспільства і держави у безпеці.

До зазначеного, *володіння персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення приватності персональних даних в незмінному вигляді; *користування персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення використання відомостей про себе на власний розсуд; *розпорядження персональними даними* – це наявність можливості людини та нормативно-правових умов забезпечення права на управління доступу до відомостей про себе, крім випадків визначених законом. Більш детально йдеться у [27, зокрема, с. 105-108].

Вважаємо важливим звернути увагу на наступне. У зв'язку з різноманітністю, різнобічністю життєдіяльності та потребами безпеки суспільства, "абсолютного" права приватної власності на самого себе в інформаційній сфері не існує. Проте це право стосується кожної людини в контексті історично визначених у суспільстві та пошуків напрямів подальшого удосконалення "принципів моралі, етики та правосвідомості", які спрямовуються природною потребою людини – визначати її тією, що для неї найкраще.

Безпека приватності персональних даних *– стан та процес забезпечення захищеності у недоторканності відомостей (даних) про особу від нецільового та несанкціонованого збирання, зберігання, використання та поширення у зв'язку з їх опрацюванням (обробкою).*

2. Визнання та обов'язковість у виконанні приписів європейських правових стандартів щодо основоположних прав захисту фізичних осіб у зв'язку з обробкою персональних даних, передбачає підвищення точності ключових юридичних дефініцій та однозначності у тлумаченні понять шляхом застосування семантичної оцінки ознак предмета захисту та безпеки приватності персональних даних. А це вимагає, зокрема, не лише внесення юридичних змін у зв'язку з появою нових міжнародно-правових документів, а, головне, концептуального оновлення відповідного законодавства.

3. Технологічно-цифрова та соціальна трансформації у суспільстві, перспективи поглиблення протистояння прав людини і прав "цифрової людини, як суб'єкта правовідносин", та спрямованість на збереження людини як виду, все більше потребують нової юридичної конструкції захисту приватності в контексті власності людини на свої персональні дані, тобто – надання людині специфічно-матеріального правового статусу "права власності на себе". Як вважаємо, ідейна підстава вищезазначеного узгоджується з поглядами англійського правознавця Д. Локка та тотожно-адекватна поглядам "батька приватності", члена Верховного Суду США Луїса Брэндейса, який ще на початку епохи індустріалізації відстоював право людини "бути наданою самій собі", хоча про "власність на приватність" у той час не могло бути й мови.

4. Зміни у соціальних процесах, зокрема завдяки застосуванню засобів електронно-інформаційного середовища, незворотне удосконалення та самовдосконалення штучного інтелекту (коли останній зможе приймати самостійні рішення, навіть на шкоду людині), захист прав людини в інформаційному середовищі в плані створення умов ефективного правового забезпечення захисту та безпеки приватності персональних даних, потребує більш значної, порівняно з сьогоденням, уваги органів державної влади не лише в правовому, але й адміністративно-організаційному та методологічному забезпеченні.

Вказане можна охарактеризувати тим, що у політичних, економічних, соціальних процесах життєдіяльності, нескінченності війн, революцій, переворотів, конфліктів, існує та завжди буде існувати (нерідко таємно, не усвідомлено) проблема пошуку людиною гарантій справедливих умов "особистої автономії". У державі воно може визначатися як "правовий суверенітет особистості", складовою якої є інформаційна приватність. Й важливим при цьому є те, що навряд чи технологічні досягнення та перспективи їх майбутнього зможуть ("забажають") надати гарантії справедливості людині, крім того, що може надати природне право власності людини на саму себе, яке є складовою дійсно правової держави.

5. В Україні законопроект про захист персональних даних розроблявся з 1997 року, мав 8 версій у 23 редакціях, та у декілька циклів неодноразово проходив узгодження з міністерствами, відомствами та експертним управлінням ВР України до 2010 року, у якому був прийнятий як закон.

З 2010 р. по наш час було прийнято не менше як 7 редакцій Закону України "Про захист персональних даних" [27, с. 74-85], які мали рамочно-базовий характер. На жаль, їх зміст, незважаючи на різні офіційні пояснення, мало що пояснював й не лише "пересічній людині" – як практично захистити свої права в умовах не повної визначеності понятійних, термінологічних та нормативних формулювань, що ускладнює розуміння та реальні можливості практичного захисту.

Сьогодні здійснюється робота з удосконалення законодавства України у плані запровадження приписів Регламенту (ЄС) 2016/679 (законопроект № 5628 від 07.06.21 р.). Преамбула проекту містить таке формулювання: *"Цей Закон визначає правові відносини, пов'язані із захистом і обробкою персональних даних, з метою забезпечення прав людини на захист персональних даних та повагу до особистого і сімейного життя"*.

Наше занепокоєння полягає в наступному.

По-перше. Як вважаємо, предметом законопроекту повинен бути не "захист даних", а ***захист основоположного права фізичних осіб*** *у зв'язку з обробкою персональних даних* (про що йдеться у п. 1 Преамбули Регламенту (ЄС) 2016/679), основу чого й складає головний принцип права – тобто, право на справедливість щодо сенсу та змісту того, що потребує захисту – тобто ***право на приватність*** *особистого і сімейного життя.*

По-друге. Також вважаємо, продовжує існувати недосконаліть термінологічного апарату. Законопроект має враховувати у повному обсязі викладене у ст. 4 Регламенту (ЄС) 2016/679 від 27.04.16 р., а також, можливо, напрацювання цієї статті.

По-третє. Деякі положення законопроекту не відповідають ***принципу правової визначеності***, який потребує *"чіткості, зрозумілості й однозначності правових норм, зокрема, їх передбачуваності (прогнозованості) та стабільності"* (абз. 6 п. 2.1 Рішення Великої палати Конституційного Суду України від 20.12.2017 р. № 2-р/2017) [7]. *"Юридична визначеність – це передовсім недвозначність"* (п. 10 Рішення Великої палати Конституційного Суду України від 14.07.2021 р. № 1-р/2021) [8]. Не врахування вказаного може ускладнювати подальше правозастосування.

По-четверте. У принципі, законопроект передбачає оцінювання *"контролюючим органом"* стану дотримання прав людини та основоположних свобод під час встановлення відповідності рівня захисту персональних даних. Проте, згідно європейських правових стандартів, відповідного *"контролюючого органу"* в Україні немає, а належна регламентація порядку проведення такої процедури у законопроекті відсутня. При цьому Уповноважений Верховної Ради України з прав людини вважає, що даний проект потрібно розглядати разом з законопроектом про створення *"спеціального органу з питань захисту персональних даних"*. Тобто мова йде про створення ще додаткового закону.

До вказаного, незрозумілі повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних у зв'язку з тим, що у проекті не передбачено виконання ним зазначених повноважень.

По-п'яте. Реалізація положень нового європейського порядку захисту персональних даних (Пакет GDPR-2016), Директиви 2002/58/ЄС, Директиви ЄС "NIS Directive", а в майбутньому Регламенти ЄС про "e-Privacy Regulation" та про "довіру до штучного інтелекту", в умовах розвитку та конвергенції цифрових технологій, зокрема, "Великі Дані", "Хмарні обчислення", "Інтернет речей" тощо, а також перманентність у змінах інтерфейсів і протоколів, безлічі стандартів та ін., дедалі більше ускладнюють реальні можливості практичного захисту права людини на приватність. Головне у тому, що кожного разу поява нових технологій та європейських актів буде вимагати переробки національного закону.

Виходячи з завдання впровадження у національне законодавство правил передбачених Регламентом (ЄС) 2016/679, з урахуванням можливості держав-членів мати простір для маневру у визначенні власних правил (п. 10 Преамбули Регламенту), та не виходячи за межі повноважень, визначених, зокрема у Article 16 (ex Article 286 TEC) зведених актів Договору про Європейський Союз та Договору про функціонування Європейського Союзу [45], можна запропонувати розробку *консолідованого законодавчого акту* України – *Про захист та безпеку приватності персональних даних*, складовими якого можуть бути:

– *основна частина*: визначення термінів; загальні положення; права суб'єкта приватності персональних даних; види діяльності з обробки персональних даних; основні принципи, підстави та спеціальні вимоги з обробки персональних даних; порядок доступу до персональних даних третіх осіб; обробка персональних даних правоохоронними органами; заходи безпеки приватності персональних даних тощо, які визначають основи регулювання відносин в сфері забезпечення приватності персональних даних на території України;

– *особлива частина*: захист приватності у зв'язку з обробкою персональних даних у сфері електронних комунікацій за суб'єктною ознакою щодо галузей (областей) інформаційної діяльності та з екстраполяцією положень основної частини; обов'язки контролера і оператора щодо захисту та безпеки приватності персональних даних; Уповноважений державний орган з питань захисту персональних даних та контроль за додержанням законодавства у сфері захисту та безпеки приватності персональних даних; відповідальність за порушення законодавства про захист та безпеку приватності персональних даних тощо на території України;

– *спеціальна частина*: приписи європейських правових стандартів у сфері захисту персональних даних – основні положення регулювання відносин суб'єктів України з міжнародними організаціями тощо; критерії транскордонної передачі персональних даних.

Враховуючи напрацювання, які надано у цій статті, результати роботи щодо закону можуть дозволити мати документ із перспективою довгострокового його функціонування, остання частина якого буде лише наповнюватися згідно з поточними змінами законодавства ЄС і РЄ, зокрема, у зв'язку з розвитком цифровізації, а також, при необхідності, внесення лише окремих змін в основну або особливу частини.

Використана література

1. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*: зб. наук. праць. № 3(90)/2017. С. 36-50.
2. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – перек. з англ.; В. Брижко – ред. тексту. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.
3. Философская энциклопедия. Справедливость. URL: https://dic.academic.ru/dic.nsf/encphilosophy/1150/%D0%A1%D0%9F%D0%A0%D0%90%D0%92%D0%95%D0%94%D9B%D%98%D0%92%D0%9E%D0%A1%D0%A2%D0%AC
4. Про захист прав людини і основоположних свобод: Конвенції Ради Європи від 4.XI.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
5. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: //www.epic.org; Смирнов С. Приватность. – (Межрег. группа "Правозащитная сеть)". Москва: Изд. "Права человека". 2002. 95 с. С. 1.
6. Бельсон Я., Ливанов К. История государства и права США. Ленинград: Изд. Ленинградского университета, 1982. 167 с. С. 69.
7. Рішення Великої палати Конституційного суду України від 20 грудня 2017 року № 2-р/2017 у справі за конституційним поданням 49 народних депутатів України щодо відповідності Конституції України (конституційності) пункту 7 частини другої статті 42 Закону України "Про вищу освіту". URL: https://zakon.rada.gov.ua/laws/show/v002p710-17#Text
8. Рішення Великої палати Конституційного суду України від 14 липня 2021 року № 1-р/2021 у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) Закону України "Про забезпечення функціонування української мови як державної". URL: https://zakon.rada.gov.ua/laws/show/v001p710-21#Text
9. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право.* № 4(19)/2016. С. 60-70.
10. Bygrave L. (2010). Privacy and data protection in an international perspective. URL: http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf
11. Брижко В.М. Персональні дані та право власності. *Українське право.* 2002. № 1. С. 152-157; Брижко В.М. Інформаційний продукт як об'єкт права власності. *Інформація і право.* № 4(23)/2017. С. 5-15; Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. Київ: ТОВ "Видавничий дім "АртЕк", 2020. 288 с. С. 93-101.
12. Джон Локк. Два трактата о государственном управлении. Кн. 2. Пункт 27. Глава V. "О собственности". URL: http://www.civis_book.ru/files/File/Lokk.Traktaty_2.pdf
13. Цит.: Olsaretti, Serena. 2004. Liberty, Desert and the Market. Cambridge University Press. P. 9.
14. Цит.: Dan-Cohen, Meir. 2002. Harmful Thoughts: Essays on Law, Self, and Morality. Princeton University Press. P. 296.
15. Богуцький П.П. Інформаційна приватність і публічність як сутнісні ознаки інформаційно- правових комунікацій: матеріали другої наук.-практ. конф. *Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах,* м. Київ, 21.05.2021. Київ, 2020. 258 с.
16. Корж І.Ф. Право на відкриті дані – як право приватного характеру. *Інформація і право.* № 1(28)/2019. С. 19-28.

17. Європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних: посібник. Кн. 2 / В. Брижко, М. Швець та ін. Київ: ТОВ "Пан Тот", 2006 р. 509 с. С. 379-392.

18. Защита персональных данных в США. URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mezhdunarodnaya-sistema-zashchity-personalnyh-dannyh/v-ssha

19. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

20. Серьогін В.О. Прайвесі у США: політико-правова теорія і практика. *Форум права*. 2011. № 1. С. 891-897. URL: http://www.nbuv.gov.ua/e-journals/FP/2011-1/11cvotip.pdf

21. S.D. Warren., L.D. Brandeis. The right to privacy. Originally published in the *Harvard Law Review*, No. 5. December 1890. Vol. IV. P. 193-220. URL: https://faculty.uml.edu/sgallagher/Brandeis privacyhtm

22. Ходорович. Расколотая база. URL: //www.aferizm.ru/bb_bd.htm

23. Михеев В. Проблема правовой защиты персональных данных. URL: www.kiev-security.org.ua/box/4/136.shtml; Цена персональных данных – рыночная цена конфиденциальности, или буря в стакане воды. URL: www.i2r.ru/article.shtml?id=1384A; Брижко В., Швець М. Про економічний аспект захисту персональних даних у контексті права власності на інформацію. *Правова інформатика.*" № 1(9)/2006. С. 47-56.

24. Берд Киви. Анонимность в Сети как залог свободы. URL: //www.sdteam.com/articles/hack058.shtml

25. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право.* № 1(32)/2020. С. 33-46.

26. Державний стандарт України "Технічний захист інформації. Терміни та визначення" (ДСТУ 3396.2-97). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69175

27. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

28. Защита персональных данных / А.А. Баранов, В.М. Брижко, Ю.К. Базанов. Київ: Национальное агентство по вопросам информатизации при Президенте Украины, 1998. 128 с.

29. 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;

30. 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; Брайчевський С.М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* № 4(31)/2019. С. 61-67; Дзьобань О.П. Цифрова людина як філософська проблема. *Інформація і право*. № 2(37)/2021. С. 2-37; Радутний О.Е. Правовий статус та характеристика цифрової людини. *Інформація і право*. № 4(39)/2021. С. 22-39.

31. Нечеловеческие способности. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863686

32. Лиев Э.Р. Внедрение механизмов искуственного интеллекта в правотворческую среду: материалы 1-й Международной научно-практической конференции *Шаг в будущее: искусственный интеллект и цифровая экономика.* Вып. 3. Москва: Издат. дом ГУУ, 2017. 369 с. С. 153-159.

33. AI Software Learns to Make AI Software. URL: https://www.technologyreview.com/2017/01/18/154516/ai-software-learns-to-make-ai-software

34. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

35. ЕС и США разработают общие принципы искусственного интеллекта. URL: https://internetua.com/es-i-ssha-razrabotauat-obsxie-principy-iskusstvennogo-intellekta; https://forklog.com/es-i-ssha-razrabotayut-obshhie-printsipy-iskusstvennogo-intellekta

36. Кривошапко Ю. Взяться за разум. URL: https://rg.ru/2020/01/14/eksperty-neobhodimo-sozdat-kodeks-povedeniia-iskusstvennogo-intellekta.htm

37. 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.

38. Больше, чем данные. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863684

39. Аблязов Н. Технологическая сингулярность. Исследование предпосылок возникновения и последствий для человечества. URL: https://mipt.ru/education/chair/philosophy/publications/aspers/a_1xes5v.php

40. ePrivacy Regulation. Proposal for a Regulation on Privacy and Electronic Communications (2017). URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications; Confidentiality of electronic communicatio ns: Council agrees its position on ePrivacy rules. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules

41. The Directive on Security of Network and Information Systems (NIS Directive). URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651

42. 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. С. 41-117; Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17; Гуцалюк М.В. Новітні тенденції кіберзлочинності. *Інформація і право.* № 1(36)/2021. С. 79-89; Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право.* № 2(37)/2021. С. 60-66.

43. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V. URL: //www.rada.gov.ua

44. Безуглий Д.С. Інформаційна безпека України: огляд останніх тенденцій. *Фізико-математична освіта*. 2018. Вип. 2(16). С. 2. URL: http://fmo-journal.fizmatsspu.sumy.ua

45. Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal*. C. 326. 26/10/2012. P. 0001-0390. URL: http://data.europa.eu/eli/treaty/tfeu_2012/oj

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

УДК 347.775 (061.1ЄС+477)

КАПІЦА Ю.М., *доктор юридичних наук*, директор Центру досліджень інтелектуальної власності та трансферу технологій НАН України.
ORCID: https://orcid.org/0000-0002-9449-8422.

ЗАХИСТ ПРАВ НА КОМЕРЦІЙНУ ТАЄМНИЦЮ ТА НОУ-ХАУ В УКРАЇНІ У СВІТЛІ ІМПЛЕМЕНТАЦІЇ ДИРЕКТИВИ (ЄС) 2016/943 ТА ПРАКТИКИ ЗАСТОСУВАННЯ

Анотація. *Розглядається практика застосування законодавства України з захисту прав на комерційну таємницю та ноу-хау; пропозиції з вдосконалення законодавства з врахуванням імплементації Директиви (ЄС) 2016/943 та забезпечення ефективного захисту прав.*

Ключові слова*: комерційна таємниця, ноу-хау, захист прав інтелектуальної власності.*

Summary. *The practice of application of the legislation of Ukraine on protection of trade secrets and know-how is considered; proposals are discussed to improve legislation taking into account the implementation of Directive (EU) 2016/943 and ensure effective protection of rights.*

Keywords*: trade secrets, know-how, enforcement of intellectual property rights.*

Аннотация. *Рассматривается практика применения законодательства Украины о защите прав на коммерческую тайну и ноу-хау; предложения по совершенствованию законодательства с учетом имплементации Директивы (ЕС) 2016/943 и обеспечения эффективной защиты прав.*

Ключевые слова*: коммерческая тайна, ноу-хау, защита прав интеллектуальной собственности.*

Постановка проблеми. Прийняття у 2016 р. Директиви (ЄС) 2016/943 Європейського Парламенту та Ради від 8 липня 2016 року щодо захисту нерозкритого ноу-хау та бізнесової інформації (комерційної таємниці) проти їх неправомірного набуття, використання та розкриття [1] (далі – Директива) поставило питання імплементації її положень у законодавство України. Підходи до імплементації широко обговорювалися на нарадах, семінарах та конференціях у 2013 – 2020 рр. та знайшли відображення у Концепції оновлення Цивільного кодексу України 2020 р. [2].

Разом з тим, актуальним є питання – наскільки в цілому існуючий механізм захисту прав на комерційну таємницю (далі – КТ) та ноу-хау є ефективним в Україні. Які є недоліки та які зміни законодавства мають бути здійснені для досягнення мети – формування в Україні ефективного інституту захисту прав на комерційну таємницю, що забезпечує можливість збереження організаціями і підприємствами у секреті інформації, важливої для розвитку бізнесу.

Результати аналізу наукових публікацій. Стан охорони комерційної таємниці в державах-членах ЄС та наслідки імплементації Директиви аналізувалися у низці публікацій Arcidiacono D., Aplin T., Aran L., Goleva P. Gronroos M., Hoeren T., Kamerling A., Lang J., Lunde T., Niebel R., Würtenberger G. та інш. Важливими для аналізу є закони держав-членів ЄС щодо імплементації положень Директиви, що мали бути ухвалені до 9 червня 2018 року[1].

[1] Див., зокрема: ФРН – Trade secrets Protection Act, 2019; Франція – Law on the Protection of Trade Secrets, 2018; Нідерланди – Wet Bescherming Bedrijfsgeheimen, 2018 тощо.

В Україні проблематику охорони та захисту прав на КТ та ноу-хау досліджували Алієв Т., Андрощук Г., Берлач А., Бєгова Т., Вапнярчук Н., Гусаров К., Дідук А., Дмитренко В., Килимник І., Мироненко Н., Назаренко Ю., Носік Ю., Подоляко А., Попова Н., Радутний О., Світличний О., Тверезенко О., Топалова Л., Чобот О., Юсупова Д. та ін. Підходи до імплементації Директиви (ЄС) 2016/943 у законодавстві України розглянуті у ряді публікацій Капіцей Ю. [3] та ін. Проблеми судового захисту прав на КТ розглядали Завертнева-Ярошенко В.А., Дюкарєва-Бержаніна К., Митнік А., Мороз І. [4 – 6] та ін.

В той же час потребує подальшого дослідження практика застосування законодавства України щодо захисту прав на КТ та виділення причин, що гальмують ефективний захист згаданих прав.

Метою статті є розгляд питань ефективності застосування діючого законодавства щодо захисту прав на комерційну таємницю та ноу-хау, а також розробка пропозицій з вдосконалення законодавства з врахуванням імплементації Директиви (ЄС) 2016/943.

Виклад основного матеріалу.

1. ***Практика захисту прав на комерційну таємницю та ноу-хау в Україні.***

Аналіз розгляду справ щодо захисту прав на комерційну таємницю та ноу-хау господарськими та загальними судами свідчить про істотну складність відшкодування майнової шкоди та наведення доказів щодо порушення прав на КТ. У переважній більшості випадків суди виносять рішення про відсутність достатніх доказів, які б свідчили про порушення прав на комерційну таємницю, ноу-хау. Вказане свідчить про неефективність діючих норм та складність або неможливість захисту права на комерційну таємницю, ноу-хау в рамках цивільного судочинства. В той же час, окремі справи свідчать про певний позитивний досвід захисту прав на КТ законодавством про недобросовісну конкуренцію та збирання доказів щодо порушення прав на КТ в рамках кримінального провадження.

1.1. Діюче трудове законодавство не дозволяє ефективно вирішувати питання відшкодування майнової шкоди працівником, а також розірвання трудового договору з працівником при порушенні ним майнових прав інтелектуальної власності на КТ. Так, обмежена матеріальна відповідальність покладається на працівника у випадку зіпсуття або знищення лише певних видів матеріальних речей, визначених ст. 133 КЗпП України. Щодо укладання з працівником договору про повну матеріальну відповідальність згідно ст. 135 КЗпП України, то до цього часу судова практика свідчить про обмеження укладання договорів лише з працівниками, посади яких визначено ще постановою Держкомпраці СРСР та Секретаріату ВЦРПС від 28.12.77 р. № 447/24 зі змінами від 14.10.81 р. № 259/16-59 [7].

Також, за ст. 135 КЗпП України розмір заподіяної підприємству, установі, організації шкоди визначається за фактичними втратами, на підставі даних бухгалтерського обліку, виходячи з балансової вартості (собівартості) матеріальних цінностей за вирахуванням зносу згідно з установленими нормами. В той же час при розкритті КТ та негативних наслідків для ведення підприємницької діяльності, встановити фактичні витрати не уявляється можливим або вони мають оціночний характер.

При порушенні майнових прав інтелектуальної власності на КТ можливим є застосування ст. 134 КЗпП України, яка встановлює, що працівники несуть матеріальну відповідальність у повному розмірі шкоди, коли шкоди завдано діями працівника, які мають ознаки діянь, переслідуваних у кримінальному порядку. Однак вказане може застосовуватися у разі винесення судом вироку.

Також, ускладненим є звільнення працівника при порушенні прав на комерційну таємницю. Можливість розірвання трудового договору при порушенні прав на КТ може бути встановлена контрактом. Проте сфера застосування контракту визначається законами України (ст. 21 КЗпП України) та стосується лише окремих видів діяльності та посад.

Інші підстава – розірвання за ст. 40 КЗпП України трудового договору у зв'язку з систематичним невиконанням працівником без поважних причин обов'язків, покладених на нього трудовим договором або правилами внутрішнього трудового розпорядку, якщо до працівника раніше застосовувалися заходи дисциплінарного чи громадського стягнення. Застосування вказаної статті не є можливим при разовому порушенні обов'язків чи правил внутрішнього розпорядку.

З врахуванням наведених складнощів забезпечення охорони прав на КТ в рамках трудового законодавства, а також того, що відносини стосовно об'єктів права інтелектуальної власності визначаються цивільним законодавством, можливим, на наш погляд, є укладання з працівником крім трудового договору – цивільно-правового, з передбаченням положень щодо заборони: розголошення КТ, її передання особам, які не мають права доступу до КТ, надсилання інформації, що становить КТ, в електронному вигляді на адреси, та розміщення такої інформації в електронних сховищах інших, ніж встановлено документами про охорону прав на КТ та без дозволу керівника організації або уповноваженої ним особи; використання КТ способами та у випадках інших ніж встановлено керівником організації тощо.

Такий договір може передбачати цивільно-правову відповідальність працівника за розголошення КТ, а також зобов'язання з відшкодування шкоди у зв'язку з неправомірними діями особи щодо КТ. У договорі є можливим, на наш погляд, передбачити обмеження права розголошення, використання конкретних відомостей, що становлять КТ, після звільнення працівника протягом певного терміну, наприклад – 3-5 років. Інформація щодо застосування такої практики, зокрема, наводиться у постанові Верховного Суду від 23.11.20 р., справа № 910/1759/19.

1.2. У зв'язку з питанням – чи можливо відшкодовувати при порушенні прав на КТ лише немайнову шкоду або майнову та немайнову шкоду, слід звернути увагу на Інформаційний лист Господарського суду України від 28.03.07 р. № 01-8/184 "Про деякі питання практики застосування господарськими судами законодавства про інформацію". Листом зазначається, що за порушення майнових прав інтелектуальної власності на комерційну таємницю чи прав на ноу-хау, зокрема, шляхом добування протиправним способом чужої комерційної інформації, розголошення її без згоди особи, уповноваженої на те, чи схилення до її розголошення або використання чужої комерційної інформації без згоди уповноваженої особи, власник цієї інформації має право на відшкодування завданих майнової та моральної шкоди відповідно до правил статей 1166 та 1167 ЦК України (п. 14).

Зазначимо, що згідно п. 3 постанови Верховного Суду України від 31.03.95 р. № 4 "Про судову практику в справах про відшкодування моральної (немайнової) шкоди" під немайновою шкодою, заподіяною юридичній особі, слід розуміти втрати немайнового характеру, що настали у зв'язку з приниженням її ділової репутації, посяганням на фірмове найменування, товарний знак, виробничу марку, розголошенням комерційної таємниці, а також вчиненням дій, спрямованих на зниження престижу чи підрив довіри до її діяльності. Вказана постанова стосується лише моральної (немайнової) шкоди та наведені у постанові положення не виключають можливості відшкодування майнової шкоди за ст. 1166 ЦК України при порушенні прав на КТ.

1.3. Ускладнення захисту прав на КТ пов'язане також із недосконалим визначенням понять "розголошення комерційної таємниці", "схилення до розголошення комерційної таємниці", "збирання комерційної таємниці" у Законі України "Про захист від недобросовісної конкуренції" (ст. 16 – 18). У визначеннях зазначених понять вказується, що неправомірне збирання, розголошення, схиляння до розголошення КТ може мати місце "якщо це завдало чи могло завдати шкоди суб'єкту господарювання".

Вказане, на наш погляд, не відповідає загальним засадам цивільного законодавства щодо справедливості, добросовісності та розумності (ст. 3 ЦК України) та призводить до того, що у випадку доведеного порушення прав на КТ та її розголошення (в умовах відсутності достовірних відомостей щодо завдання шкоди суб'єкту господарювання) – кваліфікація дій як розголошення комерційної таємниці згідно ст. 17 Закону України "Про захист від недобросовісної конкуренції" не має здійснюватися.

В той же час практика Антимонопольного комітету України (далі – АК України) свідчить про акцентування уваги під час розгляду справ на "неправомірне використання комерційної таємниці", визначення якої у ст. 19, на відміну від інших визначень, не містить вимог щодо завдання чи можливості завдання шкоди суб'єкту господарювання [8].

На наш погляд, визначення понять розголошення, схилення до розголошення, збирання комерційної таємниці у статтях 16 – 18 Закону України "Про захист від недобросовісної конкуренції" слід застосовувати лише в межах застосування зазначеного Закону. В інших випадках порушення прав на КТ доведення порушення має здійснюватися в рамках загальних правил цивільного судочинства.

1.4. Складним є доведення під час судового розгляду розміру збитків в результаті розголошення чи використання КТ. Аналогічна проблема в державах-членах ЄС, як і для інших об'єктів права інтелектуальної власності, вирішується через можливість замість відшкодування збитків сплати компенсації згідно положень ст. 14 Директиви (ЄС) 2016/943. Можливість застосування разового грошового стягнення замість відшкодування збитків за неправомірне використання об'єкта права інтелектуальної власності визначена ст. 432 ЦК України. Проте статтею зазначається, що розмір стягнення визначається відповідно до закону, що на цей час не передбачено.

Актуальним у зв'язку з зазначеним є передбачення можливості сплати компенсації при порушенні прав на КТ при імплементації положень Директиви у законодавство України.

1.5. Найчастіше при судовому розгляді справ з'ясовується, що стосовно інформації, визначеної КТ, не було запроваджено належних заходів з збереження її у секретності або не надано доказів розголошення КТ, або доказів використання КТ іншими особами.

Актуальним у зв'язку з зазначеним запровадження належних заходів з збереження секретності КТ[2], визначення переліку таких заходів на рівні Закону. При цьому

[2] Чек лист заходів з збереження секретності комерційної таємниці.

(а) чи прийняте Положення про захист прав на комерційну таємницю (далі – Положення); чи передбачено у Положенні зазначення видів відповідальності, яку несуть працівники у зв'язку з розголошенням КТ;

(б) чи віднесено конкретну інформацію (звіт, що містить технічні рішення; огляд, результати досліджень, записка, програма, що стосуються розвитку бізнесу, маркетингових досліджень; дані про постачальників, клієнтів, контрагентів тощо) до КТ з зазначення місця (місць) збереження такої інформації та носія такої інформації;

(в) чи укладено з працівниками договори, що передбачають зобов'язання з нерозголошення КТ; заборону передання КТ іншим особам, пересилання КТ без дозволу керівника організації або уповноваженої ним особою, використання КТ іншим способом та в інших випадках, ніж встановлено керівником організації; повернення всіх копій інформації, що становить КТ організації при звільненні працівника тощо;

доцільно взяти до уваги Рішення Тимчасової адміністративної колегії АК України № 30-р/тк від 13.12.18 р. та постанову Верховного Суду від 23.11.20 р., справа № 910/1759/19, що стосується вказаного рішення [9].

Рішення АК України та її розгляд судовими інстанціями свідчать про нові підходи, що були застосовані при розгляді недобросовісного використання КТ, а також про ефективні заходи, що застосовувались суб'єктом господарювання з забезпечення секретності КТ, роль при розгляді справи в АК України та судових інстанціях доказів неправомірного використання КТ, які були отримані в рамках досудового розслідування у кримінальному провадженні.

У коментарях до рішення звертається увага, що АК України було застосовано у вказаній справі підхід оцінки непрямих доказів у їх сукупності [10]. Було враховано: (і) наявність відомостей, що становлять КТ на комп'ютерах порушника; (іі) незначний часовий період (менше місяця), що минув між звільненням відповідних працівників компанії-власника відомостей, що становлять КТ, та заснуванням ними компанії-конкурента, а також, (ііі) укладання компанією-порушником господарських договорів з контрагентами власника КТ на більш вигідних для останніх умовах. При цьому, факт заподіяння шкоди законному власнику КТ не є обов'язковим елементом складу неправомірного використання КТ (ст. 19 Закону України), а тому не підлягає доведенню.

Слід вказати на важливість для практики охорони прав на КТ застосування заходів з збереження секретності КТ ТОВ "ТВК Вектор-ВС".

В матеріалах судової справи № 910/1759/19 наводиться, що ТОВ було визначено перелік відомостей, що становлять його КТ. У Пам'ятках для працівників ТОВ, які є додатками до зобов'язань та які підписувалися вказаними працівниками, що в силу своїх посадових обов'язків мають доступ до таких відомостей. До КТ, стосовно якої працівники підписували зобов'язання, було, зокрема, віднесено, такі відомості, як: собівартість продукції; розмір торгівельної націнки; відомості про постачальників, продавців та покупців продукції; відомості про способи придбання і реалізації продукції; відомості про рівень доходів ТОВ; зміст та характер договорів та контрактів, однією із сторін в яких виступає ТОВ; інші відомості, пов'язані з виробничою, економічною, фінансовою, управлінською та іншою діяльністю підприємства, розголошення яких може призвести до матеріальних збитків та шкоди діловій репутації ТОВ.

(г) чи містять документи у паперовій чи електронній формі позначення "Комерційна таємниця";

(д) чи визначено у Положенні про охорону прав на комерційну таємниці (далі – Положення), чи у рішенні щодо віднесення конкретної інформації до КТ засоби захисту (технічні, зокрема, вимога щодо застосування певного паролю до доступу до інформації у розподіленій мережі або для доступу до інформації на власному комп'ютері; порядок доступу працівників до КТ;

(є) чи визначені працівники, які мають доступ до КТ; чи повідомлені вказані працівники про зміст Положення, про відповідальність за порушення прав на КТ, про рішення щодо віднесення певної інформації до КТ; чи ними засвідчено факт повідомлення;

(ж) у випадку, якщо працівники з власного робочого комп'ютера мають змогу пересилати повідомлення та користуватися різними, у тому числі власними електронними адресами та месенджерами, чи передбачена заборона надсилання інформації, що становить КТ на електронні адреси та місця зберігання інформації інші, ніж визначені рішенням про віднесення інформації до КТ та без дозволу керівника організації чи уповноваженої ним особи;

(з) у випадку запровадження контролю за електронною кореспонденцією працівника, чи відповідає порядок та межі запровадження контролю практиці Європейського суду з прав людини та судовій практиці в Україні тощо.

Див. постанову Верховного Суду від 28.02.19 р., справа № 752/5775/16-ц.

Також працівниками ТОВ була підписана “Угода Зобов’язання про збереження комерційної таємниці та конфіденційної інформації ТОВ “ТВК Вектор-ВС”, що визначала зобов’язання осіб на період трудових відносин та протягом 3 років після їх закінчення, не розголошувати відомості, що становлять КТ ТОВ та стануть їм відомими під час виконання трудових обов’язків, не передавати третім особам відомості, що становлять КТ, без письмової згоди директора ТОВ або уповноваженої ним особи, не використовувати інформацію, що становить КТ, для зайняття будь-якою діяльністю, що може завдати шкоди ТОВ в якості конкурентної діяльності; у разі звільнення передати протягом 3 днів з моменту прийняття рішення про звільнення всі носії комерційної таємниці та конфіденційної інформації ТОВ, які перебували у їх розпорядженні у зв’язку з виконанням посадових обов`язків або з інших причин.

Крім того важливі докази для розгляду справи АМК та судами були виявлені у досудовому розслідуванні в кримінальному провадженні № 12015110130002211, розпочатому Київською місцевою прокуратурою № 8 за заявою директора ТОВ “ТВК Вектор-ВС”. На комп’ютері ТОВ “Ергон-електрік”, який було вилучено під час обшуку офісних приміщень позивача, було виявлено електронні документи та графічні файли щодо ведення господарської діяльності ТОВ “ТВК Вектор-ВС”, зокрема укладені договори (контракти), а також документи із зазначенням постачальників та активних покупців продукції заявника. Також було здійснено незалежну оцінку розміру збитків (у тому числі втраченої вигоди), понесених ТОВ “ТВК Вектор-ВС” дій ТОВ “Ергон-Електрік”, результати якої були розглянуті в рамках судової економічної експертизи.

Розгляд вказаної справи АК України та судовими інстанціями свідчить про актуальність здійснення захисту прав на КТ в рамках цивільного, господарського, адміністративного судочинства разом з кримінальним, що дозволяє отримати необхідні докази порушення прав на КТ та уникнути знищення доказів.

1.6. Порівняння норм ЦПК України з забезпечення позову (ст. 150) та забезпечення доказів (ст. 133) з нормами КК України (ст. 93) свідчить про обмежені можливості застосування цивільного судочинства для здійснення термінових дій з встановлення наявності неправомірно отриманої інформації в електронному вигляді в електронних приладах та носіях інформації, що може бути швидко знищена.

1.7. Частина перша ст. 505 ЦК України вимагає невідомості інформації, що становить КТ. Якщо зазначена інформація стала відомою, згідно ст. 508 ЦК України право інтелектуальної власності на таку інформацію припиняється. Вимога повної невідомості інформації суттєво обмежує можливості захисту комерційної таємниці. Інформація може стати відомою внаслідок правомірного одержання ідентичної інформації різними особами; при незалежному, як і для винаходів, створенні тотожних технічних рішень; її розголошенні колишнім працівником організації або особою, яка на порушення угоди про збереження конфіденційності розголосила таку інформацію, проте зазначені дії не призвели до того, що така інформація стала загальновідомою. Ст. 39 Розділу 7 “Захист нерозкритої інформації” Угоди про торгівельні аспекти прав інтелектуальної власності від 15.04.94 р. (далі – Угода TRIPS), яка була зразком для написання гл. 46 ЦК України, як і законодавство багатьох іноземних країн вимагає, щоб інформація не була “загально відома”[3]. Крім того, ст. 162 ГК України передбачає, що особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд. Ці положення

[3] Протокол про вступ України до СОТ був ратифікований Законом України від 10.04.08 р. № 250-VI та набрав чинності 16.05.08 р.

підтверджують можливість збереження ознак охороноздатності КТ, якщо тотожні відомості отримані особами незалежно або в результаті реінжинірингу та якщо виконуються вимоги щодо відсутності легкодоступності та запровадження заходів із збереження секретності, та такі відомості не використовуються іншою особою або використовуються для інших продуктів чи способів, що не призводить до зниження комерційної цінності КТ.

Вказане свідчить, що положення ст. 505 ЦК України стосовно невідомості інформації, яка становить комерційну таємницю, потребує відповідних змін ознаки "невідомість інформації" на "відсутність загальної відомості інформації".

1.8. У 1993 р. Кабінетом Міністрів України було прийнято постанову "Про перелік відомостей, що не становлять комерційної таємниці" від 9.08.93 р. № 611. Правовою підставою постанови був Закон України "Про підприємства"[4], ст. 30 якого передбачала, що відомості, які не можуть становити комерційної таємниці, визначаються КМУ.

ЦК України та ГК України не встановлюють повноваження Кабінету Міністрів України, інших органів виконавчої влади щодо затвердження відомостей, що не становлять комерційну таємницю. Закон України "Про підприємства" втратив чинність з 1.01.04 р. у зв'язку з прийняттям ГК України (ч. 2 Розділу IX Закону України від 16.01.03 р. № 436-IV). Також, у вказаній постанові змішуються питання, яку інформацію не може бути віднесено до комерційної таємниці та яка інформація, будучи віднесеною до комерційної таємниці, має надаватися органам державної влади за прямою вказівкою на це у законах, що регламентують діяльність вказаних державних органів.

В зв'язку з зазначеним перелік відомостей, що не становлять комерційну таємницю, на наш погляд, слід визначити на рівні закону.

1.9. Судова практика свідчить про відсутність єдиного підходу до вживання поняття ноу-хау [11], що відображає, на наш погляд, різні визначення ноу-хау у Податковому кодексі України (пункт 14.1.225), законах України "Про державне регулювання діяльності у сфері трансферу технологій" (ст. 1), "Про інвестиційну діяльність" (ст. 1) та вимагає уніфікації.

2. Питання імплементації Директиви (ЄС) 2016/943 у законодавство України.

У Директиві термін "комерційна таємниця" вживається як спільна назва двох видів інформації: ноу-хау та ділової (бізнесової) інформації (п. 2 Преамбули) з визначення КТ аналогічно визначенню нерозкритої інформації ст. 39 Угоди TRIPS.

З врахуванням положень Директиви та виділення у складі комерційної таємниці двох видів інформації: творчого характеру – ноу-хау та ділової інформації у Концепції оновлення Цивільного кодексу України пропонується доповнити главу 15 ЦК України окремою статтею "Комерційна таємниця"; замість глави 46 "Право інтелектуальної власності на комерційну таємницю" передбачити главу "Право інтелектуальної власності на ноу-хау"; передбачити, що особливості охорони прав на КТ визначаються законом [2, с. 10, 32].

Передбачається, що у главі 15 ЦК України буде надано визначення КТ відповідно до визначення КТ у Директиві (ЄС) 2016/943 та нерозкритої інформації Угоди TRIPS; зазначено, що до комерційної таємниці входить інформація, що складає ноу-хау та ділову інформацію. Також мають бути внесені зміни до ЦПК України та ГПК України стосовно особливостей захисту прав на комерційну таємницю, визначено розмір компенсації, що сплачується замість відшкодування збитків.

[4] Закон України "Про підприємства" втратив чинність у зв'язку із прийняттям ЦК Законом України від 16.01.03 р. № 436-IV.

Положення Директиви містять низку нових для права України положень стосовно:

(а) складу комерційної таємниці (ноу-хау та ділова інформація); визначення власника комерційної таємниці, порушника та контрафактних товарів;

(б) сфер, на які положення директиви не розповсюджуються;

(в) випадків правомірного отримання комерційної таємниці;

(г) не віднесення комерційної таємниці до об'єктів права інтелектуальної власності;

(д) випадків неправомірного отримання комерційної таємниці, зокрема, третьою особою, яка знала або за відповідних обставин мала знати, що відомості, прямо або опосередковано отримані іншою особою, становлять комерційну таємницю.

(є) заходів та процедур захисту прав, що визначають: термін подання позову до суду; вимоги щодо охорони комерційної таємниці під час судового розгляду; тимчасові та застережні заходи; виправні заходи та альтернативні заходи; положення щодо відшкодування та публікації судових рішень. Вказані положення в основному повторюють норми директиви 2004/48/ЄС з визначенням специфіки застосування відносно захисту комерційної таємниці. Проте в Україні у повному обсязі положення директиви 2004/48/ЄС не були імплементовані.

У Директиві (ЄС) 2016/943 визначено термін подання позову до суду щодо порушення прав на комерційну таємницю до 6 років (ст. 8). Норми ст. 8 щодо особливості забезпечення конфіденційності використання КТ під час судового розгляду є важливими як уточнення положень ст. 6 Директиви 2004/48/ЄС з розгляду у конфіденційності справ, які стосуються об'єктів права інтелектуальної власності.

Відзначимо, що під час обговорення проекту Директиви розглядалися різні підходи до визначення кола осіб, які мають доступ до КТ сторін під час судового процесу. Остаточний варіант Директиви визначив зобов'язання, з одного боку, особам, які мають доступ до такої таємниці, не використовувати та розголошувати її у тому числі після закінчення судового розгляду, з іншого, визначено право суду обмежувати доступ до документів, що містять комерційну таємницю, та надавати їх обмеженій кількості осіб (ст. 9).

Новим є зазначення зобов'язань суду накладати санкції на позивача, коли з'ясується, що позивач розпочав судову справу недобросовісно (ст. 6).

Більш детально порівняно з частиною третьою ст. 9 Директиви 2004/48/ЄС наведені норми щодо запобіжних та тимчасових заходів (ст. 10, 11). У випадку їх здійснення позивач має надати докази, що

(а) комерційна таємниця існує;

(б) заявник має права на КТ;

(в) комерційна таємниця була незаконно отримана, в даний час вона незаконно використовується або незаконно розкрита, або що незаконне придбання, використання або розголошення комерційної таємниці є неминучим (ст. 11(1).

Детально зазначається, які обставини суди мають брати до уваги при ухваленні рішення. Слід вказати, що замість розподілення заходів з забезпечення доказів та тимчасових заходів у Директиві 2004/48/ЄС (ст. 7, 9), Директивою про комерційну таємницю вказані норми викладені у ст. 10 "Тимчасові і запобіжні заходи" та ст. 11 "Умови застосування та гарантії", що безумовно сприятиме правовій визначеності при прийнятті судами рішень щодо запобіжних заходів перед поданням позову по суті справи та заходів з забезпечення доказів.

Висновки.

Судова практика захисту прав на комерційну таємницю та ноу-хау в Україні свідчить про істотні недоліки діючого законодавства, що не дозволяє ефективно

здійснювати захист прав в рамках цивільного судочинства, зокрема, внаслідок неможливості забезпечити надання доказів порушення прав у цивільно-процесуальному порядку без загрози їх знищення відповідачем. Ускладненими або невирішеними є відшкодування майнової шкоди у зв'язку з порушенням прав на КТ найманим працівником, правового режиму службової КТ. Визначення комерційної таємниці в ЦК України не відповідає положенням Угоди TRIPS та Директиви. Недосконалим є визначення понять "розголошення комерційної таємниці", "схилення до розголошення комерційної таємниці" "збирання комерційної таємниці" Законом України "Про захист від недобросовісної конкуренції" тощо. Істотним фактором є недостатність досвіду захисту прав на КТ в організаціях, на підприємствах.

Основні підходи змін законодавства України щодо захисту прав на КТ та ноу-хау визначені Концепцією оновлення цивільного законодавства України 2020 р. та включають внесення доповнень до глави 15 ЦК України щодо визначення поняття КТ та її видів – ноу-хау та ділова (бізнесова) інформація; заміни Глави 46 "Право інтелектуальної власності на комерційну таємницю" на Главу "Право інтелектуальної власності на ноу-хау"; передбачення, що особливості охорони прав на КТ визначаються законом. Також мають бути внесені зміни до ЦПК України та ГПК України, Закону України "Про недобросовісну конкуренцію", інші законодавчі акти, що враховують положення Директиви (ЄС) 2016/943.

Стосовно прийняття спеціального закону щодо комерційної таємниці – у такому законі, крім імплементації Директиви, істотна увага має бути приділена положенням, що сприяли б запровадженню в організаціях та на підприємствах ефективної системи захисту прав на КТ, використання крім трудових – цивільно-правових договорів з працівниками щодо особливостей захисту прав КТ, у тому числі врегулювання у договорах питань відшкодування майнової шкоди за неправомірне використання КТ; визначення умов сплати компенсації за порушення прав на КТ тощо.

З врахуванням того, що ділова (бізнесова) інформація є об'єктом інформаційних правовідносин та врегулювання відносин стосовно ноу-хау передбачається законодавством про інтелектуальну власність, а також що Директива не відносить КТ до об'єктів права інтелектуальної власності, можливим є визначення спеціального закону як закону про захист комерційної таємниці проти її неправомірного набуття, використання та розкриття. Вказане слідувало б підходам Закону України "Про інформацію", Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та інших законодавчих актів щодо різних видів інформації.

Використана література

1. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. OJ L 157, 15.6.2016. P. 1-18. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943

2. Концепція оновлення Цивільного кодексу України / Довгерт А.С., Кузнецова Н.С., Хоменко М.М. та ін. Київ: Видавничий дім "АртЕк", 2020. 128 с.

3. Капіца Ю.М. Право інтелектуальної власності Європейського Союзу: формування, інститути, напрями розвитку. – (Центр дослідж. інтелект. власн. та трансферу технологій НАН України). Київ: Академперіодика, 2017. С. 332-350; Капіца Ю.М. Гармонізація охорони комерційної таємниці в Європейському Союзі та напрямки вдосконалення законодавства України. *Право та інновації.* 2016. № 1. С. 251-256. URL: https://ndipzir.org.ua/journal-no-13

4. Завертнева-Ярошенко В. А., Ячменська М.М. Проблеми правового захисту комерційної таємниці в Україні. *Правова держава*. 2018. № 32. С. 134-145. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S2 1CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Prav_2018_32_17

5. Дюкарева-Бережаніна К.Ю. Захист прав на комерційну таємницю: національні підходи та світовий досвід. *Право і суспільство*. 2020. № 2. С. 168-176. URL: http://pgp-journal.kiev.ua/index.php/archive-3-2020

6. Митник А., Мороз І. Комерційна таємниця як об'єкт права інтелектуальної власності. *Підприємство, господарство і право*. 2019. № 12. С. 42-46. URL: http://pgp-journal.kiev.ua/index.php/archive-12-2019

7. Постанова Верховного Суду від 13.11.19 р., справа № 523/18122/15-ц. URL: https://reyestr.court.gov.ua/Review/85934572

8. Рішення Тимчасової адміністративної колегії Антимонопольного комітету України № 30-р/тк від 13.12.18 р.

9. Постанова Верховного Суду від 23.11.20 р., справа № 910/1759/19. – (Єдиний реєстр судових рішень). URL: https://reyestr.court.gov.ua/Review/93149537

10. Сисецкая Анна. Антимонопольный комитет Украины на защите коммерческой тайны. *Юрист & Закон*. 25.04.2019. URL: https://uz.ligazakon.ua/magazine_article/EA012643

11. Дмитренко В. Аналіз судової практики України щодо вирішення спорів, пов'язаних з порушенням прав на ноу-хау: матеріали Міжнародної науково-практичної конференції *Актуальні питання державотворення в Україні*, м. Київ, 20 трав. 2016 р. Київ, 2016. URL: https://www.viconsult.com/ru/publikatsii/analiz-sudovoi-praktyky-ukrainy-shchodo-vyrishennia-sporiv-poviazanykh-z-porushenniam-prav-na-nou-khau

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

УДК 321.011:342

ТЕРНАВСЬКА В.М., *кандидат юридичних наук, доцент,* провідний науковий співробітник Київського регіонального центру НАПрН України.
ORCID: https://orcid.org/0000-0003-2102-619X.

КОНЦЕПЦІЯ ДЕРЖАВНОГО СУВЕРЕНІТЕТУ В АСПЕКТІ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Анотація. *Стаття присвячена визначенню природи інформаційного суверенітету та його значення для процесу незалежного державотворення через призму парадигми інформаційного суспільства. Досліджуються різні методологічні аспекти поняття "інформаційний суверенітет". Аналізується співвідношення категорій "державний суверенітет" та "інформаційний суверенітет". Робиться висновок, що інформаційний суверенітет не є самостійною категорією конституційного права, разом з тим, концепція державного суверенітету потребує модернізації шляхом інтеграції класичних та нових інформаційних правомочностей держави, характерних для глобалізованого інформаційного світу.*

Ключові слова: *державний суверенітет, інформаційний суверенітет, національні інтереси, національна безпека, суверенноздатність, конституційно-правова політика.*

Summary. *The article is dedicated to defining the nature of information sovereignty and its significance for the process of independent state-building through the prism of the information society paradigm. Various methodological aspects of the concept of "information sovereignty" are studied. The ratio of the categories "state sovereignty" and "information sovereignty" is analyzed. The conclusion is made that the information sovereignty is not an independent category of constitutional law, however, the concept of state sovereignty needs to be modernized by integrating the classical and new information authority of the state, which are characteristic of the globalized information world.*

Keywords: *state sovereignty, information sovereignty, national interests, national security, sovereignability, constitutional and legal policy.*

Анностация. *Статья посвящена определению природы информационного суверенитета и его значения для процесса независимого государственного строительства сквозь призму парадигмы информационного общества. Исследуются различные методологические аспекты понятия "информационный суверенитет". Анализируется соотношение категорий "государственный суверенитет" и "информационный суверенитет". Делается вывод, что информационный суверенитет не является самостоятельной категорией конституционного права, однако концепция государственного суверенитета нуждается в модернизации путем интеграции классических и новых информационных правомочий государства, характерных для глобализованного информационного мира.*

Ключевые слова: *государственный суверенитет, информационный суверенитет, национальные интересы, национальная безопасность, суверенноспособность, конституционно-правовая политика.*

Постановка проблеми. Сучасний глобалізований світ динамічно розвивається у новій парадигмі інформаційного суспільства. Стрімкий розвиток національних економік та культури, створення нових глобальних форм врядування, плідна співпраця держав у сфері міжнародної безпеки стали можливими завдяки новим технологічним можливостям та поширенню мережі Інтернет. Інтеграція сучасних інформаційних технологій створює умови для виникнення як локальних, так і національних кіберфізичних систем, що передбачають впровадження в процеси управління елементів

штучного інтелекту [1, с. 77, 78]. В той же час, перед людством постають нові виклики, зумовлені можливостями сучасних інформаційних технологій, зокрема, несанкціоноване поширення інформації, втручання у виборчий процес іноземних держав, фальсифікація результатів референдумів, кібератаки на інформаційні бази даних національних систем управління, інформаційний тероризм тощо. Враховуючи останні події у світі, науковці наголошують на необхідності розробки більш ефективних механізмів захисту державного суверенітету в рамках міжнародного права від проявів агресії з боку окремих акторів, що супроводжується не лише торгівельними чи "гібридними" війнами, але й інформаційними війнами також [2, с. 92].

Недостатня захищеність інформаційних ресурсів призводить до витоку важливої інформації політичного, економічного, науково-технічного чи оборонного характеру, що становить сутність національних інтересів, а тому спонукає уряди США, Великобританії, Китаю та держав-лідерів ЄС активно формувати нову інформаційну політику. Так, у США спричинення значної шкоди національним інтересам у галузі державної безпеки та економіки злочинними діями недержавних структур (терористичних угрупувань), а також кібератаками з боку РФ, Ірану та Північної Кореї, економічного шпіонажу у галузі інтелектуальної власності з боку КНР, стали підставою для прийняття Національної кіберстратегії США 2018 р., що передбачає зміцнення національної кібербезпеки США від кіберзагроз [3, с. 1-2]. Однак інформаційна політика домінантних акторів спрямована одночасно як на захист свого національного суверенітету, так і передбачає прямий чи опосередкований вплив на послаблення суверенноздатності всіх інших країн. З. Бжезінський відверто називає глобалізацію як глобальну взаємозалежність держав, де немає місця для рівності, де немає жодної гарантії однакової безпеки та абсолютного імунітету для всіх держав щодо наслідків технологічної революції [4, с. 13]. Дж. С. Най вважає, що глобалізація інформації прискорила обмін, поширення і проникнення всіх видів думок, переконань і цінностей, а інформаційні наддержави на чолі з США використовують т.з. "м'яку силу" для впливу на інформаційно бідні країни, інформаційна безпека яких буде з часом контролюватися цими наддержавами, а їх культура, цінності та образ життя будуть перетворені інформаційно багатими державами і навіть з'являться "інформаційний сюзерен" та "інформаційна колонія" [5, с. 126].

Внаслідок вищезазначеного, проблема належного забезпечення основного атрибуту політичної влади – державного суверенітету, піднята українськими правознавцями багато років тому [6, с. 321], має підвищену актуальність для України сьогодні та потребує ґрунтовного вивчення факторів зовнішнього та внутрішнього впливу на суверенноздатність Української держави [7, с. 72-73], що поступово ведуть до "деградації" чи то "девальвації" статусу суверенної держави у загальному контексті глобалізаційних процесів.

Результати аналізу наукових публікацій. Проблематика збереження і захисту державного суверенітету привертає увагу українських вчених протягом всього періоду незалежного державотворення. Різні політико-правові аспекти поняття державного суверенітету та сучасних технологій його захисту знайшли своє відображення у наукових розвідках М.О. Баймуратова, Ю.П. Битяка, В.Г. Буткевича, О.Д. Довганя, О.В. Задерейко, В.Н. Кубальського, І.А. Куян, О.В. Олійника, О.Е. Радутного, С.Г. Серьогіної, О.В. Скрипнюка, О.М. Солодкої, О.В. Троянського, Р.І. Чанишева, Ю.С. Шемшученка, І.В. Яковюка та ін. В той же час, питання суверенноздатності держави в інформаційному просторі, що є одним із стратегічних напрямів конституційно-правової політики, є недостатньо дослідженим в юридичній літературі.

Метою статті є теоретико-правове обґрунтування нової грані державного суверенітету – інформаційного суверенітету, що відкривається завдяки науково-технічному прогресу людства, та практичного втілення модернізованої концепції державного суверенітету у політико-правову практику задля посилення суверенноздатності Української держави в глобалізованому інформаційному світі.

Виклад основного матеріалу. Конституція України 1996 р. проголосила Україну суверенною, незалежною, демократичною, соціальною, правовою державою [8]. Однак норми конституційного права, що закріплюють суверенітет держави, не утворюють ані самостійного інституту в системі конституційного права, ані складової генерального інституту основ конституційного ладу [9, с. 384], хоча ці норми є фундаментальними для більшості інститутів конституційного права. В цілому, феномен суверенітету все ще не отримав свого належного доктринального визначення у вітчизняній науці теорії держави і права. У науці конституційного права поняття суверенітету розглядається в рамках конституційно-правового інституту державної влади в аспекті співвідношення таких категорій, як національний, народний і державний суверенітет [10, с. 253; 11, с. 173].

Державний суверенітет визначається в Декларації про державний суверенітет України як верховенство, самостійність, повнота і неподільність влади Української держави в межах її території, що є незалежним і рівноправним суб'єктом міжнародних відносин [12]. Виходячи із зазначеного, основною просторовою межею здійснення державою суверенних прав вважається її територія. Однак саме поняття «територія» в процесі історичного розвитку зазнало серйозних змін. Спершу територією вважалася материкова частина Земної кулі, у подальшому держави почали захищати свої інтереси на прилеглих територіях, що визначаються сьогодні як континентальний шельф та виключна (морська) економічна зона. У XXI ст. виникла гостра потреба визначення територіальних меж суверенних прав держави в інформаційному просторі внаслідок стрімкого розвитку новітніх технологій та переходу людства до якісно нової парадигми суспільного розвитку – інформаційного суспільства. Вважається, що природа кіберпростору вже давно не відповідає традиційним географічним концепціям [13, с. 207]. Відповідно, сьогодні існує нагальна потреба визначення суверенітету держави у новому вимірі – інформаційному, та визначення меж реалізації інформаційного суверенітету держави [14, с. 40].

Концепція інформаційного суверенітету була запропонована ще у другій половині XX ст., невдовзі після запуску першого штучного супутника Землі, що, за словами Дж. Нейсбитта, ознаменував "глобалізацію інформаційної революції" [15, с. 12]. Нові результати науково-технічного прогресу спричинили також і нові проблеми у сфері міжнародних відносин, що активно дебатуються і сьогодні. Так, Декларація керівних принципів з використання мовлення через супутники для вільного розповсюдження інформації, розвитку освіти та розширення культурного обміну 1972 р. визначає, що супутникове мовлення має поважати суверенітет і рівність всіх держав (ст. II), які мають право приймати рішення про зміст освітніх програм, що транслюються через супутник для свого народу (ст. VI) [16]. Разом з тим, залишається відкритим питання відносно конкретних масштабів кібер-генерованих ефектів, які можуть порушити обов'язкові норми міжнародного права, зокрема, застосування відображеного в ст. 2 (4) Статуту ООН *jus ad bellum*, як і питання принципу суверенітету, що діє як самостійна норма міжнародного права, котра регулює дії держави у кіберпросторі та залишає дане питання на власний розсуд держав [13, с. 207-208, 210].

У сучасній науковій літературі суверенні права держави в інформаційній сфері об'єднуються поняттям "інформаційний суверенітет" [5; 14; 17] або "цифровий суверенітет" [13; 18]. Підтримуємо позицію О.М. Солодкої, яка визначає цифровий суверенітет як різновид інформаційного суверенітету, оскільки останній включає не лише здатність впливати на інформаційно-комунікаційні технології загалом, але і на контент [19, с. 82]. Незважаючи на термінологічні розходження, ми підтримуємо думку українських науковців, що в умовах глобалізованого інформаційного світу незабезпечення суверенітету держави в інформаційній сфері може призвести до втрати суверенітету взагалі [18, с. 10].

Виходячи з концепції державного суверенітету, закономірно постає питання, чи є поняття "інформаційний суверенітет" самостійною категорією конституційного права? Аналіз юридичної літератури свідчить про те, що переважна більшість науковців не визнають інформаційний суверенітет як окремий вид суверенітету.

Так, В. Гонг не розмежовує державний та інформаційний суверенітет як два окремих види суверенітету, вважаючи інформаційний суверенітет тією частиною державного суверенітету, яка пов'язана з інформацією та має також внутрішню і зовнішню сторони прояву. Китайський вчений визначає дану категорію наступним чином: інформаційний суверенітет – це верховне право державної влади розробляти інформаційну політику та підтримувати інформаційний порядок всередині країни, а також повна юридична рівність з іншими державами і свобода від будь-якого зовнішнього контролю щодо незалежних прав на продукацію та використання інформації [5, с. 120].

Таку ж позицію має і О.Е. Радутний, який вважає, інформаційний суверенітет невід'ємною складовою загального суверенітету, однак його виокремлення та самостійне дослідження зумовлено складністю інформаціної системи та необхідністю більш детального аналізу її елементів [17, с. 24].

Натомість О.М. Солодка зазначає, що поняття "інформаційний суверенітет" є відносно відокремленим видом державного суверенітету, що відрізняється від останнього юрисдикційними межами, колом уповноважених суб'єктів та ступенем участі недержавних структур у забезпеченні, власними моделями і комбінаціями методів правового регулювання, рівнем міжнародної співпраці тощо [19, с. 82].

Не поділяючи такої позиції О.М. Солодкої, наведемо як контраргумент думку О.В. Олійника, який слушно зауважує, що суверенітет держави є єдиним і неподільним та охоплює *всі аспекти державного життя*, тобто й інформаційну сферу також, а тому слід виокремлювати нову, інформаційну функцію держави та компетенцію держави в інформаційній сфері [20, с. 56], які будуть виконувати все ті ж уповноважені державою органи – Міністерство культури та інформаційної політики України, що забезпечує сьогодні формування та реалізує державну політику, у тому числі у сфері інформаційного суверенітету України та інформаційної безпеки [21], спеціалізовані підрозділи Служби безпеки України, Державна служба спеціального зв'язку та захисту інформації України та інші органи і служби, які одночасно виконують й інші завдання і функції щодо забезпечення і захисту державного суверенітету України.

Термін "інформаційний суверенітет" вперше було введено в систему національного права на законодавчому рівні Законом України "Про інформацію" від 02.10.92 р. № 2657-XII [22], де основою інформаційного суверенітету України було визначено національні інформаційні ресурси, у тому числі вся належна Україні інформація, незалежно від змісту, форм, часу і місця створення, а також право України самостійно формувати інформаційні ресурси на своїй території і вільно розпоряджатися ними, за винятком випадків, передбачених законами і міжнародними договорами. Однак нормативне визначення самого поняття "інформаційний суверенітет держави" було закріплено лише Законом

України “Про Національну програму інформатизації” від 04.02.98 р. № 74/98-ВР як здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави [23]. Вважаємо, що законодавець має дати більш коректне визначення поняття “інформаційний суверенітет”, ніж те, що закріплено Законом України № 74/98-ВР, оскільки, як справедливо зауважують О.В. Олійник [20, с. 56] та О.Е. Радутний [17, с. 26-27], його сутність зводиться лише до “здатності держави контролювати і регулювати потоки інформації з-поза меж держави”, позбавляючи державу права вчиняти такі ж дії в межах власної території, а також права самостійно формувати інформаційні ресурси та права власності на них. Крім того, така нормативна дефініція не передбачає права самостійно формувати державну інформаційну політику.

В українському законодавстві термін “інформаційний суверенітет” вживається як в законах, так і підзаконних нормативно-правових актах, однак відсутній комплексний підхід до впорядкування всіх питань, пов’язаних з суверенноздатністю Української держави в інформаційному просторі. ***Суверенноздатність*** – це здатність держави *самостійно формувати* засади внутрішньої і зовнішньої політики та *реалізовувати* її згідно з національними інтересами в умовах впливу правової глобалізації на національні правові системи. Зміст поняття суверенноздатності становить певна сукупність юридичних прав та обов’язків, що випливають із природного права держави на самобутній розвиток і взятих на себе зобов’язань перед власним народом та міжнародно-правових зобов’язань. Однак, проблематика суверенних прав держави залишається недостатньо дослідженою у вітчизняній юридичній науці. С.Г. Серьогіна та Ю.В. Байдін справедливо вважають таку ситуацію неприйнятною, оскільки суверенні права розкривають не тільки сутність державної влади всередині країни та у відносинах із суб’єктами міжнародного права, але й послідовно відображають нагальні потреби держави, що становлять фундаментальні умови, необхідні для гідного існування держави у сучасному світі [6, с. 76-77]. Відповідно, суверенні права Української держави в інформаційній сфері в жодному нормативному акті не систематизовані, хоча Верховна Рада України, об’єктивно оцінюючи існуючі загрози для національної безпеки в інформаційній сфері, у своїй Постанові “Про діяльність Кабінету Міністрів України, інших органів державної влади щодо забезпечення свободи слова, задоволення інформаційних потреб суспільства та розвитку інформаційної сфери в Україні” від 16.02.99 р. № 430-XIV [24] визнала за необхідне прискорити розробку проектів основ державної інформаційної політики, законів про інформаційний суверенітет та інформаційну безпеку України, розвиток телерадіоінформаційного простору. Натомість, у 2011 р. Верховна Рада України прийняла нову редакцію Закону України “Про інформацію” № 2938-VI [25], де не тільки немає визначення поняття “інформаційний суверенітет”, але й положення статей 53 та 54 першої редакції Закону № 2657-XII про інформаційні ресурси як основу інформаційного суверенітету не знайшли свого відображення, хоча такі права Української держави визначені у більш вузькій сфері – у сфері науково-технічної інформації, відповідно до Закону України “Про науково-технічну інформацію” від 25.06.93 р. № 3322-XII [26]. Підставою для анулювання положень про інформаційний суверенітет став негативний висновок експертів Ради Європи, які вважають, що дане поняття “не належить до принципів, що їх ужито бодай в одному договорі про захист прав людини” [27].

Разом з тим, у міжнародному праві сьогодні вже визнається, що “суверенітет держав та міжнародні норми і принципи, що витікають з суверенітету, застосовуються до здійснення державами діяльності, пов’язаної з ІКТ, та їх юрисдикції над ІКТ-

інфраструктурою, що розташована на їх території" [28]. Крім того, держави, посилаючись на положення Таллінського статуту із застосування міжнародного права до кібервійн, зокрема Правило 1, поширюють свою юрисдикцію на всю кіберінфраструктуру, що знаходиться на її території відповідно до засад територіальності дії принципу державного суверенітету у міжнародному праві [29].

В цілому, основні засади державного суверенітету в інформаційній сфері мають бути визначені в *концепції державної інформаційної політики*, в основі якої мають бути виключно *національні інтереси*, котра має бути спрямована на забезпечення *національної безпеки* у *глобальному інформаційному просторі*. Тобто сукупність цих чотирьох категорій становить *quinta essentia* т.з. інформаційного суверенітету. Однак, у ст. 3 Закону України "Про інформацію" в редакції 2011 р. відсутнє визначення поняття "державна інформаційна політика", хоча дане поняття визначалося в ст. 6 Закону редакції 1992 р. як "сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації" [22]. І хоча дане визначення не містило базового елементу – "самостійне вироблення інформації", разом з тим ми поділяємо точку зору О.Д. Довганя, що саме на конституційно-правовому рівні має бути визначено правові та ціннісно-ідеологічні засади інформаційної політики сучасної держави, а також місце і роль держави у процесі формування інформаційного простору [30, с. 106]. Крім того, вважаємо некоректним визначення поняття "національні інтереси України" в Законі України "Про національну безпеку України" від 21.06.18 р. № 2469-VIII як життєво важливі інтереси людини, суспільства і держави, *реалізація яких забезпечує* державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [31]. На нашу думку, у даній законодавчій дефініції неправильно розставлені акценти. Річ у тім, що національні інтереси держави – це дійсно життєво важливі інтереси людини, суспільства і держави в усіх сферах життєдіяльності. Однак, *не реалізація* життєво важливих інтересів *забезпечує* державний суверенітет України, а саме *фактична наявність суверенітету* у держави робить можливою *реалізацію життєво важливих інтересів* людини, суспільства і держави, саме її суверенноздатність *забезпечує* прогресивний демократичний розвиток держави та безпечні умови життєдіяльності і добробуту її громадян.

Важливим елементом системи національної безпеки є інформаційна безпека. Конституція України в ч. 1 ст. 17 визначає забезпечення інформаційної безпеки України однією з найважливіших функцій держави [8]. У Доктрині інформаційної безпеки України 2017 р. визначено, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [32]. Однак, аналіз національного інформаційного законодавства свідчить про відсутність системного підходу нашого законодавця до вирішення питання належного правового врегулювання правовідносин в інформаційній сфері. Річ у тім, що частина нормативно-правових актів безнадійно застаріла, а тому не може належним чином врегульовувати нові суспільні явища у сфері інформаційних технологій, а нові потрібні акти ще не прийняті з різних причин. Крім того, недотримання правил нормотворчості та юридичної техніки призводить до колізій правових норм та прогалин у законодавстві. Зокрема, у законодавстві України є наявність трьох різних визначень поняття "інформація", трьох визначень поняття "захист інформації". Натомість поняття "інформаційна безпека" не визначено ані Законом України "Про інформацію" від 13.01.11 р. № 2938-VI [25], ані Законом України "Про національну безпеку України" від 21.06.18 р. № 2469-VIII [31]. Внесений у 2018 р.

до парламенту законопроект “Про внесення змін до законів України щодо інформаційної безпеки” від 26.11.18 р. № 9340 [33] містив визначення поняття інформаційної безпеки, яке хоча і потребувало свого нормативного та лінгвістичного доопрацювання, однак так і не був прийнятий. Відповідно, сьогодні застосовується поняття “кібербезпека”, що містить Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.17 р. № 2163-VIII [34]. Необхідно зазначити, що поняття “кібербезпека”, яке міститься в даному Законі, є невід’ємною та необхідною складовою кіберфізичних систем як стан безпечного, надійного, стійкого їх функціонування з урахуванням вимог конфіденційності. Натомість даний Закон не дає визначення поняття кіберфізичних систем. Виходячи з вищезазначеного, ми пропонуємо доповнити Закон України № 2163-VIII наступним визначенням даного поняття: “кіберфізична система (КФС) – це інтелектуальна система, що включає інженерно взаємодіючі мережі фізичних та обчислювальних компонентів” [35, с. 48].

Таким чином, захист національних інтересів від реальних та потенційних загроз у кіберпросторі потребує застосування як організаційних, матеріальних, фінансових, технічних, так і правових інструментів. Адекватність співвідношення засобів і цілей вимагає комплексного підходу до вирішення цієї важливої задачі у конституційно-правовому полі. Річ у тім, що конституційно-правова політика кожної демократичної держави формується сьогодні у форматі збалансування індивідуальних, суспільних та державних інтересів, де, з одного боку, має бути забезпечення конституційних прав громадян на доступ до інформації, а з іншого – жорсткий контроль за національним кіберпростором та його захист. Однак, як слушно зауважують українські правознавці, Україна має недостатній потенціал щодо протидії загрозам її інформаційній безпеці, зміцненню національної безпеки, оскільки відсутня цілісність системи правового регулювання суспільних відносин у галузі протидії загрозам національним інтересам України в інформаційній сфері [36, с. 5]. Крім того, в Україні все ще залишається невирішеною належним чином проблема визначення правових основ збирання, зберігання, обробки та використання інформації, яка стосується безпосередньо громадян України [37, с. 23], оскільки інформаційна безпека громадян є складовою національної безпеки. Вирішенням даної проблеми може стати, на думку фахівців, запровадження правових режимів у сфері кібербезпеки.

Так, на думку В.В. Бєлєвцевої, належно розроблена та втілена в життя категорія правового режиму кіберпростору могла б усунути надмірну розшарованість правового регулювання, більш чітко та послідовно визначити суб’єктів досліджуваних правовідносин та порядок їх взаємодії, юридичні гарантії забезпечення прав людини, форми, методи діяльності контролюючих суб’єктів, заходи юридичної відповідальності [38, с. 108-109].

Своєю чергою Н.Ф. Казакова та інші спеціалісти з питань комп’ютерних та інформаційно-вимірювальних технологій також наголошують, що для машинних і когнітивних інтерфейсів, повинен бути створений новий правовий режим функціонування, який визначить правила реагування на конфліктні ситуації між суб’єктами міжмашинної взаємодії [1, с. 78].

Висновки.

Концепція державного суверенітету потребує своєї модернізації шляхом інтеграції класичних та нових інформаційних правомочностей держави, характерних для глобалізованого інформаційного світу. Інформаційний суверенітет не є самостійною категорією конституційного права, цей термін характеризує специфіку суверенних правомочностей держави у глобальному інформаційному просторі щодо самостійного формування національної інформаційної політики та забезпечення національної

безпеки. Наявність інформаційного суверенітету дає можливості державі реалізовувати свої національні інтереси та захищати їх від негативного впливу зовнішніх та внутрішніх факторів за допомогою сучасних інформаційних технологій та поширення її юрисдикції над ІКТ інфраструктурою, що розташована на її території. Неналежне забезпечення матеріально-технічної та правової бази інформаційного суверенітету призводить до поступової "девальвації" державного суверенітету, про що яскраво свідчить досвід країн сучасного глобалізованого інформаційного світу, у тому числі і досвід України, яка програє сьогодні інформаційну війну країні-агресору – Російській Федерації. Удосконалення механізму правового регулювання діяльності держави в інформаційній сфері має здійснюватися на підставі науково обґрунтованої концепції конституційно-правової політики, питаннями якої є безпосередньо суверенноздатність Української держави як в межах її матеріальних, так й інформаційних територіальних просторів.

Використана література

1. Казакова Н.Ф., Щербина Ю.В., Фразе-Фразенко О.О. Проблеми безпеки сучасних кіберфізичних систем: матеріали Всеукраїнської науково-практичної конференції *Кібербезпека в Україні: правові та організаційні питання*, м. Одеса, 17 лист.2017 р. Одеса: Одеський державний університет внутрішніх справ, 2017. С. 77-78. URL : http://dspace.oduvs.eduua/handle/123456789/500

2. Кубальський В.Н. Поняття державного суверенітету в міжнародному праві. *Актуальні проблеми міжнародних відносин.* 2017. Вип. 132. С. 85-96. URL: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/3177/2852

3. National Cyber Strategy of the United States of America. September, 2018. 29 p. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

4. Бжезінський З. Вибір. Світове панування чи світове лідерство. Київ: Вид. дім "Києво-Могилянська академія", 2006. 204 с.

5. Wenxiang Gong. Information Sovereignty. Reviewed. *Intercultural Communication Studies*. 2005. Volume XIV, Issue 1. P. 119-135. URL: https://web.uri.edu/iaics/files/10-Wenxiang-Gong.pdf

6. Державний суверенітет в умовах європейської інтеграції: монографія / за ред. Ю.П. Битяка, І.В. Яковюка. Київ: Ред. журн. "Право України", 2012. 336 с.

7. Тернавська В.М. Суверенноздатність держави в умовах глобалізаційних процесів: матеріали міжнар. наук.-практ. конф. *Сучасні проблеми правового, економічного та соціального розвитку держави*, м. Харків, 30 лист. 2018 р. Харків: Харків. нац. ун-т. внутр. справ., 2018. С. 72-74. URL: http://univd.edu.ua/uk/dir/1957

8. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

9. Куян І.А. "Суверенітет" як базова категорія інститутів і принципів конституційного права України. *Альманах права.* 2012. Вип. 3. С. 384-388.

10. Молдован В.В., Мелащенко В.Ф. Конституційне право: опорні конспекти: навч. посібник для студентів юрид. вузів та факультетів. Київ: Юмана, 1996. 272 с.

11. Конституційне право України: підручник / за заг. ред. проф. Федоренко В.Л. 3-е вид. перероб. і доопр. Київ: КНТ, Видавництво Ліра-К, 2011. 532 с.

12. Декларація про державний суверенітет України від 16.07.90 р. № 55-XII. *Відомості Верховної Ради УРСР.* 1990. № 31. Ст. 429.

13. Corn Gary, Taylor Robert. Sovereignty in the Age of Cyber. *AJIL Unbound.* Published online by Cambridge University Press: 2017. Vol. 111. P. 207-212. URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70

14. Солодка О.М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право.* № 4(35)/2020. С. 39-46.

15. John Naisbitt. Megatrends: Ten New Directions Transforming Our Lives. New York: Warner Books, Inc., 1982. 290 p.

16. Руководящие принципы по использованию вещания через спутники для свободного распространения информации, развития образования и расширения культурных обменов: Декларация Генеральной конференция ООН по вопросам образования, науки и культуры от 15 ноября 1972 года. URL: https://zakon.rada.gov.ua/laws/show/995_388#Text

17. Радутний О.Е. Ілюзія та реальність інформаційного суверенітету. *Інформація і право.* № 4(35)/2020. С. 22-38.

18. Задерейко О.В. Троянський О.В., Чанишев Р.І. Концептуальні основи захисту інформаційного суверенітету України: монографія. Одеса: Фенікс, 2018. 112 с.

19. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискур. *Інформація і право.* № 1(32)/2020. С. 80-87.

20. Олійник О. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України. *Наукові записки Інституту законодавства Верховної Ради України.* 2015. № 1. С. 54-59.

21. Положення про Міністерство культури та інформаційної політики України: Постанова Кабінету Міністрів України від 16.10.19 р. № 885. *Урядовий кур'єр.* № 208. – (31.10.2019 р.).

22. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. URL: https://ips.ligazakon.net/document/view/t265700?an=305&ed=2004_05_11

23. Про Національну програму інформатизації: Закон України від 04.02.98 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 181.

24. Про діяльність Кабінету Міністрів України, інших органів державної влади щодо забезпечення свободи слова, задоволення інформаційних потреб суспільства та розвитку інформаційної сфери в Україні: Постанова Верховної Ради України від 16.02.99 р. № 430-XIV. Відомості Верховної Ради України. 1999. № 16. Ст. 99.

25. Про інформацію: Закон України від 02.10.92 р. № 2657-XII (в редакції від 13.01.11 р. № 2938-VI). *Відомості Верховної Ради України*. 2011. № 32. Ст. 313.

26. Про науково-технічну інформацію: Закон України від 25.06.93 р. № 3322-XII. *Відомості Верховної Ради України*. 2011. № 33. Ст. 345.

27. Висновок експертів Ради Європи щодо проекту закону про інформацію. URL: https://helsinki.org.ua/2007/03/vysnovok-ekspertiv-rady-evropy-schodo-proektu-zakonu-pro-informa tsiyu

28. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеей ООН від 5 декабря 2018 года A/RES/73/27. URL: https://undocs.org/ru/A/RES/73/27

29. Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / general editor Michael S. Schmitt. New York: Cambridge University Press, 2013. 215 p. URL: http://csef.ru/media/articles/3990/3990.pdf

30. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право.* № 3(12)/2014. С. 102-112.

31. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

32. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України": Указ Президента України від 25.02.17 р. № 47/2017. *Урядовий кур'єрю.* № 38. (28.02.2017 р.).

33. Про внесення змін до законів України щодо інформаційної безпеки: проект закону України від 26.11.18 р. № 9340. URL : http://search.ligazakon.ua/l_doc2.nsf/link1/JH77G00A.html

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

35. Хлапонін Ю.І, Тернавська В.М. Кібербезпека як засіб забезпечення інформаційного суверенітету держави: техніко-юридичний аналіз: збірник тез наукових доповідей *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем* (SITS' 2021). Миколаїв-Коблево: 2021. С. 47-49. URL: http://bit.nau.edu.ua/wp-content/uploads/2021/07/Zbirnyk-tez-Koble vo-2021.pdf

36. Калюжний Р.А., Баєв О.О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика.* № 4/(24).2009. С. 5-12.

37. Задорожня Л. До питання огляду законодавства в інформаційній сфері. *Правова інформатика.* № 3/2004. С. 20-25.

38. Бєлєвцева В.В. До питання застосування правових режимів забезпечення кібербезпеки в Україні. *Інформація і право.* № 4(35)/2020. С. 106-112.

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

УДК 177.9:340.12

КАЗАЦЬКИЙ В.Д., аспірант кафедри філософії Національного юридичного університету імені Ярослава Мудрого.

ПЕРШОДЖЕРЕЛА ІДЕЇ ПРАВ І СВОБОД ЛЮДИНИ: ВІД АНТИЧНОСТІ ДО ВІДРОДЖЕННЯ

Анотація. *У статті показано, що ідея прав людини має давнє коріння та переплітається з домодерними доктринами природного права Стародавньої Греції та Стародавнього Риму. Обґрунтовано, що в контексті історичного становлення ідей правового регулювання суспільних відносин, прав і свобод людини простежується певний змістовий зв'язок, логіка наступності та момент розвитку. Виявлені базові поняття теорії прав і свобод людини: людина, держава, право, закон.*

Ключові слова: *права людини, свобода, справедливість, суспільство, держава.*

Summary. *The article describes that the idea of human rights has ancient roots and is intertwined with the pre-modern doctrines of natural law of Ancient Greece and Ancient Rome. It is argued that in the context of the historical formation of the ideas of legal regulation of social relations, human rights and freedoms, there are certain connection, logic of succession and the moment of development. The main concepts of the theory of human rights and freedoms are revealed: human, state, right, law.*

Keywords: *human rights, freedom, justice, society, state.*

Аннотация. *В статье показано, что идея прав человека имеет древние корни и переплетается с домодерными доктринами естественного права Древней Греции и Древнего Рима. Обосновано, что в контексте исторического становления идей правового регулирования общественных отношений, прав и свобод человека прослеживается определенная содержательная связь, логика преемственности и момент развития. Выявлены базовые понятия теории прав и свобод человека: человек, государство, право, закон.*

Ключевые слова: *права человека, свобода, справедливость, общество, государство.*

Постановка проблеми. Терміни "права людини" та "свобода" в їхньому соціальному значенні набули сьогодні якнайповнішого поширення у суспільному житті, політиці, в юриспруденції, конституціях та інших нормативних актах, у мистецтві, публіцистиці та художній літературі. "Свобода" та "права людини" – неодмінні атрибути у риториці державних діячів, у молодіжній субкультурі.

Права людини окреслюють простір, який забезпечує кожній людині умови її самореалізації, тобто простір її особистісної автономії. Вони є тими моральними критеріями, якими має керуватися правопорядок. За своїм статусом права людини виступають як незалежні стандарти для критики законів та інших політико-правових інститутів, тобто як критерії легітимації.

Права людини – це, передусім, моральні права, які має кожна особа у світі просто лише завдяки тому, що він або вона є людиною. Вимагаючи дотримання наших прав людини, ми морально вимагаємо, зазвичай від держави, не робити чогось, тому що це є втручанням у нашу особисту сферу, попранням нашої особистої гідності.

Одного декларування прав людини недостатньо для їх забезпечення та виконання. Тому держава повинна ще й гарантувати забезпечення та захист прав та свобод, тобто, створити таку систему соціально-економічних, політичних та юридичних умов, засобів та способів, які забезпечують їх фактичну реалізацію, охорону та захист.

Для адекватного сучасним реаліям забезпечення прав і свобод людини конче необхідна їх філософсько-правова рефлексія, яка обов'язково повинна опиратися на історичні традиції.

Результати аналізу наукових джерел свідчать, що проблемі прав людини присвячено велику кількість наукових доробків. Разом з тим, залишається дещо поза увагою історичний контекст цієї проблеми, особливо з точки зору усвідомлення першоджерел її філософсько-правового аналізу. Відтак, є усі підстави вважати, що без такого звернення до першоджерел сучасне постмодерне бачення проблеми прав і свобод людини буде неповним.

Метою статті є оцінка поглядів мислителів минулого на права і свободи людини у історичному проміжку "Античність – Відродження", який є визначальним для подальшого розвитку філософсько-правових ідей прав та свобод людини.

Виклад основного матеріалу. Сам термін "права людини" виник порівняно недавно. Його стали вживати лише після Другої світової війни, із виникненням Організації Об'єднаних Націй. Цим новим терміном замінили інші – "природні права" та "права людей", оскільки концепція природного права, із якою він тісно пов'язаний, була піддана критиці. А отже, ідея прав людини має давнє коріння та переплітається з домодерними доктринами природного права Стародавньої Греції та Стародавнього Риму. Почасти елліністичний стоїцизм відіграв велику роль у формуванні та розповсюдженні римського права, яке, можна сказати, передбачало існування природного права [1, с. 13].

Найбільшим відкриттям античного часу є поняття "певної рівної міри". Як право взагалі, так і права окремих громадян неможливі без загальної норми поведінки, що виражає однакову для всіх суб'єктів міру дозволеного й забороненого, рівну міру свободи. Там, де немає такої рівності, немає й права. У цьому плані слід відзначити низку відомих висловів великих мудреців Стародавньої Греції про необхідність дотримуватися певної "міри" і "середини" у всіх справах і вчинках: "Середня дорога є найкращою" (Клеобул), "Нічого над міру" (Солон) та ін.

Пошук відповіді питання про об'єктивну норму справедливості і права було продовжено піфагорійцями (VI – V ст. до н.е.). Піфагорійці сформулювали дуже важливе для наступних уявлень про природні права людини положення про те, що "справедливе полягає у відплаті іншому рівним". Новизна і значущість піфагорійського погляду полягала у тому, що під поняттями "належна міра" і "справедливість" вони побачили відому числову пропорцію, тобто, деяку рівність. Це відіграло важливу роль у формуванні ідеї правової рівності людей.

Становлення теоретичних концепцій прав і прав людини у Стародавній Греції розвивалося в руслі пошуків природно-правових основ полісу та його законів. Ідея природної рівності та свободи всіх людей була вперше висловлена софістами (V – IV ст. до н.е.). Базовий принцип поглядів софістів був сформульований Протагором: людина є мірою всіх речей. Такий розгляд людини як мірила всього різко розходився з традиційними уявленнями про значущість саме божественного, а не людського начала як масштабу і міри. Основна демократична ідея Протагора полягає у тому, що існування держави передбачає рівну причетність усіх її членів до людської чесноти, до якої він відносить справедливість, розважливість і благочестя. При цьому, він посилався на те, що у всіх людей ті ж самі природні потреби. Нерівність людей виникає з людських законів, оскільки вони довільні та штучні [2, с. 320-321].

Початок понятійно-теоретичного дослідження (за допомогою загальних понять) об'єктивної розумної природи полісу та його законів пов'язане з ім'ям Сократа. Він

стверджував, що лише на шляху необхідності дотримання всіма розумних і справедливих законів полісу можна досягти свободи.

Раціоналістичні ідеї Сократа були розвинені його учнем Платоном. Характеризуючи справедливість у ідеальній державі, Платон вказував, що кожному належить займатися своєю справою. Справедливість полягає також у тому, щоб ніхто не захоплював чужого і не втрачав свого.

Відповідно до вчення Платона, справедливість передбачає "належну міру", тобто певну рівність. При цьому, він розрізняє "геометричну рівність" (гідність і чесноти) та "арифметичну рівність" (рівність міри, ваги та числа). Платон зауважує, що для нерівних рівне стало б нерівним, якби не дотримувалася "рівна міра".

Ці положення надалі були розвинені у вченні Аристотеля про два види справедливості: зрівнюючої та розподільчої. Розподільча справедливість – це прояв справедливості при розподілі всього того, що може бути поділено між членами суспільства (влада, почесть тощо). Зрівнювальна справедливість застосовується у сфері цивільно-правових угод. Принципом розподільчої справедливості, за Аристотелем, виступає розподіл загальних для усіх громадян благ гідно, тобто пропорційно до їх вкладу чи внеску до спільної справи. Право у цілому і права індивіда, за Аристотелем, носять виключно політичний характер і можливі тільки в державі (тобто в умовах полісу). У державі з деспотичною організацією влади, зауважує Аристотель, про право можна говорити лише умовно. Природні права людини, згідно з Аристотелем, реально існують лише як права політичного суб'єкта, тобто громадянина полісу. Особливо слід відзначити захист Аристотелем (у полеміці проти Платона) права особи на приватну власність та індивідуальну сім'ю.

Уявлення про державу та право як договір про загальнокорисне для забезпечення індивідуальної свободи та взаємної безпеки людей розвинув Епікур. Свобода людини, згідно з Епікуром, це її відповідальність за розумний вибір свого способу життя. Сфера людської свободи – це сфера відповідальності людини за себе. Головна мета держави полягає, за Епікуром, у забезпеченні взаємної безпеки людей, не заподіянні ними один одному шкоди. "Справедливість, що походить від природи, писав Епікур, є договір про корисне з метою не шкодити один одному і не терпіти шкоди" [3, с. 217]. Договірний характер держави і права у вченні Епікура означає, що вони не надані природою ззовні та сліпо нав'язані людям, а є їхнім власним самовизначенням, людськими встановленнями.

На переконання Епікура, справедливість має договірний характер, оскільки вона є чимось корисним у відносинах людей один з одним. У концепції Епікура справедливість, у світлі її співвідношення із законом, є природним правом із змінним (залежно від місця, часу та обставин) змістом, яким є мінлива загальна користь взаємного спілкування. Тут справедливість виступає як критерій відповідності закону змінним потребам людей і водночас їх змінним природним уявленням про саму справедливість. Епікурійське договірне тлумачення держави і права передбачає рівність, свободу і незалежність людей – членів договірної спільноти, і по суті є філософсько-правовою концепцією правового індивідуалізму. Від договірно-правової концепції Епікура тягнеться важлива лінія зв'язку до ідей суспільного договору Нового часу.

Природничо-правова ідея давньогрецьких мислителів про свободу, права та рівність усіх людей отримали подальший розвиток у Стародавньому Римі. Вона була виведена за полісні та етнічні рамки та поширена на всіх представників людського роду як співгромадян єдиної космополітичної держави. Римські стоїки (Сенека, Епіктет, Марк Аврелій) обґрунтували універсальну концепцію природного права з

космополітичних позицій, згідно з якою всі люди – громадяни єдиної світової держави, а людина – громадянин Всесвіту.

Марк Аврелій розвивав уявлення про "державу з рівними для всіх законами, керовану відповідно до рівності й рівноправності всіх, і царя, який насамперед шанує свободу підданих" [2, с. 519]. Якщо всі люди розумні істоти, припускає Марк Аврелій, "то і розум, який наказує, що робити і чого не робити, теж буде загальним; якщо так, то закон загальний; якщо так, то ми є громадянами. Отже, ми причетні до якогось цивільного устрою, а світ подібний до Граду. Бо хто міг би вказати на якийсь інший загальний устрій, до якого був би причетний весь рід людський?" [2, с. 520].

З позицій концепції природного права філософське вчення про державу, закон і права людей дуже ґрунтовно розробив Цицерон. В основі права, згідно з Цицероном, лежить властива природі справедливість. Причому справедливість трактується ним як вічна, незмінна і невід'ємна властивість природи в цілому, включаючи і людську природу. Цицерон визначає природне право як істинний, розумний закон, який відповідає природі, що поширюється на всіх людей. Значення справедливості, що лежить в основі права, у плані прав людини полягає у тому, що вона віддає кожному своє і зберігає рівність між усіма. При цьому йдеться саме про правову рівність людей, а не про зрівнювання їх майнового становища.

Природне право, згідно з Цицероном, виникло набагато раніше, аніж будь-який писаний закон, аніж була заснована будь-яка держава. Право, за Цицероном, встановлюється природою, а не людськими рішеннями і постановами. Відповідність чи невідповідність людських законів природі (природному праву) постає як критерій і мірило їх справедливості [4].

Вагомий внесок у розвиток уявлень про права людини внесли римські юристи (Ульпіан, Юліан, Модестин та ін.). Важливе значення в цьому плані мали розроблені ними положення про суб'єкт права, про правові статуси людей, про свободу людей за природним правом, про справедливе і несправедливе право тощо. Вони сприяли формуванню більш чітких поглядів на права людини в контексті систематичного наукового вчення про право і державу, про поділ природного та позитивного права, правовий характер взаємовідносин між індивідом і державою, співвідношення права особи та компетенції органу влади, державно-правових засобів та способи захисту прав людини [5 – 6].

Відповідно до римської юриспруденції, держава в її відносинах з індивідом стоїть не поза і над правопорядком, а всередині його як складова, якій притаманні всі основні властивості права взагалі [7 – 8]. Іншими словами, вже розглядався взаємозв'язок держави та особистості як правовідносини між рівними суб'єктами права.

Представники низки юридичних шкіл, що виникли у X – XI ст. у Римі та інших містах, у своєму праворозумінні орієнтувалися на ідею правової справедливості та пов'язані з нею природно-правові уявлення та концепції. Як основний принцип права визначається рівність, яка передбачає і виражає рівну справедливість і справедливу рівність усіх суб'єктів права. Саме на цьому принципі базувалася ідея римського праворозуміння. Справедливість є постійна воля надавати кожному його право. Трактування справедливості як необхідної властивості самого права означало, що всі норми, що суперечать вимогам принципу природно-правової справедливості, не можуть мати юридичної сили [9 – 10].

Юридична конкретизація смислу й значення уявлень про природно-правову справедливість, включаючи й відповідне протиставлення справедливого права несправедливому стала важливою віхою в науковому осмисленні проблем правосуб'єктності індивіда і заклала необхідні теоретичні основи для подальшого розвитку положень про природні права і свободи людини.

Ранні християни, апелюючи до божественного “закону свободи”, адаптували для своїх цілей природничу ідею рівності людей [11, с. 79]. Західне християнство, на відміну від східного, багато в чому злилося з державою, ставши державною релігією і вступивши у конкуренцію зі світською владою (“вчення про два мечі”), сприяло формуванню людської особистості – індивіда, здатного зберігати та розвивати ініціативу та свободу.

Звернення до свободи людини є у різних християнських проповідях, у тому числі константинопольського єпископа Іоанна, згодом прозваного Златоустом. Він навчав: “Цар примушує, священик переконує. Пастирі повинні звертатися до свободи та волі людини” [12, с. 9].

Небезпідставно вважається, що саме церква, а не держава заклала підвалини західної традиції права. Розкол Римської Імперії на Західну та Східну (кінець V ст.), поділ церкви на римсько-католицьку церкву на Заході з центром у Римі та православну – на Сході з центром у Константинополі поглибили нерівномірність етапів юридизації свободи у західних та східних європейських народів [13, с. 313].

Низка середньовічних мислителів (Марсилій Падуанський, Генрі Брактон, Філіп де Бомануар та ін.) захищали ідею свободи, рівності всіх перед законом. Характерною у цьому плані є антикріпосницька позиція відомого французького юриста XIII ст. Бомануара, який стверджував, що кожна людина є вільною [14, с. 21].

Нове звучання та сенс ідеї природно-правової рівності та свободи всіх людей отримали у християнстві. Зародившись в епоху рабовласництва, християнство виступило як релігія свободи і відіграло важливу роль у процесі становлення універсальних понять прав людини.

Із попередньої іудаїстської та античної традицій християнство запозичило золоте правило справедливої поведінки кожної людини, яке полягає у тому, щоб вчиняти з людьми так, як бажаєте, щоб чинили з вами. Це правило нормативної регуляції має на увазі загальну і рівну для всіх людей норму поведінки, тобто, по суті нормативну конкретизацію принципу правової рівності в різноманітних сферах людських взаємовідносин.

Подальшу розробку ідея рівності отримала у політико-правових і філософських вченнях низки християнських мислителів. Помітну роль у цьому плані зіграв Фома Аквінський, який розробив християнську доктрину права і держави під впливом вчення Аристотеля про етику і політику, політичну природу людини, природне і волевстановлене право, правову рівність вільних індивідів – членів політичного (державного) спілкування.

У дусі природничо-правових ідей Фома Аквінський стверджував, що мета держави – це загальне благо її членів, забезпечення умов для їх розумного та гідного життя. При цьому він засуджував тиранію (тобто правління на користь самого правителя в умовах беззаконня) і обґрунтовував право народу на повалення такого ладу. Фома Аквінський вважав, що тільки за своєю сутністю будь-яка влада є божественною, тоді як за своїм походженням і використанням та чи інша форма влади (наприклад, тиранія) може суперечити своїй сутності і не відповідати своєму призначенню [15 – 16] .

Для формування християнської концепції прав людини істотне значення мало вчення Фоми Аквінського про природний закон, який наказував, серед інших заповідей і положень, усім людям поважати гідність кожної людини. Дане положення про божественну за своїм першоджерелом людську гідність всіх людей і природне право кожної людини на гідність є великим внеском Фоми Аквінського і в цілому християнського гуманізму в концепцію невідчужуваних природних прав людини [17].

Слід зазначити, що ідея рівності людей, яка виникла у стародавні часи, не зникла в середні віки, вона продовжувала розвиватися у різних формах та напрямках, у творчості світських та релігійних авторів.

Розвиток філософії за доби Відродження визначався впливом низки чинників [18]. По-перше, впливом передової античної філософської думки (Сократ, Епікур та ін.). По-друге, наростаючим впливом утверджуваного капіталістичного ладу на суспільну свідомість, культуру і мораль суспільства. Дуже важливою характеристикою епохи Відродження був антропоцентризм. Він є типом філософствування, суттю якого є сприйняття людини як певного центру світу, "вінця" еволюції природи. Вираженням такої світоглядної установки став гуманізм – ідейна течія, що зародилася в італійських містах, яка проголосила людину вищою цінністю і метою суспільства і сформувала поняття особистості. Звернені до соціальних та політичних процесів, погляди ренесансних мислителів поглибили та розширили уявлення про громадське життя. У цих вченнях наголошувалося на необхідності і можливість перетворення суспільства на користь більш розумного та гармонійного існування людини. У їх рамках було сформульовано чимало ідей, які здійснили великий вплив на наступну історію.

Найбільшим представником соціально-філософської думки епохи Відродження є Ніколо Макіавеллі. Основною в його творах ("Государ" та ін.) стала тема держави та суспільного устрою. У рамках цієї теми Макіавеллі розвинув тезу про егоїстичну природу людини як глибинну основу мотивації її поведінки у суспільному житті. На переконання Макіавеллі, найдієвішим стимулом для всіх людських вчинків є інтерес. Серед безлічі різноманітних інтересів провідну роль відіграє майновий інтерес: прагнення придбати та зберегти власність. Макіавеллі вважав, що люди швидше пробачать смерть батька, аніж втрату майна. Мислитель писав: "Щоб уникнути ненависті, государю необхідно утримуватися від зазіхань на майно громадян і підданих ...Навіть коли вважає за потрібне позбавити когось життя, він може зробити це, якщо є слушне обґрунтування і очевидна причина, але він повинен остерігатися зазіхати на чуже добро, бо люди швидше пробачать смерть батька, аніж втрату майна" [19, с. 50]. Він був переконаний, що егоїзм людської природи невикорінний, і це вимагає створення в суспільстві такої організації, яка б змогла жорстко (за допомогою примушення) регулювати взаємини між людьми.

Таким інструментом була держава як центр влади і осередок сили в громадському організмі. Походження її є природним, а не божественним. Макіавеллі був прихильником сильної централізованої держави з наділенням її правителя необмеженими повноваженнями. Макіавеллі вважав, що "...государ, якщо він хоче утримати у покорі підданих, не повинен зважати на звинувачення в жорстокості. Вчинивши кілька розправ, він виявить більше милосердя, аніж ті, хто надміру його потурає безладу. Бо від безладу, який породжує грабежі та вбивства, страждає все населення, тоді як від покарань, накладених государем, страждають лише окремі особи" [19, с. 49].

Тему сильної централізованої держави також розкривав у творчості французький мислитель Жан Боден. Він розглядав державу як певну співдружність, яка заснована на приватній власності і виконує низку соціальних функцій (охорона власності, захист сім'ї та ін.) [20]. Цей інститут покликаний очолювати монарх як найвище джерело влади.

Ж. Боден був автором теорії державного суверенітету. Він вважав, що влада в державі має бути неподільна, абсолютна і не залежить від жодних законів та інших установлень. Однак при цьому государ, на переконання Ж. Бодена, все ж таки не в праві вторгатися в сім'ю і привласнювати собі чужу власність (це було б тиранією). Сім'я і

приватна власність є священними і непорушними підвалинами суспільства, над якими держава не владна.

Отже, ренесансні автори виходили з того, що кожна людина від народження (а не від Бога) наділена низкою фундаментальних прав, які уможливлюють її самостійне та вільне існування у суспільстві. Індивід – це хіба що атом, основа всього всесвіту, якій природні права дають можливість самовизначення у суспільстві. До таких прав було віднесено: декларацію про життя, на володіння майном, на свободу переконань, особисту безпеку. Всі вони природні у тому сенсі, що дані індивіду від народження і тому ніхто не має права вилучити їх, у тому числі і сама держава.

Ідея природних прав людини зіграла велику прогресивну роль в ідеологічній підготовці перших буржуазних революцій XVII століття в Європі.

Висновки.

Таким чином, ми бачимо, що в контексті історичного становлення ідей правового регулювання суспільних відносин, прав і свобод людини простежується певний змістовий зв'язок, логіка наступності та момент розвитку.

З наведеного вище можна виявити базові (ключові) поняття теорії права і свободи людини. Такими є: людина, держава, право та закон. Саме ці поняття і утворюють основу аналізованої теорії, яка полягає у розкритті сутнісного змісту даних понять, природи їх взаємовідносин та визначенні ступеня значущості кожного поняття у їх співвідношенні.

Використана література

1. Права людини: Концепції, підходи, реалізація / пер. з англ. Київ: Ай Бі, 2003. 263 с.
2. Антология мировой философии: в 4 т. Т. 1. Ч. 1. Философия древности и средневековья. Москва: Мысль, 1969. 575 с.
3. Материалисты древней Греции: собрание текстов Гераклита, Демокрита и Эпикура / общ. ред. и вступ. ст. проф. М.А. Дынника. Москва: Госполитиздат, 1955. 239 с.
4. Цицерон М. О государстве. О законах / пер. с лат. В.О. Горенштейна. Москва: Академический проект, 2016. 249 с.
5. Турянський Ю. Генезис прав людини у період античності. *Історико-правовий часопис*. 2019. № 2. С. 39-42.
6. Турянський Ю. Становлення та розвиток прав людини в античні часи. *Вісник Національного університету "Львівська політехніка". Серія: Юридичні науки*. 2019. Вип. 23. С. 39-44.
7. Вовк В.М. Бівалентність римської правової реальності: монографія. Полтава, 2011. 348 с.
8. Гуренко-Вайцман М.М. "Людський зміст" римського права. *Юридичний вісник. Повітряне і космічне право*. 2011. № 2. С. 132-133.
9. Бабич І.Г. Принцип справедливості – характеристика у римському приватному праві. *Часопис цивілістики*. 2017. Вип. 25. С. 6-10.
10. Олійник О.С. Особливості реалізації принципів добросовісності, розумності та справедливості в римському приватному праві. *Актуальні проблеми вдосконалення чинного законодавства України*. 2018. Вип. 48. С. 224-235.
11. Левакин И.В. Краткий очерк юридизации свободы в Европе. *Государство и право*. 2016. № 11. С. 77-85.
12. Берман Г. Западная традиция права: эпоха формирования. 2-е изд. Москва: Инфра-М, 1998. 624 с.
13. Лапаева В.В. Типы правопонимания: правовая теория и практика: монография. Москва: Российская академия правосудия, 2012. 580 с.
14. Дергачев И.В. Философские аспекты проблемы прав и свобод человека: дис. ...канд. филос. наук. Смоленск, 2004. 130 с.

15. Гафаров Т.Х. К вопросу о некоторых особенностях понимания правовой культуры в средневековой философии. URL: https://cyberleninka.ru/article/n/k-voprosu-o-nekotoryh-osobennostyah-ponimaniya-pravovoy-kultury-v-srednevekovoy-filosofii/viewer (дата звернення: 02.11.2021).

16. Субботин Ю.В. Развитие идей естественного права в средневековой философии. URL: https://cyberleninka.ru/article/n/razvitie-idey-estestvennogo-prava-v-srednevekovoy-filosofii/viewer (дата звернення: 02.11.2021).

17. Батиев Л.В. Закон и право в философии Фомы Аквинского. URL: https://cyberleninka.ru/article/n/zakon-i-blagodat-v-summe-teologii-fomy-akvinskogo (дата звернення: 02.11.2021).

18. Хмелевська Н.А. Історико-філософський огляд понять "право", "природні права" та "права людини". *Гуманітарний часопис*. 2011. № 3. С. 82-90.

19. Макиавелли Н. Государь. Москва: Планета, 1990. 80 с.

20. Боден Ж. Метод легкого чтения историй: в 3-х т. Т. 2: Об устройстве государств. Москва: Издат. дом Высшей школы экономики, 2021. 559 с.

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

Інформаційна і національна безпека

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.

ОГЛЯД НОВЕЛ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ (НА ПРИКЛАДІ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ НА 2021 – 2025 РОКИ)

Анотація. *Проаналізовано положення оновленої Стратегії кібербезпеки України. Визначено результативність Стратегії кібербезпеки України 2016 року. Досліджено питання організаційно-правових засад забезпечення кібербезпеки. Розглянуто складові національної системи кібербезпеки. Деталізовано практичну складову Стратегії кібербезпеки України та пріоритетні завдання сектору безпеки і оборони. Висвітлено стратегічні засади забезпечення кібербезпеки в Японії. Узагальнено перспективи реалізації Стратегії кібербезпеки України в умовах сучасного геополітичного протиборства.*

Ключові слова: *національна система кібербезпеки, стратегічне планування, кіберзагроза, кіберпростір, сектор безпеки і оборони, кібератака.*

Summary. *The provisions of the updated Cyber Security Strategy of Ukraine are analyzed. The effectiveness of the Cyber Security Strategy of Ukraine in 2016 has been determined. The issue of organizational and legal bases of cyber security is studied. The components of the national cyber security system are considered. The practical component of the Cyber Security Strategy of Ukraine and the priority tasks of the security and defense sector are detailed. The strategic principles of cyber security in Japan are highlighted. The prospects of implementation of the Cyber Security Strategy of Ukraine in the conditions of modern geopolitical confrontation are generalized.*

Keywords: *national cyber security system, strategic planning, cyber threat, cyberspace, security and defense sector, cyber attack.*

Аннотация. *Проанализированы положения обновленной Стратегии кибербезопасности Украины. Определена результативность Стратегии кибербезопасности Украины 2016 года. Исследованы вопросы организационно-правовых основ обеспечения кибербезопасности. Рассмотрены составляющие национальной системы кибербезопасности. Детализирована практическая составляющая Стратегии кибербезопасности Украины и приоритетные задачи сектора безопасности и обороны. Освещены стратегические основы обеспечения кибербезопасности Японии. Обобщены перспективы реализации Стратегии кибербезопасности Украины в условиях современного геополитического противостояния.*

Ключевые слова: *национальная система кибербезопасности, стратегическое планирование, киберугроза, киберпространство, сектор безопасности и обороны, кибератака.*

Постановка проблеми. Світ активно входить в нову епоху цифровізації. XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та потенційними ризиками, з якими стикається світова спільнота внаслідок масштабного впровадження новітніх технологій, зокрема їх використання у кіберпросторі. Значення кіберпростору в розвитку цивілізації

повсякденно зростає і поступово перетворюється на одну зі сфер міждержавного протиборства. Кіберпростір разом з іншими фізичними просторами у світовому масштабі визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Сучасна геополітика постійно стимулює діяльність політичного керівництва країн, спрямовану на пошук ефективної моделі оперативного управління кібербезпекою, підвищення ролі і значення реалізації заходів щодо розбудови її національної системи.

За оцінками експертів у сфері кібербезпеки, у переважній більшості провідних країн світу спостерігається стійка тенденція до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури. Загальновідомо, що основними цілями кібератак стають об'єкти стратегічної інфраструктури країн (ядерна, транспортна, хімічна чи будь-яка інша промисловість, системи життєзабезпечення великих мегаполісів, фінансова, продовольча, енергетична національні системи, транспортні мережі, діяльність уряду, правоохоронних органів, Збройних Сил тощо). Посягання здійснюються через інформаційно-телекомунікаційні системи, особливо автоматизовані системи управління, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади. З огляду на це, підвищення рівня забезпечення кібербезпеки неможливо уявити без чітко спланованих спільних дій та заходів відповідальних суб'єктів, які мають бути синхронізовані та здійснюватися за єдиним стратегічним вектором розвитку національної системи кібербезпеки.

Саме тому кібербезпека визнана у більшості країн світу важливою складовою національної безпеки, забезпечення якої неможливе без формування і функціонування загальнодержавної системи та скоординованої й виваженої державної політики у сфері кібербезпеки, що ґрунтується на таких засадах, як повага до норм і принципів міжнародного права, захист фундаментальних цінностей, визначених чинним законодавством, забезпечення національних пріоритетних інтересів у кіберпросторі. За таких умов, загальною усталеною практикою країн світу стає чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки у кіберпросторі у форматі документів стратегічного планування та змісту. Будь-який стратегічний документ кібербезпекової тематики державного рівня має враховувати не тільки внутрішньополітичні аспекти, але й сучасні світові тренди в глобальному кіберсередовищі як вагомі фактори впливу на розбудову національної системи кібербезпеки будь-якої держави світу.

Загальноприйнятим світовим трендом є той факт, що схвалені національні стратегії кібербезпеки відображають політичну волю та свідоме прагнення країн світу максимально забезпечити власну кібербезпеку, попередити кіберзлочинність як на національному так і міжнародному рівнях, максимально запобігти несанкціонованому витоку даних та конфіденційної інформації. Прогнозування розвитку безпекового середовища навколо України на період до 2025 року свідчить про те, що суб'єктам забезпечення національної безпеки держави необхідно терміново вжити запобіжних заходів для захисту національних інтересів в інформаційному просторі, невід'ємною частиною якого є саме кіберпростір. За таких умов огляд новел вітчизняного законодавства і зокрема Стратегії кібербезпеки України на 2021 – 2025 роки, є актуальним та доцільним як з позиції теорії, так і практики.

Результати аналізу наукових публікацій. Розгляд актуальних питань розбудови національної системи кібербезпеки та дослідження базових положень Стратегії

кібербезпеки України здійснювали у своїх наукових працях: І. Діордиця [1], К. Галинська [2], І. Доронін [3], В. Петров [4], Н. Ткачук [5], В. Шеломенцев [6]. Проте аналіз положень оновленої Стратегії кібербезпеки України, схваленої Указом Президента України від 26 серпня 2021 року [7] не здійснювався, що дозволяє констатувати практичну значущість та актуальність тематичного спрямування цієї наукової публікації.

Метою статті є висвітлення на підставі аналізу основних позицій оновленої Стратегії кібербезпеки України та заходів щодо її практичної реалізації в умовах поширення гібридних загроз, переважно російського походження.

Виклад основного матеріалу. Як правило, у стратегіях викладаються базові принципи, на яких ґрунтується стратегія, деталізовані державні інтереси, які мають бути захищені, визначаються інструменти, що використовуються з метою посування або захисту цих інтересів, окреслюються загрози та проблеми, регламентуються пріоритетні завдання державної політики та обсяг ресурсів, які виділяються для її реалізації. Оновлена Стратегія кібербезпеки України, яка схвалена 26 серпня 2021 року [7], не стала виключенням.

Це вже друга Стратегія кібербезпеки, яка схвалена за останні п’ять років. Уперше на національному рівні Стратегія кібербезпеки як фундаментальний документ держави була схвалена ще у березні 2016 року, проте вона була розрахована на поточних п’ять років та стала першим етапом розвитку національної системи кібербезпеки держави. Схвалення на державному рівні у 2016 році Стратегії кібербезпеки України стало важливим та революційним кроком у запровадженні нових підходів довгострокового планування в цій сфері. Отже, сам факт її прийняття однозначно є позитивним результатом. Проте, враховуючи позитивні здобутки та тенденції, аналіз виконання положень Стратегії кібербезпеки України 2016 року щодо результативності діяльності суб’єктів національної системи кібербезпеки засвідчує недостатню скоординованість таких дій. За результатами експертних оцінок задекларовано, що стан реалізації Стратегії кібербезпеки 2016 року за визначеними показниками не перевищує 40 %. Невирішеними залишилися низка питань оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. У положеннях Стратегії кібербезпеки 2016 року знайшли своє відображення засади створення національної системи кібербезпеки, потужним поштовхом для чого стало перетворення кіберпростору ще на одне поле протистояння і боротьби за незалежність держави, враховуючи сценарії скерованого хаосу, які намагається реалізувати політичне керівництво РФ.

Формування національної системи кібербезпеки передбачало результативність процесів державного управління як сукупності безперервних взаємопов’язаних дій та функцій, здійснюваних органами державної влади, які спрямовані на забезпечення безпеки в кіберпросторі. Тому розбудова національної системи кібербезпеки спрямована передусім на повномасштабне забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, яка досягається шляхом комплексного застосування сукупності організаційно-правових, інформаційних, технічних заходів, що визначаються відповідно до концептів державної політики, а саме: створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; боротьба з кіберзлочинністю та кібертероризмом; зниження рівня вразливості об’єктів кіберзахисту; гарантування повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки; дотримання міжнародних зобов’язань щодо боротьби з кіберзлочинністю та кібертероризмом.

Зрозуміло, що Стратегія кібербезпеки України 2016 року не була позбавлена недоліків та проблемних аспектів.

В контексті порівняння, аналіз положень Стратегії кібербезпеки України 2016 року та досвід її практичного впровадження дав змогу сформулювати проблемні питання, які або ускладнювали, або унеможливлювали її ефективну її реалізацію. Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети або було не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Об'єктивно реалізація Стратегії кібербезпеки України 2016 року була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. На жаль, не були розроблені критерії оцінки стану кібербезпеки – індикатори виконання Стратегії, що ускладнило процес моніторингу її результативності та виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, а також громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади. Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури; не створено модель державно-приватного партнерства [8, с. 117-118].

Стратегія кібербезпеки України на 2021 – 2025 роки як фундаментальний документ національного значення регламентує вектор щодо: подальших кроків розбудови національної системи кібербезпеки в нашій державі; системних заходів щодо надійного захисту національного сегменту кіберпростору; зовнішньополітичної діяльності у сфері посилення кібербезпеки тощо. Загалом Стратегія кібербезпеки України складається з 9 взамопов`язаних розділів та детально визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов задля побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, поточний та перспективний стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

У положеннях оновленої Стратегії кібербезпеки України знайшли своє відображення концептуальні методологічні підходи до подальшого розвитку й удосконалення національної системи кібербезпеки, які базуються на таких пріоритетах: всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України; перманентності заходів з удосконалення законодавства у сфері кібербезпеки; орієнтованості на економічне і соціальне зростання суспільства; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту; визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності; ризик-орієнтованому підході щодо заходів забезпечення кібербезпеки та кіберзахисту; запровадженні механізмів державно-приватного партнерства у сфері кібербезпеки; проактивному підході, що передбачає здійснення випереджувальних

заходів; забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

Нова Стратегія кібербезпеки України деталізує перспективні напрями посилення спроможностей національної системи кібербезпеки. Оскільки забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, то реалізація цього пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Також пріоритетами забезпечення кібербезпеки України визначені: 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. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, які мають бути досягнуті протягом періоду реалізації Стратегії.

За результатами практичної реалізації Стратегії кібербезпеки у співпраці з приватним сектором та із залученням міжнародних партнерів очікується забезпечення: стійкості до кіберзагроз; підвищення здатності державних інституцій, бізнесу і громадян захищати себе та реагувати на кіберзагрози; спроможності до ефективної протидії злочинним діям у кіберпросторі, забезпечення їх швидкого виявлення та розслідування, створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі; розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам.

Своїм супротивником у кіберпросторі Україні слід вважати будь-які державні чи наддержавні утворення, недержавні суб'єкти, дії яких кваліфікуються законами України та/або міжнародно-правовими актами як підготовка або здійснення воєнної агресії та інших протиправних дій в кіберпросторі та через кіберпростір. Основним ворогом для України виступає держава-агресор, яка у кіберпросторі застосовує проти нашої держави весь наявний арсенал сучасних сил та засобів. Антиукраїнська діяльність з боку Російської Федерації проводиться у вигляді інформаційної кампанії, яка включає сукупність комплексних та окремих інформаційних операцій, інформаційних акцій та інших заходів, більшість з яких здійснюється з використанням кіберпростору і містить в собі складову безпосередніх дій в кіберпросторі.

З метою досягнення рівня максимального втручання, РФ використовуються внутрішні чинники, які обмежують потенційні можливості держави з протидії негативному впливу у кіберпросторі, основні з яких наступні: нерозвиненість, моральна і фізична застарілість; уразливість від протиправного впливу існуючої інформаційної інфраструктури (в першу чергу інформаційно-телекомунікаційних мереж та систем) держави, яка використовується в інтересах функціонування критичної інфраструктури, забезпечення безпеки та оборони держави; активне впровадження та використання в державі інформаційних технологій (систем, продуктів) іноземного походження, які не гарантують належного рівня безпеки використання і складно контролюються; ускладненість щодо розмежування військових і цивільних об'єктів критичної інфраструктури держави в кіберпросторі; можливість недержавних суб'єктів та неавторизованих (індивідуальних) користувачів здійснювати протиправні дії у кіберпросторі та проблематичність з їх виявленням; порушення встановленого національним законодавством порядку обміну інформацією з обмеженим доступом у сфері оборони; зниження науково-технічного потенціалу України; недостатнє нормативно-правове регулювання діяльності суб'єктів забезпечення кібербезпеки держави;

недостатність з огляду на зростаючий обсяг завдань як кількісно-якісного складу сил суб'єктів забезпечення кібербезпеки держави, так і кваліфікованих фахівців тощо.

Знайшли своє відображення у положеннях оновленої Стратегії кібербезпеки України такі завдання, як: створення сучасної національної системи забезпечення кібербезпеки держави; організації і забезпечення її розвитку та функціонування в інтересах національної безпеки держави; підготовки до відсічі воєнній агресії в кіберпросторі (підготовки та ведення кібероборони). Основними результатами реалізації Стратегії кібербезпеки має бути створення сприятливих умов для: захисту інтересів України в кіберпросторі; створення відповідних умов для розвитку інформаційного суспільства та розвитку "цифрової" України; підготовки та застосування структур сектору безпеки та оборони в кіберпросторі до виконання завдань за призначенням та безпечного використання ними кіберпросторі.

Практична складова Стратегії кібербезпеки передбачатиме: створення ефективної національної системи кібербезпеки з урахуванням тенденцій зміни безпекового середовища та кращих практик у сфері кібербезпеки провідних країн світу; набуття суб'єктами забезпечення кібербезпеки необхідних спроможностей для виконання завдань за призначенням, створення та розвиток відповідних організаційних структур, їх комплектування, підготовку та всебічне забезпечення; створення передумов для опанування сучасних форм та способів підготовки та проведення заходів забезпечення кібербезпеки; адекватного та завчасного нарощування потужностей щодо підготовки та ведення кібербезпеки (у т. ч. кіберзахисту, кібероборони) відповідно до зростання рівня загроз, особливо в контексті підготовки та здійснення супротивником воєнної агресії в кіберпросторі; вчасного реагування на поточні загрози кібербезпеки шляхом запобігання, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу; створення системи управління забезпеченням кібербезпеки, її інтеграцію в систему державного управління; налагодження співпраці у межах повноважень з суб'єктами забезпечення національної безпеки держави, а також з НАТО, ЄС, державами-партнерами в частині спільного виконання завдань кібербезпеки.

Таким чином, в умовах російської експансійної 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 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.

Зважаючи позитивний досвід розвинених країн, вирішення завдань у сфері кібербезпеки слід реалізовувати через посилення стратегічних функцій національної системи кібербезпеки. Вважається логічним, щоб вони (за досвідом США) корелювалися з функціями, які використовуються у сфері забезпечення національної стійкості, а саме: запобігання (англ. "Prevention") – заходи з завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них; захисту (англ. "Protection") – заходи з забезпечення випереджувального захисту (в першу чергу кіберзахисту) від можливих кібератак (кібервпливу); запобігання та мінімізація загроз (англ. "Mitigation") – заходи з безпосереднього виявлення, відвернення

загрози, зменшення можливих втрат (збитків, пошкоджень) в разі безпосередньої загрози проведення кібератак. За певних умов в межах зазначеного можуть вживатися завчасні (зустрічні) заходи активного кіберзахисту; реагування (англ. "Response") – заходи комплексного реагування на факти загрози (кібератаки тощо) з боку супротивника та відповідне виконання суб'єктами забезпечення кібербезпеки держави впливу на супротивника, у т. ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з одночасним вжиттям заходів з захисту власної інфраструктури, особового складу, ресурсів тощо від впливу ворога; відновлення (англ. "Recovery") – заходи, спрямовані на відновлення інформаційної та іншої інфраструктури, які стали об'єктом кібератак, стабілізацію ситуації та ліквідацію інших негативних наслідків.

Ретельний аналіз положень Стратегії кібербезпеки України на 2021 – 2025 роки дає змогу констатувати, що складовими державного стратегічного планування у сфері забезпечення кібербезпеки є: стратегічний прогноз, стратегічний аналіз, ситуаційне моделювання, оцінка стану забезпечення кібербезпеки. Державне прогнозування – функція державного управління, спрямована на визначення прогнозних показників розвитку держави. Державний стратегічний прогноз у сфері забезпечення кібербезпеки являє собою систему уявлень та знань про можливі кіберзагрози та кіберінциденти. Він дає змогу визначити роль і місце національної системи кібербезпеки в міжнародному кіберпросторі. Як правило, стратегічний прогноз передбачає визначення періодів (етапів) у сфері реалізації запланованих заходів. Стратегічний аналіз, який складає основу системи інформаційно-аналітичного забезпечення суб'єктів забезпечення кібербезпеки, використовується як ефективний засіб для визначення умов та факторів, які сприятимуть підвищенню результативності заходів державної політики у сфері забезпечення кібербезпеки. Оцінка стану забезпечення кібербезпеки в рамках державного стратегічного планування передбачає проведення періодичного огляду національної системи кібербезпеки на підставі розроблених критеріїв та показників, зокрема галузевих індикаторів кібербезпеки, моніторингу потенційних і реальних кіберзагроз та кібератак, визначення поточного й перспективного стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, аудиту кібербезпеки.

Таким чином, у вітчизняній Стратегії кібербезпеки актуалізуються такі тематичні питання, як: побудова ефективної державної моделі, направленої на забезпечення кібербезпеки; визначення дієвого механізму забезпечення кібербезпеки; визначення переліку заходів, яких доцільно вжити з метою розбудови національної системи кібербезпеки; розробка системного та інтегрованого підходу до державного управління ризиками у сфері кібербезпеки, посилення державно-приватного співробітництва у цій площині тощо. Метою Стратегії кібербезпеки є визначення та деталізація пріоритетів, засад, завдань та заходів, які доцільно впроваджувати у практичну площину складовими сектору безпеки й оборони, та іншими відповідальними суб'єктами.

Також слід вказати, що у вересні 2021 року було презентовано трирічну оновлену Стратегію кібербезпеки Японії. Уперше в положеннях Стратегії кібербезпеки Японії визначено, що суттєву загрозу для національного сегменту кіберпростору становлять РФ та КНР. Існує вірогідність, що КНР на системній основі здійснює викрадення конфіденційної інформації щодо стратегічних оборонних та передових технологічних підприємств Японії, а РФ у той час проводить кібератаки з метою досягнення військових та політичних цілей у кіберпросторі.

Висновки.

Розроблення документів державного стратегічного планування – процедура державного стратегічного планування, що включає аналіз, моделювання, формування

бачення та визначення цілей, напрямів, пріоритетів, завдань та заходів, ресурсного забезпечення, а також показників досягнення цілей та виконання завдань.

Саме тому від ефективної реалізації державної політики у сфері кібербезпеки, і зокрема положень Стратегії кібербезпеки, особливо в частині щодо створення Україною власного потенціалу кіберзахисту та активного кібервпливу, безпосередньо залежать подальший розвиток ситуації навколо агресії РФ проти України, тимчасової окупації нею частини української території, проведення операції Об'єднаних сил на території Донецької та Луганської областей, суспільно-політична обстановка в державі та особливо на Донбасі. Саме стратегічне планування у сфері забезпечення кібербезпеки надає змогу підвищити ефективність та якість державного управління кібербезпекою.

Стратегія кібербезпеки України повинна розглядатися усіма органами державної влади та управління, відповідальними складовими сектору безпеки і оборони України як універсальний інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення кібербезпеки, у тому числі й з використанням механізму державно-приватного партнерства. Більш того, як демонструє практика, відмова від державного стратегічного планування у важливих сферах життєдіяльності держави має ризики кризових проявів та негативних наслідків для розвитку суспільства та державних інституцій. Підвищення стратегічних спроможностей та відповідальних за забезпечення кібербезпеки правоохоронних органів потребують координацію запровадження інституційних засад і стандартів системи стратегічного управління у сфері забезпечення кібербезпеки. Виходячи з аналізу положень Стратегії кібербезпеки України, реалізація заходів, спрямованих на її забезпечення, має здійснюватися чітко на планових засадах та в обмежений час. Остання тенденція схвалених сучасних стратегій кібербезпеки – визначення чіткого переліку країн, які становлять загрозу для кібербезпеки тієї чи іншої держави. Так для України у кіберпросторі ворог № 1 – це РФ, для Японії – РФ та КНР.

Використана література

1. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109-116.

2. Галинська К.Ю. Стратегія кібербезпеки як основа інформаційного правопорядку в Україні. *Форум права*. 2016. № 1. С. 37-41

3. Доронін І.М. Правові проблеми координації у секторі національної безпеки й оборони України. *Актуальні проблеми вітчизняної юриспруденції*. 2019. № 1. С. 117-121.

4. Петров В.В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети*. – (Нац. ін-т стратег. дослідж.). Київ: НІСД, 2013. № 4(29). С. 127-131.

5. Ткачук Н.А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

6. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2. С. 183-186.

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

8. Грибоєдов С.М. Удосконалення державного планування у сфері забезпечення кібербезпеки в умовах гібридних загроз. *Інформація і право*. № 1(36)/2021. С. 114-122.

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

УДК 354:340.133

ПАНЧЕНКО О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-5649-3658.

АКТУАЛЬНІ ПИТАННЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *У статті розглядаються актуальні питання оцінювання ризиків кіберзагроз. Здійснено аналіз Закону "Про основні засади забезпечення кібербезпеки України", Стратегії кібербезпеки України та інших законодавчих актів з питань забезпечення кібербезпеки. Розглядаються основні підходи до визначення оцінки кіберзагроз. Аналізуються кращі зразки зарубіжної практики оцінювання ризиків кіберзагроз, визначаються найбільш ефективні національні системи їх оцінювання. Зроблено висновок, що найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли аналіз проводиться як на національному, так і на регіональному або місцевому рівні.*

Ключові слова: *кіберзагроза, кібератака, кіберпростір, оцінювання ризиків, об'єкти національної системи кібербезпеки.*

Summary. *The article considers topical issues of cyber threat risk assessment. It contains an analysis of the Law "On Basic Principles for providing of Cyber Security of Ukraine", the Cyber Security Strategy of Ukraine and other legislative acts for providing on cyber security. The main approaches to determining the assessment of cyber threats are considered. The best examples of foreign practice of cyber threat risk assessment are analyzed, the most effective national systems of their assessment are revealed. It is concluded that multi-level risk and threat assessment systems are most effective when the relevant analysis is conducted at both the national and regional and/or local levels.*

Keywords*: cyber threat, cyberattack, cyberspace, risk assessment, objects of the national cyber security system.*

Аннотация. *В статье рассматриваются актуальные вопросы оценки рисков киберугроз. Осуществлен анализ Закона Украины "Об основах обеспечения кибербезопасности Украины", Стратегии кибербезопасности Украины и других законодательных актов по обеспечению кибербезопасности. Рассматриваются основные подходы к определению оценки киберугроз. Анализируются лучшие образцы зарубежной практики оценки рисков киберугроз, определяются наиболее эффективные национальные системы их оценки. Сделан вывод о том, что наиболее эффективными являются многоуровневые системы оценки рисков и угроз, когда анализ проводится как на национальном, так и на региональном или местном уровне.*

Ключевые слова: *киберугроза, кибератака, киберпространство, оценка рисков, объекты национальной системы кибербезопасности.*

Постановка проблеми. Сучасні виклики та загрози, що постали перед Україною у кіберпросторі, зумовлюють зростання ролі кібербезпеки. Нова Стратегія кібербезпеки України (далі – Стратегія), затверджена Указом Президента України від 26 серпня 2021 року № 447, містить висновок про те, що упровадження нових технологій здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків [1]. Однією з причин такого стану справ є незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки [1].

Ситуація з поширенням коронавірусної хвороби (CoVID-19) виявила низьку готовність багатьох країн світу, у т.ч. України, до реагування на загрозу масштабної пандемії, засвідчила недосконаліть національних систем оцінки ризиків кіберзагроз та вироблення заходів з кібербезпеки. Україна, як і більшість країн світу, зіштовхнулася з низкою проблемних питань у зв'язку з поширенням пандемії коронавірусу. У багатьох країнах запровадження обмежувальних протиепідемічних заходів створило додаткові ризики і загрози в інформаційній сфері. Це актуалізує питання розбудови національної стійкості, зокрема визначення ефективних механізмів комплексного реагування на кіберзагрози на всіх етапах, підвищення готовності держави і суспільства шляхом запровадження додаткових заходів з кібербезпеки, а також належної координації такої діяльності.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії таким загрозам [1]. Стратегічний оборонний бюлетень України до потенційних загроз в інформаційній сфері відносить, зокрема, неспроможність ефективно реагувати на зростаючу кількість та потужність кібератак [2].

Результати аналізу наукових публікацій. Система оцінювання ризиків кіберзагроз була предметом аналізу у роботах таких фахівців, як: О.Д. Довгань та Т.Ю. Ткачук [3], Р.В. Лук'янчук [4], О.М. Солодка [5], О.О. Резнікова [6], О.О. Тихомиров [7], Н. Ткачук [8] тощо. Водночас ефективне функціонування системи оцінювання ризиків кіберзагроз потребує удосконалення.

Метою статті є аналіз ризиків кіберзагроз та вироблення на підставі аналізу кращих світових практик шляхів удосконалення системи їх оцінювання.

Виклад основного матеріалу. Відповідно до ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України" під кіберзагрозою розуміють наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Під індикаторами кіберзагроз слід розуміти показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози [9].

Ефективне функціонування системи оцінювання ризиків і кіберзагроз є важливим елементом стратегічного планування та забезпечення національної стійкості за напрямком кібербезпеки. Такі системи називають національними, через те що вони функціонують на рівні держави, охоплюють процеси, які стосуються забезпечення безпеки держави, суспільства та кожного громадянина, а також засновані на широкій міжвідомчій взаємодії та співпраці[5, с. 4].

Для визначення найбільш небезпечних загроз для кібербезпеки застосовуються два основні підходи. Перший передбачає оцінювання всіх можливих існуючих загроз за критеріями ймовірності й тяжкості наслідків. Як і для будь-яких експертних опитувань. Інший альтернативний підхід передбачає, що спочатку проводиться аналіз безпекового середовища у розрізі певної сфери (наприклад, інформаційної) за визначеними критеріями (індикаторами) у динаміці. Критерії відбору в кожній країні можуть бути різними. Певні країни визначають сфери національної безпеки, у яких постійний моніторинг та аналіз ризиків є обов'язковими. Це дозволяє виявити небезпечні тенденції, наближення індикаторів до критичної межі, а також звузити перелік ризиків для подальшого аналізу за критеріями ймовірності й тяжкості наслідків. При цьому рівень суб'єктивізму може бути дещо нижчим, оскільки, крім експертних оцінок, використовуються статистичні показники. Для оцінювання та порівняння ризиків і

загроз використовуються різні логарифмічні шкали і спеціальні методи досліджень. Це дає змогу визначити спектр загроз, які потребують найбільшої уваги та мають найвищу ймовірність настання і найтяжчі наслідки [5, с. 34].

Крім того, для подальшого аналізу й розробки сценарних прогнозів до отриманого переліку загроз можуть бути включені ризики, які спричиняють найбільший негативний вплив, але є малоймовірними, а також ті, що мають високу ймовірність, але незначний вплив.

Відповідно до Закону України "Про національну безпеку України" Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі [10].

За результатами експертних оцінок, стан реалізації попередньої Стратегії кібербезпеки України (затвердженої Указом Президента України від 15 березня 2016 року № 96) за визначеними показниками не перевищував 40 відсотків, а отриманий досвід надав змогу виокремити низку системних проблем [1].

Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був і рівень планування заходів з реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 2016 року, оскільки заплановані заходи не завжди корелювалися із визначеними нею завданнями, а реалізація зазначеної Стратегії була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. Не були розроблені індикатори виконання Стратегії кібербезпеки України, затвердженої Указом Президента України від 2016 року, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань [1]. Крім цього, участь у реалізації названої Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, заклади освіти, наукові установи, громадськість.

Не дивлячись на таку незадовільну оцінку системи оцінювання кібезагроз, відзначимо створення умов для формування системи оцінювання кіберзагроз та певні кроки до її реалізації. Одним з важливих кроків у напрямку формування такої системи став Закон України "Про основні засади забезпечення кібербезпеки України" [9], який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1].

З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у 2016 році утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері. Утворено відповідні центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві

оборони України, Збройних Силах України [1], що свідчить про спробу координації діяльності у сфері кібербезпеки та формування системи оцінювання ризиків кіберзагроз.

Сьогодні активно розвивається співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Королівством Нідерланди, Японією тощо), поглиблюється співробітництво з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій [1].

Досвід цих країн є вельми цікавим в контексті формування національної системи оцінки ризиків кіберзагроз. Як засвідчує цей досвід, найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному, так і на регіональному та/або місцевому рівні. Подібна практика поширена у країнах з розвиненими механізмами міжвідомчої співпраці і взаємодії на регіональному рівні та достатнім рівнем децентралізації у сфері забезпечення національної безпеки. Розглянемо таку практику у частині оцінювання кіберзагроз.

У США система оцінювання ризиків і загроз охоплює величезну кількість різноманітних об'єктів та зв'язків між ними. У роботі американських вчених "Викриття, розуміння та аналіз взаємозв'язку об'єктів критичної інфраструктури" представлена така класифікація взаємозв'язків між критичною інфраструктурою: фізична, кібернетична, географічна (топологічна) та логічна [11]. Для оптимізації досліджень застосовуються методи групування об'єктів національної системи кібербезпеки відповідно до їх взаємозалежності за секторами різного рівня з урахуванням їх важливості, зміст якої відображений в Національній стратегії з фізичного захисту об'єктів критичної інфраструктури та ключових об'єктів [12]. За результатами такої оцінки найвищий рівень захисту в ієрархії ключових об'єктів отримали об'єкти військово-промислового комплексу, системи охорони здоров'я та попередження надзвичайної ситуації. Наступне місце в ієрархії посідають об'єкти фінансового сектору. І, нарешті, найнижчий рівень складають об'єкти інформаційно-телекомунікаційного та енергетичного сектору. При цьому однією з головних умов залишається дотримання критерію "вартість – ефективність", а ключова проблема полягає в тому, щоб правильно обрати способи й засоби для організації захисту таких об'єктів [13].

Сьогодні в США функціонує збалансована система забезпечення захисту об'єктів національної системи кібербезпеки, зміст якої охоплює: визначений уповноважений орган для організації, координації заходів безпекового напрямку; методичний апарат для аналізу та прогнозування наслідків кіберзагроз; систему науково-дослідних установ, які забезпечують науково-технічне супроводження функціонування системи аналізу стану об'єктів національної системи кібербезпеки та експертизу з оцінки прогнозування наслідків впливів на стійкість таких об'єктів [15, с. 92].

Система оцінювання ризиків і загроз Великої Британії забезпечує стратегічне планування у сфері національної безпеки. Зокрема, вона надає можливість британському урядові оцінити широкий спектр ризиків і загроз національним інтересам та безпеці країни в діапазоні коротко- та довгострокових змін безпекового середовища, визначити стратегічні цілі та пріоритетні завдання щодо забезпечення національної безпеки і стійкості [5, с.7]. За результатами оцінки ризиків у сфері національної безпеки визначаються пріоритети державної політики у сфері національної безпеки та оборони, а також національної стійкості. Передусім оцінюються загрози національній безпеці Великої Британії світового масштабу – міжнародного, воєнного, геоекономічного, геополітичного, техногенного, соціального та іншого характеру, а також ті, що пов'язані із масштабними стихійними лихами, кібербезпекою, тероризмом тощо [5, с. 10].

У Стратегії національної безпеки та Огляді стратегічної оборони і безпеки Великої Британії (2015 р.) зазначено, що протягом 2015 – 2020 рр. найбільш імовірними ризиками можуть бути: тероризм, кіберзагрози, міжнародні збройні конфлікти, посилення міжнародної нестабільності, ризики здоров'ю громадян, епідемії, пандемії, природні небезпеки стихійного характеру, зростання вразливості відкритої економіки країни [5, с. 10-11].

Важливу роль в оцінюванні ризиків і загроз відіграють такі державні установи: Об'єднаний центр з питань оцінювання терористичної загрози (Joint Terrorism Assessment Centre), Центр з питань захисту інфраструктури (Centre for the Protection of National Infrastructure), Національний центр з питань кібербезпеки (National Cyber Security Centre), Агентство з питань навколишнього середовища (Environment Agency), Метеорологічне бюро (Met Office) та ін. Усі ці установи проводять ретельні дослідження щодо ризиків і загроз, які відносяться до їх компетенції, надають фахові консультації міністерствам і відомствам [5, с. 12].

Система оцінювання ризиків і загроз у Королівстві Нідерландів є важливим елементом стратегічного планування та підґрунтям для розробки Стратегії національної безпеки. Вона охоплює низку процесів, серед яких: аналіз безпекового середовища, оцінювання ризиків і загроз, визначення довгострокових тенденцій розвитку безпекової ситуації, оцінювання спроможностей [5, с. 6]. Національне оцінювання ризиків проводиться щорічно. Крім щорічного оцінювання ризиків, у Нідерландах розпочали здійснювати сканування горизонту національної безпеки, що передбачає аналіз трендів і загроз національній безпеці у довгостроковій перспективі [5, с. 17].

Нині в Нідерландах розроблений та оприлюднений лише один Національний профіль ризиків (2016 р.)

Національна система оцінювання ризиків і загроз у Королівстві Нідерландів постійно вдосконалюється, що передбачає можливість подальшої її адаптації до змін стратегічного безпекового середовища. На сьогодні вона реалізується комплексно та послідовно у єдиному алгоритмі в рамках циклу стратегічного планування у сфері національної безпеки.

Національний координатор з питань безпеки і протидії тероризму (Nationaal Coördinator Terrorismebestrijding en Veiligheid), який діє у складі Міністерства юстиції і безпеки Королівства Нідерландів (Ministerie van Justitie en Veiligheid) як ключова установа, відповідальна за процеси забезпечення національної безпеки і стійкості, визначив такі загальні пріоритети для оцінювання ризиків і загроз національній безпеці: загрози від суб'єктів, яких спонсорують інші держави; поляризація у суспільстві; пошкодження критичної інфраструктури; тероризм, екстремізм; воєнна загроза злочинності; кіберзагрози [14].

Як ми бачимо, формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті, насамперед, протягом періоду реалізації Стратегії [1].

Для формування потенціалу стримування необхідним є досягнення стратегічних цілей Стратегії, серед яких виділяється ціль С.1. "Дієва кібероборона", задля реалізація якої Україна має створити та забезпечити розвиток підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, забезпечити ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку

спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності [1]. Одним із шляхів реалізації таких цілей є налагодження системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки.

Висновки.

Як видно з аналізу Стратегії [1], ефективність її реалізації визначатиметься через чітку систему індикаторів стану кібербезпеки, яка буде включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури [1], що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії та прогрес, якого досягли суб'єкти забезпечення кібербезпеки в її виконанні. Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу координації діяльності із забезпечення кібербезпеки, а також моніторингу виконання Стратегії у реальному часі.

Аналіз позитивного зарубіжного досвіду показує, що найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному, так і на регіональному або місцевому рівні з використанням сучасних веб-ресурсів (онлайн-платформ), що свідчить про прозорість вжитих заходів для суспільства і держави.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

2. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президент України від 06.06.16 р. № 240. URL: https://zakon.rada.gov.ua/laws/show/240/2016#Text

3. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С. 89-103.

4. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України. Серія : Державне управління*. 2016. № 3. С. 131-137.

5. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / Резнікова О.О., Войтовський К.Є. Лепіхов А.В. ; за заг. ред. О.О. Резнікової. Київ: НІСД, 2020. 84 с.

6. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. № 3(15)/2015. С. 36-42.

7. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія; заг. ред. Р.А. Калюжний. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

8. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

10. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

11. Rinaldi S., Peerenboom J., and Kelly T. "Idenlifying, Understanding, and Analyzing Critical Infrastructure lnterdependencies". IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25.

12. Congressional Research Service Report for Congress. Critical Infrastructures. Background, Policy and Implementation. 2002. URL: https://sgp.fas.org/crs/homesec/RL30153.pdf

13. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах. URL: http://pentagonus.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranakh_2012/19-1-0-2082

14. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право.* № 3(34)/2020. С. 88-95.

15. Priority assessment of threats and risks: which issues require extra focus. URL: https://english.nctv.nl/topics/national-security-strategy/priority-assessmentof-threats-and-risks

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

УДК 342.951

СТЕЖКО С.М., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7386-1221.
ФИЦА В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6590-8082.

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ ЖИТТЄДІЯЛЬНОСТІ ВІТЧИЗНЯНОЇ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ

Анотація. *Досліджено питання забезпечення кібербезпеки вітчизняної енергетичної галузі. Розглянуто стратегічні засади підвищення рівня кіберстійкості комунікаційних та технологічних систем підприємств енергетичної галузі. Висвітлено позитивний досвід США та Великобританії щодо організаційно-правових засад запобігання та мінімізації посягань на об'єкти критичної енергетичної інфраструктури. Деталізовано методологію аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки об'єктів енергетичної інфраструктури. Узагальнено питання забезпечення кібербезпеки енергетичних об'єктів та автоматизованих систем. Висвітлено ініціативи та напрями діяльності РНБО України в контексті розбудови кібербезпеки енергетичних систем. Визначено шляхи удосконалення формування концептуальних засад забезпечення кібербезпеки в енергетичному секторі України.*

Ключові слова: *енергетична галузь, кібербезпека, кіберстійкість, державна безпекова політика, кібератака, кіберзагроза, цифровізація, критична інфраструктура.*

Summary. *The issue of cybersecurity of the domestic energy industry has been studied. The strategic principles of increasing the level of cyber resilience of communication and technological systems of energy industry enterprises are considered. The positive experience of the United States and the United Kingdom on the organizational and legal framework for preventing and minimizing encroachment on critical energy infrastructure is highlighted. The methodology of cyber threat analysis and risk assessment of cybersecurity violations of energy infrastructure facilities is detailed. The issue of cybersecurity of energy facilities and automated systems is generalized. The initiatives and directions of activity of the National Security and Defense Council of Ukraine for the purpose of development of cybersecurity of power systems are opened. The directions of the improvement to the formation of conceptual foundations for cybersecurity in the energy sector of Ukraine are identified.*

Keywords: *energy industry, cybersecurity, cyberresilience, state security policy, cyber attack, cyber threat, digitalization, critical infrastructure.*

Аннотация. *Исследованы вопросы обеспечения кибербезопасности отечественной энергетической отрасли. Рассмотрены стратегические основы повышения уровня киберустойчивости коммуникационных и технологических систем предприятий энергетической отрасли. Освящен позитивный опыт США и Великобритании касаемо организационно-правовых основ предотвращения и минимизации посягательств на объекты критической энергетической инфраструктуры. Детализирована методология анализа киберугроз и оценки рисков нарушения кибербезопасности объектов критической энергетической инфраструктуры. Раскрыты инициативы и направления деятельности СНБО Украины в контексте развития кибербезопасности энергетических систем. Обобщены направления усовершенствования формирования концептуальных основ обеспечения кибербезопасности в энергетическом секторе Украины.*

Ключевые слова*: энергетическая отрасль, кибербезопасность, киберустойчивость, государственная политика безопасности, кибератака, киберугрозы, цифровизация, критическая инфраструктура.*

Постановка проблеми. Важливою складовою національної безпеки України є енергетична безпека як стратегічна галузь економіки нашої держави. Безперебійне функціонування енергетичної галузі України є запорукою стабільних процесів підтримання енергонезалежності, успішного процвітання України як європейської держави. Адже докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення дієвої галузевої системи забезпечення кібербезпеки енергетичних об'єктів як важливої складової системи національної безпеки. На цьому фоні розвиток інтелектуальних енергетичних систем посилює проблему забезпечення кібербезпеки в енергетиці, особливо в умовах появи нових гібридних загроз та прагнень політичного керівництва РФ дестабілізувати ситуацію в енергетичному секторі Україні.

У положеннях Стратегії енергетичної безпеки України [1] деталізовано перелік загроз енергетичній безпеці, серед яких вагому роль відіграє поширення у світі коронавірусу, що зумовлює виникнення цілого ряду викликів та ризиків функціонування вітчизняного енергетичного сектору. Оскільки запровадження карантинних заходів у всіх країнах призводить до зменшення обсягів споживання енергії та енергоресурсів і, як наслідок, погіршення фінансово-економічних показників роботи суб'єктів енергетичного ринку. Крім того, в умовах епідемії перед енергетичним сектором виникає додаткове завдання – забезпечення стабільності надання послуг з енергопостачання в умовах карантинних заходів та обмежень.

Викладене зумовлює потребу активізації діяльності держави за напрямом забезпечення кібербезпеки та фізичної безпеки критичної інфраструктури енергетичного сектору, оскільки забезпечення безпеки критичної інфраструктури в енергетиці – одна з найбільших проблем цієї стратегічної галузі вітчизняної економіки. Це підтверджується й положеннями нещодавно схваленої на державному рівні Концепції забезпечення національної системи стійкості [2], відповідно до якої важливим завданням держави є прискорення розроблення та впровадження заходів з підвищення рівня кіберстійкості комунікаційних та технологічних систем, які забезпечують функціонування органів державної влади, об'єктів критичної інфраструктури, зокрема в енергетиці. Потребує активізації процес підвищення рівня кіберстійкості критичної інфраструктури енергетичного сектору України. За таких умов визначення ефективних шляхів удосконалення кібербезпеки в енергетичній галузі є необхідним та доцільним, включаючи розробку алгоритмів забезпечення розумного балансування усієї енергетичної системи та її надійного захисту.

Результати аналізу наукових публікацій. Останнім часом проблемні питання розбудови та управління вітчизняною критичною інфраструктурою на науковому рівні досліджували такі фахівці, як: С. Вдовенко та Ю. Даник [3], І. Мальцева, Ю. Черниш, В. Овсянніков [4], О. Мельничук [5], С. Теленик [6], В. Ємельянов [7] тощо. У загальному плані, питання тлумачення кібербезпеки розглядав О. Баранов [8], забезпечення кібербезпеки та її складових були предметом праць таких науковців, як І. Діориця [9], Р. Лук'янчук [10], Н. Ткачук [11]. Проте, нажаль, у працях згаданих науковців не було приділено достатню увагу питанням забезпечення кібербезпеки в енергетичному секторі, що підкреслює актуальність цієї тематики.

Метою статті є актуалізація проблем забезпечення кібербезпеки вітчизняної енергетичної галузі, визначення перспектив доцільності схвалення на державному рівні концептуальних організаційно-правових засад забезпечення кібербезпеки в енергетичному секторі України.

Виклад основного матеріалу. Світова енергетика слідує тенденціям децентралізації у виробництві електроенергії, а також декарбонізації. Тільки тотальна цифровізація дозволить створити комплексну енергетичну систему. Величезна кількість датчиків в сучасних енергетичних системах дозволяє збирати великі обсяги даних, забезпечуючи взаємодію на абсолютно новому рівні і в новому масштабі. Штучний інтелект і аналітика великих даних докорінно змінюють процес прийняття управлінських рішень. Найважливішими факторами успіху в цифровій економіці є гнучка інфраструктура і системи, що дозволяє адаптуватися до вимог майбутнього. Крім того, захист даних фізичних осіб і підприємств має першочергове значення для мінімізації ризику кібератак.

В сучасних умовах загрозливого масштабу набувають непоодинокі спроби стороннього впливу на стійкість функціонування енергетичних систем країни, насамперед з використанням можливостей технічних та технологічних новацій у розвитку енергетичних технологій. Тобто особливого значення набуває необхідність забезпечення безпеки ланцюга постачання технологій, обладнання, а також сервісних послуг щодо їх обслуговування. Крім того, збільшення кількості та рівня складності автоматизованих систем управління, керованих віддалено через інформаційні канали, формує високі ризики здійснення різноманітних кібератак. Потужні кібератаки такого формату, спрямовані на відповідні системи, можуть спричинити критичні наслідки у функціонуванні енергетичної інфраструктури. Таким чином, не можна недооцінювати масштаби та наслідки кіберзагроз, які посягають на об’єкти критичної інфраструктури енергетичного сектору.

Проникнення сучасних цифрових технологій в енергетику, як і в інші сфери зростає. Паралельно виникають загрози, пов’язані із суцільною цифровізацією. Країни світу, де “розумні” мережі і цифрові технології розвиваються швидше, змушені вживати дедалі більш потужних заходів з метою захисту власної енергосистеми, оскільки останнім часом на інфраструктурні енергетичні об’єкти по всьому світу здійснюються серйозні кібератаки, які спричиняють масштабні відключення електроенергії. Однією із найбільш серйозних ініціатив в зазначеному контексті став Акт США про безпеку енергетичної інфраструктури (Securing Energy Infrastructure Act) [12]. В американському Акті про безпеку енергетичної інфраструктури враховується, в тому числі, й концепція фізичної ізоляції, яка передбачає кіберзахист локальних мереж. Але цю концепцію можливо обійти, як демонструє досвід поширення вірусу Stuxnet, який успішно атакував ядерні об’єкти Ірана ще у 2010 році, уразивши комп’ютерні мережі, які керували їх роботою. У зв’язку з чим “розумні технології”, які контролюють роботу тих чи інших об’єктів залишаються потенційно уразливими для кібератак, навіть якщо вони фізично ізольовані від мережі Інтернет. Передбачувано, що причиною розробки цього документу стала потужна кібератака на енергосистему України ще у 2015 році, яка залишила без електроенергії понад 200 тис. осіб. Слід вказати, що у травні 2021 року Міністерство енергетики США оголосило про 100-денний план щодо посилення кібербезпеки електроенергетичної інфраструктури. Цей план передбачає активну співпрацю міністерства енергетики, приватних компаній, а також агентства з кібербезпеки й інфраструктурної безпеки з метою реагування на кіберзагрози.

Адже широке застосування старих технологій для захисту від втручань хакерів – це логічна стратегія, яка використовується в різних сферах енергетичного сектора.

Наприклад, для моніторингу, експлуатації, контролю та захисту ядерних ректорів (в тому числі і в Україні) використовуються як цифрові, так і аналогові системи. Цифрові активи, критично важливі для систем підприємства, є ізольованими від зовнішніх мереж та Інтернету. Це забезпечує їхній захист від багатьох кіберзагроз. Таким чином, саме низька цифровізація і відсутність цифрових комунікацій, які зв'язують той чи інший актив з іншими інформаційними системами, можуть вберегти енергетичний об'єкт від кіберзагроз. Ручне управління об'єктами енергетичної інфраструктури у рази безпечніше в плані реагування на потенційні кіберзагрози, але дорожче обходиться і вимагає наявності кваліфікованого персоналу. Крім того, ручне управління може бути менш безпечними для співробітників того чи іншого енергопідприємства.

Проте останньою світовою тенденцією розвитку ринку енергетики стало масштабне запровадження новітніх технологій, зокрема "Smart Grid" (розумні мережі електропостачання). "Smart Grid" – набір технологій, які перетворюють енергетичну інфраструктуру на сучасну цифрову систему. Тобто електронне керування параметрами електроенергії, керування її виробництвом і розподілом є важливими аспектами інноваційної розумної енергосистеми. Запровадження інноваційних технологій розумних енергосистем також передбачає фундаментальний перегляд сфери послуг енергетики, хоча типове використання цього терміна фокусується на технічній інфраструктурі [13]. Основними очікуваними результатами впровадження цієї концепції мають стати контрольованість та автоматизація процесів управління енергетичною системою, які мають забезпечувати її високу надійність та високі економічні показники. Інтелектуальна енергетична система передбачає інтеграцію енергетичних систем з новими інформаційно-комунікаційними технологіями та цілісною багаторівневою автоматизованою системою управління. Підвищення рівня тотального запровадження інтелектуальних енергетичних систем посилює проблему забезпечення кібербезпеки.

Таким чином, кібербезпека є життєво важливим фактором існування енергетичного комплексу та його складових. В сучасних умовах критично важливим є не лише запровадження новітніх технологій забезпечення енергоефективності, але й виконання завдання щодо захисту енергетичної системи від реальних та потенційних загроз у кіберпросторі. Кібератаки можуть бути спрямовані як на об'єкти генерації енергоресурсів, так і на об'єкти транспортування та споживання. Найбільш уразливою ланкою є системи управління та диспетчеризації енергетичних систем. При цьому уразливість буде постійно посилюватися по мірі поширення концепції та технологій "Smart Grid".

Проблеми кібербезпеки енергетичних систем посилюються тим, що понад 75 % енергетичного обладнання має іноземне походження, не враховуючи 100 % комп'ютерного та програмного забезпечення. На цьому фоні важливим завданням є забезпечення безпеки критичної інфраструктури й зокрема енергетичної інфраструктури, що являє собою сукупність енергетичних об'єктів та систем енергетики, включаючи енергетичні транспортні магістралі. Тобто подальше зростання ролі ІТ-технологій обумовлює виключне значення, якого набуває кібербезпека для забезпечення безпеки та стійкості функціонування енергетичної галузі.

Методологія аналізу кіберзагроз та оцінки ризиків порушення кібербезпеки об'єктів енергетичної інфраструктури включає: поточний аналіз стану кіберзагроз об'єктів енергетичної інфраструктури, формування сценаріїв ймовірних екстремальних ситуацій, пов'язаних з реалізацією кіберзагроз, моделювання та оцінювання ризиків порушення кібербезпеки енергетичної інфраструктури. Критерії захищеності вказаних об'єктів також включають інструменти попередження та запобігання некоректних або помилкових дій та

процесів, потенційну уразливість програмного забезпечення, яка непомітна на етапах проведення тестування. До переліку ризиків, які специфічні для підприємств енергетичної галузі, належать: використання в автоматизованих системах застарілого програмного забезпечення, обладнання та комунікаційних протоколів, які не передбачають можливості та вірогідності щодо кіберзагроз; наявність адміністративних та технологічних труднощів оновлення програмного забезпечення; неконтрольоване підключення автоматизованої системи управління до мережі Інтернет; можливий доступ "сторонніх" компаній до технологічної мережі об'єкта критичної інфраструктури. Енергетична галузь залишається найбільш уразливою з позиції ризиків техногенних катастроф. На цьому фоні вірогідним та прогнозованим є збільшення кількості кіберзагроз щодо енергетичної галузі. Це логічно особливо в умовах глибокої інформатизації та цифровізації. Також очікується тенденційна зміна ландшафту таких загроз.

Доцільно враховувати той факт, що підприємства енергетичної галузі у переважній більшості перебувають у стані модернізації, особливо щодо систем релейного захисту та автоматики. Як наслідок цих процесів виникає чимало частково реконструйованих об'єктів із різноманітними рівнями цифровізації вторинних систем та різними рівнями доступу як до програмних пристроїв, так і систем передачі сигналів й управління модулями. В результаті цього виникають непрямі проблеми, пов'язані із кібербезпекою, які не призводять до моментального виникнення несправностей, але які мають накопичувальний характер та стають "бомбою уповільненої дії". Тому на підприємствах енергетичної галузі кожен встановлений інтелектуальний електронний пристрій повинен мати працездатне програмне і мікропрограмне забезпечення. Захисні пристрої оснащуються комунікаційним і основним модулями, кожен з окремим мікропрограмним забезпеченням. Маршрутизатори мають власне мікропрограмне забезпечення, а на ПК встановлюється операційна система і додаткове програмне забезпечення. Для забезпечення кібербезпеки і функціональної безпеки необхідно здійснювати постійне оновлення компонентів такого мікропрограмного і програмного забезпечення.

Таким чином, питанням кібербезпеки енергетичних об'єктів та автоматизованих систем необхідно приділяти особливу увагу. Основною метою вирішення цієї проблеми є забезпечення стабільного та надійного функціонування відповідних систем та модулів при одночасному зменшенню ризиків та ймовірних збитків. Загрози кібератак безумовно існують, проте їх вірогідність та спричинені збитки необхідно оцінювати застосовуючи до кожної системи окремо. Також велике значення для забезпечення кібербезпеки має захист периметру мережі енергетичного об'єкта (фізичної та інформаційної). Зменшенню ризиків також сприяє запровадження заходів організаційного характеру, здійснення моніторингу мереж системи автоматичного управління, періодичний аналіз стану захищеності.

Враховуючи наявні виклики та ризики світового масштабу МАГАТЕ опікується вказаною проблематикою у зв'язку з чим розробило стандарт стосовно посилення рівня кібербезпеки на АЕС у 2020 році. Цей стандарт дозволить грамотно проводити тренування та навчання з комп'ютерної безпеки. Він враховує позитивні практики та напрацювання в системах захисту, а також містить рекомендації для оперативного реагування на атаки, що можуть виникнути. Таким чином, вказаний документ стане інструкцією для тренувань з кібербезпеки в атомній енергетиці. Забезпечення безпеки критичної енергетичної інфраструктури представляє собою концепцію протидії серйозним загрозам роботи важливих об'єктів інфраструктури та об'єктів підвищеної загрози в регіоні чи державі, особливо в умовах розповсюдження інформаційних

технологій, тоді як динамічний розвиток інформаційних технологій обумовлює появу нових видів кібератак, націлених на об'єкти національної енергосистеми.

У липні 2021 року Великобританія схвалила на державному рівні Стратегію цифровізації вітчизняної енергосистеми та план заходів щодо її реалізації [14]. Достатня увага приділяється саме кібербезпеці енергетичних систем. До 2050 року в енергетичному секторі планується запровадити мільйони низьковуглецевих технологій, включаючи сонячні батареї, теплові насоси та електромобілі. На цьому фоні роль та значення кібербезпеки потужно зростає.

Розуміючи необхідність посилення стану кібербезпеки, у свою чергу, Міністерство енергетики України як профільний орган має намір створити галузевий операційний центр кібербезпеки (Security operations center, SOC). Операційний центр безпеки — це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюються, оцінюються та захищаються. Це означає запровадження та розбудову кібер-фізичної інфраструктури для інформаційних систем децентралізованого інтелектуального управління енергосистемами. Одним із стратегічних завдань галузевого операційного центру кібербезпеки є навчання та інформування користувачів, зокрема, прищеплення їм культури кібербезпеки, а також оперативне їх інформування про виникнення загроз та план дій на випадок скоєння кібератак.

Проблематикою забезпечення кібербезпеки енергетичної галузі останнім часом також переймається і РНБО України. 22 грудня 2020 року Укренерго підписало Меморандум з Радою національної безпеки та оборони України про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту. Співпраця здійснюватиметься шляхом обміну технічною та технологічною інформацією у сфері забезпечення кібербезпеки, зокрема індикаторами кіберзагроз, інформацією про кіберінциденти тощо. На виконання положень меморандуму Міністерство енергетики України планує створити проєктний офіс для залучення міжнародної технічної допомоги, провести аудит поточного стану кібербезпеки в енергетиці та організувати секторальний центр кібербезпеки критичної інфраструктури енергетичного сектору.

29 квітня 2021 року в Апараті Ради національної безпеки і оборони України у рамках співпраці між Національним координаційним центром кібербезпеки при РНБО України (НКЦК) і Фондом цивільних досліджень та розвитку Сполучених Штатів Америки (CRDF Global) (за підтримки Державного департаменту США) відбулося третє засідання Національного кластера з кібербезпеки [15]. За підсумками зустрічі було визначено, що розбудова цілісної системи забезпечення кібербезпеки ОКІ держави вимагає також чіткого визначення переліку їх ІТС, створення та ведення загальнодержавного реєстру ОКІ, проведення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, а також ухвалення відповідного законодавства.

29 – 30 вересня 2021 року в Одесі відбулося виїзне засідання (у рамках конференції Energy CyberCon 2021) Робочої групи з питань розбудови кіберзахисту об'єктів критичної інфраструктури енергетичної галузі Міністерства енергетики України, на якому було презентовано кращі проекти захисту енергетичного сектору від провідних виробників та постачальників рішень у сфері цифровізації та кібербезпеки. Також учасники заходу обмінялися думками щодо місця секторальної кібербезпеки в організаційно-технічній моделі національної кібербезпеки, стандартів кібербезпеки в енергетичному секторі та законодавства в сфері критичної інфраструктури. Слушно висловився з цього приводу заступник Секретаря РНБО С. Демедюк щодо необхідності посилення координації дій державних та приватних суб'єктів енергетичної галузі у

питаннях забезпечення надійного кіберзахисту. На його переконання, критично важливим є не лише запровадження новітніх технологій забезпечення енергоефективності, а й захист енергетичної системи від загроз у кіберпросторі [16].

Таким чином, кібербезпека енергетичної галузі перебуває у фокусі уваги державного апарата, сектору безпеки і оборони та приватних компаній. Атаки на об'єкти критичної енергетичної інфраструктури можуть привести до масштабних катастрофічних наслідків для галузі, екології та економіки країни. Ситуація з атакою у травні 2021 року на американську трубопровідну систему Colonial Pipeline переконливо це продемонструвала. Атака зупинила роботу всіх трубопроводів системи на цілих 5 днів. В результаті атаки Президент Д. Байден оголосив надзвичайний стан, а за оцінками експертів – це була найбільша успішна кібератака на нафтову інфраструктуру в історії США.

Враховуючи виклики та загрози світового масштабу, Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки [17].

Висновки.

Сучасне суспільство практично повністю залежить від стану захищеності інформації та кібер-інфраструктури у всіх сферах життєдіяльності. Україна вже тривалий час є об'єктом регулярних і масштабних кібератак, які ставлять під загрозу стабільну роботу критичної інфраструктури. На території України в кожному регіоні є енергетичні системи, які відносяться до об'єктів критичної інфраструктури. Проблема забезпечення кібербезпеки в енергетичній галузі актуалізується та посилюється у зв'язку з поширенням практичного впровадження концепції інтелектуальних енергетичних систем. На жаль, прогнозується подальша уразливість енергетичної інфраструктури та її об'єктів від кібератак, несанкціоноване втручання у роботу вітчизняних енергосистем та здійснення її збоїв, що провокує посилення їхньої кіберстійкості. Кіберстійкість енергетичної критичної інформаційної інфраструктури – це такий її стан, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз. Вітчизняна енергетична галузь не є виключенням. Однією із важливих складових енергетичної галузі України є система управління, яка відіграє важливу роль функціонування усього енергетичного комплексу України. Автоматизована система управління вітчизняною енергетичною галуззю повинна бути стійкою до будь-яких кібервпливів та мати сучасну комплексну систему протидії кібератакам.

Гібридна війна РФ проти України, елементом якої є також акції кібервпливу, залишається на сьогодні найбільшою загрозою національній безпеці держави. В цьому контексті важливим елементом функціонування національної системи кібербезпеки є забезпечення кібербезпеки об'єктів критичної інфраструктури, зокрема, енергетичного сектору. За таких умов саме кібербезпека має стати одним з пріоритетів розвитку підприємств енергетичної галузі. Підвищення рівня кіберстійкості критичної інфраструктури енергетичного сектору України є важливим стратегічним завданням держави.

Враховуючи викладене, доцільно прискорити схвалення на державному рівні Концепції забезпечення кібербезпеки в енергетичному секторі України на 2022 − 2024 роки. Серед інших завдань Концепції кібербезпеки в енергетичному секторі виділяється: прискорення впровадження сучасних технологій кібербезпеки на базі європейських та

євроатлантичних принципів та стандартів; врегулювання нормативно-правових і організаційно-технічних аспектів галузевої кібербезпеки в енергетичній галузі; впровадження механізмів моніторингу та оцінки якості виконання рекомендацій та вимог підприємствами та суб'єктами забезпечення кібербезпеки в енергетиці; впровадження засад державно-приватного та приватно-публічного партнерства тощо.

Використана література

1. Про схвалення Стратегії енергетичної безпеки: розпорядження Кабінету Міністрів України від 4.08.21 р. № 907. URL: https://zakon.rada.gov.ua/laws/show/907-2021-р#Text
2. Концепція забезпечення національної системи стійкості: Указ Президента України від 27.09.21 р. № 479/2021: URL: https://www.president.gov.ua/documents/4792021-40181
3. Даник Ю.Г., Вдовенко С.Г. Ланцюгові ефекти в кібердіях: зб. наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2019. № 64. С.71-90.
4. Мальцева І., Черниш Ю., Овсянніков В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2021. № 12. Т. 4. С. 29-35.
5. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. *Державне управління та місцеве самоврядування*. 2019. № 3 (42). С. 13-27.
6. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя, 2021. 37 с.
7. Ємельянов В.М., Бондар Г.Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. *Публічне управління та регіональний розвиток*. 2019. № 5. С. 493-523.
8. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*. № 2(42)/2014. С. 54-62.
9. Діордиця І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя, 2018. 40 с.
10. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Серія: Державне управління*. 2016. № 3. С. 131-137.
11. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.
12. Securing Energy Infrastructure Act of the USA 2021. URL: https://www.congress.gov/bill/116th-congress/senate-bill/174
13. Релейний захист та кібербезпека енергетичних систем: підручник / Є.І. Сокол та ін. ; під заг. ред. проф. Є.І. Сокола. Харків: Панов А.М., 2019. 389 с.
14. Digitalising our energy system for net zero. Strategy and Action Plan 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004011/energy-digitalisation-strategy.pdf
15. В Апараті РНБО України відбулося третє засідання Національного кластера з кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/4887.html
16. Демедюк С. Кібербезпека сьогодні – життєво важливий фактор існування енергетичної галузі. URL: https://www.rnbo.gov.ua/ua/Diialnist/5024.html
17. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

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

УДК 351.81

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.

ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Анотація. *У статті розглядаються правові та організаційні аспекти забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. Звертається увага на позитивний досвід США у забезпеченні стійкості об'єктів критичної інфраструктури. Аналізуються положення нової Стратегії кібербезпеки України, одним з пріоритетів якої визначено удосконалення нормативного забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури. Відзначаються недоліки попередньої Стратегії кібербезпеки України 2016 року. Міститься детальний аналіз законодавчих актів та ініціатив з питань забезпечення кібербезпеки. Розглядаються загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. На підставі аналізу чинного законодавства з питань забезпечення кібербезпеки України запропоновані шляхи удосконалення правового та організаційного забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак.*

Ключові слова: *кіберпростір, кібератака, об'єкти критичної інфраструктури, кіберзахист об'єктів критичної інфраструктури, правове забезпечення, організаційне забезпечення.*

Summary. *The article considers the legal and organizational aspects of ensuring the protection of the critical information infrastructure from cyberattacks. Attention is drawn to the positive experience of the United States in ensuring the resilience of the objects of critical infrastructure. The provisions of the new Cyber Security Strategy of Ukraine are analyzed, one of the priorities of which is to improve the regulatory framework for cyber security of critical information infrastructure. The shortcomings of the previous Cyber Security Strategy of Ukraine (2016) are noted. Contains a detailed analysis of legislation and initiatives on providing cybersecurity. General requirements for cyber protection of critical infrastructure objects are considered. Based on the analysis of the current legislation on cyber security of Ukraine, ways to improve the legal and organizational support for the protection of the critical information infrastructure from cyber attacks are proposed.*

Keywords: *cyberspace, cyber attack, critical infrastructure objects, cyber protection of critical infrastructure objects, legal support, organizational support.*

Аннотация. *В статье рассматриваются правовые и организационные аспекты обеспечения защиты объектов критической информационной инфраструктуры от кибератак. Обращается внимание на положительный опыт США в обеспечении устойчивости объектов критической инфраструктуры. Анализируются положения новой Стратегии кибербезопасности Украины, одним из приоритетов которой определены совершенствование нормативного обеспечения по вопросам киберзащиты объектов критической информационной инфраструктуры. Отмечаются недостатки предыдущей Стратегии кибербезопасности Украины 2016 года. Содержится детальный анализ законодательных актов и инициатив по вопросам обеспечения кибербезопасности. Рассматриваются общие требования киберзащиты объектов критической инфраструктуры. На основании анализа действующего законодательства по вопросам обеспечения кибербезопасности Украины предложены пути совершенствования правового и организационного обеспечения защиты объектов критической информационной инфраструктуры от кибератак.*

Ключевые слова: *киберпространство, кибератака, объекты критической инфраструктуры, киберзащита объектов критической инфраструктуры, правовое обеспечение, организационное обеспечение.*

Постановка проблеми. 26 серпня 2021 року Указом Президента України №447 затверджено нову Стратегію кібербезпеки України [1] (далі – Стратегія), одним з пріоритетів якої визначено удосконалення нормативного забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, порядку її визначення та вимог до її кіберзахисту. Стратегія констатує, що зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди [1].

Як і раніше, гібридна агресія Російської Федерації проти України у кіберпросторі залишається однією із серйозних загроз кібербезпеці України. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Не меншу загрозу складають організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство). Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх запобігання, виявлення та нейтралізацію [1].

Лише протягом першого півріччя 2020 року Служба безпеки України нейтралізувала понад 300 кібератак і кіберінцидентів на об'єкти критичної інфраструктури. До цих кібератак були причетні майже 20 хакерських угруповань, які також викрито і знешкоджено спецслужбою. Значну частину хакерів напряму контролювали з Російської Федерації. Їх метою було завдання шкоди українським державним органам і підприємствам оборонно-промислового комплексу. Була за цей період і спроба кібератаки на українські ЗМІ [2].

Підвищення ризиків терористичних актів, збільшення кількості кібератак на енергетичні об'єкти, руйнування та пошкодження об'єктів інфраструктури в зоні військового конфлікту на сході України обумовлюють нагальність питання розбудови державної системи захисту критичної інфраструктури в Україні [3, с. 2]. У Стратегії відзначається, що надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р. № 96, не були виконані, зокрема: не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним [1]. Ці обставини підкреслюють актуальність досліджуваної проблематики захисту критичної інформаційної інфраструктури від кібератак.

Результати аналізу наукових публікацій. Питання захищеності об'єктів критичної інфраструктури досліджували Іванюта С.П. [3], Кондратов С.І. [4], Леонов Б.Д. [5], Серьогін В.С. [5], Суходоля О.М. [4], Рижов І.М. [6]. Питанню визначення кібербезпеки стосувалася робота Баранова О.А. [7], реалізації Стратегії кібербезпеки України розглядали такі науковці, як Гнатюк С.О. [8], Лук'янчук Р.В. [9], Ткачук Н.А. [10] та ін. Водночас, затвердження нової Стратегії висуває новий порядок

денний з правового та організаційного забезпечення захисту об'єктів критичної інфраструктури від кібератак.

Метою статті є удосконалення на підставі аналізу чинного законодавства нормативного та організаційного забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак.

Виклад основного матеріалу. Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш актуальними можна виокремити такі: природні; а) незловмисні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури; б) зловмисні: кібератаки, терористичні атаки [4].

Не випадково сьогодні набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [1]. Так, 14 травня 2021 року РНБО України прийнято рішення РНБО України "Про невідкладні заходи з кібероборони держави" (введено в дію Указом Президента України від 26.08.21 р. № 447), яким передбачено створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі. Цим рішенням також передбачено розробку та внесення на розгляд Верховної Ради України законопроекту щодо створення та функціонування у системі Міністерства оборони України кібервійськ [11].

Відповідно до Стратегії національної безпеки України [12] одним із основних напрямів державної політики в сфері національної безпеки визначено забезпечення безпеки та необхідного рівня захищеності об'єктів критичної інфраструктури України, насамперед від загроз терористичного та диверсійного характеру. Об'єктами критичної інформаційної інфраструктури є комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури (п. 19 ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України") [13].

Концепція боротьби з тероризмом [14] проголошує, що усунення та мінімізація наслідків терористичної діяльності передбачає вирішення завдань опрацювання комплексу заходів щодо забезпечення якнайшвидшого відновлення штатного режиму функціонування об'єктів, передусім об'єктів критичної інфраструктури, щодо яких вчинено терористичний акт.

Сьогодні не викликає здивування, що кіберпростір є одним з можливих театрів воєнних дій разом з іншими фізичними просторами.

На думку зарубіжних дослідників, критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об'єктів та параметрів системи; 2) важко прогнозована поведінка об'єктів, для яких характерна велика кількість взаємозв'язків, які класифіковано по різних секторах [15]. Наприклад, в США, яка є піонером у розробці та запровадженні концепції критичної інфраструктури, функціонує збалансована система забезпечення захисту критичної інфраструктури держави, зміст якої охоплює: визначений уповноважений орган для організації, координації та здійснення контрольно-наглядових функцій щодо заходів безпекового напряму; методичний апарат для аналізу та прогнозування наслідків як подій техногенного характеру, так і диверсій чи терористичних актів; систему науково-дослідних установ, які забезпечують науково-

технічне супроводження функціонування системи аналізу стану критичної інфраструктури та експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури [5, с. 93].

США продовжують зберігати свої лідерські позиції у цій сфері, у т.ч. завдяки застосуванню апробованих на інших напрямах сучасних управлінських підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і форматів підготовки кадрів і населення задля забезпечення захисту та стійкості критичної інфраструктури тощо. Інші розвинені країни світу широко використовують напрацьовані у США підходи, звичайно, враховуючи при цьому власну національну специфіку [4, с. 4, 5].

В Україні, де ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, проблематика забезпечення захисту критичної інформаційної інфраструктури від кібератак давно є предметом активних дискусій. На державному рівні активні заходи щодо розв'язання цієї проблематики почали вживатися з 2016 року.

У червні 2016 року утворено Національний координаційний центр кібербезпеки, положення про який затверджено Указом Президента України від 07.06.16 р. № 242. До основних завдань цього Центру, зокрема, віднесено: здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; здійснення аналізу: стану кібербезпеки та стану кіберзахисту критично важливих об'єктів інфраструктури; здійснення заходів щодо забезпечення кіберзахисту об'єктів критичної інфраструктури та захисту технологічних процесів на виробництві у реальному секторі економіки [16] тощо.

Затвердження у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування в цій сфері. За роки реалізації попередньої Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.16 р № 96, було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України" [13], який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [1].

Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України [1].

Рішенням РНБО від 29.12.16 р. "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" (введено в дію Указом Президента України від 16.01.17 р. № 8) заплановано внесення в установленому порядку на розгляд Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист", в якому слід передбачити врегулювання питань, зокрема, щодо: 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 та 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 [17].

Розпорядженням Кабінету Міністрів України від 06.12.17 р. затверджено Концепцію створення державної системи захисту критичної інфраструктури, де серед проблем, що потребують розв'язання, визначено відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації. Аналогічна проблема фіксується й у Концепції боротьби з тероризмом, одним із завдань якої є підвищення ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, у тому числі шляхом розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів [18].

У 2019 р. Кабінет Міністрів України на виконання вимог Закону "Про основні засади забезпечення кібербезпеки України" затвердив загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [19]. Цим актом, зокрема, установлено, що кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури відповідного об'єкта. Заходи з кіберзахисту передбачатимуться та впроваджуватимуться на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури відповідного об'єкта, а створення системи інформаційної безпеки об'єкта критичної інформаційної інфраструктури відповідного об'єкта здійснюватиметься відповідно до вимог технічного завдання на створення системи інформаційної безпеки. Таке завдання формуватиметься за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об'єкті критичної інформаційної інфраструктури. За такого підходу власник та/або керівник об'єкта критичної інфраструктури організовуватиме проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства у сфері захисту інформації та кібербезпеки. Він невідкладно інформуватиме урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузеву команду реагування на комп'ютерні надзвичайні події), а також функціональний підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідний підрозділ регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури [20].

У додатку до загальних вимог наведено перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, до змісту яких включено формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки, управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури, ідентифікацію та автентифікацію користувачів та адміністраторів відповідного об'єкта критичної інформаційної інфраструктури тощо. Зазначені вимоги є усталеною практикою в ЄС та в США і гармонізовані з вимогами міжнародних стандартів ЄС, НАТО та NIST з питань забезпечення кіберзахисту [20].

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО [1].

Ціль С.2 Стратегії визначається як ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму. Проголошується, що для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом: створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури. Цьому сприятиме реалізація інших цілей Стратегії, зокрема: завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури; створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури; постійний перегляд та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки; запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість; встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів; стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору [1].

Впровадження заходів кіберзахисту дасть змогу підприємствам, установам та організаціям, які віднесені до об'єктів критичної інфраструктури, забезпечити захист від кібератак, запобігти порушенню конфіденційності, цілісності та доступності своїх інформаційних ресурсів, порушенню режиму сталого функціонування об'єкта критичної інфраструктури [20].

Проблеми забезпечення об'єктів критичної інфраструктури все частіше стають предметом обговорення за участі зарубіжних експертів. Так, 27 травня 2021 року у рамках співпраці між Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України (НКЦК) і Фондом цивільних досліджень та розвитку Сполучених Штатів Америки (CRDF Global) (за підтримки Державного департаменту США), відбулося четверте засідання Національного кластера з кібербезпеки, присвячене питанням захисту критичної інфраструктури, її стійкості, а також проблемам, які існують у цій сфері. Майже 200 українських та американських фахівців з кібербезпеки відпрацювали захист об'єктів критичної інфраструктури та обговорили аспекти відповідного законопроєкту [21].

Заступник секретаря РНБО України С. Демедюк наголосив, що цей проєкт є платформою, на якій провідні фахівці "можуть безпосередньо обмінятися думками, пропозиціями, цікавими ідеями". Зокрема, захист об'єктів критичної інфраструктури є вкрай важливим для забезпечення життєдіяльності держави та кожного громадянина, а під час засідання кластера можна напрацювати шляхи безперервного забезпечення "безпеки цих об'єктів – починаючи від атомної енергетики і закінчуючи маленькими фінансовими компаніями, які можуть бути віднесені до об'єктів критичної інфраструктури"[21].

Висновки.

На базі аналізу законодавства з питань забезпечення кібербезпеки можна дійти висновку, що забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак потребує удосконалення за напрямами:

1) законодавчого забезпечення – прийняття Закону України “Про об’єкти критичної інфраструктури”;

2) організаційно-адміністративного забезпечення – ідентифікації об’єктів критичної інфраструктури; розробки правил антитерористичної безпеки для об’єктів критичної інфраструктури; регламентації повноважень державних органів із захисту об’єктів критичної інфраструктури від кібератак.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

2. За півроку СБУ нейтралізувала 300 кібератак на об’єкти критичної інфраструктури URL: https://ssu.gov.ua/novyny/za-pivroku-sbu-neitralizuvala-300-kiberatak-na-obiekty-krytychnoi-infrastruktury

3. Іванюта С.П. Пріоритетні напрями законодавчого та організаційного забезпечення паспортизації об’єктів критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-07/1_Ivaniuta-9af75.pdf

4. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О.М. Суходолі. Київ: НІСД, 2020. 28 с.

5. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об’єктів критичної інфраструктури (на прикладі США). *Інформація і право.* № 3(34)/2020. С. 88-95.

6. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ: Нац. акад. СБУ, 2016. 327 с.

7. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2 (42). С. 54-62.

8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129.

9. Лук’янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Сер.: Державне управління*. 2016. № 3. С. 131-137.

10. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

11. Про невідкладні заходи з кібероборони держави: рішення РНБО України від 04.05.21 р.: Указ Президента України від 26.08.21 р. № 447). URL: https://zakon.rada.gov.ua/laws/show/n0053525-21#Text

12. Про Стратегію національної безпеки України: рішення РНБО України від 06.05.15 р.: Указ Президента України від 26.05.15 р. № 287. *Офіційний вісник України*. 2015. № 43. Ст. 1353.

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

14. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

15. Congressional Research Service Report for Congress. Critical Infrastructures. Background, Policy and Implementation. 2002. URL: https://sgp.fas.org/crs/homesec/RL30153.pdf

16. Положення про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16 р. № 242. URL:https://zakon.rada.gov.ua/laws/show/242/2016#Text

17. Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури: рішення РНБО від 29.12.16 р.: Указ Президента України від 16.01.17 р. № 8. URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text

18. Концепція створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.17 р. № 1009 URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

19. Загальні вимоги 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-%D0%BF#Text

20. Визначено вимоги до кіберзахисту об'єктів критичної інфраструктури. URL: https://jurliga.ligazakon.net/ua/news/170010_zakon-pro-kberbezpeku-nabuv-chinnost

21. Українські та американські фахівці обговорили стійкість критичної інфраструктури. URL: https://www.ukrinform.ua/rubric-society/3254378-ukrainski-ta-amerikanski-fahivci-obgovorili-stijkist-kriticnoi-infrastrukturi-do-kiberatak.html

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

УДК 342.951

ЖЕРЕБЕЦЬ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-2059-2045.

РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: ЗАКОНОДАВЧИЙ АСПЕКТ

Анотація. *У статті розглядаються актуальні питання реалізації державної політики у сфері протидії кіберзлочинності. Розкриваються сутність, ознаки та види кіберзлочинів. Виокремлюються напрями протидії кіберзлочинності на концептуальному, законодавчому та інституціональному рівнях. Виявляються недоліки імплементації положень Конвенції про кіберзлочинність у чинне законодавство України. Пропонуються шляхи підвищення ефективності протидії кіберзлочинності.*

Ключові слова: *кіберзагроза, кіберзлочинність, кіберзлочин, протидія, законодавство.*

Summary. *The article considers topical issues of state policy implementation in the field of combating cybercrime. The essence, signs and types of cybercrimes are revealed. Areas of combating cybercrime at the conceptual, legislative and institutional levels are identified. The shortcomings of the implementation of the provisions of the Convention on Cybercrime in the current legislation of Ukraine are revealed. Ways to increase the effectiveness of combating cybercrime are proposed.*

Keywords*: cyberthreat, cybercrime, counteraction, legislation.*

Аннотация. *В статье рассматриваются актуальные вопросы реализации государственной политики в сфере противодействия киберпреступности. Раскрываются сущность, признаки и виды киберпреступлений. Выделяются направления противодействия киберпреступности на концептуальном, законодательном и институциональном уровнях. Выявляются недостатки имплементации норм Конвенции о киберпреступности в действующее законодательство Украины. Предлагаются пути повышения эффективности противодействия киберпреступности.*

Ключевые слова: *киберугроза, киберпреступность, киберпреступление, противодействие, законодательство.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій створює умови для появи нових ризиків та кіберзагроз. Незважаючи на позитивний вплив на всі сфери людського життя, цей розвиток зумовив зростання й поширення кіберзлочинів. З упевненістю можна сказати, що кіберзлочини – це одна з основних проблем XXI ст., вирішення якої потребує сучасних методів, активних, рішучих заходів і своєчасного нормативного реагування [1].

Як на міжнародному, так і національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці [2].

Оцінки загроз кіберзлочинності національній безпеці окремих держав та міжнародному порядку визначають, що: 1) це небезпечна тенденція, пов'язана зі збільшенням технико-технологічної залежності держави від транскордонних проявів кібертерористів;

2) комп'ютерні атаки практично неможливо прогнозувати або прослідкувати в реальному часі [3, с. 10].

Отже, протидія кіберзлочинності на сьогодні є одним з пріоритетних напрямків забезпечення національної безпеки держави.

Результати аналізу наукових публікацій. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Брижко [4], В. Бутузов [5], С. Лівчук, О. Петровський [6], В. Пилипчук, В. Сірко [7], А. Тарасюк [8], А. Марущак [9], М. Швець [4], О. Юрченко та інші. Водночас ефективність протидії кіберзлочинності зумовлює необхідність вжиття додаткових заходів на законодавчому та організаційному рівнях.

Метою статті є аналіз реалізації державної політики у сфері протидії кіберзлочинності та вироблення шляхів її удосконалення.

Виклад основного матеріалу. У Законі України "Про основні засади забезпечення кібербезпеки України" кіберзлочинність розуміється як сукупність кіберзлочинів, а кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [10].

Сутність кіберзлочинів або ІТ-злочинів полягає в тому, що це протиправні суспільно небезпечні діяння, тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача [3, с. 11].

Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми: Європейської Конвенції про взаємну правову допомогу у кримінальних справах 1959 р. (ратифікована із застереженнями і заявами Законом України від 16.01.98 р. № 4498-ВР), Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 року (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV), Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року (ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV), загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору [3, с. 17].

Відповідно до Конвенції про кіберзлочинність кіберзлочини поділяються на наступні категорії:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані "CIA-злочини"), зокрема:

незаконний доступ, наприклад, шляхом злому, обману і іншими засобами;

нелегальне перехоплення комп'ютерних даних;

втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на критичну інформаційну інфраструктуру;

зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу з метою здійснення "CIA-злочинів";

2) правопорушення, пов’язані з комп’ютерами, включаючи підробку і шахрайство, здійснені з використанням комп’ютерів;

3) правопорушення, пов’язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

4) правопорушення, пов’язані з порушенням авторських і суміжних прав, наприклад, незаконне відтворення і використання комп’ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і літератури

5) правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем[11].

Згадана Конвенція (ратифікована 58 державами, серед яких усі держави-члени Ради Європи (за винятком Російської Федерації) й такі, що не входять до Європейської спільноти, зокрема Канада, Ізраїль, США, Японія та країни Південної Америки) – це договір, згідно з яким держави, що до неї приєдналися, узяли на себе зобов’язання відносно зближення між собою внутрішньодержавних положень кримінального права щодо кіберзлочинів та створення можливостей для застосування ефективних засобів розслідування таких правопорушень [3, с. 17]. Тому Конвенцією прямо передбачено заходи, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч. 1 розділ 2) й кримінально-процесуальному (так званому “процедурному”) праві (ч. 2 розділ 18), а також систему міжнародного співробітництва (розділ 3) та питання юрисдикційного характеру (ч. 3 розділ 2) [3, с. 17-18]. Зазначене зумовлює потребу завершення процесу імплементації положень цієї Конвенції в чинне законодавство України, що є одним із напрямів реалізації державної політики у сфері протидії кіберзлочинності.

Виокремити інші напрями протидії кіберзлочинності дуже складно через багатогранність цього соціального явища [12, с. 34-35]. В юридичній літературі виділяють два основних напрямки [7, с. 104]. До першого напряму відносять: попередження кіберзлочинності, що передбачає створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного і програмного захисту інформації; створення спеціалізованих організаційних структур організацій і служб кібербезпеки, спрямованих на забезпечення надійного функціонування засобів захисту, генерація ключів і паролів, контроль щодо їх використання, зміні й знищенню. Другий напрямок протидії кіберзлочинності містить виявлення і попередження кіберзлочинів. Нині проблема кінцевого вирішення організації ефективної взаємодії та координації суб’єктів протидії кіберзлочинності знаходиться на стадії завершення. Саме багатогранність суб’єктів протидії кіберзлочинності передбачає багаторівневу координацію їх діяльності [7, с. 104]. Питанням кібербезпеки сьогодні опікуються різноманітні суб’єкти забезпечення кібербезпеки: Державна служба спеціального зв’язку і захисту інформації, Служба безпеки України, Міністерство внутрішніх справ, Національний банк. Водночас, цілісна політика у цій сфері поки що відсутня, як і універсальні індикатори кібербезпеки, що могли б охарактеризувати її рівень [13].

Для ефективної боротьби з кіберзлочинністю в Україні, за прикладом зарубіжних країн, варто було б: створити політичне підґрунтя (концептуальний рівень), удосконалити систему законодавства (законодавчий рівень), визначити систему органів, основними функціями яких було б забезпечення кіберзахисту України (інституціональний рівень) [6, с. 54]. Перші кроки у напрямку формування політичного підґрунтя (концептуальний рівень) та системи суб’єктів забезпечення кібербезпеки (інституціональний рівень) відбулися ще у 2016 році. Зокрема на концептуальному та інституціональному рівні:

- у березні 2016 року Урядом України схвалено Стратегію кібербезпеки України, яка мала на меті створення національної системи кібербезпеки;
- у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки. Першим етапом його роботи стало здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки;
- у вересні 2016 року Верховна Рада України у першому читанні прийняла Закон "Про основні засади забезпечення кібербезпеки України" [13].

Розпорядженням Кабінету Міністрів України від 10.03.17 р. № 155-р "Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України" було затверджено заходи, спрямовані на: удосконалення нормативно-правового регулювання кібербезпеки; створення технологічної складової національної системи кібербезпеки; налагодження більш тісного співробітництва з міжнародними партнерами України; налагодження процесу підготовки кадрів у сфері кібербезпеки [14].

Із введенням 14 вересня 2020 року в дію нової Стратегії національної безпеки України було дано старт і підготовці проектів низки стратегічних документів, одним з яких є Стратегія кібербезпеки України, яку було затверджено Указом Президента України від 26.08.21 р. № 447 [15]. У цій Стратегії зазначається, що подолання негативної ситуації, що склалася у світі й в Україні з кіберзлочинністю, потребує спільних скоординованих дій світового співтовариства, усунення суперечностей між законодавством різних країн.

Важливим є і врахування у новій Стратегії базових стратегічних засад, визначених (ст. 4) у Стратегії національної безпеки України 2020 року – стримування, стійкості та взаємодії [16].

Відповідно до Стратегії для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування) [15].

Кіберстійкість, у свою чергу, передбачає спроможність всіх суб'єктів кібербезпеки своєчасно ідентифікувати загрози кібербезпеці, розбудовувати захист, впроваджувати інструменти виявлення кібератак, забезпечувати належну реакцію на них та швидко відновлювати стабільну роботу під час та після кібератак [16].

Для формування потенціалу стримування необхідним є досягнення стратегічних цілей Стратегії, серед яких заслуговує на увагу ціль С.3, яка сформульована так: "Ефективна протидія кіберзлочинності – Україна має забезпечити набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів" [15].

Проголошується, що для досягнення цієї цілі Україна посилить спроможності у протидії кіберзлочинності шляхом:

завершення імплементації в законодавство України положень Конвенції про кіберзлочинність;

врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав-членів ЄС та враховуючи сучасні виклики і тенденції у сфері кібербезпеки;

розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних веб-сайтах;

проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати та реагувати на кіберзагрози;

забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів;

забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

залучення приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів [15].

Підвищить ефективність розслідування кіберзлочинів імплементація у вітчизняне законодавство статей 16 – 18 Конвенції про кіберзлочинність, а саме невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки, тощо) із забезпеченням їх цілісності [9, с. 130]. Потребують впровадження у вітчизняне законодавство норми статті 19 (Обшук і арешт комп'ютерних даних, які зберігаються) Конвенції про кіберзлочинність шляхом закріплення можливості копіювати електронні дані, здійснювати їх пошук, а також їх блокувати/арештовувати.

Відповідні процесуальні дії доцільно здійснювати на підставі ухвали слідчого судді, суду, а фактичні дані, отримані подібними способами вважати допустимими доказами у кримінальному провадженні [9, с. 130].

Висновки.

Урахування прогресивного та ефективного міжнародно-правового досвіду у сфері протидії кіберзлочинності є вкрай необхідним для розробки національної системи заходів забезпечення кібербезпеки.

Для досягнення проголошених у Стратегії [15] цілей в контексті підвищення ефективності протидії кіберзлочинності доцільно:

завершити імплементацію в чинне законодавство України положень Конвенції про кіберзлочинність, зокрема, шляхом встановлення відповідальності за: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних;

провести чітке розмежування повноважень суб'єктів забезпечення кібербезпеки;

підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів, які використовуються для здійснення кіберзлочинів;

підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів, як це передбачено положеннями Стратегії [15].

Використана література

2. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

3. Леонов Б.Д., Серьогін В.С. Поняття кіберзлочинності: дискусія триває: матеріали наук.-практ. конф. *Актуальні питання кримінального права,* м. Київ, 20 жовт. 2019 р. Київ: КНУВС, 2019.

4. Самойленко О.А. Протидія кіберзлочинам: криміналістичний аспект: навчально-методичний посібник. Одеса, 2020. 133 с.

5. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

6. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КИТ, 2010. 148 с.

7. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Young Scientist*. 2019. № 12.1 (76.1). С. 55-59.

8. Сірко В.С. Організаційно-правові питання протидії кіберзлочинності. *Право*. 2020. № 2 (68). С. 103-105.

9. Тарасюк А.В. Кібербезпека на сучасному етапі державотворення: теоретико-правові основи: монографія. Київ-Одеса: Фенікс, 2020. 404 с.

10. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право.* № 1(24)/2018. С. 127-132.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

12. Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning 455 the criminalisation of acts of a racist and xenophobic nature committed through 456 computer systems. URL:https://rm.coe.int/168008160f

13. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет "ІДМУ", 2003. 296 с.

14. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/.

15. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.17 р. № 155-р. URL: https://zakon.rada.gov.ua/laws/show/155-2017-%D1%80#Text

16. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

17. Дубов Д. Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування? – (Аналітична доповідь). URL: https://niss.gov.ua/doslidzhennya/informaciyna-politika/formuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo

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

УДК 341.1

БЄЛЄВЦЕВА В.В., *доктор юридичних наук, с.н.с.,* завідувач Наукової лабораторії правових проблем та відповідальності у сфері цифровізації ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0001-5573-3744.

ЗАСТОСУВАННЯ ПРИНЦИПІВ МІЖНАРОДНОГО ПРАВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ БЕЗПЕКИ

Анотація. *Статтю присвячено обґрунтуванню значення загальновизнаних міжнародних принципів у сфері забезпечення міжнародної безпеки. У висновках окреслені правові основи існування права міжнародної безпеки та підстави збільшення кількості основних принципів міжнародного права.*

Ключові слова: *міжнародний принцип, міжнародне право, право міжнародної безпеки, міжнародна безпека.*

Summary. *The article substantiates the importance of universally recognized international principles in the field of international security. The scientific article outlines legal framework of international security law and grounds for increasing the number of basic principles of international law.*

Keywords: *international principle, international law, international security law, international security.*

Аннотация. *Статья посвящена обоснованию значения общепризнанных международных принципов в сфере обеспечения международной безопасности. В работе очерчены правовые основы права международной безопасности и предпосылки к увеличению количества основных принципов международного права.*

Ключевые слова: *международный принцип, международное право, право международной безопасности, международная безопасность.*

Постановка проблеми. Світові трансформаційні процеси сьогодення переконливо демонструють, що міжнародне право є системою, яка знаходиться у постійному динамічному розвитку, оскільки змінюється коло відносин між державами та іншими суб'єктами міжнародного права. Відбувається формування нових галузей міжнародного права, а це, у свою чергу, тягне за собою зміни у змістовному навантаженні вже існуючих галузей. Це положення стосується й права міжнародної безпеки.

Право міжнародної безпеки науковцями визначається по-різному. Головні відмінності пов'язані з різним розумінням безпосередньо категорії "безпека", а отже, з предметом регулювання.

Міжнародна безпека базується, у першу чергу, на дотриманні основних принципів міжнародного права. Можна констатувати, що регулювання сучасних міжнародних відносин досить часто базується на нових концепціях і доктринах, які вступають у протиріччя з визнаними основними принципами міжнародного права, змінюють їх сутнісну природу, системні основи міжнародного права і права міжнародної безпеки.

Результати аналізу наукових публікацій. Проблемами права міжнародної безпеки на фрагментарному рівні займались такі вчені, як: П.М. Бірюков, В.Г. Буткевич, К.А. Бекяшев, В.А. Василенко, В.Н. Денисов, Ф.І. Кожевніков, Ю.М. Колосов, Е.С. Крівчікова, В.М. Кулагін, І.І. Лукашук, Г. Моргентау, Д. Мюллер, К. Райт, В.М. Репецький, В.К. Собакін,

Л.Д. Тимченко, Р.А. Тузмухамедов, Г.І. Тункін, А.М. Талалаєв, Н.А. Ушаков, М.Ю. Черкес та ін.

Принципи міжнародного права досить ґрунтовно досліджені у вітчизняній науці. Їм присвячені наукові праці В.Г. Буткевича, Ю.Л. Бошицького, М.В. Буроменського, А.С. Довгерта, В.М. Корецького, І.І. Лукашука, Л.Д. Тимченка та багато ін. У теорії міжнародного права є стійка тенденція пов'язувати поняття міжнародної безпеки з наявністю міжнародних правовідносин, що регулюються принципами і нормами міжнародного права (І.П. Бліщенко, Ю.Г. Даник, І.І. Лукашук, А.П. Мовчан, Ю.А. Решетов, Н.А. Ушаков, М.Л. Ентін та ін.).

Метою статті є узагальнення принципів міжнародного права у сфері забезпечення міжнародної безпеки.

Виклад основного матеріалу. Необхідно відзначити, що загально-засадчі принципи сучасного міжнародного права можна визначити як його загальновизнані норми, що мають найбільш важливе значення для забезпечення стабільного функціонування міждержавної системи й, отже, для вирішення міжнародних конфліктів, тобто для забезпечення міжнародної безпеки. Таке визначення знайшло підтвердження у Рішенні Міжнародного Суду 1974 року щодо конфлікту між США і Канадою про кордон у затоці Мен, в якому наголошується, що слова "принципи і норми" визначають одну ідею, а саме – термін "принципи" означає правові принципи, тобто він включає норми міжнародного права. Використання терміну "принципи" виправдано, оскільки йдеться про загальні і фундаментальні норми [1, с. 256].

Проблема основних принципів міжнародного права досить ґрунтовно вивчена у міжнародно-правовій науці. Як наголошується у Декларації про принципи міжнародного права 1970 року, добросовісне дотримання принципів міжнародного права, що стосуються дружніх стосунків і співпраці між державами, і добросовісне виконання державами зобов'язань, прийнятих відповідно до Статуту, мають найважливіше значення для підтримки міжнародного миру і безпеки та для досягнення інших цілей ООН [2].

Загальновідомо, що основні принципи сучасного міжнародного права закріплені, перш за все, у Статуті ООН. Проте, деякі з них сформульовані дуже стисло. Тому за ініціативою низки держав у 1960-ті роки в ООН була проведена робота з кодифікування основних принципів. Вона завершилася прийняттям у 1970 році Генеральною Асамблеєю ООН Декларації про принципи міжнародного права, що стосуються дружніх стосунків і співпраці між державами відповідно до Статуту ООН. Декларація містить сім принципів:

- незастосування сили або загрози силою;
- мирного вирішення міжнародних конфліктів;
- невтручання у справи, що відносяться до внутрішньої компетенції держави;
- щодо обов'язку держав співпрацювати один з одним відповідно до Статуту ООН;
- рівноправ'я і самовизначення народів;
- суверенної рівності держав;
- добросовісного виконання державами зобов'язань, прийнятих ними відповідно до Статуту ООН [2].

У Заключному акті Наради з безпеки та співробітництва в Європі (СБСЄ, нині – ОБСЄ) від 1 серпня 1975 р. (м. Хельсінкі) міститься десять основних принципів. Принципи, перераховані у Декларації 1970 років, доповнено принципами недоторканності кордонів, територіальної цілісності держав, поваги до прав людини та її основних свобод.

Доцільно відзначити, що класифікація основних принципів у міжнародному праві умовна, адже усі вони взаємозв'язані, і кожен принцип має значення для всієї

міждержавної системи безпеки. Проте, класифікація має практичну користь [3, с. 11-34], оскільки регулююча роль окремих принципів виявляється переважною у різних сферах міжнародних відносин. З врахуванням цього вважаємо погодитись з наступною класифікацією основних принципів міжнародного права, що зустрічається у юридичній літературі. Зокрема, принципи мирного співіснування держав незалежно від їх економічних, соціальних і політичних систем; принципи, що безпосередньо відносяться до підтримки міжнародного миру і безпеки; загальні принципи міжнародного співпробітництва.

Сьогодення показує, що зростання ролі міжнародних відносин у суспільстві та поява нових глобальних викликів та загроз ведуть до збільшення кількості основних принципів міжнародного права.

Отже, для подальшого зміцнення і розвитку принципів міжнародного права у сфері забезпечення міжнародної безпеки великого значення набувають цінності і принципи, визначені у Декларації тисячоліття ООН 2000 року, в якій відзначаються наступні наміри держав: “Ми визнаємо, що окрім індивідуальної відповідальності перед нашими власними суспільствами ми несемо також колективну відповідальність за затвердження принципів людської гідності, справедливості і рівності на глобальному рівні... Ми знов заявляємо про нашу прихильність цілям і принципам Статуту Організації Об’єднаних Націй, які довели свою непідвладність часу та універсальний характер. Їх актуальність і здатність служити джерелом натхнення зростають у міру того, як країни і народи стають усе більш взаємозв’язаними і взаємозалежними. Ми сповнені рішучістю встановити справедливий і міцний мир у всьому світі відповідно до цілей і принципів Статуту. Ми підтверджуємо своє зобов'язання прикладати усі зусилля, спрямовані на забезпечення суверенної рівності усіх держав, повагу до їх територіальної цілісності та політичної незалежності, урегулювання суперечок мирними засобами і відповідно до принципів справедливості і міжнародного права, права на самовизначення народів, які ще знаходяться під колоніальним пануванням та іноземною окупацією, невтручання у внутрішні справи держав, поваги до прав людини і основних свобод, дотримання рівних прав для усіх, без відмінності раси, статі, мови і релігії і міжнародної співпраці у вирішенні міжнародних проблем економічного, соціального, культурного і гуманітарного характеру... Ми вважаємо, що важливе значення для міжнародних відносин у XXI столітті матиме ряд фундаментальних цінностей. До них відносяться: свобода, рівність, солідарність, терпимість, повага до природи і загальний обов'язок. Останнє, зокрема, передбачає: усунення загрози міжнародному миру і безпеці повинне розділятися між народами світу і здійснюватися на багатосторонній основі. Центральну роль в цьому повинна відіграти ООН, як найбільш універсальна і найпоказніша організація у світі...” [4].

Висновки.

1. Зміст, значення та особливості принципів забезпечення міжнародної безпеки визначаються сучасним міжнародним правом, як сукупністю певних юридичних норм, що реалізовуються у функціонуванні міжнародної спільноти, у відносинах держав у відповідних аспектах конкретної діяльності на міжнародній арені.

Отже, забезпечення міжнародної безпеки охоплює наступні завдання – забезпечення миру і справедливості на міжнародній арені, захист усіх суб’єктів міжнародного права від глобальних викликів та загроз, негативних проявів, підвищення соціально-економічних умов життя населення, гуманізація усіх сфер життєдіяльності міжнародного співтовариства.

Міжнародна безпека, будучи складовою соціально-політичних і правових явищ, характеризує стан міжнародних відносин. Інакше кажучи, міжнародна безпека є система відносин держав, що заснована на законності та нормах міжнародного права. Міжнародне право, особливо з прийняттям Статуту ООН, що закріплює справедливі принципи відносин між державами і народами, втілює нормативно-юридичну модель міжнародної безпеки, що відповідає інтересам усіх держав і народів. Міжнародне право забезпечує стан захищеності міжнародної спільноти.

2. Специфіка міжнародної безпеки обумовлена погоджувальною природою міжнародного права та особливостями його системи. Міжнародне прилюдне право – це підсистема міждержавної системи. Його особливості визначаються характером міждержавної системи, в якій воно функціонує і розвивається. Міждержавна система істотно відрізняється від будь-якої внутрішньої державної системи за своїми компонентами, ступенем їх інтеграції, структурою, характером зв'язків і взаємодій, функціонуванням, інакше кажучи, за усіма основними параметрами.

Головними компонентами і суб'єктами міждержавної системи є держави – суверенні утворення. Усі інші компоненти у міждержавній системі є утвореннями, що так або інакше створені державами. Крім того, необхідно відзначити, що міжнародне право як право специфічної соціальної системи, міждержавної системи, відрізняється від внутрішньодержавного права за способом створення норм, соціальним змістом, суб'єктами, об'єктом регулювання, способами функціонування.

Оскільки у міждержавній системі не існує судових і виконавчих органів, ідентичних тим, які існують у державах, функціонування міжнародного права і, перш за все застосування його норм, істотно відрізняється від функціонування і застосування норм внутрішнього державного права. Головну роль у функціонуванні міжнародного права відіграють держави, а також міжнародні організації. Органом забезпечення міжнародного права в аспекті верховенства права є Міжнародний Суд ООН.

3. Зміст та сутність міжнародної безпеки визначається також характером міжнародно-правових норм. У теорії міжнародного права міжнародно-правова норма розглядається як узагальнене правило поведінки суб'єктів міжнародного права. У загальній теорії права правова норма зазвичай визначається як узагальнене правило поведінки. Це положення застосовується й до норм міжнародного права. Норма міжнародного права – це правило поведінки, звернене зазвичай до персонально невизначеного кола суб'єктів міжнародного права. Норми міжнародного права поділяться на диспозитивні та імперативні. Диспозитивними нормами називаються такі норми, від яких держави можуть відступати за взаємною угодою. Імперативні норми (*jus cogens*) – це норми, від яких держави не можуть відступати навіть за взаємною угодою, і договір між державами, що суперечить таким нормам, є юридично недійсним.

4. Особливості принципів забезпечення міжнародної безпеки визначаються і специфікою міжнародних правовідносин, передумовою виникнення яких є три категорії правових норм: норми договірні, норми звичайні, норми, сформульовані у рішеннях міжнародних організацій. Тобто, усі норми міжнародного права, незалежно від порядку їх створення, виступають як вираження суверенної волі держав, що виступають єдиними творцями норм міжнародного права, здійснюючи цю свою виключно важливу функцію або безпосередньо (договірні і звичайні норми), або безпосередньо через міжнародні органи, що створені для виконання певних завдань міжнародного співробітництва. Необхідною умовою забезпечення міжнародної безпеки є юридична правомірність міжнародних правовідносин, оскільки у більшості випадків реалізація розпоряджень міжнародного права має місце у процесі правовідносин держав.

5. Міжнародна безпека тісно пов’язана із забезпеченням законності. Законність у внутрішньодержавному праві передбачає одноманітне розуміння і вживання норм права, реалізацію цих норм у повному обсязі, виконання розпоряджень норм у встановлені терміни. Усе це повною мірою відноситься і до міжнародного права. Вимогою для міжнародної життєдіяльності є дотримання загальнодемократичних принципів сучасного міжнародного права. Що стосується дотримання загальнодемократичних норм і принципів, то це обов'язково для усіх держав. Без суворого дотримання даного мінімуму не може бути забезпечений стабільний стан міжнародної безпеки та жорстке дотримання міжнародної законності.

6. Основні риси міжнародного права визначають зміст і специфіку принципів міжнародної безпеки як соціально-політичного і правового явища. Це положення знайшло своє віддзеркалення й у теорії міжнародного права. Таким чином, міжнародна безпека визначається як стан захищеності життєдіяльності міжнародного співтовариства, впорядкований на засадах міжнародного права у межах забезпечення міжнародної законності. Тобто, міжнародну безпеку можна визначити як упорядковану систему міжнародних відносин, інституційно побудовану на засадах принципів і норм міжнародного права, зі встановленою метою щодо захисту загальних інтересів міжнародної спільноти у цілому.

7. На становлення та розвиток сучасної системи забезпечення міжнародної безпеки досить серйозно вплинули найбільші події у житті суспільства і в міждержавній системі. Поява нових принципів міжнародного права стала підґрунттям становлення сучасних принципів міжнародної безпеки. До найважливих міжнародно-правових принципів забезпечення міжнародної безпеки відносяться: принцип заборони агресивної війни, принцип злочинності такої війни, право усіх народів і націй на самовизначення, принцип рівноправ’я держав, принцип недійсності нерівноправних угод, нав’язаних силою, принцип поваги до соціально-економічних прав людини.

Вирішальне значення для остаточного становлення сучасних принципів забезпечення міжнародної безпеки мали підсумки Другої світової війни і подальший міжнародний розвиток. Найважливішою віхою у затвердженні сучасних принципів міжнародної безпеки є створення Організації Об’єднаних Націй.

ООН відіграє важливу позитивну роль у розвитку міжнародних відносин, а положення її Статуту є засадничим фундаментом сучасного міжнародного права і сучасної системи принципів міжнародної безпеки. Статут ООН не лише розвинув старі демократичні принципи міжнародного права, але й розширив їх до низки нових фундаментальних принципів, таких, наприклад, як принцип незастосування сили і загрози силою у відносинах між державами, право на самовизначення усіх народів, принцип рівноправ’я усіх держав, принцип до основних прав і свобод людини. Статут ООН став основним документом сучасного міжнародного права. Відповідно до Статуту ООН був створений міжнародний механізм реалізації норм міжнародного права, ефективніший, ніж механізм Ліги Націй. Найважливішими ланками цього механізму є Рада Безпеки ООН і Міжнародний Суд ООН.

8. Динаміка розвитку міжнародного права протягом XXI століття характеризує себе істотними позитивними змінами у системи принципів забезпечення міжнародної безпеки. Сучасна система принципів забезпечення міжнародної безпеки має якісні за природою і сутнісні за характером відмінності від колишньої, що базувалася на нормах класичного міжнародного права. Це пов’язано, перш за все, зі зміною основних принципів і інститутів міжнародного права. Важливе значення у науці і практиці сучасного міжнародного права має процес виокремлення сфери прав і свобод людини як цілісний

за формою і закінчений за характером інститут сучасної міжнародної юриспруденції. Принцип поваги до прав людини став загальновизнаним принципом міжнародного права. Питання прав людини перестали повністю входити до внутрішньої компетенції держави. Так, індивід набуває дедалі більше елементів міжнародної правосуб'єктності. Істотні зміни сталися також у всіх галузях міжнародного права – у таких, наприклад, як суб'єкти міжнародного права, право міжнародних договорів, міжнародно-правова відповідальність, мирне вирішення конфліктів, дипломатичне і консульське право. З'явилися ряд нових галузей міжнародного права: право міжнародних організацій, права людини, право міжнародної безпеки, міжнародне право довкілля, міжнародне космічне право, міжнародне ядерне право, міжнародне економічне право та ін.

9. Особливу роль у становленні і підтримці міжнародної безпеки відіграють основні принципи сучасного міжнародного права. Основні принципи сучасного міжнародного права можна визначити як його загальновизнані норми, що мають важливе значення для забезпечення нормального функціонування міждержавної системи і, отже, для вирішення міжнародних проблем у цілому.

Отже, зростання ролі міжнародних відносин у суспільстві і поява нових глобальних викликів та загроз ведуть до підвищення ролі основних принципів міжнародного права у забезпеченні міжнародної безпеки.

Використана література

1. Кононенко В.П. Вирішення територіальних спорів Міжнародним Судом ООН: теорія і практика: монографія. Київ-Одеса: Фенікс. 2018. 438 с.

2. Про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту ООН: Декларація ООН від 24 жовтня 1970 року. URL: https://zakon.rada.gov.ua/laws/show/995_569

3. Устав Организации Объединенных Наций. Действующее международное право / сост. Ю.М. Колосов, Э.С. Кривчикова. В 2-х т. Т. 1. Москва: Юрайт, 2007. 768 с.

4. Тисячоліття ООН: Декларація ООН від 8 вересня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/995_621

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

УДК 343.98:004.056

ГУЦАЛЮК М.В., *кандидат юридичних наук, с.н.с, доцент,*
провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

НАПРЯМИ ПОСИЛЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Анотація. *В статті досліджуються сучасні проблеми міжнародного співробітництва у сфері протидії кіберзлочинності.*

Ключові слова: кіберзлочинність, електронні докази, конвенція про кіберзлочинність, міжнародне співробітництво

Ключові слова: *міжнародне співробітництво, кіберзлочинність, правоохоронні органи, електронні докази.*

Summary. *The article examines current problems of international cooperation in combating cybercrime.*

Keywords: *International cooperation, cybercrime, law enforcement, electronic evidence.*

Аннотация*. В статье исследуются современные проблемы международного сотрудничества в сфере противодействия киберпреступности.*

Ключевые слова: *международное сотрудничество, киберпреступность, правоохранительные органы, электронные доказательства.*

Постановка проблеми. Сучасний етап економічного та соціального розвитку суспільства характеризується високими темпами цифровізації та віддаленого обміну інформацією, які значно зросли з початком пандемії CoVID-19. Водночас до нових змін швидко пристосувалась кіберзлочинність – в усьому світі зберігається тенденція збільшення кількості кібератак, їх складності та збитків від них [1]. Однією з причин недостатньої ефективності боротьби з кіберзлочинністю є неможливість протидіяти транснаціональним високотехнологічним злочинам в межах лише однієї держави та недостатнє використання механізмів міжнародної співпраці.

Як правило, кібератаки здійснюються з інших країн, аніж там, де розташовані атаковані інформаційні ресурси, а іноді одночасно з десятків країн з різних куточків світу. Це зумовлює значні труднощі щодо їх розслідування і протидії злочинній діяльності та потребує тісного міжнародного співробітництва як правоохоронних органів так і суб'єктів кібербезпеки.

Результати аналізу наукових публікацій. Результати аналізу наукових публікацій свідчать про те, що питання міжнародного співробітництва правоохоронних органів у боротьбі з кіберзлочинністю були предметом досліджень таких науковців, як M. Maras, A. Cerezo, J. Lopez та вітчизняних Н. Ахтирська, П. Біленчук, В. Бутузов, А. Марущак, Є. Скулиш, К. Тітуніна та інші.

Водночас сучасний розвиток технологій, зростання нових кіберзагроз, складність кібератак потребують нових підходів до підвищення ефективності протидії кіберзлочинності.

Метою статті є розкриття нових напрямів міжнародного співробітництва у сфері боротьби з кіберзлочинністю.

Виклад основного матеріалу. Комп'ютерна злочинність, яка з'явилася наприкінці минулого століття, з поширенням мережі Інтернет по всьому світу постійно змінюється та набуває нових масштабів, що безумовно турбує як окремі держави, так і в цілому світову спільноту, та вимагає тісного міжнародного співробітництва для протидії цьому явищу. З 1991 року при Генеральному секретаріаті Інтерполу діє робоча група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах світу, розробляє рекомендації, допомагає в стандартизації національних законодавств, напрацьовує методичний досвід запобігання й розслідування комп'ютерних злочинів [2].

В розвинутих країнах світу кримінальна відповідальність за вчинення комп'ютерних злочинів була введена у кінці 1980-х, на початку 1990-х років. В Україні стаття 198-1 "Порушення роботи автоматизованих систем" Кримінального кодексу України 1960 року була введена у 1994 році.

Вже на межі століть такі комп'ютерні віруси як Melissa, Love Letter/I LOVE YOU призвели до значних збитків по всьому світу, а злочинці свою увагу звернули на віддалений несанкціонований доступ до банківської інфраструктури, що було менш небезпечним та більш прибутковим аніж традиційні напади на банківські відділення. Все це заважало нормальному функціонуванню як економіки держав, так і Інтернету. Власне через активне використання кіберпростору злочини з використанням його можливостей отримали назву кіберзлочини, а саме явище отримало назву кіберзлочинності, що пізніше було законодавчо закріплене [3].

В резолюції Генеральної Асамблеї ООН A/RES/53/70 від 4 січня 1999 року "Досягнення в сфері інформатизації і комунікації у контексті міжнародної безпеки" зазначається, що використання інформаційних технологій і засобів стосується інтересів всього міжнародного співтовариства і що міжнародна взаємодія сприяє забезпеченню максимальної ефективності. Вважаючи за необхідне запобігти неправомірному використанню або використанню інформаційних ресурсів чи технологій в злочинних чи терористичних цілях, ООН закликає держави-члени сприяти розгляду існуючих та потенційних загроз у сфері інформаційної безпеки [4].

У зв'язку з тим, що сам по собі складний характер кіберзлочинності посилюється ще й участю організованих злочинних груп у протиправній діяльності в глобальній мережі, а кіберзлочинці та їх жертви часто знаходяться в різних регіонах, ООН підкреслює необхідність відповідного міжнародного скоординованого динамічного реагування. Для цього в рамках Комісії з питань запобігання злочинності та кримінального правосуддя функціонує міжурядова група експертів для проведення всебічного дослідження проблеми кіберзлочинності. Група на своїх засіданнях надає рекомендації, щодо вдосконалення боротьби кіберзлочинності, напрацьовані в різних країнах світу.

Для налагодження тісної співпраці правоохоронних органів різних держав у 2002 році у Лондоні був проведений Перший міжнародний стратегічний конгрес "E-Crime 2002" на якому представники правоохоронних органів, приватного сектору та державних органів з усього світу обмінювалися своїм досвідом щодо протидії злочинам, які вчиняються з використанням комп'ютерів та мереж передачі даних. У роботі конгресу брали участь і українські правоохоронці [5].

Серед основних міжнародних нормативно-правових документів щодо протидії кіберзлочинності, у тому числі організованої, на сьогодні слід виокремити такі:

– Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime), підписана у м. Палермо 12 грудня 2000 року та ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV(1433-15);

– Європейська Конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters), підписана у м. Страсбурзі 20 квітня 1959 року та ратифікована із заявами і застереженнями Законом України від 16.01.98 р. № 44/98-ВР;

– Конвенція про кіберзлочинність (Convention on Cybercrime), підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV(2824-15).

Міжнародне співробітництво правоохоронних органів України з іноземними компетентними органами здійснюється на підставі розділу IX Кримінального процесуального кодексу України "Міжнародне співробітництво під час кримінального провадження" (ст.ст. 541-550 КПК України). Співробітництво між державами здійснюється через відповідний центральний орган. Центральними органами України є:

- під час досудового провадження – Генеральна прокуратура України;
- під час судового провадження – Міністерство юстиції України.

З метою протидії транснаціональній злочинності держави-члени Європейського Союзу об'єднали свої зусилля та створили низку спеціалізованих органів, діяльність яких спрямована на підтримання правопорядку і сприяння роботі національних правоохоронних органів. До таких органів належать, зокрема: Європейське поліцейське відомство (Європол), Європейська організація з питань юстиції (Євроюст), Європейська агенція управління оперативним співробітництвом на зовнішніх кордонах ЄС (FRONTEX). Поряд із ними існує низка спеціалізованих допоміжних органів, серед яких Європейський моніторинговий центр з наркотиків та наркотичної залежності, Постійний комітет із питань оперативного співробітництва у сфері внутрішньої безпеки, Група експертів із питань торгівлі людьми, Європейська мережа попередження злочинності, Європейський офіс боротьби з шахрайством тощо. Усі ці органи створювалися в різний час, виходячи з рівня інтеграційних процесів та досягнень у рамках ЄС, а також нагальних потреб його держав-учасниць.

У 2013 році для посилення реагування правоохоронних органів на кіберзлочинність у ЄС Європол створив Європейський центр кіберзлочинності (European Cybercrime Centre – EC3) для захисту європейських громадян, бізнесу та уряду від злочинності в Інтернеті. З моменту свого створення EC3 вніс значний внесок у боротьбу з кіберзлочинністю: Центр брав участь у десятках гучних операцій та сотнях операцій щодо оперативної підтримки на місцях, що призвело до сотень арештів, і проаналізував сотні тисяч файлів, переважна більшість з яких виявилися шкідливими. EC3 продовжує проводити науково-дослідні роботи у сфері цифрової криміналістики, здійснює стратегічний аналіз організованої кіберзлочинності та забезпечує розвиток навчання правоохоронців щодо протидії кіберзлочинності [6].

Створення міжнародної нормативної бази та функціонування міжнародних та європейських інституцій по боротьбі з кіберзлочинністю надало змогу підняти на новий рівень протидію кіберзлочинності, що жодна з країн не здатна зробити самотужки.

Водночас і кіберзлочинці не зупиняються на відточенні своїх навичок, розширенні методів, створенні сервісів на кшталт "кіберзлочини як послуга" та посиленні організованості кіберзлочинності, у тому числі угруповань, які підтримуються урядами певних країн.

Сьогодні, коли кількість активних користувачів Інтернет перевищила 5 млрд. [7], питання кібербезпеки постають як ніколи гостро. Зокрема за даними компанії з кібербезпеки CrowdStrike кожен день створюється понад 360000 нових шкідливих програм (ШП), а атаки програм-вимагачів досягли "стратосферного рівня" і складають на

сьогодні 69 % всіх атак [8], пов'язаних з ШП. Середня вартість викупу програм-вимагачів у 2021 році оцінюється експертами у $6,3 млн. США. Прогноз глобальних витрат від пошкодження програм-вимагачів становитиме $20 млрд. до кінця 2021 року, що набагато більше, ніж це було у минулі роки. Особливо небезпечними є напади на об'єкти критичної інфраструктури.

Так уряд США оголосив надзвичайний стан після кібератаки хакерського угруповання DarkSide на один з найбільших трубопроводів країни Colonial Pipeline, що сталася 7 травня 2021 року. Для кібератаки хакерське угруповання DarkSide використало шкідливу програму-вимагач та погрожувало оприлюднити близько 100 ГБ даних.

Через кібератаку Colonial Pipeline перекрила частину трубопроводу довжиною майже 9 тисяч кілометрів. Компанія транспортує близько 2,5 мільйони барелів палива на схід та південь Сполучених Штатів, зокрема забезпечує паливом штат Нью-Йорк і його найбільші аеропорти [9].

Також 2 липня 2021 року було здійснено хакерську атаку на американську компанію Kaseya, що спеціалізується на розробці програмного забезпечення для мережевої інфраструктури. Як наслідок, робота принаймні 200 компаній у США була паралізована. У ЗМІ повідомляли, що кібератака вивела з ладу обчислювальні системи у 800 шведських супермаркетах, 11 школах Нової Зеландії і двох ІТ-компаніях Данії. Ймовірно, за атакою стояло хакерське угруповання з РФ REvil, кіберзлочинці якого вимагали $70 млн. викупу в криптовалюті для повернення вкраденої ним інформації [10].

А у німецькому регіоні Ангальт-Біттерфельд, що у федеральній землі Саксонія-Ангальт, 10 липня 2021 року оголосили перший в історії країни режим надзвичайного стану через кібератаку. Унаслідок дій зловмисників майже повністю заблокувалася робота місцевої влади, внаслідок чого населення регіону (157 тисяч) не могло отримати соціальні виплати й не мало доступу до інших послуг місцевої влади [10].

Таке збільшення у геометричній прогресії кіберзагроз потребує розробки нових стратегій кібербезпеки та посилення міжнародної співпраці щодо протидії кіберзлочинності.

Слід зазначити, що одночасне та скоординоване проведення розслідувань та арештів кіберзлочинців в різних країнах призводить до відчутного результату. Наприклад, під час масштабної операції за участі правоохоронців 30 країн з ліквідації кібермережі "Avalanche" у 2016 році, яка проходила за підтримки Центру боротьби з кіберзлочинністю Європолу (EC3) та Об'єднаної групи боротьби з кіберзлочинністю (J-CAT), а також Євроюсту та Європейської банківської федерації (EBF) було заарештовано 178 осіб-співучасників, у тому числі і її організатори в Україні.

Останніми роками участь українських правоохоронців у таких операціях значно поширилась. Зокрема у 2020 році кіберполіція провела 10 міжнародних поліцейських операцій із викриття "хакерських" угруповань, учасники яких завдали збитків країнам ЄС, Великої Британії та США на суму понад $300 млн. [11].

Разом з тим, під час під час досудового розслідування кіберзлочинів, особливо тих, докази про вчинення яких знаходяться в юрисдикції іншої країни, виникають певні труднощі у їх отриманні, зберіганні та оперативному аналізі. Крім того, Україною ще не імплементовані такі статті Конвенції про кіберзлочинність, як: ст. 16 – "Термінове збереження комп'ютерних даних, які зберігаються" та ст. 17 – "Термінове збереження і часткове розкриття даних про рух інформації". Відповідний законопроект за № 4004 вже більше року як зареєстрований Верховною Радою України та потребує розгляду.

Комітет Ради Європи 12 квітня 2021 року опублікував проект *"Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття*

електронних доказів", яким, зокрема, передбачається: пряма співпраця з постачальниками послуг (стаття 6) та суб'єктами, що надають доменне ім'я реєстраційні послуги (стаття 7) для розкриття інформації для ідентифікації підозрюваних; прискорення форм співпраці між Сторонами для розкриття інформації про абонентів та даних про рух (стаття 8); пришвидшення співпраці з розкриття інформації у надзвичайних ситуаціях (статті 9 та 10); додаткові інструменти взаємодопомоги (статті 11 та 12); захист даних та інші гарантії верховенства права (статті 13 та 14). Обговорення вказаних новацій та пропозиції своїх варіантів цього міжнародного акту повинні стати важливим етапом усіх зацікавлених суб'єктів протидії кіберзлочинності [12].

У грудні 2019 року в своїй резолюції 74/247 Генеральна Асамблея ООН вирішила створити Спеціальний міжурядовий Комітет експертів відкритого типу, представників усіх регіонів, для розробки всеосяжної міжнародної *Конвенції про протидію використанню інформаційно-комунікаційних технологій у кримінальних цілях* з урахуванням існуючих міжнародних документів та зусиль на національному, регіональному та міжнародному рівнях щодо протидії використанню інформаційно-комунікаційних технологій у кримінальних цілях та результатів роботи міжурядової групи експертів відкритого типу для проведення комплексного дослідження з питань кіберзлочинності.

26 травня 2021 р. Генеральна Асамблея ООН прийняла Резолюцію "Протидія використанню інформаційно-комунікаційних технологій у кримінальних цілях" № 75/282. Серед іншого у Резолюції визначено, що Спеціальний комітет скликає щонайменше шість сесій по 10 днів кожна, щоб розпочати у січні 2022 року заключну сесію в Нью-Йорку та подати проєкт Конвенції Генеральній Асамблеї на її сімдесят восьмій сесії.

Указом Президента України від 26.08.21 р. № 447/2021 затверджена нова Стратегія кібербезпеки України. У документі визначені основні виклики та загрози для України у сфері кібербезпеки на сучасному етапі, серед яких:

- активне використання кіберзасобів у міжнародній конкуренції;
- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- нарощення арсеналу кіберзброї державою-агресором, використання кібератак проти об'єктів критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсії) та здійснення розвідувальної та розвідувально-підривної діяльності.
- кіберзлочинність, яка призводить до значних матеріальних втрат та використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів тощо.
- використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності тощо.

Для ефективної протидії кіберзлочинності у Стратегії передбачена важлива ціль *"Прагматичне міжнародне співробітництво"* – Україна спрямує відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази.

Для налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед США, державами-членами ЄС та НАТО, створення платформи такого обміну.

В Стратегії також чітко зазначено необхідність забезпечення участі України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах, розширення шляхом діалогу з міжнародними партнерами доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7.

Тобто у Стратегії чітко визначені напрями посилення міжнародного співробітництва у сфері протидії кіберзлочинності. В той же час виконання зазначеної роботи залежить від якісного планування конкретних заходів та їх своєчасного виконання, що не завжди відбувалося при виконанні Стратегії кібербезпеки України 2016 – 2020 років.

Одночасно, визнаючи необхідність посилення та ефективнішої співпраці між державами та приватним сектором щодо розкриття електронних даних, інших форм збору електронних доказів кримінального правопорушення необхідно дотримуватися верховенства права та європейських приписів щодо демократії. Тобто повинні бути створені умови для вільного, відкритого та безпечного кіберпростору, без тоталітарного ведення стеження та безпідставного блокування користувачів у кіберпросторі. На практиці знайти оптимальний баланс у вказаних напрямах діяльності є досить складним завданням.

Також запровадження нових норм та правил міжнародного співробітництва повинно спростити, а не ускладнити існуючі процедури взаємодії, що є вкрай важливим під час розслідування кіберзлочинів.

Висновки.

Постійно зростаюче використання інформаційних технологій, збільшення кількості користувачів Інтернет з різних регіонів світу продовжують загострювати проблему їх безпечного використання.

Разом з тим, ефективна боротьба з кіберзлочинністю вимагає тісного міжнародного співробітництва на основі міжнародних конвенцій, договорів, завдяки обміну передовим досвідом та внаслідок проведення спільних.

Прийняття нової Стратегії кібербезпеки України та її реалізація повинні стати ефективним механізмом у боротьбі з кіберзлочинністю, у тому числі і з її організованими транснаціональними формами.

Використана література

1. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України. *Юридичний вісник "Повітряне і космічне право"*. Т. 1. № 58 (2021). С. 177-184.

2. Комп'ютерна злочинність: навч. посібник / Біленчук П.Д., Бут В.В., Гавловський В.Д., Гуцалюк М.В., Романюк Б.В. Київ: Атіка, 2002. С. 150.

3. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України". Станом на 1 січня 2019 року / Гуцалюк М.В. та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

4. Developments in the field of information and telecommunications in the context of international security / Resolution adopted by the general assembly UN A/RES/53/70 4 January 1999. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english

5. Гуцалюк М. Перший міжнародний стратегічний конгрес "E-CRIME 2002". *Крок.* 2002. № 24. С. 7.

6. European Cybercrime Centre – EC3. URL: www.europol.europa.eu/about-europol/europ ean-cybercrime-centre-ec3

7. Internet live stats. URL: https://www.internetlivestats.com

8. Отчёт: программы-вымогатели составляют 69 % всех атак, связанных с вредоносным ПО. URL: https://internetua.com/otcset-programmy-vymogateli-sostavlyauat-69-vseh-atak-svya zannyh-s-vredonosnym-po

9. US fuel pipeline hackers 'didn't mean to create problems'. URL: https://www.bbc.com/news/ business-57050690

10. Хакери, причетні до масштабної кібератаки, вимагають 70 мільйонів доларів у Bitcoin за доступ до вкрадених даних. URL: https://hromadske.ua/posts/hakeri-prichetni-do-masshtabnoyi-kiberataki-vimagayut-70-miljoniv-dolariv-u-bitcoin-za-dostup-do-vkradenih-danih

11. У 2020 році кіберполіція провела 10 міжнародних поліцейських операцій із викриття "хакерських" угруповань – Олександр Гринчак. URL: https://cyberpolice.gov.ua/news/u--roczi-kiberpolicziya-provela--mizhnarodnyx-policzejskyx-operaczij-iz-vykryttya-xakerskyx-ugrupovan--olek sandr-grynchak-5855

12. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. URL: https://rm.coe.int/0900001680a2aa1c

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

УДК 354:340.133:340.134

ОЗЕРЧУК І.М., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7011-0772.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕПРОСТОРУ ВІД ДІЯЛЬНОСТІ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ

Анотація. *Досліджено проблеми забезпечення захисту кібепростору від діяльності терористичних організацій. Розглядаються існуючі у юридичній літературі визначення тероризму у кіберпросторі. Міститься аналіз законодавчих актів у сфері боротьби з тероризмом, серед яких виділяється Стратегія кібербезпеки України, а також Концепція боротьби з тероризмом. Висвітлюються основні тенденції розвитку діяльності міжнародних терористичних організацій з використанням інформаційних технологій, основні завдання яких зводяться до: пропаганди тероризму, у тому числі з використанням мережі Інтернет; вербування та навчання нових членів; отримання інформації про об'єкти можливих терористичних посягань; забезпечення терористичної діяльності; поширення інструктивних матеріалів виготовлення вибухових пристроїв. На підставі аналізу новацій антитерористичного законодавства країн ЄС запропоновані шляхи удосконалення протидії діяльності терористичних організацій у кіберпросторі.*

Ключові слова: *тероризм, терористичні організацій, кіберпростір, кібератака, антитерористичне законодавство.*

Summary. *The problems of ensuring the protection of cyberspace from the activities of terrorist organizations have been studied. The existing definitions of terrorism in cyberspace in the legal literature are considered. There is an analysis of legislative acts in the field of counter-terrorism, among which the Cyber Security Strategy of Ukraine and the Concept of Counter-Terrorism stand out. The article covers main tendencies of development of activity of the international terrorist organizations with use of information technologies, main tasks of which are reduced to: propaganda of terrorism, including with use of the Internet; recruiting and training new members; obtaining information about the objects of possible terrorist attacks; ensuring terrorist activities; distribution of instructional materials for the manufacture of explosive devices. On the basis of the analysis of innovations of the anti-terrorist legislation of the EU countries the ways of improvement of counteraction of activity of the terrorist organizations in cyberspace are offered.*

Keywords: *terrorism, terrorist organizations, cyberspace, cyber attack, antiterrorist legislation.*

Аннотация. *Исследованы проблемы обеспечения защиты киберпространства от деятельности террористических организаций. Рассматриваются существующие в юридической литературе определения терроризма в киберпространстве. Содержится анализ законодательных актов в сфере борьбы с терроризмом, среди которых выделяется Стратегия кибербезопасности Украины, а также Концепция борьбы с терроризмом. Освещаются основные тенденции развития деятельности международных террористических организаций с использованием информационных технологий, основные задачи которых сводятся к: пропаганде терроризма, в том числе с использованием сети Интернет; вербовки и обучения новых членов; получение информации об объектах возможных террористических посягательств; обеспечения террористической деятельности; распространение инструктивных материалов изготовления взрывных устройств. На основании анализа новаций антитеррористического законодательства стран ЕС предложены пути совершенствования противодействия деятельности террористических организаций в киберпространстве.*

Ключевые слова: *терроризм, террористические организации, киберпространство, кибератака, антитеррористическое законодательство.*

Постановка проблеми. У Стратегії кібербезпеки України (далі – Стратегія), затвердженій Указом Президента України від 26.08.21 р. № 447, відзначається, що використання кіберпростору терористичними організаціями набуває глобального масштабу. Пріоритетними цілями кібертероризму є об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо. Саме тому використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності визначено однією із загроз кібербезпеки України [1].

Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [1]. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій.

За таких умов дослідження проблеми забезпечення захисту кібепростору від діяльності терористичних організацій є вкрай необхідним. Зазначене завдання є надзвичайно актуальним в контексті зростання нових викликів і загроз національній безпеці України, пов'язаних зокрема із застосуванням інформаційних технологій.

Результати аналізу наукових публікацій. Останнім часом питання протидії кібертероризму досліджували Б.Д. Леонов [2], Серьогін В.С. [3], Нізовцев Ю.Ю. [4], Корченко О.Г. [5], Бутузов В.М. [6], Погорецький М.А. [7], Пилипчук В.Г. та Дзьобань О.П. [8]. Питанню визначення кібербезпеки стосувалася робота Баранова О.А. [9], забезпечення кібербезпеки стало предметом праць Гнатюка С.О. [10], Лук'янчука Р.В. [11], Ткачука Н.А. [12] та ін. Водночас, проблемні питання забезпечення захисту кібепростору від діяльності терористичних організацій залишаються недостатньо дослідженими.

Метою статті є удосконалення протидії діяльності терористичних організацій у кіберпросторі з урахуванням антитерористичного законодавства та зарубіжного досвіду боротьби з тероризмом.

Виклад основного матеріалу. У юридичній літературі тероризм розглядається як складне, багатовимірне та багаторівневе явище реальної дійсності, яке розглядається в сучасній правовій науці у двох аспектах: 1) як негативне явище дійсності, що становить певну соціальну систему, детермінована взаємодією негативних факторів суспільного життя та відповідних рис особистості терориста; 2) як правову оцінку та відображення цього явища в чинному законодавстві [13, с. 672]. Іноді тероризм визначають як специфічну форму ведення війни, метою якої є не матеріальний Інтернет-ресурс, і не геополітичний інтерес (сфера впливу та ринки збуту), а інтерес інформаційний – механізм соціального управління в суспільстві [14, с. 6]. Останнім часом з'явився новий термін "інформаційний тероризм", під яким пропонується розуміти антисоціальне явище, для якого характерним є умисне застосування інформаційно-психологічного та інформаційно-технічного впливів, спрямованих на маніпуляцію чи залякування населення або заподіяння шкоди інформаційному 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 інформаціного

простору, пов'язаного з використанням Інтернету, інформаційних технологій і(або) інформаційних ресурсів [15, с. 250].

Окремим різновидом інформаційного тероризму є кібертероризм, який Закон України "Про основні засади забезпечення кібербезпеки України" визначає як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням. Відповідно до ч. 5 ст. 5 цього Закону суб'єкти забезпечення кібербезпеки у межах своєї компетенції здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях [16].

Сучасний тероризм набув суттєвого поширення за допомогою мережі Інтернет. У Концепції боротьби з тероризмом, затвердженій Указом Президента України від 05.03.19 р. № 53, фіксується положення про те, що терористичні загрози, котрі постали перед Україною, вимагають удосконалення функціонування загальнодержавної системи боротьби з тероризмом, яке має здійснюватися з використанням досвіду та найкращих світових практик у сфері боротьби з тероризмом, у тому числі на основі поетапного впровадження положень Глобальної контртерористичної стратегії ООН [17]. Відповідні зусилля повинні спрямовуватися на впровадження дієвих механізмів усунення (локалізації) терористичних ризиків для об'єктів можливих терористичних посягань, що органічно поєднуватимуть політичні, правові, організаційні, інформаційні, соціальні, контррозвідувальні, розвідувальні, оперативно-розшукові, режимні, фінансові й інші заходи [17].

Слід відзначити, що нові тенденції у розвитку тероризму створюють додаткові виклики для національної і міжнародної безпеки і потребують належного реагування. З огляду на це, заходи з удосконалення антитерористичної політики як на національному, так і на міжнародному рівнях мають носити перманентний характер навіть за умов низького рівня відповідної загрози. На даний час, зусилля багатьох країн спрямовані на посилення захисту від терористичної загрози [18].

У червні 2021 року Європол опублікував щорічний звіт про ситуацію з тероризмом та його основні тенденції в країнах Європейського союзу. Автори звіту звернули увагу на той факт, що протягом останніх років кількість здійснених терористичних атак в Європі залишається приблизно на одному рівні. У 2020 році таких атак було зафіксовано 57 в країнах ЄС, 62 – у Великобританії і 2 – в Швейцарії (всього 121). У 2019 р. зафіксовано 119, а у 2018 р. – 129 атак. За останній рік від рук терористів в країнах ЄС загинула 21 людина. При цьому практично всі жертви були обрані випадково [19]. Фіксується також тенденція зниження кількості заарештованих терористів.

Згідно з оприлюдненим Європолом інформаційним звітом усі терористичні атаки були поділені на три основні групи за ідеологічною мотивацією їх виконавців: джихадисти, ультраправі і ультраліві радикали. Відзначається тенденція розширення присутності терористичних та екстремістських груп у віртуальному Інтернет-просторі (у першу чергу в соціальних мережах).

З огляду на активне використання терористичними організаціями Інтернету та соціальних мереж для пропаганди та вербування нових послідовників, планується створення Європейського центру боротьби з тероризмом та радикалізацією в Інтернеті. Він має стати елементом існуючого при Європолі довідкового бюро в мережі Інтернет. При МВС Чехії нещодавно утворено Центр боротьби з тероризмом і гібридними загрозами, діяльність якого зосереджена на аналізі Інтернет контенту і відповідному реагуванні [18].

Інтернет надав додаткові можливості оперативно і скоординовано керувати діями членів терористичних організацій, спілкуватися між собою, поширювати інформацію в режимі реального часу, стимулюючи саморадикалізацію серед потенційних членів радикальних організацій з перспективою їх вербування до терористичних груп [20, с. 76].

Слід погодитися з Леоновим Б.Д., що використання терористами досягнень науково-технічного прогресу, активне використання сучасних інформаційно-комунікаційних технологій, мережі Інтернет з терористичною метою є основною тенденцією поширення терористичної злочинності [20, с. 85].

З використанням сучасних інформаційних технологій, у тому числі мережі Інтернет, міжнародні терористичні організації виконують завдання: 1) пропаганди тероризму (за допомогою великої кількості Інтернет-форумів, онлайн "AQAP", журналу "Inspire" тощо); 2) вербування та навчання нових членів; 3) отримання інформації про об'єкти можливих терористичних посягань; 4) забезпечення терористичної діяльності (планування, зв'язок, збір грошей тощо); 5) демонстрації звітів про результати терористичних актів; 6) поширення інструктивних матеріалів виготовлення вибухових пристроїв [20, с. 76].

Останнім часом спостерігається тенденція зрощування соціальних мереж із ресурсами мобільного зв'язку, що дозволяє розміщати інформацію в соціальних мережах і відслідковувати повідомлення інших абонентів. Це, наприклад, активно використовувалося для загострення протестних акцій у низці арабських країн шляхом поширення дезінформації, провокаційних фото- та відеоматеріалів. Терористичні структури активно використовують медіа-сферу як для звернення до широкої аудиторії, так і для впливу на цільові групи користувачів, тим самим створюючи "свій бренд" і "піар-акції" перед світовою спільнотою [21, с. 43]. Крім цього, слід відзначити, що глобальна електронна мережа сприяла появі багатьох незалежних одна від одної децентралізованих терористичних мереж. На даний час терористичні організації практикують тактику "некерованого супротиву", суть якої зводиться до того, що відповідальність за планування та здійснення терористичної діяльності лягає виключно на децентралізованого виконавця. Тоді як діяльність самої терористичної організації концентрується на складанні інструктивних матеріалів аудіо- та відеозакликів в мережі Інтернет, які допомагають децентралізованим групам не виходити за межі терористичної стратегії, яку виробляють ідеологи та лідери терористичних організацій [21, с. 43].

Активізувалася та перейшла на новий рівень Інтернет-ресурсна база низки терористичних і екстремістських організацій, зокрема "Руху Талібан", "Союзу ісламського джихаду" (СІД), "стамбульські сайти" (//www.sehadetzamani.com; www.sehadetvakti.com). Пропаганда стала більш організованою, активною і агресивнішою, використовуються сучасні методи "промивки мізків" та дезінформація [20, с. 76].

З приводу останнього слід звернути увагу ще на один принциповий момент. Не завжди злочини вчиняються під впливом спілкування у групі. Іноді рішення про вчинення злочину та способи його здійснення навіяні впливом книг, ЗМІ, у тому числі мережі Інтернет.

Потужним інструментом психологічного впливу на прибічників і потенційних терористів-одинаків є публікація терористичними угрупованнями власних електронних журналів, у яких містяться релігійне обґрунтування, рекомендації з підготовки, або прямі заклики до вчинення терактів чи інших насильницьких дій проти конкретних осіб або об'єктів [20, с. 43].

Це нас виводить на проблему терориста-одинака, діяльність якого не пов'язана з міжнародними терористичними організаціями. Тип терориста-одинака, для якого характерна підвищена активність в Інтернеті й відсутність зв'язків з терористичними

організаціями, є відносно новим соціальним феноменом, який дедалі більше привертає увагу правоохоронних органів. Цей тип терористів діє, як правило, під впливом гніву та відчаю, зумовлених пропагандою ідей тероризму, закликів до вчинення певних терористичних дій, висвітлених у друкованих виданнях або в Інтернеті. Особи цієї категорії нерідко є емігрантами або вихідцями з емігрантських родин, які незадоволені політикою країни, де вони перебувають. Зазвичай це спокійні та непомітні люди, які скоюють терористичний акт для того, щоб привернути увагу громадськості до певної події (наприклад, війни в Афганістані) [20, с. 285]. Яскравим прикладом таких актів є напад, який вчинив Андрес Брейвік у Норвегії у липні 2011 року, в результаті якого було вбито 77 людей.

С. Атран, на підставі широких досліджень визначає соціальні характеристики "джихадистів", у тому числі терористів-смертників. Здебільшого це – добре освічена людина, ідеалістично налаштована, політично активна й водночас позбавлена культурного коріння, переважно це молодь із мусульманських і європейських країн. Ці молоди люди, як правило, новоявлені апологети вчення, яке сповідують "радикальні ісламісти". Їхні переконання формуються під впливом історій, у яких демонструється повсюдна соціальна несправедливість та політичні репресії проти мусульман, що поширюються каналами супутникового телебачення та в мережі Інтернет [22, с. 127]. Учений акцентує увагу, що радикалізація молоді відбувається в соціальних мережах: безпосередньо у невеликих групах із числа друзів або в процесі спілкування у віртуальних Інтернет-спільнотах [22, с. 130]. З потенційним смертником ведуть розмову про почесну смерть шляхом знищення "невірних" під час якої навіюється думка про пов'язані з нею надії всього клану, у зв'язку з чим створюється мікросередовище майбутнього смертника. Кінцева мета подібної обробки – добровільне бажання йти на смерть [21, с. 37]. Прояви індивідуального тероризму потребують постійного моніторингу з боку правоохоронних органів.

Використання терористами новітніх інформаційних технологій для вербування нових членів та поширення в мережі Інтернет терористичної ідеології вимагає впровадження нових методів і засобів боротьби з тероризмом. Це зумовлює оновлення антитерористичного законодавства, зміни до якого нещодавно внесені законодавцем низки країн ЄС.

Так, німецьким законодавцем у 2016 р. внесено зміни до Закону "Про Федеральну розвідувальну службу" (BND), якими розширюються повноваження цієї служби. Зокрема, передбачено надання 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 [18]. Серед інших додаткових заходів, спрямованих на протидію тероризму в Німеччині, також можна виокремити: надання 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; підвищення спроможностей спецслужб з виявлення та припинення протиправної діяльності у кіберпросторі [18], особлива увага приділятиметься "Даркнету", який активно використовується терористичними угрупованнями.

У 2016 році Парламентом Франції до Кримінального кодексу внесено зміни, якими передбачено встановлення відповідальності за нові види злочинів, зокрема, створення сайтів терористичної спрямованості за межами Франції [18]. 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 [18].

7 червня 2016 парламент Угорщини вніс зміни до Конституції та низки законів, що стосуються реагування на терористичні загрози. Конституція відтепер містить положення про можливість оголошення урядом стану терористичної загрози (потребує затвердження парламентом протягом наступних 15 днів). Серед заходів, що можуть запроваджуватись урядом виділяється більш строгий контроль Інтернету і поштового зв'язку. При МВС Угорщини створено Інформаційно-аналітичний центр по боротьбі з тероризмом та злочинністю, основним завданням якого є моніторинг та аналіз даних про загрози національній безпеці [18].

Україна також не стоїть осторонь проблеми забезпечення захисту кіберпростору від діяльності терористичних організацій. Так, у Стратегії одним з важливих пріоритетів забезпечення кібербезпеки України визначено забезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства. Стратегією передбачено, що за допомогою розгалуженої системи індикаторів буде визначатися стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Серед цілей Стратегії виділяється посилення спроможності національної системи кібербезпеки для мінімізації загроз кіберзлочинності та кібертероризму (стримування) [1].

Ціль С.2 Стратегії сформульована так: "Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму – Україна забезпечить безперервне здійснення 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". Для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму, зокрема, шляхом створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури [1].

Висновки.

Одним з важливих напрямів антитерористичної діяльності є забезпечення захисту кіберпростору від діяльності терористичних організацій шляхом удосконалення системи виявлення кібератак та проявів кібертероризму.

Важливе значення для України має посилення взаємодії між правоохоронними органами України із відповідними органами та спеціальними службами інших країн з питань протидії кібертероризму.

Оскільки розв'язання проблеми кібретероризму можливе лише на міжнародному рівні, потребує активізації міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних цілях.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

2. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. № 2(37)/2021. С. 72-79.

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право.* № 4(31)/2019. С. 98-106.

4. Нізовцев Ю.Ю. Судово-експертне дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні: методичні рекомендації. Київ: Видавничий дім "АртЕк", 2016. 118 с.

5. Корченко О.Г. та ін. Ознаковий принцип формування класифікацій кібератак. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2010. № 4 (146). Ч. 1. С. 184-193.

6. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов, В.Д. Павловський, Л.П.Скалозуб та ін.; за ред. Б.В. Романюка, Є.Д. Скулиша. Київ, 2011. 404 с.

7. Погорецький М.А., Шеломенцев В.П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. № 2 (2), 2009. С. 80.

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

9. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика.* № 2(42)/2014. С. 54-62.

10. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129.

11. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Сер.: Державне управління*. 2016. № 3. С. 131-137.

12. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

13. Велика українська кримінологічна енциклопедія. У 2 т. Т. 2: М-Я / редкол.: В.В. Сокуренко (голова), О.М. Бандурка (співголова) та ін. ; наук. ред. О.М. Литвинов. Харків: Факт, 2021. 870 с.

14. Рижов І. М. Основи аналізу терогенності соціальних систем: монографія. Київ: Магістр – XXI сторіччя. 2008. 288 с.

15 Енциклопедія соціогуманітарної інформології / ред. проф. К.І. Бєляков. Одеса: Вид. дім "Гельветика", 2021. Т. 2. 432 с.

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

17 Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

18 Іноземний досвід протидії тероризму: висновки для України: аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini

19 Новый отчет Европола о терроризме в странах ЕС: поводов для оптимизма по-прежнему нет. URL: https://vot-tak.tv/novosti/24-06-2021-otchet-evropola

20 Леонов Б.Д. Запобігання тероризму: кримінологічний аспект: монографія. Київ: Видавничий дім "АртЕк". 2020. 435 с.

21 Использование современных методов вовлечения лиц в террористическую деятельность: аналитический обзор / автор. кол.: Бондаренко А.Е. и др. ; под общей ред. А.П. Новикова. Москва: "Энциклопедия антитеррора", 2013. 57 с.

22. Aron, R. Paix et guerre entre les nations. Paris: Calmann-Levy, 1962. Pp. 15-19.

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

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.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ ДЕРЖАВИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРОБОРОНИ

Анотація. *Досліджено питання забезпечення кібероборони. Розглянуто вітчизняні стратегічні документи, присвячені питанням кібербезпеки та кібероборони. Деталізовано засади реалізації державної військової політики з метою розвитку кібероборонного потенціалу. Окреслено перспективи утворення в Україні кібервійськ. Розкрито підхід НАТО до поняття та особливостей кібероборони. Висвітлено турецький досвід забезпечення кібероборони держави. Узагальнено перспективи удосконалення кібероборонного потенціалу з урахуванням результативних здобутків зарубіжного досвіду.*

Ключові слова: *національна система кібербезпеки, кібероборона, кіберпростір, кібервійська, військова політика, інформаційно-телекомунікаційні системи, державне оборонне планування.*

Summary. *The issue of providing cyber defense has been detailed. Domestic strategic documents on cyber security and cyber defense are considered. The principles of implementation of the state military policy for the purpose of development of cyber defense potential are fixed. Prospects for the formation of cyber troops in Ukraine are outlined. NATO's approach to the concept and features of cyber defense is revealed. The Turkish experience of providing state cyber defense is highlighted. The prospects of improving the cyber defense potential of our country are identified, taking into account the effective achievements of foreign experience.*

Keywords: *national cyber security system, cyber defense, cyberspace, cyber troops, military policy, information and telecommunication systems, state defense planning.*

Аннотация. *Исследованы вопросы обеспечения кибероборонны. Рассмотрены отечественные стратегические документы, посвященные вопросам кибербезопасности и кибероборонне. Детализированы основы реализации государственной военной политики с целью развития кибероборонительного потенциала. Определены перспективы создания в Украине кибервойск. Раскрыт подход НАТО касаемо понятия и особенностей кибероборонны. Освещен турецкий опыт обеспечения кибероборонны государства. Обобщены перспективы усовершенствования кибероборонительного потенциала с учетом результативных достижений зарубежного опыта.*

Ключевые слова: *национальная система кибербезопасности, кибероборона, киберпространство, кибервойска, военная политика, информационно-телекомуникационные системы, государственное оборонное планирование.*

Постановка проблеми. Останнім часом прискіплива увага держави сконцентрована на питаннях забезпечення кібербезпеки і особливо кібероборони. Саме кібероборона стає невід'ємною частиною безпекового потенціалу будь-якої держави. Ця вимога пов'язана із реаліями сьогодення, враховує всесвітній технологічний прогрес та появу нових гібридних загроз у цьому сегменті. Беззаперечно, на перманентній основі зростає небезпека використання кіберпростору для завдання шкоди національним інтересам України, включаючи виведення з ладу критично важливих об'єктів інфраструктури. Фактор поширення CoVID-19 переконливо довів, що епідемії здатні вражати держави

та суспільства одразу в багатьох вимірах. Заходи протидії CoVID-19 порушують усталені практики міжнародного спілкування, передбачають обмеження основних прав і свобод та при цьому все одно можуть бути недостатніми для захисту життя і здоров'я людей. Така ситуація провокує необхідність пошуку шляхів посилення кібероборони держави.

Агресивна політика РФ, яка проявляється в проекції її силового потенціалу в Азово-Чорноморському регіоні, на Південному Кавказі, у Східній і Південно-Східній Європі та у Середземномор'ї, спричинює ерозію регіональної безпекової архітектури. Саме держава-агресор залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, яка базується на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Враховуючи виклики та загрози, які провокує РФ, серед важелів та засобів гібридної війни, які держава-агресор застосовує, у першу чергу, проти України – це масштабні кібератаки на критично важливі об'єкти інфраструктури. На цьому фоні важливим меседжем держави стало схвалення на державному рівні у серпні 2021 року низки важливих рішень РНБО України, якими затверджені актуальні для держави стратегічні документи (Стратегія кібербезпеки України, Стратегічний оборонний бюлетень), які змістовно та безпосередньо присвячені, у тому числі, й питанням посилення кібероборони в умовах ескалації збройного конфлікту на Донбасі. Тому висвітлення останніх здобутків організаційно-правового характеру нашої держави за напрямом посилення стану кібероборони є своєчасним та актуальним.

Результати аналізу наукових публікацій. Деякі проблемні питання забезпечення кібероборони держави досліджували у своїх наукових працях такі фахівці: О. Вітер [5], С. Вдовенко [6], В. Роллер [7], К. Соколов [8] тощо. На дисертаційному рівні засади державної політики у сфері розбудови вітчизняної системи кібероборони розглядали: І. Діордиця [9], О. Островий [10]. Проте жоден із зазначених авторів не розглядав питання забезпечення кібероборони в контексті схвалення в Україні оновленої Стратегії кібербезпеки України на 2021 – 2025 роки та Стратегічного оборонного бюлетеня України.

Метою статті є визначення на підставі контент-аналізу схвалених стратегічних документів, присвячених питанням посилення стану кібероборони, перспективних шляхів удосконалення кібероборонного потенціалу нашої держави з врахуванням позитивного зарубіжного досвіду у цій сфері.

Виклад основного матеріалу. Важливим завданням державного стратегічного планування є раціональний розподіл державою потенційних можливостей та наявних ресурсів (людських, інформаційних, фінансових, телекомунікаційних, технічних, технологічних), завдяки яким держава гарантує забезпечення національної безпеки та стабільний соціально-економічний і цифровий розвиток громадянського суспільства в цілому. Для досягнення цієї мети необхідно мати досить високий рівень управлінської культури державного апарату, що зумовлює застосування методів системного аналізу й прогнозування, а також спеціальних методів забезпечення безпеки в кіберпросторі тощо. Важливим завданням концептуального проектування системи забезпечення кібербезпеки є її методологічне забезпечення, в основі якого перебуває розуміння природи цього виду діяльності. Важливою складовою кібербезпеки є саме кібероборона. У вітчизняному законодавстві кібероборона визначається як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових,

організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [1].

Таким чином, кібероборона об'єднує усі можливі оборонні заходи та потужності держави на фоні яких інформаційно-комунікаційні технології цілеспрямовано застосовуються у якості оборонних технологій, а кіберпростір виступає "театром військових дій". Проте, тривалий час питання забезпечення кібероборони на державному рівні не розвивалося. Розуміючи актуалізацію питань забезпечення кібероборони, 26 серпня 2021 року Президент України увів в дію рішення РНБО України "Про невідкладні заходи з кібероборони держави" від 14.05.21 р. [2]. Цим актом підкреслюється необхідність термінового вжиття невідкладних заходів щодо створення передумов для формування у системі Міністерства оборони України кібервійськ для захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії у кіберпросторі. Задекларовано, що Кабінет Міністрів України має розробити та внести на розгляд Верховної Ради України законопроект щодо створення та функціонування у системі Міністерства оборони України підрозділу кібервійськ. Тобто важливою складовою побудови вітчизняної системи кібероборони є саме інституційне утворення кібервійськ. Адже це є лише однією із важливих композитних складових розбудови системи кібероборони.

На жаль, у 2016 – 2019 роках законодавчо визначені завдання щодо здійснення Міністерством оборони України та Генеральним штабом Збройних Сил України заходів із забезпечення кібероборони держави, нарощування її кібероборонних спроможностей не були належним чином імплементовані у документах оборонного планування, що призвело до гальмування процесів у сфері розбудови національної кібероборони. У зв'язку з чим з 2019 року в Україні (після зміни політичного керівництва країни) розпочато новий цикл оборонного планування.

Революційним здобутком сучасності стало схвалення нової Стратегії кібербезпеки України на 2021 – 2025 роки [3]. Оновлена редакція Стратегії кібербезпеки містить перелік викликів і загроз, які стоять перед Україною в сфері кібербезпеки, визначає засади розбудови національної системи захисту від кіберзагроз, деталізує основні пріоритети та стратегічні цілі забезпечення кібербезпеки України, а також напрями зовнішньополітичної діяльності і стратегічні завдання, які стоять перед державою в зазначеній сфері. Згідно з оприлюдненим текстом Стратегії, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, а реалізація зазначеного пріоритету очікувано здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Досконалий аналіз положень Стратегії кібербезпеки України на 2021 – 2025 роки дає змогу визначити пріоритетні цілі та стратегічні завдання щодо розвитку та побудови власної системи надійної кібероборони. Формування нової сучасної якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, важливою з яких виступає дієва кібероборона. З метою її забезпечення Україна має консолідувати зусилля на таких напрямах, як: створення та забезпечення динамічного розвитку підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, формування організаційно-правової та технологічної моделі їх функціонування та застосування, забезпечення ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення

кібернавчань, здійснення оцінки спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності.

Важливим завданням для нашої держави на стратегічному рівні є формування системи кібероборони шляхом: утворення у системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору; запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони; розроблення та виконання плану кібероборони як складової частини плану оборони України; проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав-членів НАТО задля досягнення оперативної сумісності; створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійній основі співпрацю із європейською військовою CERT-мережею; забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; запровадження у системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки.

Таким чином, кібероборона є важливим чинником сучасної оборони держави. Забезпечення кібероборони України відповідно до чинного законодавства покладено на Міноборони та Генштаб ЗСУ, які у рамках своєї компетенції повинні вживати заходи із забезпечення кібероборони з метою захисту суверенітету держави та забезпечення її обороноздатності, відсічі збройної агресії.

Президент України своїм Указом від 17 вересня 2021 року № 473/2021 увів у дію рішення РНБО України від 20 серпня 2021 року [4], яким затвердив концептуальний документ – оновлений Стратегічний оборонний бюлетень України, в якому відображається стратегія воєнної безпеки України, її засади, чинники й складові компоненти. Згідно із положеннями цього документа, військова політика України реалізується за кількома основними напрямами, один із яких – це забезпечення відсічі і стримування збройної агресії РФ, відновлення суверенітету і територіальної цілісності України, запобігання військових конфліктів з будь-якими іноземними державами. Зокрема, достатня увага приділяється побудові ефективних механізмів забезпечення кібероборони. Нормативно акцентовано, що створення національної системи кібероборони має бути орієнтовано на набуття необхідних спроможностей суб'єктами підготовки та здійснення заходів кібероборони, створення і розвиток сил, засобів та інструментів протиборства в кіберпросторі, які забезпечать створення необхідного потенціалу сил оборони для відбиття воєнної агресії в кіберпросторі.

У Стратегічному оборонному бюлетені України, зокрема п. 5.6, присвячений питанням утворення системи кібероборони. При цьому кінцева мета такої діяльності – використання силами оборони кіберпростору та створення системи кібероборони, які забезпечують запобігання виникненню воєнного конфлікту та загрози з використанням кіберпростору, підготовку та ведення кібероборони.

На виконання цієї мети мають бути вжиті такі заходи: розвиток спроможностей щодо ведення протиборства в інформаційному просторі (включаючи кіберпростір) Збройними Силами України та іншими складовими сил оборони; створення системи кібероборони як основного засобу стримування та відбиття воєнної агресії в кіберпросторі; створення та розвиток у складі Збройних Сил України необхідних військових організаційних структур

для дій у кіберпросторі, їх комплектування, підготовка та всебічне забезпечення; створення системи управління підготовкою та веденням кібероборони, її інтеграція в системи управління (керівництва) обороною держави та забезпеченням кібербезпеки, включаючи створення в системі Міністерства оборони України ситуаційного центру кібербезпеки; розвиток спроможностей системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України; нормативне визначення та включення до системи операцій Збройних Сил України сучасних форм і способів дій військ (сил) у кіберпросторі, ведення ними кібероборони; впровадження сучасних апаратно-програмних комплексів кібербезпеки, засобів з кіберзахисту, інших систем (зразків) кіберзброї у Збройних Силах України та інших складових сил оборони; розвиток спроможностей сил оборони щодо забезпечення кіберзахисту критичної інформаційної інфраструктури держави в умовах надзвичайного і воєнного стану; розширення військової співпраці з НАТО щодо забезпечення безпеки кіберпростору та спільних дій у кіберпросторі тощо.

Таким чином, кібероборона України базується на готовності та здатності сил оборони виконувати завдання кібероборони в будь-який час та в складних умовах функціонування кіберпростору. При цьому сили оборони для досягнення військового та стратегічного паритету в кіберпросторі мають застосовувати належні можливості реагування на зовнішні та внутрішні кіберзагрози воєнного характеру [11, с. 33].

На початку серпня 2021 року Україна у рамках посилення співпраці з НАТО у кіберпросторі подала офіційний запит на приєднання до Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), який базується в м. Таллінні (Естонія). Унікальність центру НАТО з кібербезпеки полягає в тому, що там спільно працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання. Зокрема, делегація Національного координаційного центру кібербезпеки при РНБО України здійснила робочий візит до Естонської Республіки, в межах якого було проведено низку двосторонніх зустрічей з метою розвитку паритетної співпраці між Україною та Естонією у сфері посилення кібербезпеки. Сторони дійшли згоди, що ефективним кроком на шляху до приєднання України до кібербезпеки НАТО є залучення українських експертів до роботи в рамках тематичних груп CCDCOE [12].

Для НАТО протидія кіберзагрозам визначена поняттям "кібероборона", яка входить до переліку головних цілей колективної оборони, що підкреслює його безпеково-оборонну спрямованість. Вперше кібероборона була включена в політичний порядок денний Альянсу на Празькому саміті ще у 2002 році. На Уельському саміті 2014 року НАТО схвалено посилену політику з кібероборони і відповідний план дій з її імплементації. На Варшавському саміті 2016 року Альянс вже зосереджував увагу на посиленні кібероборони національних мереж та промисловості. Тоді ж був підтверджений мандат НАТО на проведення операцій у кіберпросторі, який прирівняли до інших сфер проведення операцій – суші, повітря і моря. На Брюссельському саміті НАТО 2018 року кібератаки віднесені до головних гібридних загроз. НАТО погодило необхідність доведення операцій з кібероборони до рівня операцій в інших трьох сферах як за загальної координації Альянсу, так і в межах окремих груп союзників. На саміті НАТО у 2021 році було наголошено на необхідності постійно модернізувати та удосконалювати кібероборону, а кіберпростір визначено як окрему сферу військових операцій.

За таких умов забезпечення кібероборони є важливою складовою забезпечення кібербезпеки держави. Як переконливо засвічує зарубіжний досвід функціонування кібервійськ, чималі витрати на утримання відповідних підрозділів у арміях передбачені у

переважній більшості держав світу. Наприклад, у США щорічний бюджет на утримання штату у кількості 9 тис. кібервійськових складає $7 млрд. США, у Великій Британії $450 млн. США на 2 тис. персоналу, у Франції – $220 млн. на 800 осіб. Держава-агресор щорічно витрачає $300 млн. США при загальній чисельності 1 тис. вояків, у тому числі й "білих" хакерів, Ізраїль – $150 млн. США на утримання 1 тис. штату. Тобто функціонування кібервійськ передбачає й належний обсяг фінансування.

17 вересня 2021 року під головуванням Президента України відбулося засідання РНБО України, на якому було розглянуто бюджет сектору безпеки й оборони на 2022 рік. За результатами розгляду РНБО ухвалила рішення рекомендувати уряду при підготовці проекту державного бюджету на наступний рік збільшити фінансування сектору безпеки та оборони до 5,95 % ВВП, або 319,4 млрд. грн. (з 5,93 % ВВП у 2021 році). У бюджеті закладено витрати на забезпечення кібербезпеки та зокрема утримання кібервійськ.

На початку 2020 року Естонія, Хорватія, Литва, Нідерланди, Румунія, Польща підписали меморандум, відповідно до положень якого у перелічених країнах будуть утворені спільні міжнародні команди реагування на кіберзагрози. Зокрема, меморандумом передбачено практичні механізми роботи команд, їхній правовий статус та компетенція. До складу вказаних команд увійдуть цивільні та військові експерти вказаних країн, а їхня діяльність буде спрямована на нейтралізацію та розслідування будь-яких кіберінцидентів. Таким чином, на виконання політичної волі військових структур вказаних країн була утворена міжнародна група швидкого реагування з метою протистояння будь-яких кібератакам. Новоутворена структура буде опікуватися не тільки віртуальними питаннями, але й при необхідності і фізично брати участь під час розслідування потужних кіберінцидентів.

Одночасно у 2020 році в Туреччині з'явилися власні кібервійська (Türk Siber Ordusu) у кількості орієнтовно 13 тис. осіб. До складу кібервійськ Туреччини входять військові та цивільні особи, які є фахівцями у сфері кібербезпеки, переважну більшість складають хакери, які перейшли на роботу до державного сектора. Ядро турецької кіберармії складається з 5 тактичних груп (правоохоронна, морська, космічна, комплексної оборони та група "армія"). В авангарді турецької кіберармії перебувають великі хакерські спільноти, на кшталт "Ayyıldız Tim" та "Anka Neferler" які діють автономно від національних кіберсил. Як правило, лояльні угруповання використовуються для проведення відволікаючих маневрів у кіберпросторі. Залучаються також й хакери-одинаки. Доктрина кібербезпеки Туреччини має комплексний (оборонно-наступальний) характер та передбачає не тільки захисні, але й розвідувальні заходи, а також проведення кібератак на упередження. Таким чином, Туреччина як стратегічний сусід України має робочу військово-цивільну структуру, яка забезпечує стабільний захист національного сегменту кіберпростору, гарантує кібероборону. При цьому в її арсеналі активно та відкрито використовуються хакери для захисту державних інтересів у кіберпросторі, проведення наступальних кібероперацій.

Висновки.

Забезпечення кібероборони неможливе без прийняття 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. В сучасних умовах перед державою постає важливе та актуальне завдання щодо створення та функціонування підрозділу кібервійськ, розробки власних напрацювань та зразків кіберзброї, прискорення розробки проекту Стратегії кібероборони України, де прискіпливу увагу слід приділити не лише кібероборонним (кіберзахисним) діям

об’єднаних сил/військ кібероборони, а й їхнім проактивним упереджувальним, кіберрозвідувальним та кібернаступальним діям. Також доцільно визначити у відповідних нормативно-правових актах структуру системи кібероборони держави, склад, функції та завдання суб’єктів її забезпечення, а також об’єкти кібероборони, деталізувати заходи, практичне впровадження яких надасть змогу значно посилити кібероборону та підвищити кібероборонні спроможності держави.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.17 р. № 2163. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про невідкладні заходи з кібероборони держави”: Указ Президента України від 26.08.21 р. № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року “Про Стратегію кібербезпеки України”: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

4. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України”: Указ Президента України від 17.09.21 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121

5. Вітер О. Законодавче забезпечення у сфері оборони та безпеки: підсумки та перспективи. *Голос України*. 2019. № 3. – (5 січня 2019 р.).

6. Вдовенко С.Г., Даник Ю.Г. Проблеми та перспективи забезпечення кібероборони держави: збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2020. Вип. № 66. С. 75-89.

7. Роллер В.М. Правове регулювання здійснення кібероборони. *Право і суспільство*. 2018. № 5. Ч. 2. С. 137-141.

8. Соколов К.О., Гудима О. П. Підхід до розробки елементів структури системи виявлення деструктивного впливу у кіберпросторі. *Наукоємні технології*. 2019. № 4(44). С. 426-432.

9. Діордиця І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя. 2018. 40 с.

10. Островий О.В. Формування державної політики забезпечення кібернетичної безпеки в Україні: автореф. дис. ...канд. наук з держ. упр.: спеціальність 25.00.02; Донец. держ. ун-т упр. Маріуполь, 2019. 20 с.

11. Живило Є.О., Черноног О.О. Стратегія кібероборони України: збірник наукових праць ВІТІ. 2017. № 4. С. 30-37.

12. Україна подала запит на приєднання до центру НАТО з кібероборони. URL: https://ua.interfax.com.ua/news/general/759797.html

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

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/0000-0003-3642-4975.

СУЧАСНІ ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ TELEGRAM-КАНАЛІВ НА ШКОДУ ДЕРЖАВНИМ ІНТЕРСАМ

Анотація. *Розкрито засади, умови та особливості функціонування месенджеру Telegram. Визначено державні інтереси в інформаційній сфері в умовах поширення соціальних Інтернет-сервісів та Telegram-каналів. Окреслено тенденції використання анонімних месенджерів, особливо Telegram-каналів проросійської орієнтації. Визначено рейтинг України щодо стійкості до російської дезінформації. Деталізовано можливості Telegram-каналів щодо маніпулювання громадською думкою та поширення дезінформації. Визначено загрози функціонування анонімних Telegram-каналів в Україні. Висвітлено здобутки держави щодо блокування забороненого контенту. Узагальнено шляхи удосконалення рівня медіаграмотності та цифрової обізнаності населення. Обґрунтовано необхідність здійснення законодавчого врегулювання діяльності мережі Telegram-каналів в Україні.*

Ключові слова: *дезінформація, деструктивний контент, гібридна загроза, Telegram-канал, російська експансія, медіаграмотність, анонімний месенджер, фейк.*

Summary. *The principles, conditions and features of Telegram messenger operation are revealed. The state interests in the information sphere in the conditions of spreading of social Internet services and Telegram channels are defined. The tendencies of using anonymous messengers, especially pro-Russian Telegram channels, are outlined. Ukraine's rating of resilience to Russian misinformation has been determined. The possibilities of Telegram channels for manipulating public opinion and spreading misinformation are detailed. Threats of the functioning of anonymous Telegram channels in Ukraine have been identified. The state's achievements in blocking banned content are highlighted. The directions of the improvement of the level of media literacy and digital awareness of the population are summarized. The necessity of legislative regulation of the Telegram channel activity in Ukraine is substantiated.*

Keywords: *disinformation, destructive content, hybrid threat, Telegram channel, Russian expansion, media literacy, anonymous messenger, fake.*

Аннотация. *Раскрыты основы, условия и особенности функционирования месенджера Telegram. Определены государственные интересы в информационной сфере в условиях распространения социальных Интернет-сервисов и Telegram-каналов. Обозначены тенденции использования анонимных месенджеров, особенно Telegram-каналов пророссийской ориентации. Определен рейтинг Украины в отношении стойкости к российской дезинформации. Детализированы возможности Telegram-каналов в сфере манипуляции общественным мнением и распространении дезинформации. Определены угрозы функционирования анонимных Telegram-каналов в Украине. Освещены достижения государства в отношении блокировки запрещенного контента. Обобщены направления усовершенствования уровня медиа грамотности и цифровой осведомленности населения. Обоснована необходимость осуществления законодательного регулирования деятельности Telegram-каналов в Украине.*

Ключевые слова*: дезинформация, деструктивный контент, гибридная угроза, Telegram-канал, российская экспансия, медиаграмотность, анонимный месенджер, фейк.*

Постановка проблеми. Реалізація Російською Федерацією своїх імперських амбіцій та агресивних зовнішньополітичних цілей, спрямованих проти України, має загрозливий системний та комплексний характер, зокрема, в інформаційній сфері.

З метою деструктивного інформаційного впливу, маніпуляцій суспільною думкою російські спецслужби інфільтрують в український і світовий інформаційний простір назви, терміни та словосполучення, за допомогою яких намагаються легітимізувати псевдодержавні утворення на Сході України, спробу фізичної анексії Криму, всесвітньо просувати російські пропагандистські стратегії. Потужну інформаційну загрозу для України становить масове використання засобів комунікації для підриву довіри до державних інститутів, поширення дезінформації та ворожої пропаганди, поляризації суспільства, формування негативного сприйняття України у світі [1]. РФ широко демонструється прагнення піднести на якісно вищий рівень застосування інструментів т.зв. "м'якої сили". Значні зусилля неодноразово докладалися для забезпечення підтримки українським населенням інтеграційних ініціатив РФ на пострадянському просторі, приєднання до них України та дискредитації її євроінтеграційних спрямувань.

В сучасних умовах масштаби та тенденції використання месенджерів не можна недооцінювати. Особливо це стосується месенджеру Telegram. На жаль, останнім часом дедалі частіше трапляються випадки використання Telegram-каналів з метою реалізації прагнень політичного керівництва РФ через своїх сателітів та прихильників дестабілізувати суспільно-політичну ситуацію в Україні шляхом системного поширення за їх допомогою деструктивних інформаційних матеріалів та забороненого контенту із закликами до вчинення терористичних актів, насильницької зміни чи повалення конституційного ладу, захоплення державної влади, порушення територіальної цілісності, а також закликами, які розпалюють національну, расову чи релігійну ворожнечу. Ці загрози не можна ігнорувати та нівелювати ризики їх поширення.

Особливу шкоду для державних інтересів в інформаційній сфері становить злочинна діяльність адміністраторів антиукраїнських Telegram-каналів, які працюють на шкоду державним інтересам України у складі розгалуженої агентурної мережі під керівництвом російських кураторів. Непоодинокі випадки виявлення та блокування у ході моніторингу ресурсів мережі Інтернет (видання, соціальні мережі, блогосфера, форуми, особисті сторінки) зазначених інформаційних ресурсів найбільш активними радикально налаштованими представниками громадсько-політичних організацій, окремих мас-медійних структур для поширення резонансної інформації тенденційного характеру, оприлюднення закликів до організації масових протестних акцій, актів непокори, підриву авторитету української влади тощо. У зв'язку із викладеним, досліджувана тематика є актуальною в сучасних умовах.

Результати аналізу наукових публікацій. Конструктивно проблеми методологічного забезпечення інформаційної безпеки як важливої складової національної безпеки на науковому рівні досліджували такі фахівці, як: І.Р. Боднар [2], О.Д. Довгань та Т.Ю. Ткачук [3], О.О. Тихомиров [4], О.М. Солодка [5], І.М. Доронін [6] тощо. Питання забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах розглядали Р.В. Грищук [7], С.В. Горова [8]. Проте питанням функціонування анонімних месенджерів та поширення завдяки ним деструктивного контенту у Telegram -каналах, спрямованого на шкоду державним інтересам, не приділялася достатня увага.

Метою статті є визначення загрозливих тенденцій використання Telegram-каналів на шкоду державним інтересам України та пошук шляхів мінімізації та блокування їхнього негативного впливу.

Виклад основного матеріалу. Месенджер Telegram є одним з найбільш популярніших серед українців. Основна аудиторія цього месенджера – люди віком від 18 до 34 років, кількість яких наближується до 500 млн. активних користувачів. Їх приваблює не тільки зручність, але й одна з конкурентних переваг – анонімні Telegram-канали. Це внутрішні медіа, які публікують дуже різний контент – від мемів до політичних і бізнес-інсайдів. Створення такого медіа коштує дешево, а отже їх легко запускати в ефір. В ідеальному світі за анонімними каналами стояли би галузеві інсайдери, експерти та активісти, які не можуть висловлювати свою думку публічно. На практиці ж це створило умови для появи мінімедіа, які транслюють вигідні третім особам політичні меседжі, просувають шкідливі для суспільства тренди або атакують конкурентів.

Telegram використовує наскрізне (*end-to-end*) шифрування, яке вважають одним із найбезпечніших. Месенджер дає можливість створити "секретний чат", де комунікацію перехопити майже неможливо, оскільки повідомлення шифрується на пристрої відправника й розшифровується безпосередньо вже пристроєм отримувача. У всіх інших каналах, чатах та групах, комунікація теж є захищеною, але шифрування йде через сервер. Окрім комунікації між двома людьми, Telegram дає можливість створювати канали, які теж є візитівкою месенджеру. У контексті поширення дезінформації, маніпуляції та закидів, напевно, найпривабливішим є формат анонімних каналів. Тобто щоденне чи щогодинне інформування своїх підписників. До того ж вікового обмеження для українських користувачів не існує. Хоча канали інколи пишуть "18+", фактично приєднатися до них може кожен. Telegram не має обмежень на кількість повідомлень, розміри файлів чи кількість підписників. Для прикладу, у квітні 2021 року, найбільше підписників у двох каналів самого месенджеру – "Telegram Tips" (@TelegramTips) – 6,3 мільйона підписників; "Telegram News" (@telegram) – 5,6 мільйона підписників. На третьому місці канал "Bollywood HD Movies Latest" (@Movies_Bollywood_ Hollywood _hindi) з 4 мільйонами підписників. Найпопулярнішим в українському сегменті є зараз канал "Коронавірус_інфо", який налічує понад 600 тисяч підписників. Канали є публічними на відміну від груп, де можна розмістити до 200 тисяч користувачів. На відміну від каналів групи не можна знайти в пошуку за ключовими словами. Якщо публічні канали можна моніторити на предмет дезінформації профільним громадським організаціям чи відповідним державним органам, то приватні групи є закритими.

Хоч Telegram має багато функцій від соціальних мереж, в основі це месенджер. Його основна мета – донести повідомлення. Людина підписується на Telegram-канал і за замовчуванням отримує всі сповіщення з каналу на своєму телефоні чи комп'ютері. Таке сповіщення є у Фейсбуці чи Інстаграмі, але в Telegram це не просто сповіщення про те, що в певному каналі щось опублікували. Telegram виводить текст допису у "push"-сповіщення. Він може дати його не повністю, якщо текст доволі довгий, але для новин це працює зазвичай так, що весь текст повідомлення потрапляє у сповіщення, що є досить зручним. В Україні анонімні Telegram-канали вже перетворилися на повноцінний бізнес. На ринку є команди, які розробляють їх "під ключ" і наповнюють відповідним контентом. Теми можуть бути різними – від оборонної промисловості й війни на Донбасі до інфраструктурних проблем столиці. Інформаційний порядок будується на "інсайдах від анонімних джерел". Співвідношення правди та фейків становить приблизно 50/50.

Telegram-канали досить часто працюють у форматі мереж. Наприклад, зацікавлена особа діє через три канали: 1) нейтральний; 2) такий, що підтримує певну точку зору; 3) опозиційний. Так, можна нав'язувати великій аудиторії певний наратив. Багато анонімних каналів пов'язані між собою через взаємну рекламу, рекомендації, згадки й репости. Це сприяє не тільки зростанню аудиторії, але і трансляції, які потрібні третім

особам у меседжі. Такі канали непогано монетизуються. Наприклад, у топових пост коштує майже $1000.

Таким чином, через можливості Telegram-каналів легко маніпулювати суспільною думкою і залучати аудиторію нових користувачів. Читач навряд чи захоче або зможе відстежити початкове джерело інформації або почне перевіряти її вірогідність.

Ще одна проблема – зміна власника. Про продаж або перехід контролю над Telegram-каналом ніхто не буде оголошувати публічно. Якщо контент зміниться, то за умови правильної подачі значна частина аудиторії цього навіть не помітить. Або навпаки – перетече в інший канал від тих же осіб, де продовжить споживати "інсайди".

Розуміючи загрозливий характер функціонування Telegram-каналів та негативні наслідки їх деструктивної діяльності, деякі держави світу вживають превентивних заходів, зокрема й блокування. Так в Ірані у 2018 році було заблоковано Telegram. Підставами для цього став той факт, що у грудні 2017 року в Ірані почалися антиурядові протести, які призвели до сутичок з поліцією. У справу втрутився популярний Telegram-канал @amadnews, де протестантів закликали до використання "коктейлів Молотова". Міністр із комунікацій та інформаційних технологій Ірану звернув увагу засновника Telegram Павла Дурова на цей канал. У результаті Telegram заблокував @amadnews та його дзеркала. Офіційна причина – критикувати в Telegram можна, але закликати до насильства забороняється. Після цього в Ірані популярними стали неофіційні клієнти месенджера. До того ж значна частина іранців вміє користуватися VPN та іншими інструментами для обходу блокування. Кількість переглядів в новинних каналах впала в середньому на 20 %. У решти цей показник знизився приблизно на 50 %. 13 січня 2018 року Telegram розблокували, оскільки іранський бізнес зазнав збитків. Утім, 30 квітня 2018 року його забанили повторно. В кінцевому підсумку, Telegram все одно продовжують використовувати в Ірані.

У Німеччині все частіше лунають критика та невдоволення з боку політичного керівництва цієї країни щодо функціонування Telegram-каналів за наслідками та масштабами поширення дезінформації. Саме Telegram-канали сприяють односторонній масовій комунікації, яка може використовуватися для пропаганди. Схвалений у Німеччині у 2017 році Закон "Про Facebook" зобов'язує соціальні мережі з кількістю користувачів понад 2 млн. осіб прибирати пости з дезінформацією та закликами до насилля та ксенофобії протягом 24 годин з моменту надходження скарги під загрозою штрафів, сума яких може сягати до $50 млн. США.

Проте у Німеччині Telegram під законодавчо встановлені обмеження не підпадає. Цим активно користуються його прихильники для поширення різноманітної дезінформації. Відсутність контролю з боку держави вказаної комунікаційної платформи зумовлює активність радикально налаштованих користувачів, особливо тих, хто пропагує екстремістські настрої та нацистські ідеї. Німецькі закони передбачають обов'язкове посилання не тільки на контактні дані власників сайтів, але й форму власності та номер реєстраційного посвідчення для юридичних осіб. При цому, Telegram жодної інформації про себе не поширює, що викликає занепокоєння та невдоволення політичного керівництва держави. Для німецьких ЗМІ Telegram залишається одним з каналів поширення контенту поряд з іншими соціальними мережами та платформами. Свої канали Telegram має у таких видань як "Der Spiegel", "Süddeutsche Zeitung", "FAZ", а також у "Tagesschau" – інформаційної програми першого каналу німецького телебачення ARD.

Невипадково кіберзлочинці використовують Telegram як площадку для торгівлі даними. Зловмисники діляться ними на каналах, які нараховують декілька сот тисяч користувачів. Вони цінують Telegram за простоту використання та легкість модерації.

Питання збереження особистих даних користувачів Telegram актуально постало після того, коли у червні 2020 року у Даркнеті з'явилася у вільному продажу база даних мільйонів користувачів цього месенджера Ірану та РФ – двох країн, де критика урядовців може стати причиною неприємностей та у яких Telegram користується великою популярністю серед представників опозиції. Буквально відразу російська влада відмовилася від блокування Telegram та повідомила розробників про готовність плідної співпраці у справі боротьби з тероризмом та екстремізмом.

Влітку 2019 року активісти демократичної опозиції Гонконгу з'ясували, що популярний у цій країні Telegram абсолютно не гарантує анонімність учасникам групових чатів, оскільки китайські спецслужби у будь-який час можуть встановити перелік осіб та його користувачів. Проте переходити на нову площадку для комунікацій було вже занадто пізно, оскільки уся опозиція зареєструвалася у Telegram.

Також час від часу лунають новини про судові рішення заблокувати месенджер або окремі його канали в певній країні. Україна не є виключенням. Наприклад, 24 лютого 2021року Київський районний суд м. Харкова вирішив заблокувати чотири проросійськи налаштованих Telegram-канали [9]. Рішення суду про блокування сайтів постановляє "накласти арешт на майнові права інтелектуальної власності, які виникають у користувачів мережі Інтернет при використанні веб-ресурсів". З іншого боку, на переконання експертів, жодних майнових прав інтелектуальної власності у користувачів Інтернету, які переглядають контент того чи іншого вебресурсу, не виникає. Навіть якщо ви залишаєте допис на сайті, майнові авторські права можуть виникнути лише щодо цього допису, а не до сайту як такого. За наслідками реалізації вказаного рішення судових органів з'ясувалося, що оператори технічно не можуть вибірково блокувати окремі канали. Також, це судове рішення з технічної точки виконати буде складно, адже провайдери не можуть блокувати доступ до Telegram. У налаштуваннях месенджера є можливість увімкнути проксі-сервіс, що дозволить обійти блокування.

Ці ситуації переконливо демонструють, що заблокувати Telegram або окремі канали досить складно, а обійти урядові обмеження – навпаки. Звичайно, Україна це не Іран. У нас користувачі можуть перейти в інші месенджери, як перейшли в Facebook після блокування "ВКонтакте". У свою чергу, з метою боротьби з блокуваннями Telegram використовує стратегію, яка отримала назву "цифровий супротив". Це децентралізований рух, діяльність якого спрямована на захист цифрових свобод і прогресу. Власник Telegram оголосив про його старт ще у 2018 році після блокування месенджера в РФ. За цією стратегією постійно виплачуються гранти адміністраторам проксі-серверів і VPN. Останні ж допомагають Telegram залишатися доступним для широкої аудиторії. Таким чином, філософія, яку сповідує Telegram Павла Дурова, це транскордонний та необмежений характер інформаційних комунікацій. Проте український досвід блокування кремлівських рупорів активно використовується Німеччиною, яка заблокувала YouTube-канали пропагандистських ресурсів Russia Today та DFP. Це єдиний спосіб боротися з інформаційними атаками Кремля.

Нещодавно світовою спільнотою було презентовано оновлений "Індекс стійкості до дезінформації в Центральній і Східній Європі" (Disinformation Resilience Index, DRI) [10]. Він охопив 10 країн: це Польща, Чехія, Угорщина, Словаччина (Вишеградська група), Україна, Вірменія, Азербайджан, Білорусь, Грузія, Молдова (держави Східного партнерства). У дослідженні ретельно описано стан протидії зовнішній дезінформації в кожній країні окремо й окреслена ситуація загалом. Оцінка відбувалася за такими трьома критеріями: стійкість суспільства, інституційна та правова стійкість, стійкість ЗМІ та сфери диджитал. За результатами цього звіту Україна демонструє найвищу стійкість до

дезінформації з боку РФ. У свою чергу, дослідники додали, що Білорусь і Молдова залишаються найслабшими в протистоянні зовнішнім інформаційним загрозам, не дивлячись на значні зусилля місцевих й іноземних організацій, спрямовані на розвиток медіаграмотності та журналістської етики. Вірменія та Угорщина посіли середні сходинки цього рейтингу.

Проаналізуємо поступальні кроки держави, які реалізуються з метою запобігання та протидії використанню Telegram-каналів на шкоду державним інтересам. Вітчизняні спецслужби на постійній основі опікуються питаннями блокування забороненого контенту та притягнення до відповідальності осіб, які поширюють заборонену деструктивну інформацію. Так, 1 лютого 2021 року Служба безпеки України прозвітувала про викриття масштабної агентурної мережі, яка займалася розвідувально-підривною діяльністю на замовлення спецслужб РФ [11]. Слідство встановило, що агентурну мережу створив так званий 85 Головний центр спеціальної служби Головного управління Генерального Штабу Збройних сил РФ. До її складу входили мешканці Харкова та Одеси, активісти так званої "руської весни". Було виявлено та доведено, що спецслужби країни-агресора залучали українських громадян до створення та адміністрування низки політичних всеукраїнських і регіональних Telegram-каналів. Мова йде про канали: "Легитимный", "Резидент", "Картель", "Сплетница", "Чорний квартал", "Политический расклад", "Нетипичное Запорожье", "Трампель Харьков", "Одесский фраер", "Днепр live", "Николаев live", "Херсон live". Головним фігурантом агентурної мережі став організатор масових заворушень під час одеського "Антимайдану". Також було встановлено, що спецслужби Росії дозволили учасникам мережі самостійно організувати механізм монетизації. Транзакції проводили через мережу спільників, які відкрили рахунки в українських банках для отримання "гонорарів" за публікацію замовних матеріалів. У жовтні 2021 року РНБО України офіційно оприлюднила список українських Telegram-каналів, які просувають проросійські наративи. Йдеться, перш за все, про такі канали, як "Klymenko Time", "VESTI", "Шептун", "First", "Novostnoy" тощо. Також РНБО склала та затвердила список персональних проросійських блогів у мережі Telegram.

20 жовтня 2021 року РНБО України оприлюднило "Глосарій назв, термінів та словосполучень, які рекомендовано використовувати у зв'язку з тимчасовою окупацією Російською Федерацією Автономної Республіки Крим, м. Севастополь і окремих районів Донецької та Луганської областей" [12]. Публікація Глосарію супроводжується скоординованою кампанією дискредитації з боку проросійських каналів у Telegram. На його публікацію миттєво відреагували Telegram-канали, які безпосередньо пов'язані з дезінформаційною діяльністю на користь РФ. Основним наративом стало приниження національної гідності українців, особливо Революції Гідності, яку канали називають "переворотом". Центр протидії дезінформації проаналізував акаунти та Telegram-канали, які відреагували на глосарій РНБО щодо російської пропаганди та інформаційних впливів. РНБО України прозвітувала, що з метою поширення дезінформаційних матеріалів на користь РФ були використані наступні Telegram-канали: "Шептун" (57 тисяч підписників) – один з популярних анонімних Telegram-каналів, де пишуть про політику. Характерною ознакою є публікація інсайдів та неперевіреної інформації. Активно цитує прокремлівських пропагандистів "First" (447 тисяч підписників) – один з великих Telegram-каналів, де описується політика в Україні. На перший погляд він не виділяється з-поміж інших різкими проросійськими публікаціями. Проте аналіз взаємодії з іншими каналами свідчить, що він належить до пулу, підтримуваного РФ.

Таким чином, в Україні чимало Telegram-каналів активно використовуються з метою проведення скоординованої діяльності великої розгалуженої мережі пропагандистських

ресурсів, які працюють виключно на користь інтересів РФ. Ця мережа зорієнтована на проведення дискредитаційних та дезінформаційних кампаній проти України з метою розхитування внутрішньополітичної ситуації.

Висновки.

Російська Федерація, її спеціальні служби протягом тривалого часу проводять свої спеціальні інформаційні операції, більшість з яких спрямовані на ліквідацію української державності та знищення української ідентичності. Відбувається провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізація суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні з використанням саме деструктивного контенту Telegram-каналів. Невипадково в РФ Telegram перетворився на головний інформаційний майданчик для вкидань і маніпуляцій. Феномен популярності Telegram в РФ пояснюється тим, що склалася ситуація, що у багатьох людей, в тому числі російських політиків, була відсутня платформа, куди можна було "зливати" інформацію. І вони виявили такий популярний майданчик як Telegram. В кінці 2016 року він був лідером з видачі псевдо-інсайда та продовжує утримувати лідерські позиції.

В Україні функціонує чимало анонімних Telegram-каналів, які наповнюються фейками, маніпуляціями та подекуди мають чіткий "проросійський слід". Багато анонімних каналів пов'язані між собою. Цей зв'язок легко простежити завдяки репостам, згадкам, рекомендаціям на каналі. Більшість анонімних Telegram-каналів в сучасних умовах являють собою інструментарій гібридної війни проти нашої держави. Вітчизняними експертами доведено, що переважна більшість інформації з подібних Telegram-каналів є маніпуляціями та фейками. Обсяг фейків та маніпуляцій в анонімних Telegram-каналах часто сягає понад 80 %. Здебільшого розміщується інформація такого характеру, яка жодній верифікації не піддається.

В сучасному світі відбувається зростання значення цифрових технологій на фоні низького рівня медіаграмотності та цифрової обізнаності населення. Викладене зумовлює необхідність активізації проведення серед населення України роз'яснювальної роботи для того, щоб навчати громадян медіа грамотності, що дозволить мінімізувати деструктивну пропаганду, яка поширюється з анонімних Telegram-каналів. Загальновідомо, що уся інформація в Telegram-каналах – це не лише суб'єктивна думка, але й інформація, яка часто може бути пропагандою (як внутрішньою, так і зовнішньою). Тому пересічному українцю усі повідомлення потрібно фільтрувати, перевіряти та критично аналізувати.

На жаль, у новій редакції вітчизняного законопроекту "Про медіа" [13] парламентарії відмовилися від запровадження механізмів блокування Telegram-каналів. Причиною для цього став той факт, що у РФ провайдерів законодавчо зобов'язали придбати обладнання, яке дозволяє блокувати Інтернет-ресурси, однак впоратися не змогли і врешті відмовилися від такої ідеї, оскільки Telegram побудований "у найкращих анархічних традиціях Інтернету". Тобто загальною позицією є відмова від блокування, оскільки це сумнівне рішення. На жаль, на сьогодні у операторів і провайдерів немає технічної можливості здійснювати вибіркове блокування окремих груп, каналів або акаунтів у соціальних мережах, не зачіпаючи водночас доступ до всього Інтернет-ресурсу.

Проте вважається, що в сучасних умовах все такі існує необхідність законодавчого врегулювання та унормування діяльності мережі Telegram у вітчизняному сегменті мережі Інтернет, зокрема, через коригування алгоритмів цієї мережі, які би унеможливили поширення персональних даних і фейків та створення екстремістських груп, терористичної ідеології. Також з фейковим та неприпустимим контентом в Telegram варто боротися, насамперед, шляхом викриття спецслужбами тих людей, які його

розміщують. Це завдання є особливо актуальним в умовах реформування Служби безпеки України та удосконалення її оперативно-службової діяльності в інформаційній сфері. Доцільно посилити її спроможності щодо моніторингу спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері.

Також варто скоригувати механізми, які є зараз в країні, щоб заборонити, суттєво обмежити або накласти санкції за посилання на анонімні джерела інформації з каналів месенджера Telegram. Відповідні державні органи повинні більш оперативно реагувати на інформацію з журналістських розслідувань, де наводяться конкретні факти шкідництва певних Telegram-каналів, та домагатися запровадження щодо них відповідних санкцій.

Використана література

1. Про схвалення Стратегії інформаційної безпеки до 2025 року: Розпорядження Кабінету Міністрів України від 15.09.21 р. URL: https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku

2. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation.* 2014. № 1. С.68-75. URL: http://nbuv.gov.ua/UJRN/Mre_2014_1_8

3. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С. 89-103.

4. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія; заг. ред. Р.А. Калюжний. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

5. Солодка О.М. Пріоритети удосконалення інформаційної безпеки України *Інформація і право*. № 3(15)/2015. С. 36-42.

6. Доронін І.М. Трансформація національної безпеки в інформаційну епоху: загальна доктрина та її правова складова. *Інформація і право*. № 1(24)/2018. С. 104-111.

7. Грищук Р.В., Молодецька-Гринчук К.В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах. *Сучасний захист інформації.* 2017. № 3 (31). С. 86-96.

8. Горова С.В. Проблеми інформаційної безпеки в контексті розвитку соціальних мереж. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 2. С. 237-244. URL: http://nbuv.gov.ua/UJRN/boz_2013_2_32

9. 24 лютого 2021 року Київський районний суд Харкова вирішив заблокувати чотири проросійські налаштованих Telegram-каналів. URL: https://hromadske.ua/posts/harkivskij-sud-zablokuvav-dostup-do-kilkoh-telegram-kanaliv-yaki-pidozryuyut-u-zvyazkah-zi-specsluzhbami-rf

10. Disinformation Resilience Index 2021. URL: DRI https://east-center.org/wp-content/uploads/2021/09/DRI-report-2021.pdf

11. СБУ викрила агентурну мережу спецслужб РФ, яка дестабілізувала ситуацію в Україні через Telegram-канали. URL: https://ssu.gov.ua/novyny/sbu-vykryla-ahenturnu-merezhu-spetssluzhb-rf-yaka-destabilizuvala-sytuatsiiu-v-ukraini-cherez-telegramkanaly

12. Глосарій назв, термінів та словосполучень, які рекомендовано використовувати у зв'язку з тимчасовою окупацією Російською Федерацією Автономної Республіки Крим, м. Севастополь і окремих районів Донецької та Луганської областей. URL: https://www.rnbo.gov.ua/files/2021/ГЛОСАРІЙ.pdf

13. Про медіа: проект закону України від 27.12.19 р. № 2693. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812

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

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.

МОЖЛИВОСТІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ В КІБЕРПРОСТОРІ

Анотація. *Актуалізовано загрозливі тенденції розвитку цифрової економіки. Узагальнено роль, місце та значення криптовалют та технології блокчейн у сучасному світі. Зроблено акцент на проблемних питаннях використання криптовалют як платіжного засобу у мережі Інтернет, який використовується у протиправній діяльності. Розглянуто особливості проведення трансакцій з криптовалютами, які здійснює криміналітет для фінансування протиправної діяльності. Деталізовано напрями правоохоронної діяльності з метою запобігання та технологічного блокування незаконних операцій з криптовалютами. Висвітлено здобутки та досягнення використання програмного забезпечення "Crystal". Окреслено проблемні питання накладання арешту та здійснення конфіскації криптовалютних засобів, які використовувалися у злочинних цілях. Визначено засади удосконалення правоохоронної діяльності у сфері розслідування кримінальних правопорушень, скоєних в кіберпросторі.*

Ключові слова: *блокчейн, цифрові технології, цифровізація, криптовалюта, злочинність, фінансові активи, правоохоронна діяльність, міжнародно-правове регулювання криптовалюти.*

Summary. *The threatening trends in the digital economy have been reviewed. The role, place and significance of cryptocurrencies and blockchain technologies in the modern world are generalized. Emphasis is placed on the problematic issues of using cryptocurrencies as a means of payment on the Internet, which is used in illegal activities. The peculiarities of conducting transactions with cryptocurrencies carried out by criminals to finance illegal activities are considered. The directions of law enforcement activity aimed at prevention and technological blockade of illegal operations with cryptocurrencies are detailed. The achievements and accomplishments of the use of "Crystal" software are highlighted. The problematic issues of seizing and confiscating cryptocurrency funds used for criminal purposes are outlined. The principles of improving law enforcement activities in the field of investigation of criminal offenses committed in the cyber space are determined.*

Keywords: *blockchain, digital technologies, digitalization, cryptocurrency, crime, financial assets, law enforcement, international legal regulation of cryptocurrencies.*

Аннотация. *Актуализированы угрожающие тенденции развития цифровой экономики. Обобщены роль, место и значение криптовалют и технологии блокчейн в современном мире. Акцентировано внимание на проблемных вопросах использования криптовалют в качестве платежного средства в сети Интернет, используемого в противоправной деятельности. Рассмотрены особенности проведения трансакций с криптовалютами, осуществляемых криминалитетом для финансирования противоправной деятельности. Детализированы направления правоохранительной деятельности для предотвращения и технологического блокирования незаконных операций с криптовалютами. Освещены результаты и достижения использования программного обеспечения "Crystal". Определены проблемные вопросы ареста и конфискации криптовалютных средств, используемых в преступных целях. Определены основы усовершенствования правоохранительной деятельности в сфере расследования уголовных правонарушений, совершенных в киберпространстве.*

Ключевые слова: *блокчейн, цифровые технологии, цифровизация, криптовалюта, преступность, финансовые активы, правоохранительная деятельность, международно-правовое регулирование криптовалют.*

Постановка проблеми. Розвиток цифрової економіки не тільки відкриває нові можливості для суспільства та держави, але й озброює злочинців новими методами здійснення правопорушень, створює додаткові загрози для численних сфер громадського та суспільного життя. Інформатизація кредитно-фінансової системи зумовила появу нових сучасних механізмів фінансових розрахунків. При цьому технічні засоби та методи, що використовуються у фінансовій діяльності постійно удосконалюються. В умовах поширення пандемії у світових масштабах був спровокований вимушений перехід на дистанційний режим роботи, що призвело до збільшення кількості кримінальних правопорушень, вчинених з використанням передових інформаційних технологій. Шахрайства з платіжними картками, крадіжки грошей із банківських рахунків, розповсюдження комп'ютерних вірусів, викрадення хакерами персональних даних громадян, онлайн-торгівля наркотиками, поширення протиправного контенту – це лише невелика частина злочинів, які мають розслідувати та припиняти правоохоронні органи в сучасних умовах. Разом із динамічним розвитком інформаційних технологій та прагненням держави до суцільної цифрової трансформації усіх сфер суспільного життя, цифровий прогрес зумовлює появу нових та вдосконалення існуючих інструментів для здійснення кримінальних правопорушень.

Таким чином, тотальна цифровізація суспільства має зворотній бік, негативним проявом якого є поява нових кримінальних ризиків. Як свідчить статистика, різноманітні злочини, які вчинюються з використанням мережі Інтернет та інших інформаційних технологій, мають тенденцію до зростання. У зв'язку із появою нових форм суспільних відносин, які проникають у віртуальне середовище, актуальною та витребуваною технологією для передачі інформації у зашифрованому вигляді стала саме блокчейн технологія, на основі якої функціонує система обігу криптовалют. Свідченням того, що фінансові технології вийшли на світовому ринку на якісно новий рівень, є широке розповсюдження криптовалюти (віртуальної валюти), яка працює на основі децентралізованої системи блокчейн. Криптовалюти, які опанували світ, змінили уявлення не тільки про умови ведення бізнесу, але й приватних фінансів. Криптовалюта набирає популярності завдяки можливості розрахунку у віртуальному просторі, оскільки не потребується їх реальний вираз у вигляді грошових коштів, адже для таких розрахунків використовується лише цифровий ключ, захищений криптографічним кодом, що надійно захищає криптовалютні трансакції анонімного характеру. Принцип функціонування блокчейн технології зводиться до того, що усі списки операцій з криптовалютою об'єднуються у блоки, а блоки, у свою чергу, у ланцюги. При формуванні ланцюгів блоків через мережеві з'єднання децентралізований сервер формує базу даних, яка керується автономно без єдиного центру. Блокчейн технологія використовує криптографію та цифрові підписи для засвідчення певної особи: трансакції відслідковуються до криптографічних ідентифікаційних даних, які теоретично анонімні, проте можуть бути закріплені за реальними даними певного користувача.

Таким чином, функція блокчейн технологій полягає у реєстрації кожної трансакції з криптовалютою. Будь-яка передача криптовалюти підтверджується у мережі внесенням трансакційного блоку з використанням процесу шифрування, що забезпечує необхідну конфіденційність та анонімність. Ця технологія передачі та зберігання даних стала об'єктом уваги злочинців. Йдеться саме про криптовалюту, яка не платіжним засобом у буквальному значенні, проте фактично стала сурогатом емісійних платіжних засобів. Схема роботи криптовалют не регулюється будь-якими державними органами або фінансовими установами, а операції, що відбуваються з криптовалютами не регламентовані міжнародним законодавством, а тому ідентифікувати їх як злочинні не

можна. Однак, при здійсненні протиправної діяльності у мережі Інтернет, криптовалюта виступає засобом скоєння злочину та використовується у якості платіжного засобу для придбання вогнепальної зброї, наркотиків, легалізації злочинних доходів, фінансування тероризму тощо. Злочинці, використовуючи криптовалюту, здійснюють чималі грошові перекази через мережу Інтернет. Таким чином вони ігнорують використання звичайних фінансових систем, спричиняючи масштабні економічні збитки та посягаючи на основи національної безпеки тієї чи іншої держави. Враховуючи викладене, актуальним та своєчасним є розгляд особливостей використання можливостей технології блокчейн у розслідуванні злочинів, вчинених в кібепросторі.

Результати аналізу наукових публікацій. Кримінологічні засади злочинної діяльності з використанням криптовалют та технології блокчейн розглядали у своїх наукових працях: Благута Р.І. та Мовчан А.В. [1], Гребенюк М.В. та Черняк А.М. [2], Казначеєва Д.В. та Дорош А.О. [3], Клименко О.А. та Гуцалюк М.В. [4] та інші фахівці. Проте питання висвітлення кращих практик та методології розслідування злочинів, скоєних в Інтернет просторі за допомогою технології блокчейн, не було предметом окремого аналізу, що посилює актуальність обраного напрямку дослідження.

Метою статті є визначення особливостей інформаційно-аналітичного забезпечення правоохоронної діяльності з використанням блокчейн-технології, спрямованого на виявлення фактів та спроб використання криптовалют у протиправній діяльності в мережі Інтернет.

Виклад основного матеріалу. Уперше про ризики використання продуктів технології блокчейн повідомив Європол ще у 2015 році. У його звіті проаналізовано тренди обігу криптовалюти та використання нових фінансових інструментів у злочинних цілях. Було констатовано, що дедалі частіше криптовалюта використовується у мережі тіньового Інтернету – DarkNet (“Даркнет”) під час придбання вилучених з обігу речовин та наркотичних засобів. У 2018 році Європол прозвітував, що напрямки кримінального використання криптовалюти значно збільшилося, а криптовалюта переважно використовується як засіб розрахунків на тіньових Інтернет-ринках. У 2018 році ринок незаконної діяльності з Біткоїном складав близько $76 млрд. США. У 2019 – 2020 роках найбільша кількість злочинів, вченених з використанням криптовалют, стосувалася саме сфери мережевого шахрайства.

Популярність нового фінансового інструменту у кримінальному середовищі пояснюється тим, що на сьогодні не розроблені юридичні параметри криптовалюти та не встановлені кордони її безпечного обігу. Це обумовлено неповним розумінням вітчизняних та міжнародних експертів важливості дослідження криптовалюти у рамках ризик-орієнтованого підходу, коли одночасно робиться співвідношення економічних важелів та криміногенного потенціалу криптоінструментів. Відсутність комплексних досліджень кримінального використання криптовалюти негативно впливає результативність роботи у сфері запобігання та профілактики такої злочинної діяльності. Таким чином, своєчасним та практично значущим є кримінологічний аналіз криптозлочинності як самостійного об’єкта наукового пізнання та одночасно підсистеми кримінологічної моделі інтернет-злочинності.

Під криптозлочинністю слід розуміти сукупність системних протиправних дій, які здійснюються щодо криптовалюти або з її використанням. Оскільки це явище перебуває на стадії свого інституційного становлення, застосування цього поняття є досить умовним. Можна виділити 3 сектора криптозлочинності: незаконний продаж психоактивних речовин (наркотичних та психотропних засобів), інших заборонених товарів та послуг; відмивання злочинних доходів з використанням криптовалюти; крадіжка криптовалюти

та інші злочини проти власності. В сучасних умовах за криптовалюту можна придбати широкий спектр нелегальних товарів та послуг. Віртуальні гроші використовуються у сферах: порно індустрії; незаконного обігу персональних даних; торгівлі підробленими документами. Іноді навіть оплачуються замовні вбивства. Проте, найбільш поширеним сегментом криптозлочинності залишається саме незаконний обіг наркотичних засобів та психотропних речовин (80 % від загального обсягу ринку нелегальних товарів).

На жаль, на сьогодні світова статистика кримінального обігу наркотиків, порнографії, заборонених послуг з використанням криптовалюти не ведеться, проте згідно із даними експертів само криптовалюта є засобом розрахунків у 95 % операцій. При цьому спостерігається принципово нові кримінологічні тренди розвитку DarkNet: поступова специфікація окремих кримінальних сервісів та покращення їх технологічних характеристик; поступова монополізація криптовалютного ринку тощо. Відбувається тренд розширення спектру використання криптовалют для удосконалення трансакцій.

Якщо раніше абсолютним монополістом на криптовалютному ринку був Біткоїн, то зараз все частіше застосовуються нові цифрові валюти з високим ступенем анонімності (ZCash, Dash, Monero). Про це вказує у своїх звітах Європол. Дійсно, криптовалютні операції є анонімними, оскільки адреси криптовалютних гаманців, як правило, не пов’язані з певною особою. Проте, сам ланцюг трансакцій, який пов’язаний з певним гаманцем, не є анонімним. За необхідності, певний ланцюг трансакцій може бути проаналізовано, в результаті чого існує доля ймовірності ідентифікувати певну особу, якій належить конкретний криптовалютний гаманець, за зв’язками з іншими адресами у ланцюгу. Водночас існують системи, які дозволяють зберегти криптовалютні трансакції конфіденційними. Наприклад, це мережева система “Blender”, яка доступна за адресою //blender.io. Ця система надає послугу приховування реальних адресатів криптовалютних гаманців, з яких були отримані криптовалютні платежі. Це досягається тим, що сума, яку необхідно “замаскувати”, поділяється на частини та надсилається на адреси криптовалютних гаманців, які були створені для клієнта та не пов’язані з основною адресою криптовалютного гаманця, де грошові кошти зберігалися спочатку. Ця схема має за мету заплутати сліди походження засобів та ввести в оману правоохоронців у випадку розслідування злочинів з криптовалютами та блокування будь-яких спроб визначити реальну особу клієнта. Система “Blender” має достатню кількість резерву криптовалютних засобів, що надає змогу клієнту отримати свої засоби з початку ланцюга блоків. Саме тому походження засобів не буде відображатися. Наприклад, мережева система “Blender” не зберігає інформацію про оброблені трансакції, оскільки уся історія трансакцій знищується без можливості її майбутнього відновлення після того, як усі криптовалютні засоби надіслані на цільові адресати криптовалютних гаманців.

По факту розвитку нелегального та злочинного криптобізнесу формується його направленість з одночасною спеціалізацією осіб, які залучаються до злочинних схем. Виділяються такі нові кримінальні професії, як: координатори (адміністратори одночасно декілька сервісів); “єксроу” (гаранти угод); “гровери” (особи, які вирощують або комплектують наркотичні засоби); “кладмени” (особи, які розміщають відповідні об’яви та рекламу); “дропи” (особи, які приймають товар або здійснюють переказ криптовалют). Основна проблема використання криптовалюти у злочинних цілях полягає у наявних технічних труднощах ідентифікації особи або групи осіб, які здійснюють криптовалютні операції протиправного характеру. Злочинна діяльність може бути направлена на: легалізацію грошових коштів, тобто приховування їхнього

походження; здійснення платежів з метою організації шахрайських схем, злому інформаційних систем; фінансування тероризму тощо.

Наприклад, новим та популярним засобом легалізації кримінальних доходів є їх відмивання через сайти азартних ігор. Саме через ці сервіси відмиваються майже ¾ усіх "брудних" віртуальних грошей. Згідно даних "Trend Micro" злочинці все частіше використовують ігрову валюту як засіб зберігання вартості криптовалют. Для цього придбається валюта найбільш популярних віртуальних ігор. Вона продається за криптовалюту, а потім на спеціальних сервісах відбувається її конвертація на гроші. Існують великі ризики використання криптовалюти під час фінансування тероризму. Для більшості терористичних організацій єдиним способом залишається фізичне транспортування готівкових коштів. Однак, з огляду на розширення практики використання криптовалют та розвитку інфраструктури трансакцій, віртуальна валюта у майбутньому дедалі частіше буде використовуватися для фінансування тероризму.

Ще одну групу злочинів, які вчиняються з використанням криптовалюти, складають злочини проти власності, коли криптовалюта є об'єктом посягання. Особи, які викрадають криптовалюту, використовують фейкові (підробні) електронні гаманці. Потерплі, придбаючи товар або послуги на популярних сервісах, перераховують гроші на фішингові гаманці, які мають інші адреси, через використання вірусних програм. Це може бути створення фішингових сайтів популярних ресурсів. Використання криптовалюти у шахрайський спосіб також практикують краудінвестиційні проекти. Розвиток нової моделі колективного інвестування призвело до появи шахрайських компаній, які збирають від потерпілих гроші у криптовалютах без наміру займатися підприємницькою діяльністю.

Загалом, під час розслідування злочинів з використанням криптовалют правоохоронним органам необхідно мати відомості про: умови, порядок обігу криптовалют, особливості здійснення трансакцій, специфіку функціонування криптовалютних бірж тощо. Успішне розслідування вказаної категорії злочинів також є можливим лише при наявності кваліфікованих спеціалістів ІТ-сфери (інформаційно-комунікаційних технологій). Розслідуючи злочини, які вчиняються з використанням криптовалюти, доцільно враховувати той факт, що ці злочини мають свої специфічні особливості. Проте існують складності щодо визначення належності певної Біткоїн-адреси. Тому співробітники правоохоронних органів шукають засоби прив'язати певну IP-адресу або адресу електронної пошти до конкретної особи.

Однак, якщо особа використовує декілька IP-адрес, проксі-сервери, то цей процес стає набагато складнішим. Також, враховуючи технічну специфіку та особливості проведення криптовалютних операцій, існування процедур можливого маскування походження криптовалютних активів, доцільним вбачається розвиток засобів дослідження слідоутворення, розробки алгоритму встановлення та закріплення криміналістично вагомих відомостей для цього типу злочинів. Для досягнення цього ефекту, доцільно провести гармонізацію права у цьому напрямку. Трансакції у мережах технології блокчейн анонімні по відношенню до користувачів, проте не є анонімними щодо самих трансакцій. Тому технології блокчейн з різноманітними трансакціями мають бути піддані ґрунтовному аналізу, що надає змогу ефективно протидіяти злочинам, пов'язаним із криптовалютами. Для проведення такого аналізу необхідно мати спеціальні знання та спеціальне програмне забезпечення.

Наприклад, таким програмним забезпеченням є "Crystal", яке належить голландському підприємству – розробнику "Bitfury Group". Це програмне забезпечення здатне виявляти та відслідковувати незаконну діяльність у мережах технології блокчейн,

а саме: виявляти злочинну та протиправну діяльність у системах блокчейну; надавати докази щодо укладених підозрілих угод на криптовалютних біржах, зазначаючи при цьому адреси гаманців, які пов'язані з підозрюваною особою; прискорювати процес розслідування кіберзлочинів (дозволяє автоматизовано відслідковувати найбільш підозрілих учасників мережі) тощо. Вказане підприємство пропонує своє програмне рішення, у першу чергу, для правоохоронних органів. Доцільно вказати, що "Crystal" не обмежує свої можливості тільки у напрямку аналізу криптовалютної мережі. Воно здатне знаходити та структуризувати інформацію про адреси та змістовність мережі з інших джерел, таких як форуми або інші інтернет–портали. Завдяки такому комплексному підходу "Crystal" може встановити не тільки адресу певного об'єкту, а також його реальне ім'я та інші реквізити. Це програмне забезпечення активно використовується як правоохоронними органами, так і фінансовими організаціями у США, ЄС та країнах Азії.

Прикладом успішної роботи цього програмного забезпечення є боротьба з вірусом "WannaCry", в результаті чого були відслідковані платежі від жертв вірусу та встановлено особу, яка вимагала платежі. Існують також й інші програмні забезпечення, наприклад, "Chainalysis", "CipherTrace", "CryptoFinance" тощо. В основному завдання та функції даних програмних засобів схожі, проте відрізняються між собою алгоритмом аналізу та порядком отримання даних. Враховуючи здобутий досвід протидії цих програм злочинній діяльності, а також той факт, що вказане програмне забезпечення здатне здійснювати комплексний аналіз у криптовалютній мережі, їх практичне впровадження у правоохоронну діяльність неможливо недооцінювати. Доцільно вказати, що у випадку розкриття злочину постає закономірне питання арешту та у подальшому конфіскації криптовалютних засобів.

Однак, для вирішення цього питання правоохоронці стикаються як з правовими, так і технічними труднощами. На даний момент не існує єдиного загальноприйнятого правового врегулювання цих питань, яке б передбачало порядок арешту або конфіскації криптовалюти. Таким чином, не зрозуміло як бути, коли постає питання про арешт або конфіскацію криптовалюти, якщо правоохоронцям не відомий приватний цифровий ключ криптовалютного гаманця правопорушника. Це можливо, якщо правопорушник пам'ятає та знає свій приватний цифровий ключ, але розголошувати його ніхто не має права примусити. Тому якщо слідству відомо, що конкретній особі належить криптовалютний гаманець, без сприяння самого правопорушника арешт або конфіскація не можливі з технічних причин. У випадку неможливості арешту або конфіскації криптовалютних засобів, адреси криптовалютних гаманців, котрі використовуються у незаконній діяльності, можливо вносити до "чорних" списків, як це робить Департамент казначейства США. З метою запровадження подальших санкцій доцільно було б створити "чорний" список криптовалютних гаманців користувачів.

Проте непоодинокі випадки, коли криптовалютний гаманець прив'язаний до певної криптовалютної біржі. Тоді є можливість звернутися із запитом до суб'єкта, який здійснює обслуговування конкретної криптовалютної біржової системи з вимогою надати дані або здійснити арешт чи конфіскацію, наприклад, здійснити переказ засобів правопорушника на інший, створений для арешту або конфіскації криптовалютний гаманець. Водночас не усі криптовалютні біржі публікують свою контактну інформацію, а також інформацію про свій правовий статус, що не дає можливості для такого звернення. Також не завжди визначена юрисдикція таких підприємств. У результаті, якщо правопорушник надає сприяння або іншим способом можливо дізнатися про приватний цифровий ключ його криптовалютного гаманця, найбільш

оптимальним є переказ злочинних криптовалютних засобів на інший гаманець з метою подальшого арешту або конфіскації цих активів, оскільки залишати їх на поточному криптовалютному гаманці не можна. Інакше, криптовалютні активи можуть бути переказані на інші криптовалютні гаманці без відома правоохоронних органів.

Масштабне використання криптовалют у незаконній діяльності – це комплексна міжнародна проблема світової спільноти, а не однієї держави, оскільки криптовалютні операції здійснюються завдяки глобальної мережі Інтернет, яка не має територіальних та юрисдикційних кордонів. Проте, розуміючи ризики та загрози у вказаному сегменті, деякі держави світу активізують свої зусилля за напрямком протидії злочинному використанню криптовалют. Так, у 2021 році Міністерство юстиції США створило національну команду з захисту криптовалют (NCET) з метою проведення складних розслідувань і судового переслідування злочинних зловживань з криптовалютою. До складу команди увійдуть фахівці з декількох секторів Мін'юсту США – відділу з боротьби з відмиванням грошей і поверненням активів, а також відділу комп'ютерних злочинів та інтелектуальної власності. Основна мета та завдання діяльності цієї команди – зміцнити здатність протидіяти структурам, які процвітають і отримують прибуток завдяки зловживанням із криптовалютними платформами. Ця група має не тільки розслідувати складні фінансові злочини, а й відігравати допоміжну роль під час міжнародних та федеральних розслідувань, а також під час розслідувань на рівні штатів [5]. Також у 2021 році США вперше запроваджено санкції проти платформи для обміну криптовалюти, яка, як вважається, сприяла проведенню фінансових транзакцій осіб, причетних до програм-вимагачів. Казначейство США запровадило санкції проти чесько-російської криптовалютної біржі SUEX з реєстрацією в Москві та Празі, яка сприяла проведенню фінансових транзакцій осіб, причетних до програм-вимагачів. SUEX полегшувала транзакції, пов'язані з незаконними доходами. Аналіз відомих транзакцій SUEX демонструє, що понад 40 % транзакцій SUEX пов'язано з незаконними суб'єктами. Біржі віртуальних валют, такі як SUEX, мають вирішальне значення для прибутковості атак програм-вимагачів, які допомагають фінансувати діяльність кіберзлочинців. На переконання міністра фінансів США Джанет Єллен, програми-вимагачі та кібератаки заподіюють значну шкоду малому та великому бізнесу і становлять загрозу економіці країни.

На жаль, світовою спільнотою все ще не схвалено єдиного міжнародно-правового механізму, відсутність якого призводить до проблем визначення юрисдикцій впливу, наприклад, мережевих криптовалютних обмінних або біржових систем. Мережеві криптовалютні обмінні або біржові системи, а також інші системи, які надають будь-які криптовалютні послуги, які не афішують на своїх сайтах юридичну інформацію, наприклад, назву, реєстраційний номер підприємства, контактну інформацію тощо – це системи, які переважно здійснюють свою діяльність незаконно, оскільки приховують юридичну інформацію про свою діяльність, або взагалі здійснюють свою господарську діяльність без реєстрації. Це певним чином, ускладнює направлення запитів від правоохоронних органів до таких організацій. Можливо, такі не добропорядні системи доцільно блокувати або вносити їх у спеціальні "чорні" списки. Завдяки існуванню різноманітних аналітичних програм, які здатні проводити комплексні аналізи криптовалютних мереж, збільшуються можливості розкриття кримінальних правопорушень, які вчиняються з використанням криптовалюти.

Тому той факт, що адреси криптовалютних гаманців не пов'язані з конкретними особами не означає, що злочини, у скоєнні яких використовуються криптовалюти не розкриваються. Навпаки, сучасне програмне забезпечення сприятиме розкриттю

правоохоронцями не тільки фактів злочинної діяльності, але й дозволяє ідентифікувати не тільки особу правопорушника, але й відслідкувати маршрути потоків незаконних криптовалютних засобів. Проте потребує прискорення розробка міжнародно-правових механізмів інституту арешту та конфіскації незаконно отриманих криптовалютних засобів. Сучасні тенденції переконливо свідчать про те, що трансакції в криптовалютних мережах не є абсолютно анонімними, та можуть перебувати у фокусі уваги правоохоронних органів, зокрема шляхом організації проведення комплексного аналізу завдяки спеціальному програмному забезпеченню та іншим методам верифікації.

Висновки.

Технологія блокчейн, на основі якої функціонує криптовалютна індустрія має такі переваги: 1) стабільність; 2) безпечність; 3) прозорість роботи з даними; 4) транскордонний характер операцій з обміну даними. На цьому фоні основний пріоритет під час використання криптовалюти у злочинній діяльності – це відсутність прив'язки особи до певного криптовалютного гаманця та збільшення кількості кібератак з використання програм-вимагачів. Одним із найбільш популярних засобів обігу криптовалюти у злочинних цілях є функціонування криптовалютних бірж. У мережі Інтернет представлено чимало криптовалютних обмінних систем з невизначеною юрисдикцією. Внаслідок цього існує вірогідність, що ці сервіси можуть використовуватися у злочинній діяльності. Доцільно вказати, що досить активно криптовалюти як розрахункові засоби використовуються у мережі DarkNet, у якій дані передаються у зашифрованому вигляді. Також функціонує чимало площадок–сайтів, на яких здійснюється незаконна діяльність. Наприклад, тільки у 2019 році у прихованій мережі функціонувало понад 2,5 тис. магазинів наркотичних та психотропних речовин, у яких розрахунки відбувалися за допомогою криптовалюти.

Тому важливим напрямом протидії такому явищу залишається використання сучасного програмного забезпечення у правоохоронній діяльності. З метою ефективності розкриття злочинів, що вчинюються з використанням криптовалют, доцільним вбачається: прискорити схвалення правових засад, які мають врегулювати криптовалюти та розробку методологічних основ щодо розкриття та розслідування цієї категорії кримінальних правопорушень. Також правоохоронним органам необхідно налагодити концептуальну взаємодію з криптовалютними компаніями з метою блокування незаконної та протиправної діяльності у блокчейн платформах. Вирішення цієї проблеми має комплексний характер та вимагає розробки стратегії, направленої на запобігання використанню злочинцями нових сучасних фінансових механізмів.

Серед пріоритетних напрямків розвитку міжнародної кримінально-правової політики у сфері попередження використання криптовалют у злочинній діяльності виділяється: визначення моделі податкового адміністрування криптовалюти та правового статусу криптовалют; обов'язкове ліцензування діяльності у сфері обігу криптовалют (біржових сервісів, обмінних площадок, компаній, які випускають токени); встановлення міжнародних стандартів протидії легалізації злочинних доходів та фінансуванню тероризму. Також доцільно створити міжнародну базу даних про осіб, які займаються незаконним обігом та застосуванням цифрових фінансових активів в контексті технологій, що використовуються у протиправній діяльності. В нашій країні в умовах інституційного становлення новоствореного у 2021 році правоохоронного органу – Бюро економічної безпеки України [6], гостро стоїть питання утворення в його складі спеціального підрозділу, до компетенції якого слід віднести проведення розслідування протиправної діяльності з криптовалютами.

Використана література

1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

2. Гребенюк М.В., Черняк А.М. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємництво, господарство і прав*о. 2019. №3. С. 297-303.

3. Казначеєва Д.В., Дорош А.О. Кримінальні правопорушення у сфері обігу критовалюти. *Вісник кримінологічної асоціації У*країни. 2021. № 2 (25). С. 149-157.

4. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України: наукові праці Національного авіаційного університету. *Повітряне і космічне право*. 2021. № 1(58). С. 177-184.

5. US DOJ To Bolster Newly Created “National Cryptocurrency Enforcement Unit” URL: https://cryptodaily.co.uk/2021/10/US-DOJ-To-Bolster-Newly-Created-National-Cryptocurrency-Enforcement-Unit

6. Про Бюро економічної безпеки України: Закон України від 28.01.21 р. № 1150. *Відомості Верховної Ради України.* 2021. № 23. Ст. 197. URL: https://zakon.rada.gov.ua/laws/ show/1150-20#Text

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

УДК 342.951

НОВИЦЬКИЙ В.Я., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7386-1221.
ФИЦА В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6590-8082.

СТАНОВЛЕННЯ ТА РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ОБІГУ ВІРТУАЛЬНИХ АКТИВІВ

Анотація. *Окреслено проблемні питання функціонування та подальшого розвитку ринку віртуальних активів в Україні. Досліджено історичний аспект правового регулювання питань обігу криптовалют як в Україні, так і за кордоном. Визначено засади розбудови ринку віртуальних активів в Україні. Висвітлено законодавчі ініціативи деяких держав світу щодо створення національних цифрових валют. Уточнено загрози та ризики використання криптовалют у світових масштабах. Окреслені загальносвітові тенденції розвитку та використання віртуальних активів, зокрема криптовалют. Визначено шляхи удосконалення законодавчого забезпечення обігу віртуальних активів в Україні.*

Ключові слова: *блокчейн, цифрові технології, криптовалюта, віртуальні активи, організована злочинність, міжнародний тероризм, національний сегмент кіберпростору, економічна безпека, тінізація економіки, цифрова економіка, відмивання коштів.*

Summary. *Problematic issues of functioning and further development of the market of virtual assets in Ukraine are outlined. Historical aspects of legal regulation of cryptocurrency circulation both in Ukraine and abroad are researched. The principles of development of the market of virtual assets in Ukraine are determined. Globally threatening trends in the use of virtual assets and cryptocurrencies have been identified. Legislative initiatives of some countries in the world to create national digital currencies are detailed. The threats and risks of using cryptocurrencies worldwide have been specified. The global trends in the development and use of virtual assets, in particular cryptocurrencies are outlined. The directions of the improvements of the legislative support for the circulation of virtual assets in Ukraine have been identified.*

Keywords: *blockchain, digital technologies, cryptocurrency, virtual assets, organized crime, international terrorism, national segment of cyberspace, economic security, shadowing of the economy, digital economy, money laundering.*

Аннотация. *Очерчены проблемные вопросы функционирования и дальнейшего развития рынка виртуальных активов в Украине. Исследован исторический аспект правового регулирования вопросов оборота криптовалют как в Украине, так и за рубежом. Определены основы развития рынка виртуальных активов в Украине. Освещены законодательные инициативы некоторых государств мира касаемо создания национальных цифровых валют. Уточнены угрозы и риски использования криптовалют в мировых масштабах. Очерчены общемировые тенденции развития и использования виртуальных активов, в частности, криптовалют. Определены направления усовершенствования законодательного обеспечения оборота виртуальных активов в Украине.*

Ключевые слова: *блокчейн, цифровые технологии, криптовалюта, виртуальные активы, организованная преступность, международный терроризм, национальный сегмент киберпространства, экономическая безопасность, тенизация экономики, цифровая экономика, отмывание денег.*

Постановка проблеми. Технологія блокчейн, на якій базується велика кількість технологічних інноваційних розробок, знайшла широке застосування в багатьох сферах суспільства, таких як діяльність у сфері криптографії, криптовалюти, у державній сфері управління. Україна входить до переліку країн-лідерів у сфері застосування криптовалюти і технології блокчейн та є ідеальним місцем для розвитку новітніх цифрових технологій.

Необхідним елементом сучасної економічної парадигми будь-якої держави стає розвинений ринок віртуальних активів. В Україні такий ринок фактично існує протягом останніх п'яти років, але знаходиться, на жаль, поза межами правового регулювання. Поточний розвиток цифрових технологій зумовлює створення нових об'єктів цивільних прав, які існують виключно у цифровій (нематеріальній) формі та фактично перебувають у цивільному обігу. Це істотно впливає на суспільно-економічні відносини, формуючи особливий новий ринок.

Як свідчить світова практика, питання правового врегулювання віртуальних активів є не лише доцільним, а й необхідним, оскільки криптовалюта як важлива складова віртуальних активів стає дедалі більше популярною в усьому світі, а її розвиток заборонити технічно неможливо й економічно недоцільно. Відтак ринок віртуальних активів потребує належного законодавчого врегулювання, яке покликане не лише надати можливість учасникам суспільних правовідносин розпоряджатись такими об'єктами, але й забезпечити баланс інтересів учасників ринку та сприяти надходженню інвестицій в Україну, одночасно розвивати технологічну базу блокчейну. Разом с тим розбудова повноцінно функціонуючого ринку віртуальних активів є вкрай важливим завданням на сучасному етапі розвитку вітчизняної цифрової економіки, зважаючи на важливість її інтегрування у європейську та світову економічну спільноту. Сьогодні законодавці більшості зарубіжних країн врегульовують ці питання з урахуванням особливостей національного законодавства. Наприклад, відповідне законодавче врегулювання у тій чи іншій формі існує у США, Німеччині, Мальті, Гібралтарі, Швейцарії, Ліхтенштейні, Естонії, Японії.

На даний час не визначено єдиних підходів до регулювання обігу віртуальних активів, зокрема криптовалют. Міжнародними фінансовими установами та центральними банками досі не розроблено системних підходів до використання віртуальних валют. Міжнародна банківська спільнота звертає увагу на те, що використання віртуальних валют потребує належного моніторингу та осмислення з боку державних регуляторів. Європейський центральний банк у своїх дослідженнях щодо віртуальних цифрових валют не висловлює однозначного рішення щодо використання віртуальних валют, застерігаючи про існуючі ризики безпеки платежів та потенційні загрози у розрахункових операціях.

Законодавство ЄС класифікує криптовалюту "Bitcoin" ("Біткоїн") як "цифрове представлення вартості, яке не підтверджено центральним банком або державним органом і не прив'язане до офіційних валютних курсів, та може використовуватися як засіб обміну для покупки товарів і послуг, їх передачі та зберігання і може купуватися в електронному вигляді".

Законодавство окремих зарубіжних держав по-різному трактує статус криптовалюти. Так, за законодавством Ізраїлю "Bitcoin" під юридичне визначення валюти не підпадає як фінансове забезпечення, так й оподатковуваний актив. У КНР та Японії "Bitcoin" вважається віртуальним товаром, а не валютою. Тоді як у Канаді це – нематеріальний актив.

Проте, на даний час в Україні повноцінному функціонуванню та подальшому розвитку ринку віртуальних активів заважає низка невирішених проблем, серед яких виділяється: відсутність правового регулювання відносин, що виникають у сфері обігу віртуальних активів; відсутність механізмів оподаткування доходів, отриманих від операцій з віртуальними активами; відсутність правових гарантій захисту права власності учасників ринку віртуальних активів; регулювання діяльності професійних учасників ринку віртуальних активів; відсутність механізмів контролю за обігом віртуальних активів, які можуть використовуватись з метою легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення; відсутність дієвих механізмів залучати іноземні інвестиції в високотехнологічні галузі економіки України тощо. За таких умов розгляд процесів становлення та розвитку правового врегулювання обігу віртуальних активів є актуальним та своєчасним.

Результати аналізу наукових публікацій. Певною мірою питання особливостей обігу віртуальних активів та криптовалют розглядали у своїх наукових працях такі фахівці, як: М. Гребенюк [1], О. Кудь [2], В. Логойда [3], В. Михайловський [4], А. Овчаренко [5], В. Прокопенко [6] та інші. Проте вбачається недостатньо висвітленим питання щодо визначення шляхів удосконалення правового врегулювання обігу віртуальних активів, що засвідчує необхідність проведення цього наукового дослідження.

Метою статті є визначення на базі аналізу розвитку вітчизняного та зарубіжного законодавства шляхів удосконалення законодавчого врегулювання принципів функціонування ринку віртуальних активів.

Виклад основного матеріалу. Питання обігу віртуальних активів й зокрема криптовалюти в Україні неодноразово порушувалося на державному рівні. Так, ще 10 листопада 2014 року на сайті Національного банку України було оприлюднено роз'яснення "Щодо правомірності використання в Україні "віртуальної валюти/ криптовалюти" "Bitcoin". Так, згідно з позицією НБУ віртуальна валюта (криптовалюта) "Bitcoin" визначалася як грошовий сурогат, який не забезпечений реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це суперечить нормам вітчизняного законодавства. Також НБУ задекларував свою позицію, що не нестиме відповідальності перед громадянами за усі курсові коливання та їх наслідки, пов'язані із криптовалютами, зокрема Біткоїнами. У своєму листі НБУ від 08.12.14 р. № 29-208/72889 вчергове підкреслив небезпечність криптовалют. Позиція, викладена у листі, зводиться до того, що Біткоїн не має будь-якого забезпечення та не контролюється державними органами влади жодної з країн. Національний банк вкотре дійшов висновку, що діяльність з купівлі-продажу Біткоїнів за долари США або іншу іноземну валюту має ознаки функціонування фінансових пірамід, що може свідчити про потенційні ризики здійснення незаконних та сумнівних операцій.

За результатами проведеного засідання Вищої експертної ради при Раді НБУ у жовтні 2017 року акцентовано, що державні органи, які мають повноваження контролю та регулювання фінансових ринків, ще досі не визначилися щодо рамкових засад функціонування ринку криптовалют. Внаслідок цього було сформульовано рекомендації з метою нівелювання таких потенційних ризиків, а саме: можливого зниження довіри до національної грошової одиниці, яка є єдиним законними засобом розрахунків в Україні; ймовірності обслуговування криптовалютами тіньової економіки. На думку НБУ нормативна неврегульованість використання криптовалют створюватиме умови для

підвищення питомої ваги тіньової економіки, що може спричинити зменшення обсягів сплати податків до Державного бюджету.

Згодом усі три позиції Національного банку України стосовно криптовалют та їх статусу були нівельовані та визнані неактуальними. Більше того, перші два роз'яснення були офіційно відкликані НБУ. Незважаючи на те, що у третій заяві НБУ в цілому продовжено попередню риторику, еволюція позиції явно прослідковується – від повного невизнання у 2014 році до обережного згадування про позитивний міжнародний досвід регулювання в останній спільній заяві регулятора.

Враховуючи актуальність вказаної проблематики, в нашій державі було розроблено законопроект "Про обіг криптовалюти в Україні" від 06.10.17 р. № 7183, який мав би створити правове поле для її обігу в якості офіційного платіжного засобу. Однак у цьому законопроекті не було враховано специфіки обігу криптовалют, він містив неоднозначні та суперечливі положення, не враховував інтереси вітчизняної криптоіндустрії, у зв'язку з чим був відкликаний.

28 квітня 2021 року Комітет з питань цирової трансформації рекомендував Верховній Раді ухвалити у другому читанні законопроєкт "Про віртуальні активи" від 11.06.20 р. № 3637 [8], який має легалізувати криптовалюти в Україні та остаточно врегулювати операції з ними. Серед іншого, законопроектом запроваджено перевірки операцій з криптовалютами на суму понад 30 тис. грн, а також блокування криптогаманців та конфіскацію криптовалюти за скоєння порушення.

Україна має потужний потенціал для того, щоб посісти провідне місце у світовій цифровій економіці. Зокрема, цьому сприятиме й запуск легального ринку віртуальних активів. Схвалення цього законопроекту дозволить українським блокчейн-компаніям легалізувати власні бізнес-процеси та офіційно працювати з банківською системою. Крім того, таку можливість матимуть і громадяни, які отримують доходи від операцій з віртуальними активами, що сприятиме усуненню юридичних ризиків для роботи міжнародних криптокомпаній й залученню іноземних інвестицій у нову прогресивну галузь.

Заплановано, що в Україні законодавчо термін "криптовалюта" в нормативних документах використовуватись не буде, проте це буде один з видів віртуальних активів. Згаданий законопроект має на меті сформувати правове поле ринку віртуальних активів (правовий статус, класифікація, права власності та інші ключові юридичні дефініції) та адаптувати рекомендації FATF щодо фінансового моніторингу ринку віртуальних активів. Також документ визначає регулятора ринку – ним стане Мінцифри (в окремих випадках НБУ та НКЦПФР) та перелік професійних постачальників послуг віртуальних активів та їх реєстрацію. Після нормативного врегулювання криптовалютного ринку міжнародні компанії зможуть легально реєструвати блокчейн-бізнес в Україні. Додатково цим законопроєктом пропонується внести зміни до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом", згідно з якими з моменту створення центрального органу виконавчої влади, що реалізує політику у сфері обороту віртуальних активів, до нього від Міністерства цифрової трансформації передаються функції державного фінансового моніторингу у галузі обігу віртуальних активів. Адже Україна враховує позитивний міжнародний досвід законодавчого забезпечення обігу віртуальних активів у інших країнах світу, оцінює потенційні та реальні ризики.

Сьогодні загальносвітовим трендом є безперешкодна торгівля віртуальними активами у цифровій формі з високим ступенем анонімності та з можливістю обміну (купівлі або продажу) на долари США, Євро та інші валюти. Будь-хто може

завантажити безкоштовний відкритий програмний додаток з веб-сайту для відправки, отримання та зберігання криптовалюти. Найпоширенішим способом видобутку криптовалюти є майнінг, який здійснюється за рахунок обчислювальної потужності комп'ютерного обладнання.

Віртуальні активи та криптовалюти не випускаються центральними банками держав і не залежать від кредитно-грошової політики будь-якої країни. Емісія криптовалюти відбувається виключно в цифровому вигляді. Хто завгодно може здобувати криптовалюту (займатися майнінгом) використовуючи комп'ютерні технологічні можливості. Наприклад криптовалюта Біткоїн має достатньо високу волатильність, тобто значну амплітуду коливання вартості в еквіваленті до вільноконвертованих валют світу, що засвідчує нестабільний характер номінальної вартості даної криптовалюти. Підвищення та падіння вартості Біткоїна безпосередньо залежить від балансу попиту та пропозицій на криптовалютних біржах. Оскільки вони працюють з децентралізованою технологією, блокчейном (ланцюжком блоків інформації), транзакції з криптовалютами не вимагають наявності посередників або органу для їхньої перевірки. Через гігантську мережу комп'ютерів з вузлами, розкиданими по всьому світу, вони використовують криптографічні методи для захисту інформації, яка міститься в грошових переказах, а також створення нових одиниць криптовалют. Ця автономія в діяльності ускладнює контроль і нагляд з боку урядів, центральних банків та регуляторів за мільйонами доларів, які циркулюють через мережі.

Проте є й інший бік обігу віртуальних активів. У січні 2021 року Мережа з боротьби з фінансовими злочинами (FinCen) запропонувала створити закон, який зобов'яже компанії повідомляти прізвища та адреси людей, які роблять операції з криптовалютою на суму понад $3 тис. США. Такі заходи мають допомогти відстежувати незаконні транзакції. Адже найбільший ризик віртуальних активів, зокрема криптовалют, полягає у тому, що вони можуть загрожувати грошовому суверенітету тієї чи іншої країни світу. Враховуючи такі загрози, очікується, що у найближчому майбутньому уряди країн мають створити свої власні цифрові валюти, які будуть конкурувати на ринку з криптовалютами. Такий важливий крок надасть змогу врегулювати ринок цифрових валют з метою захисту людей від шахрайства і гарантії, що гроші використовують в належних цілях.

Виходячи із викладеного, наприклад у США вивчається можливість емісії цифрового долара. Держава-агресор (РФ), у свою чергу, опановує засади запровадження цифрового російського "крипто-карбованця". Центральний банк РФ визначився з архітектурою платформи цифрового карбованця та має намір завершити його створення до кінця 2021 року, у зв'язку з чим очікується внесення змін до законодавчих актів, після чого має розпочатися тестування платформи. Для запровадження цифрового карбованця доцільно створити нову платіжну інфраструктуру, яка дозволятиме здійснювати онлайн та офлайн платежі (як додаткову до існуючої). Напередодні у 2020 році було схвалено концепцію цифрового російського карбованця та затверджено його дорожню карту. Цифровий карбованець матиме унікальний цифровий код, який буде випускатися та зберігатися у спеціальному електронному гаманці у Центробанку РФ. Клієнти отримуватимуть доступ до цифрового карбованця через свої банки. При цьому для офлайн-розрахунків необхідно користуватися іншим гаманцем, створеним у смартфоні. Передача цифрового карбованця між користувачами буде відбуватися у вигляді переміщення цифрового коду з одного гаманця до іншого.

Тобто більшість центробанків країн світу вивчають можливість та розробляють концептуальні засади запровадження власних криптовалют. Свого часу НБУ був одним

із перших центральних банків у світі, що почав досліджувати таку можливість. Цифрові валюти країн світу мають використовуватися для обслуговування національних платіжних систем, а наступним етапом має стати використання цифрових валют для здійснення міжнародних розрахунків.

Латиноамериканська країна Сальвадор – перша держава світу, яка у 2021 році оголосила Біткоїн офіційним платіжним засобом. На практиці це означає, що будь-який бізнес в країні буде зобов'язаний приймати Біткоїни як оплату своїх товарів і послуг, за винятком ситуацій, коли він не матиме технологій, необхідних для виконання транзакцій. Цікаво, що 80 % населення цієї країни не мають доступу до мережі Інтернет. Президент Венесуели Ніколас Мадуро у листопаді 2017 року оголосив про намір держави створити власну криптовалюту під назвою "El Petro" для боротьби з наслідками економічної кризи в умовах санкцій з боку США, що буде забезпечена наявними нафтовими, газовими та алмазними ресурсними запасами.

У Новій Зеландії в листопаді 2017 року Управління фінансового контролю та нагляду прирівняло операції з цифровими валютами до операцій з цінними паперами.

В Австралії набув чинності закон, який регулює діяльність обмінників криптовалюти. Так, відповідно до нормативних вимог, усі обмінники криптовалюти мають бути зареєстровані в Австралійському центрі аналізу транзакцій і звітності.

В Індії уряд розглядає можливість запуску власної криптовалюти під назвою "лакшмі".

Таким чином, криптовалюти у більшості країн світу стають повноцінним платіжним засобом та потужним інвестиційним активом. Зацікавленість до використання криптовалют сприяє інвестиційній привабливості платіжних інфраструктур.

У ЄС все ще відсутні єдині правила для забезпечення того, щоб провайдери віртуальних валют застосовували вимоги щодо протидії відмиванню коштів та фінансуванню тероризму. Саме тому потенційним способом розв'язання цієї проблеми є створення та впровадження європейської правової бази, яка регулюватиме питання контролю за обігом криптовалюти та здійснення транзакцій з використанням цифрових валют.

Вагомим ризиком використання криптовалют залишаються спонсорство міжнародного тероризму та транснаціональної злочинної діяльності, які утворюють суттєву загрозу світовій фінансовій системі. Внаслідок стрімкого розширення платіжних можливостей у мережі Інтернет пов'язані ризики істотно збільшилися. У 2020 році обсяг незаконних транзакцій з криптовалютами становив $10 млрд. США. Досить часто злочинці використовують криптовалюти з метою незаконного придбання або продажу зброї, наркотиків, торгівлі людьми. Цифрові валюти адаптовані для використання організованими злочинними угрупованнями, оскільки вони досить широко використовуються в міжнародному обігу та забезпечують необхідний рівень анонімності. Маючи спеціальні технічні навички та вміння, міжнародні терористичні угруповання можуть використовувати віртуальні валюти для фінансування терористичних заходів. Оцінка реальної загрози відмивання грошей, пов'язаної з віртуальними активами та криптовалютами, демонструє, що кримінальний світ може використовувати віртуальні валюти для доступу до "чистої готівки". При застосуванні віртуальних валют організовані злочинні угруповання можуть анонімно отримувати доступ до грошових коштів і приховувати сліди своїх транзакцій.

Правоохоронці, виявляючи майнерів криптовалют, переважно інкримінують їм незаконне підключення до електромереж, фіктивне підприємництво, ухилення від сплати податків. За таких умов необхідним є розробка стратегії спільної правоохоронної

діяльності з метою забезпечення контролю за обігом криптовалюти, що посилить правові можливості відповідальних силових структур у боротьбі з відмиванням брудних коштів, торгівлею людьми та фінансуванням тероризму.

Враховуючи актуалізацію перспективного поширення цифрових валют, перед будь-якою державою постає важливе завдання створення захищеного національного сегменту кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством, нейтралізація посягань на інформаційні ресурси держави з боку інших країн. З метою запобігання будь-яким проявам фінансування тероризму з використанням криптовалюти, наприклад, американські правоохоронні органи взаємодіють із спеціалізованими Біткоїн-компаніями для виявлення протиправної діяльності у блокчейн-платформах. За позицією уряду Австралії криптовалюти сприяють поширенню організованої злочинності, оскільки вони досить широко використовуються в онлайн-казино та потенційно можуть застосовуватися для торгівлі людьми. Проте у доповіді Державного казначейства Великої Британії "National risk assessment of money laundering and terrorist financing 2020" від 17 грудня 2020 року зазначено, що фінансування тероризму за допомогою криптовалюти обмежується відсутністю широкого використання цифрових активів. Тому не прогнозується проблема масштабного використання криптовалюти з метою фінансування тероризму [8].

10 серпня 2021 року хакер зламав "Poly Network" (платформу на основі блокчейну) та вивів з неї понад $600 млн. США у криптовалютах. Ймовірно, це одна з наймасштабніших подібних крадіжок в історії децентралізованих фінансових сервісів. Усього зловмисники вивели 2858 токенів криптовалюти "Ethereum" на суму близько $267 млн. США, 6610 токенів "Binance" на суму понад $252 млн. США та приблизно $85 млн. США у токенах "USDC" у мережі "Polygon". Адже хакери, які зламали проєкт "Poly Network" і викрали $611 млн. США, почали повертати вкрадені кошти, що створило прецедент світового масштабу. Це переконливо засвідчує уразливість та неможливість належного кібернетичного захисту віртуальних криптобіржових інфраструктур.

Висновки.

Динаміка змін сьогодення зумовлює появу в XXI столітті новітніх дефініцій. Фінансові системи окремих країн удосконалюються та прогресують у контексті розвитку ІТ-технологій та загальної комп'ютеризації економіки. З'являються нові фінансові інститути, інструменти та форми взаємодії між людьми. Так, з'явився аналог традиційних валют – криптовалюта. "Bitcoin" уперше з'явився у 2009 році і став децентралізованою конвертованою валютою та першою криптовалютою. Сьогодні у світі існує близько 1600 видів криптовалют ("Bitcoin", "Litecoin", "Ethereum", "Peercoin"), але найвідомішою з огляду на швидкий розвиток залишається саме "Bitcoin". Криптовалюта – це цифровий ресурс, призначений для роботи в якості засобу обміну, який використовує криптографію для забезпечення своїх транзакцій, контролю створення додаткових одиниць та перевірки передачі активів . Функціонування системи відбувається децентралізовано в розподіленій комп'ютерній мережі.

На жаль, на міжнародному рівні все ще нормативно не врегульовано уніфікований розвиток цифрових технологій, зокрема блокчейну, що створює передумови для серйозних викликів світовій фінансовій стабільності та безпеці будь-якої держави. Анонімність транзакцій та відсутність фактичного контролю за обігом криптовалют з боку державних структур сприяє тінізації економіки, до того ж навіть добросовісні власники криптовалют фактично позбавлені можливості захистити свої інтереси в адміністративному чи судовому порядку. У зв'язку із цим головна проблема, що виникає

навколо криптовалют полягає в тому, що до цього часу відсутня уніфікована міжнародна конвенція щодо обігу криптовалют, зокрема “Bitcoin” [2, с. 220].

Для України в сучасних умовах актуальним є схвалення законопроекту “Про віртуальні активи” [9], проект якого передбачає комплексне регулювання відносин, що виникають з приводу створення, випуску та обігу віртуальних активів. Реалізація запропонованих положень сприятиме забезпеченню відкритості та прозорості угод, які укладаються на ринку віртуальних активів, та запобіганню зловживанням на цьому ринку з боку недобросовісних учасників. З набуттям чинності цим законом власники віртуальних активів, й зокрема криптовалют, отримають низку переваг. Завдяки тому, що з’явиться законодавче регулювання цієї сфери, вони, як мінімум, зможуть захистити свої статки у віртуальних активах, якщо щось трапиться.

Крім того, будуть вирішені питання щодо розбудови інфраструктури ринку віртуальних активів, забезпечення його відкритості та ефективності. Метою прийняття цього акту є: впорядкування нормативно-правового регулювання для ринку віртуальних активів, його учасників; визначення правового статусу віртуальних активів як об'єктів цивільних прав; впорядкування цивільно-правових відносин між фізичними та юридичними особами, які виникають в процесі використання віртуальних активів; визначення правового статусу учасників ринку та користувачів у сфері віртуальних активів; встановлення основних засад та принципів державної політики у сфері віртуальних активів; державне регулювання та контроль на ринку віртуальних активів.

Використана література

1. Гребенюк М.В., Лук’янчук Р.В. Правовий режим криптовалют: досвід ЄС. *Науковий вісник Національної академії внутрішніх справ*. 2017. № 4. С. 310-323.

2. Гребенюк М.В., Черняк А.М. Деякі аспекти обігу криптовалют: сучасний зарубіжний досвід правової регламентації. *Підприємництво, господарство і право*. 2018. № 8. С. 218-221.

3. Кудь О.О., Кучерявенко М.П., Смичок Є.М. Цифрові активи та їх правове регулювання у світі розвитку технології блокчейн: монографія. Харків: Право, 2019. 216 с.

4. Логойда В.М. Перспективи врегулювання правового статусу криптовалюти в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. № 63. С.152- 157.

5. Михайловський В.І., Костюк О.В. Визначення поняття “криптовалюти”: міжнародний досвід. *Науковий вісник публічного та приватного права.* 2019. Вип. № 1. Т. 2. С. 226-231.

6. Овчаренко А.С. Правове регулювання віртуальних активів та криптовалют в Україні: сучасний стан та перспективи. *Юридичний науковий електронний журнал*. 2020. № 4. С. 200-202.

7. Прокопенко В. Віртуальні активи. *Юридична газета.* 2021. № 1(731).

8. National risk assessment of money laundering and terrorist financing UK 2020 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf (дата звернення: 20.06.20210).

9. Про віртуальні активи: проект закону України від 11.06.20 р. № 3637. URL: https://w1c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3 (дата звернення: 20.06.20210).

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

УДК 342.95

ЛІСОВСЬКА Ю.П., *кандидат юридичних наук.*
ORCID: https://orcid.org/0000-0001-9278-4487.

ДИВЕРСИФІКАЦІЯ ЯК КОДИФІКОВАНО-ЦИФРОВА СИСТЕМА АДМІНІСТРАТИВНО-ПРАВОВОГО УПРАВЛІННЯ: МІЖІНФРАСТРУКТУРНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО КАПІТАЛУ

Анотація. *В статті досліджується диверсифікація як система адміністративно-правового управління в міжгалузевому забезпеченні діджиталізації України, яка розширює семантичний взаємозв'язок права та економіки в сучасному квантово-електронному світі. Показано диверсифікацію в якості правової політики світового порядку, що зумовлена планомірним та креативним взаємозв'язком з метою захисту правових потреб та інтересів особи, держави, а також суспільства. У роботі здійснено аналіз перспектив диверсифікації як кодифікаційно-цифрової системи адміністративно-правового управління в міжінфраструктурі інформаційного капіталу. Висвітленню диверсифікаційного механізму реалізації норм чинного законодавства у сфері захисту критичної інфраструктури і присвячена ця стаття.*

Ключові слова: *диверсифікація, діджиталізація, критична інфраструктура, квант, управління, інформаційний капітал.*

Summary. *The article examines diversification as a system of administrative and legal management in the intersectoral provision of digitalization in Ukraine, which expands the semantic relationship between law and economics in the modern quantum-electronic world. Diversification is shown as a legal policy of the world order, which is due to a planned and creative relationship to protect the legal needs and interests of the individual, the state and society. This paper analyzes the prospects of diversification as a digital codification system of administrative and legal management in the inter-infrastructure of information capital. This article is devoted to highlighting the diversification mechanism for the implementation of current legislation in the field of critical infrastructure protection*.

Keywords: *diversification, digitalization, critical infrastructure, quantum, management, information capital.*

Аннотация. *В статье исследуется диверсификация как система административно-правового управления в межотраслевом обеспечении диджитализации Украины, которая расширяет семантическую взаимосвязь права и экономики в современном квантово-электронном мире. Показана диверсификация в качестве правовой политики мирового порядка, обусловленной планомерной и креативной взаимосвязью с целью защиты правовых потребностей и интересов личности, государства, а также общества. В работе проведен анализ перспектив диверсификации как кодификационно-цифровой системы административно-правового управления в межинфраструктуре информационного капитала. Освещению диверсификационный механизм реализации норм действующего законодательства в сфере защиты критической инфраструктуры и посвящена эта статья.*

Ключевые слова: *диверсификация, диджитализация, критическая инфраструктура, квант, управление, информационный капитал.*

Постановка проблеми. За сучасних умов актуальною категорією, яка визначає систему адміністративно-правового управління в міжгалузевому забезпеченні діджиталізації України, є диверсифікація. Саме такий якісно новий тренд міжгалузевих відносин як диверсифікація розширює семантичний взаємозв'язок права та економіки в сучасному квантово-електронному світі. При цьому фундаментальною матрицею суспільного життя у кіберпросторі є цифрова економіка як диверсифікаційна система

господарювання. Адже ця система міжгалузево забезпечує ефективне використання обмежених ресурсів, необхідних для задоволення нагальних потреб. Так, категоріальний термін "диверсифікація" як оптимальний спосіб мінімізації корупційних ризиків у сучасному кіберкапіталі використовують у багатьох сферах суспільного життя. Навіть лексико-семантичне тлумачення означеного терміну вказує на його багатоаспектність і поширеність, оскільки, на наш погляд, може бути використано в наступних значеннях: правова політика світового порядку, що зумовлена планомірним та креативним взаємозв'язком; продумана плановість та законнність в міжнародній економіці; сукупність господарчих одиниць, міжнародних установ, об'єднаних структурно з метою захисту правових потреб та інтересів особи, держави, а також суспільства.

Результати аналізу наукових публікацій. Цієї проблематики торкались такі вітчизняні дослідники як: О. Бригінець, А. Гриценко, М. Курко, П. Лісовський, М. Недюха, Д. Неліпа, С. Подоляка тощо. Їх фундаментальні праці стали науково-теоретичним підгрунтям вирішення проблемних питань диверсифікації як якісно нового адміністративно-правового управління цифровою економікою.

Метою статті є аналіз та визначення перспектив диверсифікації як кодифікаційно-цифрової системи адміністративно-правового управління в міжінфраструктурі інформаційного капіталу.

Виклад основного матеріалу. В сучасних умовах цифрової економіки виробництва, розподілу, обміну і споживання матеріальних благ визначаються якісно нові форми адміністративно-правового управління. Своєю чергою, правова форма диверсифікації як надання різнобічного, комбінованого та міжгалузевого характеру оптимізує та поширює виробництво різнорідних товарів та надання різних інтелектуальних послуг. Це виявляється у диверсифікації як генеративно-цілісному визначенні правовою державою розміру податків, мінімізації корупційних ризиків, мінімальної заробітної плати, строку відпустки, встановлення правил квантової (радіобіокосмічної), екологічної та техногенної безпеки тощо.

Диверсифікація як комплексна система суб'єктів управління та координації в міжгалузевих відносинах.

Із наведеного витікає, що управління містить у собі один із видів діяльності, тобто може бути охарактеризоване як активне, динамічне явище. "Це діяльність суб'єкта, що виявляється в цілеспрямованому, організуючому впливі на об'єкт управління, здійснюваному з метою приведення його в бажаний для суб'єкта стан" [1, с. 8]. Іншими словами, диверсифікація як управлінська діяльність має генеративно-цілісний характер. Тому, саме управління в контексті диверсифікації може бути розглянуто в якості системи із спектром набору відповідних елементів, які визначають міжгалузевість її сутності. Так, Д.Д. Цабрія в своєму монографічному дослідженні "Система управління (державно-правові аспекти)", систему управління визначає як упорядковану сукупність взаємопов'язаних елементів, які відрізняються функціональними цілями, діють автономно, але спрямовані на досягнення загальної мети" [2, с. 12].

Крім того, щодо дослідження вертифікаційних особливостей організаційно-правових основ управління варто вважати конструктивну думку вченого М.К. Якимчука, що система управління – це передусім структурно-організаційне утворення, що віддзеркалює побудову системи, характеризується складом і підлеглістю його елементів, способом їхнього зв'язку та взаємодії, єдністю елементів, об'єднаних у достатнє число підрозділів [3, с. 90]. Також обґрунтованим є методологічний підхід, згідно з яким система управління містить у собі форму реалізації взаємодії та розвитку

відносин управління, які виражаються в законах і принципах управління, а також у цілях, функціях, структурі, методах і процесі управління [4, с. 25].

З аналізу вищенаведених підходів, сутність системи управління розкривається в силу взаємодії суб'єкта та об'єкта управління, що цілеспрямовано на контроль та координацію певної галузі в суспільних відносинах. З огляду на це, як підкреслює В.М. Момот, між суб'єктом та об'єктом управління можуть встановлюватись субординаційні чи координаційні зв'язки. Адже відносини субординації – це такі відносини між суб'єктами управлінської діяльності, які виражають підпорядкованість одного суб'єкта іншому в процесі управління єдиним об'єктом. У свою чергу, відносини координації мають місце між суб'єктами управлінської діяльності, які не підпорядковані один одному, оскільки для них властивим є узгодження діяльності, поєднання зусиль під час реалізації окремих і загальних цілей [5, с. 106].

Отже, в диверсифікаційному аспекті об'єкт управління необхідно розуміти свідомо спрямований, планомірний, організований, генеративно-цілісний вплив суб'єкта управління.

Диверсифікаційна природа квантових електронних ресурсів щодо кіберзахисту критичної інфраструктури.

Основу державного управління національною системою кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, розвідувальні та контррозвідувальні структури, органи прокуратури, Національна поліція України, Національний банк України, паливно-енергетичний комплекс тощо.

На Службу безпеки України покладаються: попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на протидію з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Аналіз положень Стратегії кібербезпеки України свідчить, що найбільш поширеними ризиками, що сприяють деструктивному впливу загроз у кіберсфері, можна вважати недостатній рівень захищеності критичної інфраструктури, безсистемність заходів кіберзахисту критичної інфраструктури, недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів тощо.

Серед основних моментів забезпечення кіберзахисту виділено доцільність таких першочергових заходів: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури та визначення критеріїв належності інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури; впровадження державного реєстру об'єктів критичної інформаційної інфраструктури; розробка вимог до кіберзахисту об'єктів критичної інфраструктури; розробка вимог до кіберзахисту об'єктів критичної інфраструктури; покладання на власників (розпорядників) об'єктів критичної інфраструктури обов'язку створення підрозділів кіберзахисту; зміцнення державно-приватного партнерства у запобіганні та локалізації кіберзагроз та захисту інформації, а також сприяння власниками (розпорядниками) об'єктів критичної інфраструктури державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту; відпрацювання належного механізму обміну інформацією між партнерами з державного та приватного сектору стосовно загроз критичній інформаційній інфраструктурі [6].

Так, координація діяльності у сфері кібербезпеки як складової національної безпеки України зідйснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. При цьому, Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Своєю чергою, Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини та громадянина; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури в банківській системі України).

Окремо варто зупинитись на тому, що законодавець дає визначення критично важливим об'єктам інфраструктури. Зокрема, в кіберпросторі під ними необхідно розуміти підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають стратегічне значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, довкілля, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Крім того, визначено й "об'єкт критичної інформаційної інфраструктури" – це комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака, яка безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [7].

Водночас необхідно визначити, що саме завдяки положенням постанови, міністерствам, іншим центральним органам виконавчої влади разом із Службою безпеки, іншим заінтересованим державним органам передбачено подати пропозиції до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури в цій сфері [8].

На наш погляд, диверсифікаційний механізм реалізації норм чинного законодавства у сфері захисту критичної інфраструктури вдається посилити завдяки передбаченим завданням щодо підготовки за участю Служби безпеки України законопроекту щодо розмежування кримінальної відповідальності за злочини у сфері використання комп'ютерних систем і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності [9].

Диверсифікація як міжгалузеві нормативно-правові акти трансформації цифрового порядку.

Трансформація цифрового порядку в часи квантово-електронної епохи, що має ознаки непередбачуваності, є значним фактором впливу, в тому числі й на національну безпеку України та окремих держав. Характер цієї цифрової трансформації є складним та швидкоплинним, що зумовлює зміну загроз, які виникають. Такий стан речей вимагає адекватного реагування, зокрема – постійних змін у державній політиці на законодавчому рівні.

Державне реагування на процеси, що існують в сучасному квантово-електронному світі, стосується перманентного впливу нанотехнологій на суспільство та його інститути. Так, наприклад, в кіберсучасності існують два основні документи концептуальних засад розвитку цифровізації – схвалена розпорядженням Кабінету Міністрів України від 17.01.18 р. № 67-р "Концепція розвитку цифрової економіки та суспільства на 2018 – 2020 роки" і "Цифрова адженда України – 2020". Зазначені документи є досить ґрунтовними,

але їх зміст значною мірою презентує сучасні інформаційні технології, аніж виробляє державну стратегію.

При цьому, використання математичного моделювання за допомогою систем і методів квантової електроніки є перспективним напрямом дослідження, описання та прогнозування, зокрема як окремих агробіопроцесів та явищ, такі і агроекологічних систем у цілому. Це є інструментальною основою для подальшого проведення інформаційного моніторингу агроекосистеми, що сформувалась як диверсифікаційна система спостережень, оцінки та прогнозування станів досліджуваного об'єкта або групи об'єктів з метою прийняття раціональних управлінських рішень. Саме необхідність отримання різнобічних квантово-електронних моделей та застосування їх у агроекосистемі обумовлена можливістю аналізувати та керувати їх станом, прогнозувати майбутні технології для підтримання ґрунтового покриву в стані, за умов якого зберігається властивість до регуляції циклів біофільних елементів, забезпечення контролю розвитку антропогенних процесів. Так, дослідження, пов'язані з розробкою науково обґрунтованої методології комплексного прогнозу екологічного стану конкретної агроекологічної системи залежно від рівня антропогенного навантаження та рекомендацій щодо його регламентації на основі знань просторово-часових особливостей цієї системи, дозволяють з упередженням, шляхом системного моделювання складних процесів, визначити оптимальну агротехнологічну електронну карту польових робіт, оцінити наявний та спрогнозувати необхідний рівень екологічної безпеки.

Крім того, саме такі квантово-електронні модулятори як радіодальноміри є перспективними для використання також у нафтогазовій системі з метою мінімізації ризиків щодо ґрунтової поверхні земель, а саме: її аномалій, а також діагностики якості нормоконтролю щодо корозійної стійкості металевих труб. Для цього, значною мірою формують диверсифікаційну систему таких показників контролю та об'єктивних критеріїв, за допомогою яких можна відслідковувати стан та захищати екоенергетичну безпеку. На цьому етапі внаслідок недостатності необхідної інформації та потужної різноманітності явищ, що характеризують трансформацію ґрунтів залежно від комбінацій природних та антропогенних факторів, можуть виникати відповідні перешкоди. Іншими словами, квантова електронна система, що має міжгалузевий характер диверсифікації, дозволяє конструктивно визначити критерії та отримати кількісну оцінку функціонування, спрогнозувати майбутні стани екоенергосистеми, виявити її інші функціональні особливості. Адже квантова електронна система дозволяє моделювати різні можливі ситуації (навіть ситуації функціонування диверсифікаційної системи в екстремально критичних умовах, створених шляхом імітаційного моделювання).

Таке забезпечення аерокосмічного моніторингу поверхні земель за допомогою квантової електроніки дозволяє мобільно та автономно вивчати напрямки, швидкості розвитку грунтовних процесів та відтворення родючості ґрунту, оптимізації екологічної ситуації з врахуванням можливих наслідків. При вирішенні означених нагальних проблем необхідно враховувати ґрунтово-кліматичні умови, господарсько-економічні особливості досліджувальної екоенергосистеми, кількісний та якісний стан всіх її складових (ґрунт – рослина – зона аерації – ґрунтові води – атмосфера).

Висновки.

Таким чином, стан диверсифікації як системи адміністративно-правового управління у кіберсфері є стратегічним завданням щодо забезпечення національної безпеки України. У процесі дослідження встановлено, що законодавство із зазначеного питання перебуває ще у стадії створення та становлення, що потребує подальшого удосконалення. Крім того, невизначеними залишаються передбачені ч. 2 ст. 6 Закону

України “Про основні засади забезпечення кібербезпеки України” критерії та порядок зарахування об’єктів до критичної інфраструктури, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, оскільки вони мають бути визначені Кабінетом Міністрів України, а в банківській сфері – Національним банком України.

У цьому відношенні головною метою диверсифікаційної системи керування є механізм управління нанотехнологічними впливами (та їх оптимізація) на природні процеси за умови мінімізації енерго- та ресурсовитрат, збереження довкілля, а також розробка методів прогнозу стану екоенергосистеми та її складових на різних структурних рівнях для оцінки функціонування визначення оптимального комплексу різних заходів, планування розвитку та аналізу післядій управлінських рішень або невиконання рекомендованих заходів.

Використана література

1. Колпаков В.К. Адміністративне право України. Київ: Юрінком Інтер, 1999. 736 с.

2. Цабрия Д.Д. Система управления (государственно-правовые аспекты). Москва: Юрид. лит, 1990. 271 с.

3. Якимчук М.К. Організаційно-правові основи управління в органах прокуратури України [дисертація]. Чернівці, 2002. 470 с.

4. Долгополова М.М. Управління загальнодержавною системою забезпечення безпеки дорожнього руху: дис. ...канд. юр. наук. – (Запорізький юридичний ін-т МВС України). Харків, 2003. 229 с.

5. Момот В.М. Робота з персоналом в органах та підрозділах державної податкової адміністрації України: теоретичні та організаційно-правові засади: дис. ...канд. юр. наук. Харків: Ун-т внутр. справ, 2006. 204 с.

6. Про Стратегію кібербезпеки України: Указ Президента України “Про уведення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року” від 15.03.16 р. № 96/2016. *Урядовий кур’єр.* 2016. № 52.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Урядовий кур’єр.* 2017. № 215.

8. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. *Урядовий кур’єр*. 2016. № 168.

9. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеного в дію Указом Президента України від 13 лютого 2017 р. № 32: Указ Президента України “Про рішення РНБО від 10 липня 2017 р.” від 30.08.17 р. № 254/20177. *Урядовий кур’єр*. 2017. № 162.

10. Лісовська Ю.П. Інформаційна безпека України: навчальний посібник. Київ: Видавничий дім “Кондор”, 2017. 199 с.

11. Лісовська Ю.П. Кібербезпека: ризики та заходи: навчальний посібник. Київ: Вид. дім “Кондор”, 2019. 272 с.

12. Лісовська Ю.П. Правова держава як кіберінфраструктурне забезпечення інформаційного капіталу: монографія. Київ: Міжрегіональна Академія управління персоналом, 2020. 252 с.

13. Литвиненко В.І., Заросило В.О., Лісовська Ю.П. Антикорупційна інфраструктура країн світу: контроль, моніторинг, представництво: навч. посіб. Київ: Видавництво Ліра-К, 2021. 200 с.

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

УДК 343.2/.7:004.056(477)

ТАРАН О.В., *доктор юридичних наук, професор*, провідний науковий співробітник наукової лабораторії з проблем протидії злочинності Національної академії внутрішніх справ.
ORCID: https://orcid.org/0000-0003-4752-9924.
ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, старший науковий співробітник*, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0001-7496-9904.

ОРГАНІЗОВАНА КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: ПРОБЛЕМИ ФОРМУВАННЯ ОФІЦІЙНОЇ СТАТИСТИКИ ТА ЇЇ АНАЛІЗУ

Анотація. *У статті проаналізовані види, форми та зміст статистичної звітності, що відображають стан і структуру кіберзлочинності в Україні. Визначено способи інтерпретації статистичної інформації й використання її можливостей у запобіганні й протидії кіберзлочинності. Узагальнено та розкрито недоліки структури офіційних статистичних даних, що полягають у безсистемності, непогодженості й непослідовності їх формування. Відзначається, що дотепер у національному та міжнародному законодавстві не вистачає загальновизнаного визначення киберзлчинів, а тому і єдиного підходу до розробки підстав віднесення протиправних діянь до таких злочинів. Звіти розроблено без обліку подальшого аналізу кіберзлочинності. І якщо у звіті Національної поліції України містяться дані про певну кількість злочинів, які можна віднести до киберзлочинів, в офіційних статистичних звітах, крім Розд. XVI КК України, такі відсутні. Тому, про офіційну статистику, яка повно та вірогідно віддображає структуру кіберзлочинності, сьогодні не йдеться. Можливо проаналізувати тільки динаміку цього виду злочинності, структуру злочинності на основі врахованих злочинів.*

Ключові слова: *кіберзлочинність, організована кіберзлочинність, латентна кіберзлочинність, аналіз стану кіберзлочинності, статистичні звітності.*

Summary*. The article analyzes the types, forms and content of statistical reporting that reflects the state and structure of cybercrime in Ukraine. Ways to interpret statistical information and to use its capabilities in preventing and combating cybercrime are identified. The shortcomings of the structure of official statistical data, namely unsystematic character, inconsistency and incoherence of their formation, are generalized and revealed. It is noted that the national and international legislation lacks a generally accepted definition of cybercrime so far, and therefore a single approach to defining the grounds for classifying illegal acts as such crimes. The reports were developed without considering further analysis of cybercrime. And while the report of the National Police of Ukraine contains data on a number of criminal offenses that can be attributed to cybercrime, the official statistical reports prepared by the Office of the Prosecutor General of Ukraine and the State Judicial Administration of Ukraine, except for Chapter XVI of the Criminal Code, are missing the mentioned data. Therefore, official statistics, which fully and accurately reflect the state and structure of cybercrime cannot be introduced today. It is possible to analyze only the dynamics of this type of crime, the structure of crime on the basis of recorded crimes. The number of criminal offenses under the articles of chap. XVI of the Criminal Code of Ukraine, is growing unevenly, and this growth in the last 4 years is insignificant. The share of these criminal offenses is growing more dynamically. But their share of the total crime rate in Ukraine today is insignificant and is less than one percent - in 2020 0.69. In the first quarter of 2021, employees of cyber police units of the National Police of Ukraine, for the first time detected 4 criminal offenses under Art. 255 of the Criminal Code of Ukraine ("Creation of a criminal organization"). During 2013 – 2010, 112 persons were found to have committed criminal offenses of this category as part of a group,*

16 of them as part of an organized group. Also during this period, 171 persons who committed criminal offenses in the group in previous years were identified, including 68 in the organized group. The number of convicted persons who committed criminal offenses in the group during this period is 64, 9 of them committed crimes in an organized group.

Keywords: *cybercrime, organized cybercrime, latent cybercrime, cybercrime analysis, statistical reporting.*

Аннотация. *В статье проанализированы виды, формы и содержание статистической отчетности, отражающие состояние и структуру киберпреступности в Украине. Определены способы интерпретации статистической информации и использования ее возможностей в предотвращении и противодействии киберпреступности. Обобщены и раскрыты недостатки структуры официальных статистических данных, заключающиеся в бессистемности, несогласованности и непоследовательности их формирования. Отмечается, что до сих пор в национальном и в международном законодательстве не хватает общепризнанного определения киберпреступлений, а потому и единого подхода к разработке оснований отнесения противоправных деяний к таким преступлениям. Отчеты разработаны без учета дальнейшего анализа киберпреступности. И если в отчете Национальной полиции Украины содержатся данные об определенном количестве преступлений, которые можно отнести к киберпреступлениям, в официальных статистических отчетах, кроме разд. XVI УК Украины, таковые отсутствуют. Поэтому, об официальной статистике, которая полно и достоверно отражает структуру киберпреступности, сегодня речь не идет. Возможно проанализировать только динамику этого вида преступности, структуру преступности на основе учтенных преступлений.*

Ключевые слова: *киберпреступность, организованная киберпреступность, латентная киберпреступности, анализ киберпреступности, статистические отчетности.*

Постановка проблеми. Відповідно до досліджень, що були проведені Atlas VPN, у 2020 році у всьому світі кіберзлочинність обійшлася підприємствам, урядовим установам і споживачам більш ніж в 1 трильйон доларів. Це близько одного відсотка світового ВВП. Деякі експерти з кібербезпеки очікують, що до кінця цього року фінансовий збиток від кіберзлочинності досягне 6 трильйонів доларів [1].

Сьогодні практично всі фахівці визнають, що ситуація з кіберзлочинністю у світі має сталу тенденцію до погіршення. При цьому посилюється зв’язок між кіберзлочинністю та організованою злочинністю [8].

Найбільшої небезпеки організована злочинність набуває у формі транснаціональної протиправної діяльності, не обмеженої державними кордонами та географічними відстанями. Транснаціоналізація злочинності, набуття нею якісно нових рис, сприяє використанню організованими злочинними угрупуваннями новітніх телекомунікаційних технологій як для забезпечення вчинення “традиційних” злочинів так і здійснення принципово нових видів протиправної діяльності, безпосередньо пов’язаних із функціонуванням кіберпростору [9].

Проте на сьогодні у світі не існує ні релевантної статистики, яка відображає реальний стан кіберзлочинності, ні надійних методів збору таких даних. Справа не тільки у відсутності ідентичності національного кримінального законодавства країн в сфері боротьби з кіберзлочинністю і різної практики його застосування, а й у відмінності у формуванні кримінальної статистики та особливості правоохоронної системи.

Потрібно констатувати, що і в Україні про офіційну статистику, яка повно й достовірно відбиває стан і структуру кіберзлочинності, сьогодні не йдеться. Ми можемо проаналізувати тільки динаміку цього виду злочинності, структуру злочинності на основі облікованих злочинів [7].

Результати аналізу наукових публікацій. Окремі аспекти аналізу кіберзлочинності, зокрема організованої, вивчали О.В. Амелін, О.М. Бандурка, В.В. Василевич, Б.М. Головкін, В.В. Голіна, М.В. Гуцалюк, О.М. Джужа, А.П. Закалюк, О.Г. Кулик, О.М. Литвинов, В.В. Марков, Д.М. Прокоф'єва-Янчиленко, В.І. Трапезніков, В.О. Туляков та ін. Водночас, проблемам аналізу організованої кіберзлочинності, зокрема і у частині офіційної статистики, приділяється недостатньо уваги. Крім того, зважаючи на те, що більша частина кіберзлочинів, які вчиняються організованими групами, злочинними організаціями, знаходяться поза межами статистики, актуалізується проблема латентної кіберзлочинності в Україні.

Метою статті є системний аналіз національних статистичних даних, що стосуються кіберзлочинності, організованої кіберзлочинності, осіб, які вчинили кіберзлочини та інших даних, що відображені у різних офіційних джерелах; об'єктивна оцінка структури і змісту таких даних та можливостей їх використання для запобігання і та протидії кіберзлочинності.

Виклад основного матеріалу. У вітчизняному законодавстві не існує чіткого визначення поняття кіберзлочин [6].

У Законі України "Про основні засади забезпечення кібербезпеки України" від 05.10.17 р. № 2163-VIII, визначено: "Кіберзлочинність – сукупність кіберзлочинів", "Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України" [4].

Отже терміном "кіберзлочинність" охоплюється широкий спектр правопорушень, що ускладнює розробку системи типології або класифікації кіберзлочинності.

У доктрині існують різні підходи щодо класифікації кіберзлочинів.

Дослідники пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета посягання: нові злочини, що стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені Розділом XVI Кримінального кодексу України); традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету [6].

На нашу думку, під поняттям "кіберзлочини" слід розуміти кримінальні правопорушення, передбачені Розділом XVI КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку", та кримінальні правопорушення із кваліфікуючою ознакою – з використанням високих інформаційних технологій і телекомунікаційних мереж [6].

Найбільш повно статистичні дані про кіберзлочини в Україні відображено у відомчій статистичній звітності Національної поліції України, зокрема у "Звіті про результати роботи підрозділів Національної поліції України" у Розділі XVII "Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції", де, крім злочинів, окреслених Розділом XVI КК України, вказана ще низка інших злочинів, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст.ст. 176, 185, ч. 3 і 4 ст. 190 , ст. 200, 229, 231, ч. 3, 4 і 5 ст. 301 КК України.

Окремі показники про обліковані кіберзлочини, передбачені іншими статтями КК України, відображені в інших статистичних звітах, зокрема злочини, передбачені ст. 376-1 у Єдиному звіті про кримінальні правопорушення, що готується Офісом Генерального прокурора України (за 2020 рік обліковано 30 кримінальних правопорушень).

Також варто зазначити, що об'єктивна сторона, суб'єкт, суб'єктивна сторона, кваліфікований та особливо кваліфікований склад злочину, передбаченого ст. 301 КК України, у цілому збігаються з відповідними ознаками посягання, предметом якого є твори, що пропагують культ насильства і жорстокості (ст. 300 КК України). При цьому кримінальні правопорушення, передбачені ст. 301 КК України, вчинені з використанням високих інформаційних технологій, враховуються у звіті, а передбачені ст. 300 КК України – не враховуються [6].

А.В. Савченко вважає, що, крім кримінальних правопорушень, зазначених у вищевказаному звіті (НПУ), під категорію кіберзлочинів можуть підпадати й інші злочини, передбачені КК України, за умови, що знаряддям їх вчинення будуть інформаційні мережеві технології та(або) їх наслідки позначатимуться у кіберпросторі [5].

Серед кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій у 2020 році, найбільшу питому вагу становили кримінальні правопорушення, передбачені ч. 3,4 ст. 190 КК України – 25,9 % (1355). Організованими групами вчинено 111 шахрайств.

Разом з тим варто зауважити, що у 2020 році зареєстровано близько 1800 кримінальних правопорушень, передбачених ч. 1 та ч. 2 ст. 190 КК України, які вчинені з використанням високих інформаційних технологій.

Окрім різних причин, на думку фахівців, це пов'язано, певною мірою, з невірною кваліфікацією таких кримінальних правопорушень. Так нерідко органи досудового розслідування відкривають кримінальні провадження за ч. 1 або ч. 2 ст. 190 КК України без урахування кваліфікуючої ознаки – "вчинено з використанням електронно-обчислювальної техніки".

Проте ці кримінальні правопорушення не відображені у звітності, як вчинені з використанням високих інформаційних технологій.

Отже, не всі кримінальні правопорушення, що зареєстровані в ЄРДР і відображені у звітах, враховані як злочини, вчинені з використанням високих інформаційних технологій, тобто як кіберзлочини. Вони створюють певну штучну латентність кіберзлочинності в Україні.

Отже наразі можна проаналізувати лише динаміку та структуру кіберзлочинності на основі облікованих злочинів.

Проаналізуємо офіційну статистичну звітність Офісу Генерального прокурора України щодо облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Із Таблиці 1 видно, що рівень таких кримінальних правопорушень зростає нерівномірно, і це зростання впродовж останніх чотирьох років є незначним. Питома вага цих кримінальних правопорушень зростає більш динамічно, але це викликано, в першу чергу, зниженням загального рівня злочинності.

Варто наголосити, що Офісом Генерального прокурора України готується Звіт про результати боротьби з організованими групами та злочинними організаціями (форма № 1-ОЗ). Але наразі у цьому Звіті не передбачено відомостей ні про кіберзлочини, ні про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Окремі показники щодо кримінальних правопорушень, учинених групою осіб у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, відображені у Єдиному звіті про кримінальні правопорушення.

Таблиця 1

Обліковані кримінальні правопорушення, передбачені статтями Розділу XVI КК України, їх питома вага у загальній злочинності та кількість зареєстрованих кримінальних правопорушень

	2013	2014	2015	2016	2017	2018	2019	2020
Всього зареєстровано	563560	529139	565182	592604	523911	487133	444130	360622
Розділ XVI КК України	595	443	598	865	2573	2301	2204	2498
Питома вага (в %)	0,11	0,08	0,11	0,15	0,49	0,47	0,54	0,69

В Україні у 2020 році відповідно до звітності Офісу Генерального прокурора, обліковано 58 кримінальних правопорушень, учинених групою осіб у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що становить 2,3 % від облікованих і у 2,3 рази менше порівняно з 2019 роком (135). Із них – 54, передбачених ст. 361 КК України, у 2019 р. – 132. У 2020 році було обліковано ще 24 кримінальних правопорушення, які були вчинені групою осіб у минулих роках, і за якими провадження направлені до суду.

Із 58 кримінальних правопорушень, учинених групою осіб у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у 56 випадках досудове розслідування здійснювалося органами Національної поліції, у 2 –ДБР.

Із Таблиці 2 видно, що кількість кримінальних правопорушень, вчинених групою осіб, протягом восьми років збільшилася, хоча і відзначалися періодичні коливання.

Таблиця 2

Обліковані кримінальні правопорушення, передбачені статтями Розділу XVI КК України та кількість зареєстрованих кримінальних правопорушень вчинених групою осіб протягом 2013 – 2020 рр.

	2013	2014	2015	2016	2017	2018	2019	2020
Усього кримінальних правопорушень	595	443	598	865	2573	2301	2204	2498
Групою осіб	14	17	9	48	42	44	135	58

Протягом 2013 – 2020 рр. значно змінювалася питома вага кримінальних правопорушень, вчинених групою осіб, відносно кількості облікованих кримінальних правопорушень, передбачених статтями Розділу XVI КК України і складала від 1,5 % у 2016 р. до 6,1 % у 2019 р., див. Рис. 1.

Проаналізуємо статистичні дані про осіб, які вчинили кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI КК України).

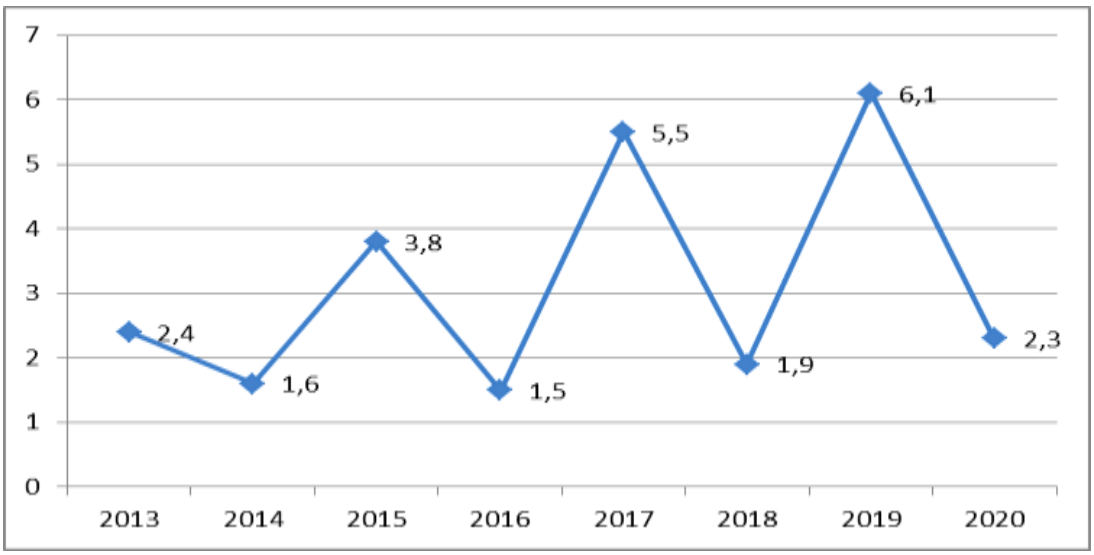

Рис. 1. Графічне зображення питомої ваги кримінальних правопорушень, вчинених групою осіб у кількості зареєстрованих кримінальних правопорушень, передбачених статтями Розділу XVI КК України протягом 2013 – 2020 рр.

В Україні у 2020 році, відповідно до звітності Офісу Генерального прокурора України (Єдиний звіт про осіб, які вчинили кримінальні правопорушення), виявлено 19 осіб, які у складі групи вчинили кримінальні правопорушення, передбачені статтями Розділу XVI КК України, у т.ч. 4 у складі організованої групи або злочинної організації. Це у 2,4 рази більше порівняно з 2019 роком (виявлено 8 осіб). 14 осіб вчинили кримінальні правопорушення, передбачені ст. 361 КК України, див. Таблицю 3.

Таблиця 3

Кількість виявлених осіб, які вчинили кримінальні правопорушення, передбачені статтями Розділу XVI протягом 2013 – 2020 рр.

	2013	2014	2015	2016	2017	2018	2019	2020
Всього виявлено осіб:	54	41	46	52	103	136	103	152
у групі	16	10	7	15	28	9	8	19
у складі ОГ або ЗО				0	12			4

У 2020 році виявлено 4 особи, які вчинили кримінальні правопорушення у складі організованої групи у 2019 році – жодної. Проте у 2019 році виявлено 2 особи з міжрегіональними зв’язками.

На нашу думку, варто також звернути увагу на аналіз статистичних даних про виявлених осіб, які вчинили кримінальні правопорушення у минулих роках. До речі, таких осіб у 2020 році виявлено на 10,5 % більше порівняно з тими, що вчинили кримінальні правопорушення у 2019 році.

У 2020 році виявлено 168 осіб, які вчинили кримінальні правопорушення у минулих роках, що на 43,6 % більше порівняно з 2019 роком (117 у 2019 р.), див. Таблицю 4.

Таблиця 4

Кількість виявлених осіб, які вчинили кримінальні правопорушення, передбачені статтями Розділу XVI у минулих роках, протягом 2013 – 2020 рр.

	2013	2014	2015	2016	2017	2018	2019	2020
Всього виявлено осіб:	26	31	34	38	65	118	117	168
у групі	7	10	7	11	19	44	23	50
у складі ОГ або ЗО		2		1	2	28	9	26

Осіб, які вчинили кримінальні правопорушення у складі групи, у 2020 році виявлено 19, а осіб, які вчинили кримінальні правопорушення у складі групи в минулих роках виявлено у 2,3 рази більше – 50. Осіб, які вчинили кримінальні правопорушення у складі організованої групи, у минулих роках виявлено у 6,5 рази більше порівняно з тими, що вчинили кримінальні правопорушення у 2020 році. За 3 місяці 2021 року виявлено 22 особи, які вчинили кримінальні правопорушення у складі організованої групи або злочинної організації у минулих роках.

Проаналізуємо статистичні дані щодо кількості засуджених, в т.ч. які вчинили злочин у складі групи та організованої групи, за статтями, передбаченими Розділом XVI Кримінального кодексу України, що готуються Державною судовою адміністрацією України.

Як видно зі судової звітності, у судах першої інстанції у 2020 році за статтями передбаченими Розділом XVI КК України, кількість осіб, судові рішення щодо яких набрали законної сили зменшилася на 4,2 % порівняно з попереднім роком (72 у 2019 р. проти 69 у 2020 р.). Разом з тим кількість засуджених осіб збільшилася на 12 % (50 у 2019 р. проти 56 у 2020 р.). При цьому кількість засуджених осіб, які вчинили злочини у складі групи, складає по 7 осіб.

Посилаючись на офіційні дані судової статистики, розглянемо динаміку кількості засуджених, в т.ч. які вчинили злочин у складі групи та організованої групи, за статтями, передбаченими Розділом XVI Кримінального кодексу України протягом 10 років.

Відповідно, у 2011 році за вчинення такої категорії злочинів засуджено 56 осіб. У 2012 році законної сили набрали обвинувальні вироки стосовно 80 осіб. Починаючи з 2013 року, з’явилася тенденція до зменшення кількості засуджених осіб – до 24: 2014 рік – 37 осіб, 2015 – 31 особа, 2016 – 24 особи. Але починаючи з 2017 року кількість засуджених осіб почала зростати: 2017 – 42 особи, 2018 – 49 осіб, 2019 – 50 осіб, і у 2020 році кількість осіб засуджених за вказані злочини зросла до 56 осіб.

При цьому варто зауважити, що кількість засуджених осіб, які вчинили злочини у групі, також не відповідає загальній тенденції щодо всіх засуджених. Їхня питома вага також збільшувалася і зменшувалася від найменшої у 2011 році – 8,9 % до найбільшої у 2016 році – 37,5 %. У 2020 році питома вага становила 12,5 %.

Протягом 2011 – 2020 років засуджено 9 осіб, які вчинили злочини у складі організованої групи: 2012 р., 2017 р., 2018 р. – по 3 особи., див. Таблицю 5.

Найбільше інформації щодо вчинення кіберзлочинів організованими групами або злочинними організаціями, виявлених працівниками підрозділів кіберполіції, можна отримати з відомчої звітності Національної поліції України, зокрема Звіту про результати роботи підрозділів Національної поліції України за 2020 р. (форма № 1-АВ).

Таблиця 5

Кількість засуджених осіб, які вчинили злочини,
передбачені статтями Розділу XVI КК України, протягом 2011–2020 рр.

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Засуджених	56	80	49	37	31	24	42	49	50	56
Вчинили злочин у складі групи	5	12	10	8	6	9	11	6	7	7
Питома вага (в %)	8,9	15,0	20,4	21,6	19,4%	37,5	26,2	12,2	14,0	12,5

Кіберполіція як структурний підрозділ Національної поліції України, була створена 5 жовтня 2015 року, а відомості про виявлені організовані групи та злочинні організації і вчинені ними кримінальні правопорушення, виявлені працівниками підрозділів кіберполіції, були введені у Звіт у 2016 році. У зв'язку з цим цей вид злочинності можна проаналізувати за 5 років.

Протягом 2016 – 2020 рр. було виявлено 38 організованих груп і жодної злочинної організації.

Динаміка виявлення організованих груп також є несталою. Так у 2016 році було виявлено 2 організовані групи. В подальшому, у 2017 році, позначилася тенденція щодо їх збільшення (у 3,5 рази порівняно з 2016 роком). Ця тенденція посилилася у 2018 році, оскільки було виявлено 11 організованих груп (на 57,1 % більше порівняно з 2017 р.), однак їх кількість у 2019 р, зменшилася у 2,8 рази до 4, у 2020 році різко зросла у 3,5 рази до 14 виявлених організованих груп.

Протягом 5 років було виявлено 8 організованих груп з міжрегіональними зв'язками: 2017 р. – 4, 2018 р. – 1, 2019 р. – 1, 2020 р. – 2.

Тривалість дії організованих груп у 65,8 % (25 ОГ) становила до одного року, до двох років – 23,7 % (9 ОГ), від 3-х до 6-ти років – 10,5 % (4 ОГ).

Виявленими кіберполіцією організованими групами вчинено у 2016 р. 77 кримінальних правопорушення, з них більшу частину складає шахрайство – 64 (83,1 %), у 2017 р. із 166 кримінальних правопорушення шахрайство складає 131 (78,9 %), у 2018 р. із 142 учинених кримінальних правопорушень шахрайство – 100 (70,4 %), у 2019 р. із 84 – шахрайство – 66 (78,6 %) і у 2020 р. питома вага шахрайств складає 56,3 % – 111 із 197.

Зменшення питомої ваги шахрайств із загальної кількості кримінальних правопорушень вчинених організованими групами, пов'язане з тим, що працівниками кіберполіції були виявлені кримінальні, правопорушення, які раніше не виявлялися ними, зокрема 18 крадіжок, 21 виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну з метою збуту або збут підроблених грошей, державних цінних паперів чи білетів державної лотереї.

Організованими групами вчинено 46 злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж у 2017 р. – 13, 2018 р. – 6, 2019 р. – 17 і у 2020 р. – 10.

Працівниками підрозділів кіберполіції протягом останніх 5 років було виявлено 138 осіб, які вчинили кримінальні правопорушення у складі організованих груп: у

2016 р. 8 (2 організатори, 6 виконавців), 2017 виявлено у 3,4 рази більше – 27 (7 організаторів, 20 виконавців), у 2018 р. кількість виявлених збільшилася до 41 особи (+ 51,9 %) (10 організаторів, 31 виконавець), у 2019 р. значне зниження у 3,4 рази до 12 (4 організатори, 8 виконавців) і значне збільшення у 4,2 рази до 50 (15 організаторів, 34 виконавців).

Висновки.

У вітчизняному законодавстві нині не існує чіткого визначення поняття кіберзлочин, дискутуються різні точки зору щодо класифікації кіберзлочинів, відсутній перелік "традиційних" злочинів, які можуть відноситися до категорії кіберзлочинів, а отже і відсутня офіційна статистична звітність щодо облікованих кіберзлочинів.

Зазначене негативно позначається на можливості запобігання цим злочинам, зумовлюючи труднощі у боротьбі з кіберзлочинністю.

Аналіз такої статистичної звітності надав би можливість проаналізувати динаміку цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів та розробляти на їхній основі організаційно-правові заходи для більш ефективної протидії кіберзлочинності на національному рівні [6; 7].

Використана література

1. The Future of Cybersecurity in 2021 and Beyond. URL: https://www.technewsworld.com/story/The-Future-of-Cybersecurity-in-2021-and-Beyond-87018.html April 15, 2021.

2. К вопросу о латентности киберпреступлений. URL: https://infourok.ru/statya-k-voprosu-latentnosti-kiberprestupleniy-1460496.htm (дата звернення: 07.11.2018).

3. Про основні засади забезпечення кібербезпеки України: Законі України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

5. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України" / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

6. Хахановський В.Г., Гавловський В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. № 2(33)/2020. С. 99-110.

7. Гавловський В.Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право*. № 2(30)/2019. С. 105-110.

8. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. № 1(28)/2019. С. 118-128.

9. Гриненко І., Прокоф'єва-Янчиленко Д., Прокофьєв М. Структура кримінальних відносин у кіберпросторі: наук.-техн. зб. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2013. Вип. 1. С. 27-33.

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

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

УДК 347.45/.47

ШАХБАЗЯН К.С., *кандидат юридичних наук*, учений секретар Центру досліджень інтелектуальної власності та трансферу технологій НАН України.
ORCID: https://orcid.org/0000-0002-2205-374X.

ДОГОВІРНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗБЕРЕЖЕННЯ РЕЗУЛЬТАТІВ НАУКОВИХ ДОСЛІДЖЕНЬ У КОНФІДЕНЦІЙНОСТІ ТА ВИКОРИСТАННЯ ТАКОЇ ІНФОРМАЦІЇ ПРИ ПРОВЕДЕННІ ДОСЛІДЖЕНЬ І РОЗРОБОК: ДОСВІД ЄС ТА КРАЇН СВІТУ

Анотація. *У статті аналізується категорія договорів у сфері проведення наукових досліджень – договори щодо нерозкриття інформації (договори зі збереження конфіденційності), надаються приклади таких договорів при проведенні досліджень з різними джерелами фінансування. Окремо розглянуто формулювання положень щодо конфіденційності в загальних угодах на проведення досліджень і розробок, порівнюється практика застосування в ЄС та країнах світу. Розглянуто вимоги щодо врегулювання питань охорони прав інтелектуальної власності саме в аспекті дотримання конфіденційності і розподілу прав на використання отриманої інформації та наданні прав доступу до такої інформації третім особа. Запропоновано аспекти, які слід включити до подібних видів договорів в Україні.*

Ключові слова: *договори у сфері проведення наукових досліджень та розробок, договори щодо нерозкриття інформації (договори зі збереження конфіденційності).*

Summary. *The article analyzes the category of agreements in the field of research and development – non-disclosure agreements (confidentiality agreements), provides examples of such agreements with different sources of funding; as well as there are being considered the wordings of confidentiality provisions in general agreements for research and development – the article compares the practice of application of these provisions in the EU and countries of the world. The requirements are considered for settling the issues of protection of intellectual property rights in the aspect of confidentiality and distribution of rights to use the information, obtained during the research in the project, use of such info during the further researches and granting access rights to such information to third parties. Aspects that should be included in similar types of agreements in Ukraine are proposed.*

Keywords: *contractual and legal regulation of intellectual property during scientific research, agreements in the field of research and development, agreements on non – disclosure of information (agreements on confidentiality).*

Аннотация. *В статье анализируется категория договоров в сфере проведения научных исследований – договора о нераскрытии информации (договора о сохранении конфиденциальности), предоставляются примеры таких договоров при проведении исследований с различными источниками фінанування, а также отдельно рассмотрены формулировки положений о конфиденциальности в общих соглашениях на проведение исследований и разработок, сравнивается практика применения в ЕС и других странах. Рассмотрены требования относительно урегулирования вопросов охраны прав интеллектуальной собственности именно в аспекте соблюдения конфиденциальности и распределения прав на пользование полученой информации при проведении исследований в проекте и предоставлении прав доступа к такой информации третьим лицам. Предложены аспекты, которые следует включить в подобные виды договоров в Украине.*

Ключевые слова: *договора в сфере проведения научных исследований и разработок, договора о нераскрытии информации (договора о сохранении конфиденциальности).*

Постановка проблеми. В цілому, міжнародна практика свідчить про загально-прийнятий підхід: в угодах з досліджень та розробок включено певні положення щодо конфіденційності – на рівні певних принципів щодо поводження з раніше створеною ІВ та результатами, а також – щодо їхньої публікації. В той же час, сторони угод ДР або члени консорціумів, зазвичай, укладають окремі угоди про конфіденційність (чи угоди про нерозголошення) ще на етапі ведення перемовин щодо участі в проекті.

В статті розглянуті підходи до формування положень конфіденційності в угодах на рівні ЄС (угоди Рамкових програм наукових досліджень та інновацій), модельних угодах країн ЄС (наукові фонди і міністерства Австрії, ФРН, політика відомства інтелектуальної власності (далі – ІВ) Великобританії – в угодах Ламберта), програми наукових досліджень, що фінансуються на державному рівні та збереження конфіденційності при співробітництві між університетами та промисловістю.

Результати аналізу наукових публікацій. Дослідження іноземної практики формування та застосування модельних договорів у сфері наукових досліджень та розробок, а також режиму конфіденційності в цих угодах, відбувається не досить активно. Загалом науковців цікавить або законодавче регулювання такої діяльності, або конкретні приклади таких угод, наприклад, угоди Ламберта (Капіца Ю.М. [1]), приклади угод країн СНД (Махновський Д.С. [2]). Є роботи, які стосуються комерційної таємниці і конфіденційної інформації в українському правовому просторі: Кравченко О.М. [3], Сляднєва Г.О. [4], Кодинець А.О. [5]), Стародуб І. [6], Кохан А. [7], Мельниченко А. [8], типи договорів про нерозголошення, обов'язкові елементи таких договорів [9]. Більшість досліджень знаходяться в площині економіки та формування державної правової політики в сфері НДДКР (Данилова І., Андрощук Г.О., Христинченко Н.П. [10] (організація наукової діяльності в США та Німеччині).

Метою статті є оцінка проблем з питань режиму конфіденційності в угодах держав-членів ЄС в цілому та на рівні окремих країн, а також надання пропозицій в контексті укладання угод між українськими партнерами та представниками ЄС.

Виклад основного матеріалу.

Умови участі в рамковій Програмі наукових досліджень та інновацій "Horizon Europe" Європейського Союзу (2021- 2027).

Умови участі в Програмі викладені в Регламенті (ЄС) 2021/695 Європейського Парламенту та Ради від 28 квітня 2021 р., який встановлює "правила участі та розповсюдження" [11]. У п. 78 Регламенту визначено необхідність дотримання умов збереження конфіденційної інформації (чутлива раніше створена інформація та класифіковані дані включно) від доступу неуповноваженими особами, згідно законодавства ЄС та держав-членів.

Згідно ст. 39 "Використання та поширення результатів" бенефіціари забезпечують застосування відкритого доступу до наукових публікацій згідно умов, викладених у грантовій угоді, зокрема, це стосується балансу дотримання прав інтелектуальної власності та вимог відкритого доступу, відповідно – забезпечення можливості винятків з умов відкритого доступу за принципом "якомога більш відкритий доступ, закриття доступу – за необхідністю", беручи до уваги легітимні інтереси бенефіціарів, включаючи комерційну експлуатацію та будь-які інші обмеження, такі як правила захисту даних, конфіденційність, комерційна таємниця.

Положення договорів програми "Горизонт Європа" стосовно умов конфіденційності [12]. Модельна Грантова Угода укладається між Єврокомісією та керівником проекту від імені всіх членів консорціму виконавців проекту. В нинішній Грантовій Угоді ст. 13 прісвячена "питанням конфіденційності та безпеки".

В статті 13 надано визначення терміну "чутлива інформація". Сторони повинні зберігати конфіденційність будь-яких даних, документів або інших матеріалів (у будь-якій формі), які ідентифіковані у письмовій формі як "чутлива інформація" під час реалізації проекту та принаймні до закінчення терміну, визначеного у Переліку даних проекту (див. пункт 6).

Якщо між сторонами не узгоджено інше, вони можуть використовувати конфіденційну інформацію лише для виконання Угоди по проекту. Бенефіціари можуть розкривати конфіденційну інформацію своєму персоналу або іншим учасникам, які беруть участь в проекті, лише у тому випадку, якщо вони: (a) повинні знати це з метою реалізації угоди та (b) зв'язані зобов'язаннями конфіденційності. Фінансуючий орган (Єврокомісія) може розкрити конфіденційну інформацію своїм співробітникам та іншим інституціям та органам ЄС. Крім того, він може розкривати конфіденційну інформацію третім особам, якщо: (a) необхідно впроваджувати угоду або захищати фінансові інтереси ЄС та (б) одержувач інформації зв'язаний обов'язком конфіденційності. Обов'язки щодо дотримання конфіденційності більше не застосовуються, якщо: (a) розкриваюча сторона погоджується звільнити від зобов'язань іншу сторону; (б) інформація стає загальнодоступною, без порушення будь-яких зобов'язань конфіденційності; (c) необхідно здійснити розкриття конфіденційної інформації, яка вимагається ЄС, міжнародним або національним законодавством. Спеціальні правила конфіденційності (якщо такі є) мають бути викладені у Додатку 5 до Угоди "спеціальні/окремі положення" (стор. 98 Модельної Грантової Угоди). Крім того, питання конфіденційності висвітлені в статтях: ст. 9. Субконтракти, ст. 15. Захист даних, ст. 25. Проведення перевірок, огляди та аудит, ст. 32. Закінчення дії Грантової угоди.

Положення договорів консорціуму, що використовуються в РП "Горизонт": Угоди консорціуму, офіційно визнані Єврокомісією як такі, що рекомендовані для укладання між бенефіціарами – спеціально для відповідних Рамкових програм з досліджень та інновацій ЄС, зокрема, Угода Консорціуму DESCA [13] (Development of a Simplified Consortium Agreement – Розробка спрощеної угоди консорціуму). Стосовно конфіденційності зазначено, що положення щодо конфіденційності мають ретроактивний характер, але бажано укласти окрему угоду, підписану на етапі підготовки проекту.

Продовження дії прав та обов'язків. Положення, що стосуються конфіденційності, продовжують бути чинними і після завершення або припинення дії Консорціуму.

Обмеження договірної відповідальності. Жодна сторона не несе відповідальності за будь-які прямі або непрямі втрати іншої сторони, для будь-яких збитків, таких як втрата прибутку, втрата доходів або втрата договорів, за умови, що така шкода не була викликана навмисним актом або шляхом порушення конфіденційності.

Сторони можуть забажати збільшити відповідальність щодо певних випадків. Це завжди слід розглядати у кожному випадку окремо і закріплювати в угоді консорціуму дуже чітко та визначено: наприклад, питання конкретної відповідальності за порушення умов дотримання конфіденційної інформації. Однак слід пам'ятати, що сторони угоди Консорціуму завжди можуть укласти двосторонні угоди щодо умов надання доступу до певної конфіденційної інформації.

Координатор забезпечить виконання угоди про нерозголошення між усіма сторонами та кожним членом Зовнішньої експертної ради проекту. Його умови не повинні бути менш жорсткими, ніж ті, що передбачаються у цьому договорі консорціуму.

Зобовязання по співпраці. Сторони зобов'язуються співпрацювати, щоб дозволити своєчасне подання, експертизу, публікацію та захист дисертації, що включає їх результати, або раніше створеної ІВ, що підлягає конфіденційності та публікації, узгоджених у цьому консорціумі.

Розділ "Права доступу". Всі запити на права доступу будуть здійснюватись у письмовій формі. Надання прав доступу може бути здійснене за умови наявності відповідних зобов'язань конфіденційності.

Права доступу до афілійованих об'єктів. Асоційовані зі сторонами Угоди суб'єкти, які отримують права доступу, виконують всі зобов'язання по дотриманню конфіденційності, згідно угоди Консорціуму або грантової угоди, так само, ніби такі афілійовані суб'єкти є сторонами угод.

Секція "Нерозголошення інформації". Вся інформація, незалежно від форми або режиму повідомлення, яка розкривається стороною ("розкриваюча сторона") будь-якій інший стороні ("одержувач") у зв'язку з проектом під час його реалізації має бути явно позначена як "конфіденційна".

Одержувачі інформації, додатково та без шкоди для будь-якого зобов'язання щодо нерозкриття інформації за грантовою угодою протягом 4 років після закінчення проекту зобов'язані: не використовувати конфіденційну інформацію з іншою метою, ніж та, задля якої її було розкрито; не розкривати конфіденційну інформацію без попередньої письмової згоди від розкриваючої сторони; забезпечити, щоб внутрішній розподіл конфіденційної інформації одержувача відбувався за умови суворої необхідності; забезпечити повернення такої інформації розкриваючій стороні або знищити її за згодою розкриваючої сторони. Одержувачі можуть зберігати копію тією мірою, якою це потрібно, архівувати або зберігати таку конфіденційну інформацію через дотримання чинних законів та нормативних актів або для підтвердження поточних зобов'язань, за умови, що одержувач дотримується зобов'язань щодо конфіденційності по відношенню до такої копії до тих пір, поки копія зберігається.

Потрібна згода власника конфіденційних даних, перш, ніж надати їх субпідрядникам/афілійованим установим, навіть якщо у них є роль у проекті. Одержувачі несуть відповідальність за виконання зазначених вище зобов'язань з боку своїх працівників або третіх сторін, залучених до проекту та забезпечують, щоб вони залишалися зобов'язаними дотримуватись вимог конфіденційності, наскільки це можливо, – під час та після закінчення проекту та/або після припинення договірних відносин з працівником або третьою стороною. Потрібна згода власника конфіденційної інформації, перш, ніж надати таку інформацію третім особам (наприклад, субпідрядники та філії).

Розглянемо особливості режиму конфіденційності в окремих державах-членах ЄС – ФРН, Австрії, а також у Великій Британії.

ФРН. Модельні угоди "Керівництва із співробітництва між науково-дослідними установами та промисловістю. Типові договори із співробітництва у сфері досліджень та розробок" (підготовлені Міністерством з питань економіки та енергетики ФРН) [14]. Угоди, які включено до Керівництва: контракт на проведення досліджень (варіант поширення результатів через ліцензію) та контракт на проведення досліджень (варіант поширення результатів через передачу прав), мають однакові статті щодо передачі конфіденційної інформації, зазначено умови використання патентної інформації (стосовно таких питань як надання кампанією прав університету користуватись

конфіденційною інформацією, а натомість, кампанія отримує право реєструвати патентні права на результати роботи університета); зазначено "нові права" – університет/науково-дослідна установа (далі – НДУ) не залучає треті сторони до проекту, допоки вони не будуть зв'язані зобов'язаннями зі збереження конфіденційності.

В статті "Конфіденційність" містяться умови: термін застосування укладеної раніше угоди про конфіденційність; зусилля щодо збереження конфіденційності іншої сторони; отримуюча сторона дотримується умов непоширення інформації третім сторонам та своїм співробітникам, допоки вони не укладуть відповідних угод. Перелічені випадки, коли вимоги зі збереження конфіденційності не застосовуються (інформація опинилась у публічному доступі, вже знаходилась в розпорядженні отримуючої сторони на законних підставах, отримана від третьої сторони на законних підставах і без зобов'язань зберігати конфіденційність, розроблена незалежно самою отримуючою стороною, тощо).

Угода про співпрацю у сфері ДР: загалом, умови щодо конфіденційності повторюються ті ж самі, що і в попередніх угодах, але більш розгалужені щодо опису нових прав: університет (дослідницька установа) утримується від залучення третіх осіб до отримання інформації по проекту, допоки вони не погодяться на дотримання зобов'язань згідно цієї угоди, а також сторони угоди на взаємній основі не погодяться зберігати конфіденційну інформацію одне одної. Також підкреслено, що на положення з конфіденційності не впливають такі види діяльності університета як дослідницька, викладацька та експериментальна конфіденційна інформація. Якщо університет плануватиме використоувати конфіденційну інформацію для подальшої наукової діяльності з комерційними або некомерційними партнерами в рамках теми данного проекту – це можливо лише за згоди промислових партнерів. Розділ "Конфіденційність" повністю співпадає з попередними угодами.

Додаток 3 до такого договору містить "Декларацію співробітника університету", в якій зазначено, що співробітник приєднується до угоди про співпрацю між університетом та компанією, а самое – до тих положень, що стосуються регламентації конфіденційності ноу-хау та до якої університет матиме доступ.

Співробітник отримує невиключне, неперадаване право використовувати результати своїх досліджень в науковій та викладацькій діяльності, але без порушення положень щодо дотримання вимог конфіденцийності. Співробітник також погоджується не публікувати результати роботи без згоди промислової сторони. Якщо співробітник є стороною будь-яких угод про нерозголошення інформації, це зазначається в "Декларації".

Австрія. Як приклад вдалої і досить детальної угоди щодо дотримання конфіденційності можливо навести Угоду з "Керівництва по угодах з питань ІВ" під егідою Міністерства економіки та цифровізації Австрії [15]), в якій запропоновано кілька варіантів формулювання положень статей, залежно від поточної ситуації. Розглянемо Угоду зі збереження конфіденційності (односторонню) між Університетом (науковою установою), що є Розкриваючою стороною, та компанією (Отримуюча сторона).

Деякі статті мають кілька варіантів формулювань, від найбільш узагальнених суджень до суто конкретних визначень. Так, у розділі "Визначення КІ" подано кілька формулювань: (а) будь-яка інформація, повідомлена Університетом компанії згідно даної угоди, або (б) будь-яка інформація, повідомлена Університетом компанії згідно даної угоди, яка вважається такою, що має конфіденційний характер згідно розумного ділового судження, або (в) яка має відповідну помітку на час її розкриття, або була чітко зазначена такою Розкриваючою стороною у письмовій формі протягом 30 днів з моменту її повідомлення, або (г) яка зазначена як конфіденційна, розголошується в

умовах конфіденційності, або вважається такою, що має конфіденційний характер згідно розумного ділового судження, включаючи інформацію, яку переглядає або дізнається Отримуюча Сторона під час відвідування приміщень Сторони, що розкриває інформацію. Всі торговельні секрети, згідно законодавства – конфіденційна інформація.

Досить детально і, знову ж таки, з декількома варіантами надані визначення афілійованих компаній, що також впливає на обсяг прав отримуючої сторони з поширення конфіденційної інформації серед своїх співробітників та пов'язаних компаній. Також надано визначення "Третьої Сторони".

В Преамбулі визначено "Мету" – співробітництво між сторонами згідно, наприклад, певного проекту, "Конфіденційну інформацію" – перераховується яка саме інформація розкриватиметься стороною; якщо в угоді перелічені кілька сторін, визначається механізм розкриття і передачі такої інформації між кількома сторонами проекту.

Розділ "Обмін інформацією до укладення контракту" визначає принцип, що умови даної угоди зі збереження конфіденційності в проекті поширюються і на інформацію, яку нададуть під час проведення перемовин у переддоговірний етап.

Розділ "Розкриття інформації афілійованим компаніям" – має кілька варіантів формулювання процедури, серед яких: (а) отримуюча сторона має право розкрити КІ одній із своїх афілійованих компаній лише після отримання попередньої згоди розкриваючої сторони і за умови, що афілійовані компанії дотримуватимуться зобов'язань даної угоди, або (б) так само, але афілійованим компаніям надано можливість також обмінюватись між собою конфіденційною інформацією. При цьому отримуюча сторона зобов'язана здіснювати контроль за дотриманням вимог цієї угоди задіяними афілійованими компаніями і не допускати будь-яких порушень умов конфіденційності.

Розкриття інформації своїм працівникам та третім сторонам: (а) дозволено тим працівникам, які повинні мати до неї доступ через необхідність роботи за проектом, або (б) дозволено Розкриваючій стороні надати своїм співробітникам доступ до конфіденційної інформації – для досягнення мети цієї угоди, при цьому співробітники мають бути зв'язані в свою чергу угодою про нерозкриття інформації. Отримуюча сторона терміново повідомляє Розкриваючу сторону щодо третьої сторони, якій була передана конфіденційна інформація.

Інформація, яка не є конфіденційною. Інформація не буде кваліфікуватись як конфіденційна за умови наявності певних умов (перераховані стандартні випадки – опинилась у публічному доступі, вже знаходилась в розпорядженні отримуючої сторони на законних підставах, отримана від третьої сторони на законних підставах і без зобов'язань зберігати конфіденційність, розроблена незалежно самою отримуючою стороною, (варіативно: отримана конфіденційна інформація підлягає розголошенню через судовий припис або нормативні вимоги).

Зобов'язання підтримувати конфіденційність підтримується через нерозголошення, непоширення, утримання від публікації, запобігання поширенню іншими, зберігати конфіденційність наданої інформації на такому ж рівні як і власну конфіденційну інформацію, використовуватиметься виключно з метою, зазначеною в Угоді.

Термін збереження конфіденційності – детально зазначено через який термін припиняється дія Угоди і на яких підставах (які саме мають бути дії сторін). Однак, зазначено, що всі положення цієї угоди стосовно зобов'язань конфіденційної інформації, яку було розкрито протягом дії цієї угоди, лишаються чинними після закінчення її дії протягом терміну – а саме, визначеної кількості років.

Крім того, в Угоді є Розділи стосовно умов повернення, знищення наданої інформації, умов виготовлення копій; неприйняття претензій щодо гарантій та відповідальності з боку третіх сторін стосовно розкритої конфіденційної інформації; принцип – через укладання даної угоди жодна зі сторін не підлягає зобов'язанням розкривати будь-яку спеціальну інформацію; юрисдикція, право яке застосовується – пропонується у випадку конфлікту юрисдикції – обирати юрисдикцію власноруч, альтернативний варіант: умови арбітражного вирішення суперечок або арбітраж та медіація – згідно умов Правил медіації ВОІВ та умов Правил арбітражу ВОІВ; принцип: передача конфіденційної інформації не надає отримуючій стороні жодних матеріальних прав та прав ІВ, прав на реєстрацію ІВ, принцип: отримуюча сторона, маючи результати використання Конфіденційної інформації, повідомляє про них Розкриваючу сторону та отримані результати належать виключно їй; умови поводження з персональними даними, переданими як конфіденційна інформація; принцип: всі права і кожне право, яке виникає згідно даної угоди, не повинно передаватись третій стороні без згоди відповідної іншої стороні проекту; умови внесення змін до угоди; закріплено принцип, що зміна, скасування, втрата чинності будь-яких положень цієї угоди не впливає на чинність інших положень угоди. положення, які втратили чинність, мають бути замінені на альтернативні.

Велика Британія. Загальні пояснення щодо використання угоди щодо дотримання конфіденційності на сайті відомства ІВ Великої Британії [16] включають певні моменти, на які варто звернути увагу: деякі Сторони угод про конфіденційність вважають, що вся раніше створена ІВ, яку вони надають для виконання спільного проекту – чутлива, а отже, має бути конфіденційною. Також, деякі учасники проектів вважають, що вся інформація, яку вони розкривають, має зберігатись як конфіденційна, альтернатива: конфіденційною є лише та інформація, щодо якої це чітко висловлено відкиваючою стороною, або цей статус слідує з її природи чи обставин її розкриття. Тож, рекомендовано, відкриваючи таку інформацію сторонам угоди чи іншим особам, завжди позначати її "Конфіденційно". Також цьому питанню слід приділити особливу увагу, визначаючи саме "раніше створена ІВ", адже конфіденційність найчастіше виникає саме в цьому аспекті поширення інформації. Тож, слід домовитись, чи буде вважатись конфіденційною вся "раніше створена ІВ" автоматично, чі тільки та "раніше створена ІВ", яка буде відповідним чином маркована в момент її розкриття чи до нього.

Положення конфіденційності в Угодах Ламберта [17].

Розділ "Раніше створена ІВ" (перелічено "раніше створену ІВ", яка належить науковій установі, і яка є конфіденційною, перелічено "раніше створену ІВ", яка належить іншій співпрацюючій стороні, і яка є конфіденційною).

Розділ "Конфіденційність та академічні публікації". Кожна сторона проекту зберігає в конфіденційності конфіденційну інформацію іншої сторони без обмежень у часі (або протягом зазначеного часу __ кількості років). Студенти та співробітники наукової установи будуть уповноважені публікувати в журналах та репозиторіях, повідомляти на конференціях Результати проекту та "раніше створену ІВ", яка належить іншій співпрацюючій стороні, згідно застережень, закріплених в угоді зі співпраці.

Розділ "Конфіденційність". Зміст угоди є конфіденційним для обох сторін. Жодна із сторін угоди ніколи/або протягом __ років після укладання цієї угоди не розкриє будь-якій особі будь-яку конфіденційну інформацію, яка стосується іншої стороні (можливо перерахувати), або інших членів групи кампаній, до яких належить інша Сторона угоди, за винятком, якщо це дозволено згідно певного пункту даного розділу:

Кожна сторона може розкрити конфіденційну інформацію іншої сторони лише якщо: це дозволено угодою про співробітництво, це необхідно для збереження отримання зовнішнього фінансування і з дотриманням всіх вимог конфіденційності та у необхідному обсязі, своїм співробітникам, представникам, офіційним особам, радникам – тобто, особам, яким необхідно її знати для ведення перемовин щодо цієї угоди або отримання зовнішнього фінансування, згідно вимог закону, судового припису тощо.

Жодна зі сторін не використовуватиме конфіденційну інформацію іншої сторони з іншою метою, ніж ведення переговорів, або якщо це дозволено запропонованою угодою про співробітництво, якщо сторони уклали її між собою.

Розділ "Юрисдикція та права третіх осіб". Хоча юрисдикція країни для розгляду суперечок визначена чітко (Велика Британія), але вибір юрисдикції для розгляду питань, що стосуються конфіденційності чи ІВ можливий на розсуд постраждалої сторони.

Угоди консорціуму (consortium agreement). Положення угод, що стосуються конфіденційності:

Розділ "Раніше створена ІВ"– перелічено раніше створену ІВ кожної зі сторін, яка є конфіденційною.

Розділ "Конфіденційність та академічні публікації". Кожна сторона проекту зберігає в конфіденційності конфіденційну інформацію іншої сторони без обмежень у часі (або протягом зазначеного часу __ кількості років) після її отримання згідно угоди консорціуму

Студенти та співробітники кожної наукової установи – сторони консорціуму будуть уповноважені публікувати в журналах та репозиторіях, повідомляти на конференціях Результати проекту та раніше створену ІВ, яка належить іншій співпрацюючій стороні, згідно застережень, закріплених в угоді консорціуму.

Розділ "Конфіденційність". Майже співпадає з угодою із співробітництва, але зазначено, що зміст угоди є конфіденційним для всіх сторін. До випадків можливого розкриття конф. інформації додано можливість "розкриття інформації будь-якій іншій стороні угоди з метою ведення переговорів".

Розділ "Юрисдикція та права третіх осіб" – той же самий принцип обрання юрисдикції, що і в попередній угоді.

Для порівняння візьмемо режим конфіденційності в угодах за участю відомих університетів Великої Британії, а саме приклад Оксфорду. Інтелектуальна власність в Оксфорді регламентується "Статутом № XVI: Майно, контракти та трасти", в якому викладені основні принципи поводження з ІВ, до створення якої має відношення Університет. Отже, Університет зазначає положення щодо конфіденційності в усіх модельних угодах, з розрахунку на основний принцип: він претендує на право власності на всю інтелектуальну власність, яка розроблена, виготовлена або створена особами, під час їх працевлаштування в університеті; студентами – за визначених обставин; іншими особами, які займаються навчанням або дослідженнями в Університеті, зокрема Стандартні угоди про проведення наукових досліджень (Standard Research Agreements) – ключові положення у стандартній угоді про дослідження. Конфіденційність – Угода визнає, що сторони можуть побажати розкрити приватну інформацію одна одній у зв'язку з проектом, і що необхідні механізми збереження конфіденційності такої інформації. Важливо зазначити, що ці положення не повинні поширюватися на публікацію результатів проекту, про які йдеться в окремому пункті угоди.

Угода університету про конфіденційність. У вищезазначених обставинах Університет рекомендує використовувати свою стандартну Угоду про конфіденційність, яка була

розроблена, щоб дозволити відкриті дискусії та обмін інформацією, захищаючи конфіденційну інформацію як Університету (та його дослідників), так і іншої сторони.

Висновки.

В міжнародній практиці у сфері договірно-правового регулювання НДДКР є два визнаних підходи щодо врегулювання питань дотримання конфіденційності: включення до загальних угод з досліджень та розробок певних положень щодо конфіденційності, або укладення сторонами – виконавцями наукових проектів або членами науково-дослідних консорціумів, окремих угод про конфіденційність (угод про нерозголошення). Найчастіше, такі угоди укладають ще на етапі ведення перемовин щодо участі в проекті.

Щодо структурних особливостей таких угод або відповідних положень загальних угод ДР, то, зазвичай, вони містять положення з наступних питань (на досліджених прикладах з практики укладання таких угод в ЄС, США, модельних угодах ВОІВ тощо):

- умови передачі та збереження нерозголошеною наданої стороною інформації
- чітко зазначені умови визначення\маркування інформації, яка отримує статус "конфіденційної"
- визначення певних принципів щодо поводження з раніше створеною ІВ, що належить іншій стороні (сторонам);
- принципи поводження з т.зв. результатами проекту (мається на увазі ІВ, створена в процесі проекту),
- якщо така інформація включає дані щодо патентоспроможних винаходів, детально зазначаються умови дотримання всіма сторонами проекту конфіденційності: терміни зберігання, умови припинення дотримання такого режиму, умови публікації таких матеріалів та повноваження щодо цього різних категорій суб'єктів
- умови публікації матеріалів, що можуть містити конфіденційну інформацію (звітів проекту, звітів наукової установи, які включатимуть конф. інформацію проекту, наукові публікації в журналах тощо)
- визначення кола осіб, які мають права доступу до такої інформації та режим користування нею, в залежності від особливостей статусу такої особи (сторони проекту, треті особи, афілійовані зі сторонами проекту особи, умови визначення таких осіб та умови надання їм доступу до конфіденційної інформації)
- умови розкриття такої інформації державним, судовим органам, органам дізнання, тощо
- випадки, при яких надана конфіденційна інформація втрачає свій статус
- терміни збереження режиму конфіденційної інформації
- визначення юрисдикції (права країни, яке застосовується) при розгляді суперечок щодо конфіденційності
- умови поводження з персональними даними, переданими як конфіденційна інформація

Ці питання більш детально викладені в модельних угодах про нерозголошення в окремих країнах ЄС, США (університети пропонують майже завжди власну модельну угоду). В Грантовій угоді та угодах консорціуму Рамкової програми досліджень та інновацій ЄС визначені далеко не всі вищезазначені аспекти, і вони менш деталізовані. В Регламенті із запровадження Рамкової програми до конфіденційної інформації включено "чутливу інформацію та класифіковані дані" мають бути збережені від доступу не уповноваженими особами – згідно законодавства ЄС та держав-членів. Для загальної політики щодо результатів наукових досліджень на рівні ЄС характерним є дотримання відкритого доступу до них за принципом "якомога більш відкритий доступ, закриття доступу – лише за жорсткою необхідністю", беручи до уваги невеликий перелік обмежень

(легітимні інтереси бенефіціарів, включаючи дотримання конфіденційності та комерційної таємниці. Відповідно, в Грантовій угоді та інших угодах для РП основній акцент здійснено саме на відкритості інформації щодо результатів проектів, умови з конфіденційності пропонується закріплювати в окремих угодах про нерозголошення за необхідності.

В модельних угодах з досліджень та розробок країн ЄС розглядаються ті ж самі аспекти, що і в угодах РП ЄС, але з деякими особливостями, характерними для співпраці науковиих установ з компаніями: наприклад, в модельній угоді ФРН про співпрацю у сфері ДР: зазначено, чи впливають на положення з конфіденційності такі види діяльності ВНЗ як викладацька, експериментальна, дослідницька. Зазначено, яким чином зберігатиметься режим конфіденційності (якщо взагалі зберігатиметься), якщо університет запланував подальшу роботу з матеріалами поточного проекту (подальша наукова діяльність з комерційними і некомерційними партнерами в рамках теми) – яким чином на це має надаватись згода промислового партнера проекту (якщо це буде визнано прийнятним в межах такого партнерства). Іноді промислові партнери вимагають від університету укласти із своїми співробитниками "Декларацію", де зазначено, що вони приєднуються до угоди між своїм університетом та компанією в тій частині, яка стосується дотримання вимог конфіденційності.

В Австрії (керівництво з ІВ Міністерства економіки), Данії (Модельні угоди Міносвіти) пропонується цікавий підхід, коли в угоді з конфіденційності пропонується кілька варіантів формулювання однієї тієї ж статті з різним ступенем деталізації положень і відповідною зміною обсягу і ступеню захисту конфіденційної інформації. Характерним є закріплення кількох принципів в таких угодах: всі права, які виникають згідно угоди, не повинні передаватись третій стороні без згоди іншої сторони; при внесенні будь-яких змін до угоди, скасуванні чі втраті чинності якихось положень, інші положення лишаються чинними (особливо це стосується положень щодо конфіденційності); принцип, що передача конфіденційної інформації не надає отримуючій стороні жодних матеріальних прав та прав на ОПІВ. В Угодах Ламберта з'являється цікавий принцип про можливість розкриття конфіденційної інформації для отримання зовнішнього додаткового фінансування.

Державні дослідницькі організації та їхні промислові партнери часто мають конфлікти щодо прав на публікації результатів досліджень та вимог щодо дотримання конфіденційності. Зокрема, це стосується випадків, коли промисловий партнер намагається завадити/затримати публікацію результатів проекту до того, як буде подано патентну заявку. Також, підприємство може вимагати довготермінового відтермінування публікації, якщо обере інший спосіб захисту ІВ, ніж патентування, через збереження в секретності (ноу-хау, комерційна таємниця – коли результати проекту не є патентоспроможними, але на ринку додаватимуть перевагу у конкурентоздатності, якщо будуть збережені у конфіденційності). Здатність промислового партнера вимагати довготривалої секретності від наукової установи залежить від типу проекту – чи це угоди про спільне проведення досліджень чи контракт на замовлення проведення досліджень. В першому випадку промисловий партнер не здатен наголошувати на довготривалій конфіденційності, а у другому випадку, якщо наукова установа була повністю профінансована промисловим партнером, то він може наполягати на постійному дотриманні конфіденційності.

Отже, в роботі з міжнародними партнерами українській стороні слід враховувати наступні особливості:

- у міжсекторальній співпраці різницю між національними системами доведеться враховувати при вирішенні того, як найкраще вирішувати питання конфіденційності та публікації. Визначний фактор цього питання є (згідно національної системи) – які джерела фінансування, тобто фінансування державне чи від бізнес-структур;

- загальний принцип, що якщо промисловий партнер хоче більшого контролю над публікацією та конфіденційності своїх результатів, він повинен збільшити свій внесок у роботу за проектом, включаючи оплату роботи НДУ. Це має також відповідати будь-яким юридичним вимогам до НДУ для публікації результатів;

- суттєва проблема полягає в тому, щоб визначити можливу потребу щодо дотримання короткострокової або довгострокової конфіденційності проекту, а також погодити умови цієї конфіденційності в угоді про співпрацю. Сторони повинні розглянути питання, чи інформація повинна бути конфіденційною на невизначений термін;

- хоча може виникнути конфлікт між короткостроковою або довгостроковою потребою в конфіденційності та необхідності НДУ або дослідника опублікувати результати, експертна група не вважала, що це забезпечило бар'єр для транскордонного співробітництва, який можна буде подолати завдяки: кращому розумінню кожною Стороною потреб іншої сторони і завдяки розробці національних керівних принципів; надання практичних національних або європейських керівних принципів і прикладів того, як вирішувати таку проблему у договорах ДР.

Використана література

1. Капіца Ю.М. Підходи до розподілу прав інтелектуальної власності у договорах з проведення досліджень та розробок між університетами, науковими установами та підприємствами в державах-членах ЄС та України: матеріали науково-практичної конференції *Створення, охорона, захист і комерціалізація об'єктів права інтелектуальної власності*, м. Київ, 26 квіт. 2019 р. Київ, НТУ "КПІ імені Ігоря Сікорського". С. 14-19.

2. Махновський Д.С. Підходи до розподілу прав інтелектуальної власності у договорах на виконання НДДКР у нових незалежних державах: матеріали науково-практичної конференції *Створення, охорона, захист і комерціалізація об'єктів права інтелектуальної власності*, м. Київ, 26 квіт. 2019 р. Київ, НТУ "КПІ імені Ігоря Сікорського". С. 100-103.

3. Кравченко О.М. Адміністративно-правові засади охорони комерційної таємниці в Україні. – (Кваліфікаційна наукова робота на здобуття ступеню кандидата наук). Київ, 2019. URL: http://ippi.org.ua/sites/default/files/kravchenko_o.m._disertaciya_.pdf

4. Сляднєва Г.О. Правове регулювання передачі комерційної таємниці в договірних відносинах. *Університетські наукові записки*. 2005. № 3(15). С. 163-169. URL: http://old.univer.km.ua/visnyk/819.pdf

5. Кодинець А.О. Договір про конфіденцінйність: істотні умови та особливості регулювання. *Право і суспільство*. 2018. № 2. С. 72-77.

6. Стародуб І. Угода про конфіденційність. Хто підписує? *Юридична газета он-лайн*: URL: https://yur-gazeta.com/dumka-eksperta/ugoda-pro-konfidenciynist-hto-pidpisue.html

7. Кохан А. Угода про конфіденційність (NDA): як це працює та чи працює в Україні? *Юрист та Закон*. URL: https://uz.ligazakon.ua/ua/magazine_article/EA012622

8. Мельниченко А. Навіщо укладати угоду про конфіденційність? URL: https://bargen.com.ua/2020/12/14/navishcho-ukladati-ugodu-pro-konfidencijnist

9. Яновський Г. Договори про конфіденційність, нерозголошення, NDA. URL: https://zkg.ua/dohovory-pro-konfidentsijnist-nerozholoshennya-nda

10. Христинченко Н.П. Міжнародний досвід організації наукової діяльності на прикладі США та Німеччини. *Наше право*. 2014. № 6. С. 17-21.

11. Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri =CELEX:32021R0695

12. General Model Grant Agreement of the Horizon Europe Programme (HORIZON)& EURATOM Research and Training Program (Multi&Mono). URL: https://ec.europa.eu/info/funding-tenders/opp ortunities/docs/2021-2027/common/agr-contr/general-mga_horizon-eurat om_en.pdf

13. DESCA Consortium Agreement. URL: https://www.desca-agreement.eu/fileadmin/user_upl oad/Desca/DESCA2020_v1.2_March_2016_with_elucidations.pdf

14. Federal Ministry of Economics and Technology (BWMi), Sample Agreements for research and development cooperation - Guidelines for cooperation between the academics sector and industry, second edition, April 2010. URL: https://www.bmwi.de/Redaktion/EN/Publikationen/sample-agreem ents-for-research-and-development-cooperation.html (03.2019)

15. Intellectual property Agreement Guide (IPAG) Model Contracts. URL: https://www.ipag. at/en/model-contracts

16. UK IP Office -Non-disclosure agreements - GOV.UK. URL: //www.gov.uk

17. GOV.UK. Guidance on University and business collaboration agreements: model heads of terms agreements. URL: https://www.gov.uk/government/publications/university-and-business-colla boration-agreements-model-heads-of-terms-agreements

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

УДК 342.9(004.9)+34.096

УСЕНКО Я.О., начальник відділу з питань персоналу управління з організаційного забезпечення Апеляційної палати апарату Вищого антикорупційного суду України.
ORCID: https://orcid.org/0000-0003-1438-1337.
КОСТЕНКО О.В., *доктор філософії (Ph.D.) з юридичних наук*, завідувач наукової лабораторії теорії цифрової трансформації і права наукового центру цифрової трансформації і права ДНУ ІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-2131-0281.

ПРАВОВЕ РЕГУЛЮВАННЯ УПРАВЛІННЯ ПЕРСОНАЛОМ В СУДОВІЙ СИСТЕМІ

Анотація. *У статті розглянуто проблеми організаційно-правового регулювання процедур кадрового забезпечення та організації діяльності судів всіх спеціалізацій із урахуванням курсу України на цифровізацію державних послуг. Запропоновано розробити сучасну модель управління персоналом в судах різних спеціалізацій з урахуванням трансформації суспільних відносин із застосуванням сучасних інформаційно-комунікаційних технологій.*

Ключові слова: *судова система, персонал, управління персоналом, кадрове забезпечення, суд.*

Summary. *The article considers the problems of organizational and legal regulation of staffing procedures and organization of courts of all specializations, taking into account the course of Ukraine on the digitalization of public services. It is proposed to develop a modern model of personnel management in courts of different specializations, taking into account the transformation of public relations with the use of modern information and communication technologies.*

Keywords: *judicial system, staff, personnel management, staffing, court.*

Аннотация. *В статье рассмотрены проблемы организационно-правового регулирования процедур кадрового обеспечения и организации деятельности судов всех специализаций с учетом курса Украины на цифровизацию государственных услуг. Предложено разработать современную модель управления персоналом в судах разных специализаций с учетом трансформации общественного отношения с применением современных информационно-коммуникационных технологий.*

Ключевые слова: *судебная система, персонал, управление персоналом, кадровое обеспечение, суд.*

Постановка проблеми. На сьогодні судова система, як частина державного апарату з високим ступенем незалежності та неупередженості, зазнає суттєвої трансформації. Цей процес характеризується не тільки модернізацією системи судоустрою та законодавства, що регулює суддівську діяльність, а й формуванням нових більш інформаційно та технологічно сучасних підходів управління персоналом. Зміни в організації кадрового забезпечення та організації діяльності судів всіх спеціалізацій здійснюються із урахуванням напряму держави на максимальну цифровізацію державних послуг.

Зокрема, від того, наскільки вміло підібрано склад апарату суду, наскільки він компетентний у професійному відношенні та раціонально реалізує наявний кадровий потенціал судових установ, залежить стабільність і ефективність функціонування всієї системи правосуддя Української держави.

Для стабільного економічного розвитку держави важливе значення має підвищення якості формування та використання людських ресурсів на всіх рівнях управління.

Головною метою кадрової політики в судах є стратегічне бачення підбору, формування, професійного розвитку та раціонального використання кадрів. У сучасних умовах вирішення кадрових питань є однією з найактуальніших проблем державного будівництва в Україні, визначальним аспектом формування та функціонування судової влади. Тому, особлива роль інституту правосуддя у забезпеченні ефективного функціонування держави і суспільства визначає потребу дослідження організаційно-правових засад управління персоналом в органах судової влади та сьогодні є досить актуальною.

Метою статті є визначення сучасних напрямів формування правового регулювання управління персоналом в межах спеціалізованих судів із застосуванням сучасних практик та інформаційно-комунікаційних технологій.

Виклад основних положень. Проблематика управління персоналом в органах судової влади досліджувалася українськими науковцями В. Авер'яновою, А. Безнасюком, В. Бринцевим, С. Гайдученком, Ю. Гончаруком, О. Зарудіною, В. Кривенком, О. Сорочаном, Ю. Стрижаком, В. Маляренком, М. Мельником, Х. Рустамовим, І. Хахудою та іншими. Разом з тим аналіз досліджень свідчить про те, що проблема правового регулювання управління персоналом в межах спеціалізованих судів не має достатнього комплексного висвітлення.

Основною метою управління людськими ресурсами в органах судової влади має бути поєднання ефективного навчання та підвищення кваліфікації персоналу із широким застосуванням сучасних інформаційно-комунікаційних технологій. Персонал – це важливий елемент системи управління суду. У статті 152 Закону України "Про судоустрій і статус суддів" зазначено, що організаційне забезпечення роботи суду здійснює його апарат, який очолює керівник апарату. Керівник апарату суду несе персональну відповідальність за належне організаційне забезпечення роботи суду, суддів та судового процесу, функціонування автоматизованої системи документообігу, інформує збори суддів про свою діяльність [1].

Обсяг повноважень і обов'язків працівників апарату суду врегульовано низкою нормативно-правових актів, насамперед Законом України "Про судоустрій і статус суддів", актами Державної судової адміністрації України та профільними нормативними актами. Крім того, діяльність окремих категорій працівників суду (секретар судового засідання, судовий розпорядник суду) регулюється нормами процесуального права.

З прийняттям Закону України "Про судоустрій і статус суддів" до повноваженнь голови суду входить контроль ефективності діяльності апарату суду. Контроль – це вид управлінської діяльності, завданням якої є кількісна і якісна оцінка й облік результатів роботи організації. Виділяють два напрями контролю: контроль для оцінки отриманого результату; контроль для вжиття заходів з коригування істотних відхилень від плану або коригування самого плану [2].

Структура і штатна чисельність апарату Вищого антикорупційного суду (далі – ВАКС) затверджуються Державною судовою адміністрацією України за погодженням із Головою ВАКС. Правовий статус працівників апарату суду визначається Законом України "Про державну службу". Умови оплати праці, матеріально-побутового, медичного, санаторно-курортного і транспортного забезпечення працівників апарату суду визначаються на засадах, встановлених для відповідної категорії працівників апаратів центральних та місцевих органів виконавчої влади.

Для кадрового та фінансового обслуговування до апарату суду прикріплюються помічники суддів. Правовий статус та умови діяльності помічників суддів визначаються Законом України "Про судоустрій і статус суддів" і Положенням про помічника судді

(Рішення Ради суддів України від 18.05.18 р. № 21). Нині на помічників суддів також поширюється дія Закону України “Про державну службу”.

Діяльність ВАКС забезпечується наявністю чіткої організаційної структури суду, а також визначенням компетенцій, умов та порядку діяльності підрозділів і посадових осіб.

Організаційна структура суду є елементом механізму діяльності суду. Забезпечення діяльності суду охоплює сукупність організаційно-розпорядчих та технічних дій по проходженню судових справ.

Апарат суду очолює керівник апарату, який відповідно до наданих повноважень здійснює безпосереднє керівництво апаратом суду, забезпечує організацію роботи структурних підрозділів суду, працівників апарату суду, їх взаємодію у виконанні завдань, покладених на апарат суду. Керівнику апарату суду безпосередньо підпорядковані його заступник та керівники структурних підрозділів апарату суду.

Складовими системи управління персоналом ВАКС є: вивчення, аналіз і планування потреб у персоналі (внутрішнє середовище, зовнішнє середовище, аналіз праці), підбір персоналу (рекрутинг, адаптація нових працівників), управління показниками роботи персоналу (професійні компетентності, оцінка і покращення показників роботи), управління винагородами персоналу (система оплати й фінансового стимулювання), навчання і розвиток персоналу (організаційне вдосконалення, індивідуальне навчання, розвиток керівництва, управління кар’єрою), підтримка персоналу (дотримання прав працівників, створення умов праці, піклування про безпеку і здоров’я працівників, адаптація нових працівників). Головні складові системи управління розглянемо детальніше.

Так, однією важливою складовою у системі управління персоналом ВАКС є застосування компетенційного підходу. Керівництво ВАКС розробляє вимоги до професійної компетентності посад державних службовців як один з пріоритетних напрямів підвищення об’єктивності процесів відбору державних службовців. Сутність компетенційного підходу до управління людськими ресурсами полягає в застосуванні критеріїв компетентності в управлінні людськими ресурсами, які сприятимуть досягненню відповідного рівня роботи, а також забезпечать продуктивне функціонування організації в цілому.

Управління персоналом ВАКС – це складний, багатосторонній та специфічний процес, який охоплює не тільки функції, що традиційно пов’язують з кадровою роботою, а й знання, навички, вміння та здібності, за допомогою яких судові управлінці моделюють принципи ставлення та поведінки персоналу, якими відзначається високоефективний суд. Управління людськими ресурсами в суді є особливим видом діяльності, яке потребує спеціальних функцій і наявності особливих якостей в управлінців, які займаються цією діяльністю. Управління людьми зумовлює наявність творчого підходу, індивідуалізації та врахування довгострокової перспективи при прийнятті рішень.

Внутрішню основу, а отже, і сутність управління персоналом становлять управлінські відносини, які формують систему управління, забезпечують взаємодію працівників та успішне розв’язання можливих конфліктів між ними в організаційному середовищі. Ступінь розв’язання суперечностей є основним показником ефективності здійснення управління персоналом. Тому в суді необхідно створити таку систему управління персоналом, що забезпечить оптимальне балансування організаційної поведінки працівників підрозділів та дасть можливість знайти організаційний порядок, який підтримуватиме організаційне середовище управління.

Фактично необхідно сформувати сучасну модель управління персоналом в судах різних спеціалізацій з урахуванням трансформації суспільних відносин із застосуванням

сучасних інформаційно-комунікаційних технологій. Така модель на нашу думку може складатися із наступних модулів:

- практичні та теоретичні основи управління персоналом на сучасному етапі;
- констеляція нормативно-правових актів в сфері управління персоналом суду;
- класифікація суб'єктів в сфері управління персоналом суду;
- концепція політики формування персоналу;
- інформаційно-комунікаційні технології та ресурси суду.

Практичні та теоретичні основи управління персоналом на сучасному етапі повинні охоплювати правовідносини у сфері управління персоналом не тільки в сфері права, але й соціологію, конфліктологію, менеджмент, маркетинг тощо.

Питання констеляції нормативно-правових актів в сфері управління персоналом суду повинно включати в себе класифікацію нормативно-правових актів з управління персоналом, а саме: спеціалізовані, локальні та індивідуальні акти законодавства щодо управління персоналом.

Також потребують оновлення або перегляду питання суб'єктності в сфері управління персоналом в судах, класифікація, коло обов'язків та функціональних завдань, порядок делегування і розмежування повноважень суб'єктів, що здійснюють управління персоналом.

Таким чином, створення Концепції кадрової політики доцільно здійснювати спираючись на міжнародно-правовий досвід управління персоналом (американська, японська, європейська та бразильська моделі), організації, підбору, адаптації, оцінювання, атестації, підвищення кваліфікації, навчання й розвитку персоналу [3].

Окрему і більш детальну увагу слід приділити застосуванню сучасних інформаційно-комунікаційних технологій, що забезпечують та підтримують інформаційні процеси (збір, накопичення, обробка та інтерпретація обробки даних та високу швидкість одержувати доступ до інформаційних ресурсів), у процесі роботи і можливості суду.

Цифровізація України торкнулась і судової діяльності. У липні 2019 року Президентом України видано Указ № 558/2019, яким передбачено заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг [4]. Також розроблено Концепцію побудови Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), а на її основі створення "Електронного суду" [5]. Останню редакцію Концепції побудови Єдиної судової інформаційно-телекомунікаційної системи затверджено наказом ДСАУ від 07.11.19 р. № 1096. До Електронного суду були приєднані Касаційний адміністративний і Касаційний господарський суди у складі Верховного Суду. З 01.06.20 р. підсистему переведено в дослідну експлуатацію на підставі наказу ДСАУ "Про запровадження в дослідну експлуатацію підсистем "Електронний суд" та "Електронний кабінет" від 01.06.20 р. № 247. Постановою Кабінету Міністрів України від 17.07.19 р. № 650 та Постановою Кабінету Міністрів України від 02.12.20 р. № 1556-р "Про утворення робочої групи щодо рекодифікації (оновлення) цивільного законодавства України" передбачено початок робіт зі створення та використання технологій штучного інтелекту у сфері юриспруденції та здійсненні правосуддя [6; 7]. Вищою радою правосуддя погоджено проект розпорядження Кабміну щодо реалізації Концепції розвитку штучного інтелекту в Україні та запропоновано пілотний проект із застосування штучного інтелекту на базі одного із судів першої інстанції в частині розгляду адміністративних правопорушень [8; 9]. Крім того, Міністерством юстиції України впроваджено проект "Касандра" – програмне забезпечення з елементами штучного інтелекту, яке аналізує можливість повторного порушення закону злочинцем [10; 11].

В судовій системі доцільно переглянути низку нормативно-правових актів, що стосуються впровадження інформаційно-комунікаційних технологій, а також необхідно розробити нові, якими визначити поняття інформації, яка відноситься до сфери управління персоналом. Необхідно розробити Положення про інформаційну політику ВАКС та відповідні документи для організації захисту персональних даних. Здійснити порівняльний аналіз та підбір спеціалізованих програмних продуктів для спеціалістів по роботі з персоналом юридичного профілю та порівняльну характеристику автоматизованих робочих місць фахівців з управління персоналом. Також підготувати нормативні документи якими впорядкувати процедури застосування кваліфікованих електронних підписів та порядок дій у разі їх компрометації. Доцільно розробити правову регламентацію використання комп'ютерного поліграфу під час прийняття на роботу, відеофіксації процесу роботи персоналу, проведення конкурсів на заміщення вакантних посад тощо.

Зважаючи на багатовекторність запропонованої моделі управління персоналом в судах різних спеціалізацій, завдання з її реалізації доцільно покласти на керівника апарату суду. Сьогодні кваліфіковані працівники – це пріоритетний ресурс, тому його дефіцит може ослабити потенціал суду, що призведе до негативних наслідків. Слід звернути увагу на те, що крім вказаних вище пунктів слід вивчити можливість автоматизації процесів оцінки та атестації кадрів, що застосовується в судах в тій чи іншій модифікації. Це сприятиме підвищенню професійної складової складу кадрового потенціалу судів, вдосконалення індивідуальних фахових здібностей працівників.

Питання оцінки ефективності управління відділом є актуальним зокрема на державній службі, де переважає консервативний підхід до такої оцінки, а іноді – формальний. Як відомо, ступінь самовіддачі працівника прямо пропорційний матеріальній зацікавленості. У судах невисока, але постійна заробітна плата, тому необхідно максимально зацікавити працівника і надати йому можливість реалізувати себе у всіх дозволених законодавством напрямах: науковій, творчій, викладацькій діяльності. При цьому левова частка часу витрачатиметься на виконання службових обов'язків, а вищезазначені напрями діяльності сприятимуть розвиткові особистості. Робота в суді передбачає матеріальне мотивування діяльності фахівця, зокрема виплату премій, надбавок, присвоєння позачергового рангу тощо. При цьому керівникові відділу в разі матеріального заохочення працівника потрібно враховувати два основних критерії: результативність і компетентність.

У сучасних умовах розвитку ринку праці, підвищення вимог до компетенції працівників апарату суду, демографічного старіння робочої сили, недосвідченості молодих кадрів, внаслідок чого їх компетентність не відповідає сучасним вимогам, розвитку наявних і розробці нових технологій, що потребує нових знань та вмінь працівників. Кадрові процеси повинні базуватись на оновленій моделі судового адміністрування, стратегіях розвитку судів, що враховують короткострокові і середньострокові прогнози потреби в кадрах. Подальше успішне реформування системи кадрового управління в судах може бути успішним лише в тому разі, якщо воно буде реалізовуватись комплексно із застосуванням комунікативних технологій.

Здійснюючи стратегічне планування кадрової роботи, важливо: визначити реальну потребу в кадрах за етапами стратегічного періоду, встановити наявність кадрів у розрізі якісних параметрів та можливі прогнозовані їх зміни в стратегічному періоді, виявити нестачу кадрів в аспекті їх якісних параметрів за етапами стратегічного періоду, у тому числі з урахуванням потреби в нових фахівцях відповідно до передбачуваних

стратегічних змін в організації, визначити джерела покриття дефіциту кадрів за роками стратегічного періоду і в аспекті якісно-кваліфікаційних груп.

З метою оптимізації управління в суді важливо враховувати особистий чинник установи, що впливає на роботу суду загалом, а також особистий потенціал окремо взятого працівника. Останній віддзеркалює психологічні, управлінські, інноваційні чинники праці.

Установлення відповідності структури кадрової служби вимогам сьогодення та чинного законодавства, визначення основних напрямів їх гармонізації, виокремлення соціально-психологічних чинників є істотним кроком на шляху підвищення ефективності кадрової системи в судових органах.

Значна роль у підготовці висококваліфікованих кадрів для судової системи України належить Національній школі суддів України, яка була створена 21 грудня 2010 року на базі Академії суддів України.

Відповідно до Закону України "Про судоустрій і статус суддів" Національна школа суддів України є державною установою із спеціальним статусом, що забезпечує підготовку висококваліфікованих кадрів для судової системи та здійснює науково-дослідницьку діяльність.

Національна школа суддів здійснює: спеціальну підготовку кандидатів на посаду судді; підготовку суддів, які призначені на посаду судді вперше; яких обрано на посаду безстроково; яких призначено на адміністративні посади в судах; періодичне навчання суддів з метою підвищення рівня кваліфікації; підготовку працівників апаратів судів та підвищення їх кваліфікації; вивчення міжнародного досвіду організації діяльності судів; науково-методичне забезпечення діяльності судів загальної юрисдикції, Вищої кваліфікаційної комісії суддів України та Вищої ради юстиції.

Різнобічний розвиток особистості працівника судової системи неможливий без постійної, свідомої, наполегливої праці фахівця над собою. Самоосвіта, самовиховання, саморозвиток та самовдосконалення – це глибоко особисті процеси, а їх результати – неодмінна умова і найважливіший чинник набуття та зростання рівня професійної компетентності упродовж кар'єри.

Варто зазначити, що сучасна система підвищення кваліфікації працівників судів, незважаючи на певні досягнення, є недостатньо ефективною та не в повній мірі задовольняє потреби органів судової влади у високопрофесійних кадрах. Основними її проблемами є недосконаліть нормативно-правової бази та невідповідність ресурсного забезпечення її функціонування, відсутність ефективного механізму вивчення якісних і кількісних навчальних потреб, забезпечення актуалізації і практичної спрямованості змісту підвищення кваліфікації на основі компетенційного підходу, а також контролю та оцінки якості навчання.

Мотивація працівників є однією з провідних функцій управління, оскільки досягнення основної мети залежить від злагодженості роботи людей у колективі. Для керівництва суду персонал є найбільш цінним ресурсом, адже саме персонал може постійно вдосконалюватися. Уміло керуючи персоналом, можна постійно вдосконалювати організацію роботи суду [12]. Мотивація діяльності є одним з головних методів управління персоналом, які спонукають працівників на досягнення цілей. Наразі є потреба в осучасненні наявних методів мотивації персоналу, що має ґрунтуватися на потребах людей і не обмежуватися тільки змінами в оплаті праці.

Планомірне та обґрунтоване формування кадрового потенціалу суду дозволить вирішувати такі завдання: установлення співвідношення чисельності працівників з різними професійно-кваліфікаційними характеристиками для досягнення максимальної

відповідності між структурами робіт, робочих місць і персоналом; забезпечення оптимального ступеня завантаження працівників для повного використання їх особистого потенціалу та підвищення ефективності їх праці; оптимізація структури працівників із різним функціональним змістом праці.

Підсумовуючи вищевикладене, слід відзначити, що сьогодні система формування кадрового потенціалу судів, незважаючи на певні досягнення, є недостатньо ефективною та не в достатною мірі задовольняє потреби органів судової влади у високопрофесійних кадрах. Основними її проблемами є недосконаліть нормативно-правової бази та невідповідність ресурсного забезпечення її функціонуванню, відсутність ефективного механізму вивчення якісних і кількісних навчальних потреб, забезпечення актуалізації і практичної спрямованості змісту підвищення кваліфікації на основі компетенційного підходу, а також контролю та оцінки якості навчання, недостатність рівня насиченості сучасними уніфікованими цифровими технологіями, комп'ютерами, програмним забезпеченням тощо.

Висновки.

Стрижень будь-якої організації – персонал, який в ній працює. Система управління персоналом дуже різнобічна та багатоманітна. Вона вміщує в себе всі аспекти взаємодії працівників з організацією. Управління персоналом організації є цілеспрямованою діяльністю керівного складу організації, керівників і спеціалістів підрозділів системи управління персоналом.

Управління персоналом суду – це складний, багатосторонній та специфічний процес. Компетенція щодо управління людськими ресурсами в судах охоплює не тільки функції, що традиційно пов'язують з кадровою роботою, а й знання, навички, вміння та здібності, за допомогою яких судові управлінці моделюють принципи ставлення і поведінки персоналу, якими відрізняється високоефективний суд, а також сучасні інформаційно-комунікаційні технології. Управління людськими ресурсами в суді є особливим видом діяльності, що потребує спеціальних функцій і наявності особливих якостей в управлінців, які займаються цією діяльністю.

Судові установи мають особливості, що впливають на формування їх систем управління персоналом, тому доцільно створити модель управління персоналом в судах різних спеціалізацій, а на її основі розробити організаційні, правові та технічні заходи модернізації та осучаснення процесів управління персоналом.

Використана література

1. Про судоустрій і статус суддів: Закон України від 02.06.16 р. № 1402-VIII. Дата оновлення: 16.06.2021. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text (дата звернення: 03.07.2021).

2. Веснин В.Р. Управление персоналом. Теория и практика. Москва: Проспект, 2009. 239 с.

3. Єрьоменко В.В., Кононенко В.А., Швець Н.М. Правове регулювання управління персоналом: навч.-метод. матеріали. Харків: НЮУ, 2019. 57 с.

4. Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг: Указ Президента України від 29.07.19 р. № 558/2019. URL: https://www.president.gov.ua/documents/5582019-28853

5. Концепція побудови Єдиної судової інформаційно-телекомунікаційної системи Ради суддів України: рішення від 22.11.19 р. № 97. URL: https://zakon.rada.gov.ua/rada/show/v0097414-19#n9 (дата звернення: 05.07.2021).

6. Про утворення робочої групи щодо рекодифікації (оновлення) цивільного законодавства України: Постанова Кабінету Міністрів України від 17.07.19 р. № 650. URL: https://zakon.rada.gov.ua/laws/show/650-2019-%D0%BF#Text (дата звернення: 03.02.2021).

7. Концепція оновлення Цивільного кодексу України. Київ: ТОВ “Видавничий дім “АртЕк”, 2020. 128 с.

8. В українських судах використовуватимуть штучний інтелект: громадська медіа-платформа ТМЦІНФО. URL: https://tmcinfo.com.ua/publications/2021/02/14/v-ukrajinskyh-sudah-vykorystovuvatymut-shtuchnyj-inte (дата звернення: 03.07.2021).

9. Шишка Н.В. Штучний інтелект в українському правосудді: правові передумови запровадження. *Юридичний науковий електронний журнал*. 2021. № 3. С. 143-145. URL: http://lsej.org.ua/3_2021/37.pdf

10. Дмитро Шаповал. Які проблеми може вирішити штучний інтелект в Україні. *Юридична газета*. URL: https://yur-gazeta.com/dumka-eksperta/yaki-problemi-mozhe-virishiti-shtuchniy-intelekt-v-ukrayini.html.

11. Костенко О.В. Правова відповідальність та ідентифікація суб’єктів і об’єктів зі штучним інтелектом (IoT). *Юридичний науковий електронний журнал*. 2020. № 1. URL: http://lsej.org.ua/1_2020/39.pdf.

12. Колот А.М. Мотивація персоналу: підручник. Київ: КНЕУ, 2002. 337 с.

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

УДК 351.751

НИЖНИК А.І., аспірант ДНУ ІБП НАПрН України.

СУЧАСНІ ТЕНДЕНЦІЇ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ТА ІННОВАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ В УКРАЇНІ

Анотація. *У статті на основі європейських цінностей сучасного парламентаризму та стандартів електронної демократії окреслено тенденції у вітчизняній парламентській практиці, що не сприяють посиленню інституційної спроможності Верховної Ради України в контексті удосконалення організаційно-правового механізму парламентського контролю.*

Ключові слова: *традиційна представницька демократія, парламентська коаліція, парламентська опозиція, електронний парламент, електронна демократія.*

Summary. *This article outlines main trends in domestic parliamentary practice that do not strengthen the institutional capacity of the Verkhovna Rada in the context of improving the organizational and legal mechanism of parliamentary control. Such tendencies are emphasized in comparison with European values and standards of e-democracy.*

Keywords: *traditional representative democracy, parliamentary coalition, parliamentary opposition, e-parliament, e-democracy.*

Аннотация. *В статье на основе европейских ценностей современного парламентаризма и стандартов электронной демократии описываются тенденции в отечественной парламентской практике, которые не способствуют усилению институциональной способности Верховного Совета Украины в контексте усовершенствования организационно-правового механизма парламентского контроля.*

Ключевые слова: *традиционная представительская демократия, парламентская коалиция, парламентская оппозиция, электронный парламент, электронная демократия.*

Постановка проблеми. Сучасні трансформаційні процеси українського суспільства зумовлені загальносвітовими процесами епохи інформатизації, розвитку цифрової економіки та ІТ-сфери. Ці процеси закономірно впливають на розвиток та модернізацію суспільно-політичної системи держави.

Історично сформовані та конституйовані традиційні форми демократії (безпосередня та опосередкована) розвиваються з урахуванням темпів формування інформаційного суспільства. За допомогою використання сучасних інформаційно-комунікаційних і цифрових технологій (далі – ІКТ) модернізується управлінська діяльність у публічному секторі, а також способи реалізації традиційних форм демократії. У результаті успішного впровадження ІКТ на локальному (державному) та регіональному (Європейський Союз) рівнях, за задумом творців, має сформуватися якісно нове суспільно-політичне явище, що отримало назву “е-демократія”.

Складовою е-демократії є також і е-парламент, який уже впроваджено в Європейському Парламенті та деяких національних парламентах. Парламентська практика в Україні відрізняється тривалими “експериментами” з впровадження е-парламенту та інституалізації парламентської опозиції, що об’єктивно гальмують прогресивний процес розвитку парламентаризму та парламентського контролю.

Метою статті є визначення поточного стану реалізації задекларованих політичних цілей з імплементації європейських цінностей та стандартів щодо гарантій і прав

парламентської опозиції в контексті посилення ефективності парламентського контролю на основі функціонування е-парламенту.

Виклад основного матеріалу. У тридцятирічному державотворчому процесі новітньої України мали місце події, які були спрямовані на еволюційний розвиток вітчизняного парламентаризму. Йдеться, зокрема, про наміри політичної еліти уникнути надмірної концентрації влади в руках однієї особи – глави держави, шляхом конституювання Верховною Радою України у 2004 році парламентсько-урядової коаліційної моделі організації влади та закріплення змішаної парламентсько-президентської форми правління. Власне, це квінтесенція ідеологічного аспекту конституційно-правового романтизму, що мав удосконалити механізм стримувань і противаг та забезпечити сталий розвиток на основі обраної моделі консенсусної демократії.

На основі цієї владної моделі вітчизняна політична еліта мала навчитися належним чином забезпечувати парламентсько-урядову коаліційну співпрацю, зважаючи на досвід європейських країн, у яких організаційно-правові механізми спрямовані на забезпечення партнерства та паритетний діалог. Період "олігархічного парламентаризму" та авторитарних тенденцій, що мали місце у 2010 – 2014 роках, продемонстрував розрив між бажаними конституційно визначеними змінами і суспільно-політичною реальністю та переконливо довів переваги парламентсько-урядової коаліційної моделі організації влади. Йдеться про суперечність між конституційно вираженим демократичним ладом і реальною практикою управління, яка поєднує як демократичні, так і авторитарні тенденції. Натомість проблему відповідності фактичного стану організації публічної влади ідеальній моделі демократичного устрою (закріплена Основним Законом України) автором цієї публікації винесено за межі цього дослідження.

З усіма існуючими недоліками цієї владної моделі українське суспільство живе і нині, а політична еліта намагається їх "компенсувати" шляхом ініціювання фрагментарних змін до Конституції України та демонстрації бурхливої діяльності з проведення так званої "парламентської реформи". Задекларована при цьому амбітна мета – підвищення інституційної спроможності Верховної Ради України, досягається шляхом пріоритетного впровадження е-парламенту, яка на фоні відсутності законодавчо унормованого механізму реалізації гарантій і прав парламентської опозиції виглядає у правовій державі дещо штучним способом прискорення розвитку парламентських демократичних засад функціонування законодавчого органу та посилення дієвості парламентського контролю.

Зроблені упродовж останніх семи років (станом на 1 липня 2021 року) законодавчі кроки з реалізації парламентської реформи залишають актуальною, зокрема проблему гармонійного поєднання щодо втілення у парламентську дійсність Процедурних керівних принципів щодо прав та обов'язків опозиції в демократичному парламенті (Резолюція ПАРЄ 1601 (2008)) та стандартів е-демократії як таких, що мали б сприяти інтеграції України в Європейський Союз і НАТО.

Як вбачається із Копенгагенських критеріїв членства в ЄС, майбутні держави-кандидати, які мають на меті вступ до ЄС, повинні гарантувати демократію та верховенство права, політичний плюралізм, свободу слова.

У контексті цієї статті варто нагадати, що, приєднавшись у 1995 році до Ради Європи, Україна визнала базові європейські цінності, а у рамках реалізації Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Україна має забезпечити комплексний розвиток е-урядування відповідно до європейських вимог (загальновизнаної системи демократичних цінностей). Успішне запровадження

е-урядування є базовою передумовою для розбудови в Україні цифрової економіки та формування цифрового ринку, подальшої інтеграції до єдиного цифрового ринку ЄС.

Як відомо, в Основному Законі України втілено базові цінності європейської спільноти. До цінностей європейської цивілізації належить, зокрема, демократія, яка виражається у відповідних формах здійснення народовладдя (безпосередня та представницька демократія). На сучасному етапі суспільного розвитку представницька демократія з усіма її недоліками є найпоширенішою у світі моделлю участі громадян в управлінні державою.

Таким чином, сучасна представницька демократія забезпечує право людини на участь в управлінні державними справами, яке гарантоване статтею 21 Загальної декларації прав людини [1], статтею 25 Міжнародного пакту про громадянські та політичні права [2] та статтею 38 Основного Закону України [3].

Хоча питання розвитку парламентаризму в Україні автором винесено за межі цієї публікації, проте за нинішніх українських реалій видається актуальним бачення Р. Мартинюка, що парламентаризм характеризує стабільні періоди розвитку державності. Водночас він є важливою гарантією збереження демократії. Парламентаризм – це "привілей" для країн із розвиненим, політично структурованим громадянським суспільством, заможним середнім класом і розвиненою партійною системою. Повноцінний парламентаризм утверджується лише за наявності сильних центристських партій та міцних традицій демократії, які, зокрема, мають знайти своє вираження у здатності партій до співробітництва. Парламентаризм є неможливим у політично неструктурованому суспільстві, де несформована відповідна партійна система, яка б забезпечувала створення стабільної парламентської більшості, і яка б, у свою чергу, формувала уряд, спроможний ефективно розв'язувати комплекс завдань, пов'язаних із необхідністю здійснення системних перетворень у суспільстві та державі [4].

Наразі розвитку українського парламентаризму не сприяє триваюча російська агресія, що спрямована на порушення суверенітету та територіальної цілісності України.

Попри агресивні плани та дії з боку російського політичного і військового керівництва Верховною Радою України восьмого скликання, яка є виразником волі Українського народу (єдиного джерела влади відповідно до статті 5 Конституції України), зроблено у напрямку євроатлантичної інтеграції такі фундаментальні кроки:

1) ратифіковано Угоду про Асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (Закон України від 16.09.14 р. № 1678-VII);

2) закріплено в Конституції України незворотність цивілізаційного вибору на євроатлантичний курс (Закон України від 07.02.19 р. № 2680-VIII), чим підтверджено прагнення українського суспільства до європейського та євроатлантичного членства;

3) задекларовано суспільну потребу в проведенні парламентської реформи, що мала стати основою для еволюційного розвитку парламентаризму та е-демократії.

Зокрема, про визнання суспільної потреби у проведенні парламентської реформи свідчить факт схвалення 17 березня 2016 року українським парламентом рекомендацій Місії Європейського Парламенту як основи для внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України [5]. Проте у політичному середовищі згадані рекомендації чомусь ототожнюються з парламентською реформою, що є підміною не лише понять, а й природи самих явищ, однак це окрема тема для дискусії.

Оскільки в зазначених рекомендаціях передбачено заходи, спрямовані на посилення ефективності парламентського контролю, в тому числі й шляхом впровадження е-парламенту (пункт 23), та законодавчого забезпечення гарантій і прав

парламентської опозиції (пункт 44), автор пропонує зосередитися на аналізі процесу їх реалізації у контексті дотримання відповідних європейських цінностей та стандартів.

Маємо констатувати, що станом на 1 липня 2021 року обидві ці рекомендації є актуальними. Більше того, у самому процесі їх реалізації вбачаються різновекторні тенденції імплементації законодавцем відповідних європейських цінностей і стандартів.

Аргументами на підтвердження цієї тези є факти з парламентської практики, що демонструють існування об'єктивних суперечностей між задекларованими цілями (посилення парламентського контролю шляхом законодавчого врегулювання гарантій і прав парламентської опозиції та впровадження е-парламенту) та способами їх досягнення.

Щодо процесу законодавчого забезпечення гарантій і прав парламентської опозиції.

Міжпарламентський Союз наголосив, що нові демократичні країни можуть виграти від закріплення прав парламентської опозиції в конституційних нормах та/або парламентських процедурах [6]. У зв'язку з цим варто нагадати, що упродовж 2006-2010 років в умовах існування в Україні парламентсько-урядової коаліційної моделі організації влади питання функціонування парламентської опозиції були унормовані положеннями глави 13 Регламенту Верховної Ради України [7], а після прийняття 8 жовтня 2010 року Закону України № 2600-VI [8] – ці питання, починаючи з 16 жовтня 2010 року і по нинішній час (станом на 1 липня 2021 року), залишаються законодавчо неврегульованими.

Отже, маємо констатувати існування проблемної ситуації, що виникла внаслідок законодавчої деінституалізації парламентської опозиції.

Ці обставини спонукали автора цієї роботи окреслити теоретико-прикладний аспект демократичних цінностей парламентського буття, що мають базисний характер для впровадження е-парламенту.

Досліджуючи практики парламентів європейських країн з усталеними демократичними традиціями, Шаранич С.С. зазначає, що утвердження конституційного статусу та ваги Верховної Ради України в системі стримувань і противаг залежить від успішності утворення таких усталених у зарубіжній конституційній практиці структур у представницькому органі, як парламентська більшість та парламентська опозиція [9].

Якщо розглядати парламент як ціле з точки зору діалектики парних категорій "ціле і частина", то його частинами є парламентська більшість і парламентська меншість, які у процесі взаємодії виконують свою соціальну роль з використанням відповідних форм і методів, що властиві органам представницької демократії. В умовах функціонування парламентсько-урядової коаліційної моделі організації влади парними категоріями є відповідно парламентська коаліція та парламентська опозиція. Без інституалізації останньої як політико-правового явища в умовах функціонування такої моделі організації влади сучасний парламент не може вважатися цілісним повноцінним утворенням. Ці міркування ілюструють у дещо спрощеному вигляді системо-утворююче призначення відповідних політико-правових явищ (як частин цілого), що є інституційними елементами демократичного парламентського устрою. У сенсі цієї статті принциповою відмінністю від інших парламентських систем є те, що в умовах функціонування парламентсько-урядової коаліційної моделі організації влади місія суб'єкта парламентського контролю належить парламентській опозиції. Саме вона в процесі внутрішньопарламентського діалогу є конструктивним опонентом парламентської коаліції.

Проведений автором порівняльний аналіз термінології, використаної у тексті Конституції України, унеможливлює використання понять "парламентська більшість" та "коаліція депутатських фракцій", "парламентська меншість" та "парламентська опозиція"

як синонімічних конструкцій, оскільки вони не характеризують тотожні політико-правові явища, що за конституційною логікою утворюються на основі депутатських фракцій (провладних та опозиційних).

У тексті Конституції України згадуються зазначені політико-правові явища, за винятком парламентської опозиції. Таким чином, якщо чисельність опозиційної фракції становитиме менше ніж 150 народних депутатів, то вона не зможе скористатися такими гарантованими для парламентської меншості інструментами парламентського контролю, як ініціювання питання про відповідальність Уряду та створення тимчасової слідчої комісії (статті 87 і 89 Конституції України).

У цій статті категорії "парламентська меншість" та "парламентська опозиція" розглядаються як інституціалізовані в європейській практиці політико-правові явища, що виконують контрольну місію щодо владної більшості (парламентської коаліції).

Саме таке соціальне призначення парламентської опозиції як невід'ємної частини забезпечення демократичного процесу випливає з Резолюції 1601 (2008) Парламентської асамблеї Ради Європи [10]. Зокрема, у пункті 3 цієї Резолюції зазначено, що одна з головних функцій опозиції – це можливість запропонувати надійну політичну альтернативу до більшості, що є при владі, в наданні на суспільний розгляд інших політичних варіантів. Шляхом контролю та критики роботи уряду при владі, постійної оцінки дій уряду та притягнення уряду до звітності, опозиція працює для забезпечення прозорості державних рішень і ефективності в управлінні державними справами, забезпечуючи таким чином захист державного інтересу і запобігаючи зловживанню та неправильному управлінню.

У Резолюції також викладені Керівні принципи щодо прав та обов'язків опозиції у демократичному парламенті. Зокрема, пункт 2.3.1 передбачає, що члени опозиції мають право брати участь в керівництві парламентської діяльності; вони повинні мати доступ до посад заступників голови та інших відповідальних посад в парламенті; склад керівних органів парламенту має бути відповідним до принципу пропорційного представництва і відображати політичний склад парламенту/палати. Згідно з пунктом 2.5.1 головування у постійних комітетах повинно надаватись парламентським фракціям на основі пропорційного представництва; щонайменше один постійний комітет має бути очолений членом опозиції; головування у комітетах, що здійснюють контроль за діями уряду, як, наприклад, комітет з бюджетних та фінансових питань, комітет з питань аудиту, або комітет, що здійснює нагляд за державною безпекою та розвідувальними службами – мають надаватися членам опозиції.

Політична опозиція в парламенті повинна показати політичну зрілість і повинна здійснюватись як відповідальна і конструктивна опозиція шляхом виявлення взаємної поваги та використовувати свої права з метою підсилення ефективності парламенту в цілому (пункт 5 Керівних принципів).

Цього переліку цілком достатньо для оцінки фактів вітчизняної парламентської дійсності, що свідчать про відхилення від зазначених Керівних принципів, які є універсальною ціннісною основою для організації та здійснення парламентського процесу на демократичних засадах, в тому числі в частині парламентського контролю. Натомість процес затягування інституалізації парламентської опозиції унеможливлює реалізацію її суспільного призначення як частини цілісного парламентського організму, а сам парламентський процес віддаляється від цивілізаційних засад парламентської демократії – основи сучасного парламентського контролю.

З огляду на наведений у Резолюції обсяг та характер прав і обов'язків парламентської опозиції застосування структурно-функціонального методу дозволило

автору дійти висновку, що парламентська коаліція та парламентська опозиція є інституційними елементами організаційно-правового механізму парламентського контролю в умовах функціонування парламентсько-урядової коаліційної моделі організації влади. Сама логіка функціонування коаліційної моделі зумовлює її реалізацію через демократичний механізм узгодження політичних рішень, що убезпечує від домінування однієї політичної сили та гарантує демократичний розвиток країни.

Так, у пункті 23 Звіту Венеціанської комісії "Про роль опозиції в демократичному парламенті" від 15 – 16 жовтня 2010 року [11] зазначено, що правові і фактичні умови мирної парламентської опозиції є еталоном для оцінки демократичної зрілості будь-якої політичної системи.

Зважаючи на існуючий обсяг і характер конституційних повноважень Голови Верховної Ради України (зокрема, згідно з пунктом 1 частини другої статті 88 Конституції спікер головує на засіданнях парламенту), саме він зобов'язаний відповідно до вимог частини другої статті 19 Конституції України та положень Регламенту Верховної Ради України забезпечувати додержання гарантій і прав парламентської опозиції, а один з його заступників (обраний на цю посаду за гарантованою опозиційною квотою) має вимагати від головуючого їх дотримання. Ці авторські міркування ґрунтуються на усвідомленні ролі Голови Верховної Ради України як "незалежного спікера" щодо забезпечення конструктивних та консенсусних діалогових механізмів, що випливають з Процедурних керівних принципів щодо прав та обов'язків опозиції в демократичному парламенті [10].

Проте факт відсутності законодавчого врегулювання гарантій і прав парламентської опозиції, зважаючи на вимоги статей 8, 9, 19, 88 Конституції України, позбавляє Голову Верховної Ради України (чи головуючого на засіданні) як посадову особу органу законодавчої влади законних способів забезпечення реалізації відповідних гарантій і прав представниками парламентської опозиції в обсязі, гарантованому цивілізованими стандартами внутрішньої парламентської демократії.

З іншого боку, з позиції формально-юридичної логіки автор вважає, що відсутність нормативно визначеної процедури легалізації парламентської опозиції унеможливлює ідентифікацію її представника як опозиційного парламентарія. За відсутності ж легалізованої в установленому порядку парламентської опозиції не можуть виникати правовідносини між коаліцією депутатських фракцій та парламентською опозицією, що є необхідною умовою для здійснення легітимного парламентського контролю з боку парламентської опозиції.

Інституційне закріплення в українському парламенті керівного органу у вигляді колегіальної президії Верховної Ради України відповідає не лише вітчизняній традиції, а й конституційній європейській практиці.

Постійно діюча колегіальна президія у складі Голови та його заступників, що обирається Верховною Радою на підставі положень статті 88 Конституції України, демократизує процес управління парламентом, оскільки в її управлінській природі поєднуються цільовий, діяльнісний та особистісний підходи. При цьому місія одного із заступників Голови Верховної Ради України (представника опозиції) щодо здійснення реального внутрішнього парламентського контролю також випливає з Керівних принципів щодо прав та обов'язків опозиції в демократичному парламенті [10].

Процес затягування інституалізації парламентської опозиції унеможливлює реалізацію її суспільного призначення як частини цілісного парламентського організму, а сам парламентський процес віддаляється від цивілізаційних засад парламентської демократії – основи сучасного парламентського контролю.

Моделюючи за існуючої політичної системи вітчизняний організаційно-правовий механізм забезпечення реалізації гарантій і прав парламентської опозиції з урахуванням досвіду європейських країн, парламентарії мали б спиратися на рекомендації, що містяться у згаданій Резолюції ПАРЄ. Саме такий законодавчий підхід може забезпечити системний розвиток як внутрішнього, так і зовнішнього парламентського контролю в умовах функціонування парламентсько-урядової коаліційної моделі організації влади.

Щодо поточного стану впровадження в Україні е-парламенту та меж "електронізації" роботи Верховної Ради України.

Поява Меморандуму [12], Комунікаційної стратегії Верховної Ради України [13] і Стратегії електронного парламентаризму [14] є свідченням усвідомлення керівництвом Верховної Ради України восьмого скликання та керівництвом парламентського апарату необхідності планомірного впровадження сучасних ІКТ у його роботі.

Натомість парламентська більшість Верховної Ради України дев'ятого скликання, перебуваючи в полоні ідеї тотальної цифровізації у всіх сферах життєдіяльності, попри недостатнє ресурсне забезпечення (зокрема, фінансово-матеріальне) 16 січня 2020 року прийняла рішення про невідкладне впровадження е-парламенту [15]. Проте вже через півроку та ж сама парламентська більшість визнала свою помилку у спробі "стрибкоподібного" впровадження е-парламенту і 13 липня 2020 року відтермінувала перехід на електронний режим роботи парламентської установи до дня відкриття п'ятої сесії [16], а 26 січня 2021 року – до дня відкриття сьомої сесії Верховної Ради України дев'ятого скликання [17].

Отже, ця проблемна ситуація виникла внаслідок поспішного політичного рішення про невідкладне впровадження е-парламенту (без відповідного підготовчого та перехідного періодів, об'єктивно необхідних для перевірки роботи єдиної автоматизованої системи в тестовому та дослідному режимі експлуатації).

За таких обставин, а саме: створення суспільної ілюзії першочергового впровадження е-парламенту (надання переваги технічному компоненту) та одночасно ігнорування суспільної необхідності в законодавчому забезпеченні гарантій і прав парламентської опозиції (правил для базисного компоненту), маємо констатувати відсутність відповідних організаційно-правових передумов для посилення інституційної спроможності Верховної Ради України в контексті створення ефективної та дієвої системи парламентського контролю. Відтак, законодавчий акт, що унормує гарантії та права парламентської опозиції, мав би набрати чинності до дня відкриття сьомої сесії Верховної Ради України дев'ятого скликання.

Окремою проблемою, що пов'язана з невдалою законодавчою спробою "стрибкоподібного" впровадження е-парламенту, є питання забезпечення інформаційної безпеки в контексті належного забезпечення захисту парламентської інформації з обмеженим доступом, що поряд з позитивними зрушеннями у напрямку формування е-демократії можуть мати й інші непередбачувані наслідки, у тому числі через латентні ризики, що пов'язані з триваючою агресією з боку Російської Федерації проти України.

Аби усвідомити як співвідносяться базисний[1] та технічний компоненти так званого "е-парламенту", автор цього дослідження на основі загальнофілософського підходу виходить з припущення, що роль технологій в е-демократії не є визначальною, оскільки їх обсяг та якість не зумовлюють, а лише забезпечують якість демократичного процесу.

[1] Під базисним компонентом розглядається цивілізований парламентський процес (де-факто), що здійснюється на засадах парламентської демократії, описаних у Резолюції 1601 (2008) Парламентської асамблеї Ради Європи [10].

Це судження стосується також модернізації парламентських процесів шляхом впровадження в Україні е-парламенту.

Розглядаючи е-демократію як форму політичної комунікації, Е.О. Войнова зазначає: "До складових електронної демократії можна віднести е-парламент, е-законодавство, е-суд, е-посередництво, е-вибори, е-референдум, е-голосування, е-петиції, е-кампанії, е-опитування тощо" [18].

Як же співвідносяться у науково-теоретичному та прикладному сенсі такі соціально-політичні явища: е-демократія, е-урядування та е-парламент?

Ми вважаємо, що, з точки зору філософських категорій, зазначені суспільні явища у науковому сенсі можуть розглядатися відповідно як загальне (е-демократія), особливе (е-урядування) та одиничне (е-парламент). Це твердження випливає з характерних властивостей цих явищ.

Так, у відповідних урядових концепціях містяться визначення е-демократії [19] та е-урядування [20].

Електронний парламент (E-parliament), як складова більш широкого поняття електронного урядування (E-government), є системою електронної взаємодії учасників парламентських процесів між собою, а також з іншими державними органами, бізнес-структурами, громадянами, зарубіжними та міждержавними утвореннями [21]. Це наукове видання, на думку автора цієї публікації, мало б стати фундаментальною основою для вироблення відповідного технічного завдання щодо поетапного впровадження е-парламенту з урахуванням європейських стандартів, проте парламентська практика свідчить про обрання іншого підходу – невідкладної "електронізації" роботи Верховної Ради України.

Отже, е-парламент як технічний компонент представляє собою сучасний програмний комплекс, що забезпечує роботу парламентської установи в умовах становлення е-демократії.

Спробуємо на основі європейських стандартів навести деякі характерні ознаки е-демократії, що відрізняють її від форм традиційної демократії.

Як відомо, в Рекомендаціях Комітету міністрів Ради Європи щодо е-урядування окреслено сучасний термінологічний апарат, основні критерії політики е-демократії, принципи, напрямки та інструменти е-демократії. Зокрема, "е-демократія – це використання ІКТ в демократичних процесах, яке дозволяє: (1) посилити участь, ініціативність та залучення громадян на національному, регіональному та місцевому рівнях публічного життя; (2) покращити прозорість демократичного процесу прийняття рішень, а також підзвітність демократичних інститутів; (3) покращити чутливість/ зворотну реакцію органів влади на звернення громадян; (4) сприянню публічним дебатам та увагу громадян до процесу прийняття рішень. ІКТ повинні удосконалювати доступ та комунікацію з чиновниками та обраними політиками. *Електронні засоби голосування на виборах та референдумах повинні доповнювати неелектронні традиційні способи*" [22].

У контексті ж цієї статті варто зробити наголос на таких принципах е-демократії:

"Е-демократія спирається на демократичні, гуманістичні, соціальні, етичні та культурні цінності суспільства, в якому вона запроваджується.

Е-демократія повинна бути сумісна та пов'язана із традиційними процесами демократії. *Кожен процес демократії (електронний чи традиційний) відіграє свою роль і не може застосовуватись як універсальний*" [23].

Отже, у згаданих рекомендаціях принципово розрізняються обидва процеси демократії – традиційний (безпосередній політичний діалог і волевиявлення) та електронний (дистанційний політичний діалог та волевиявлення). У зв'язку з цим варто

виділити ті найсуттєвіші характеристики, що відрізняють обидва демократичні процеси, та окреслити межі застосування ІКТ в роботі Верховної Ради України з огляду на відповідні положення Конституції України.

На відміну від традиційного процесу представницької демократії, який відбувається шляхом безпосереднього діалогу парламентаріїв та відкритого ухвалення ними рішень у залі засідань адміністративного будинку парламенту, електронний процес прямої демократії відбувається дистанційно шляхом таємного голосування виборця (е-вибори, референдум) чи е-опитування. Інакше кажучи, гарантований Основним Законом України принцип народовладдя та спосіб його реалізації (традиційний чи електронний) через закріплені форми прямої й опосередкованої демократії визначається законодавчо, і насамперед з урахуванням вимог, передбачених статтею 19 Конституції України. Порівняно з частиною першою цієї статті, згідно з якою "ніхто не може бути примушений робити те, що не передбачено законодавством", і тому процедури та альтернативні способи (традиційний – на виборчій дільниці чи дистанційний – електронний) здійснення виборцем свого політичного права регулюються законом, частина друга цієї ж статті містить принципово іншу засадничу вимогу щодо організації діяльності органів публічної влади та їх посадових осіб. Відтак, Верховна Рада України, її посадові особи та народні депутати зобов'язані керуватися насамперед вимогами Конституції України, відповідними положеннями якої визначено організаційно-правові та процедурні засади роботи парламенту, а головне – спосіб здійснення народним обранцем свого волевиявлення під час прийняття рішення парламентом.

Оскільки основними елементами традиційного парламентського процесу є безпосередня участь парламентарія в обговоренні питання порядку денного та його особисте (відкрите) голосування у залі засідань адміністративного будинку парламенту, порушення цих правил під час ухвалення рішення має визнаватися порушенням конституційної процедури (стаття 152 Конституції України). Хоча ці процедури є похідними від самої природи представницької демократії, проте саме вони окреслюють існуючі конституційно-правові межі використання інформаційно-комунікаційних та цифрових технологій у діяльності Верховної Ради України.

Зважаючи на форс-мажорні обставини, пов'язані з поширенням пандемії коронавірусної хвороби CoVID-19, виникає питання – чи можна повністю перейти на роботу парламенту в режимі віддаленого доступу без порушення конституційної процедури?

У стратегії електронного парламентаризму на 2018 – 2020 роки зазначено: "сучасні електронні технології дають змогу повністю перевести законодавчий процес у цифровий формат, починаючи з отримання урядових чи депутатських законопроектів в електронній формі і закінчуючи направленням електронної версії ухваленого закону на підпис Президенту" [14].

Наведене твердження не викликає сумніву, що суто з технічної точки зору, сучасні засоби е-парламенту здатні забезпечити роботу законодавчого органу та парламентаріїв у режимі віддаленого доступу (наприклад, дискусію під час засідання парламенту, комітету, тимчасової комісії, голосування за закон чи інший парламентський акт в електронній формі тощо). Однак, оскільки відповідними конституційними положеннями закріплено процедуру та спосіб волевиявлення (діалог та особисте голосування за рішення безпосередньо у залі засідань адміністративного будинку парламенту) як засади організації традиційної представницької демократії, то з формально-юридичної точки зору вони консервують можливість дистанційного обговорення та прийняття закону чи іншого парламентського акта в електронній формі. Крім того, з концепцією традиційної представницької демократії пов'язані також процедури підписання, оприлюднення та

опублікування закону в паперовій формі через друковані засоби масової інформації, проте ці питання винесені за межі цієї статті.

Таким чином, на основі сукупності наведених фактів, висловлених міркувань та суджень можемо зробити такі узагальнення.

1. Гарантований Процедурними керівними принципами щодо прав та обов'язків опозиції в демократичному парламенті розподіл керівних посад у президії Верховної Ради України і парламентських комітетах на основі принципу пропорційного представництва є засадничим елементом організаційно-правового механізму забезпечення реалізації гарантій і прав парламентської опозиції як основного суб'єкта парламентського контролю.

2. Гарантія наявності у складі президії Верховної Ради України на посаді заступника Голови Верховної Ради України представника парламентської опозиції має не декоративне призначення, а є формально-юридичною підставою для отримання особою, яка обіймає цю адміністративну посаду, автоматичного доступу до всіх адміністративно-розпорядчих актів внутрішньо-управлінського характеру, що можуть стати предметом внутрішнього парламентського контролю.

3. Проблема існуючого нині в Україні стану інституалізації парламентської опозиції набула системного характеру, оскільки не забезпечує її офіційної (процедурної) легалізації, що не сприяє виробленню консенсусних рішень у цивілізованих рамках співробітництва і консолідації різних політичних сил навколо інтересів громадянського суспільства та держави.

4. Відповідні положення Конституції України "консервують" тотальну "електронізацію" роботи парламенту.

Висновки.

Для усунення означених негативних тенденцій недостатньо формального законодавчого унормування правил, спрямованих на додержання гарантій і прав парламентської опозиції. Згадані у цій статті європейські цінності та стандарти мають бути імплементовані у повсякденне парламентське буття, а повноцінне впровадження електронного парламенту має виконати своє подвійне соціальне призначення – стати ключовим компонентом електронної демократії як сучасним інноваційним засобом функціонування відкритої парламентської установи та взірцевим прикладом для розвитку електронної демократії на регіональному і місцевому рівнях.

Використана література

1. Загальна декларація прав людини. *Голос України*. 2008. № 236. – (10 грудня).

2. Міжнародний пакт про громадянські та політичні права. Факультативний протокол до Міжнародного пакту про громадянські та політичні права. Київ: Укр. Правнича Фундація, 1995. 40 с.

3. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

4. Мартинюк Р. Сучасний український парламентаризм: особливості розвитку. *Юридична Україна*. 2009. № 1. С. 27-31.

5. Про заходи з реалізації рекомендацій щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України: Постанова Верховної Ради України від 17.03.16 р. № 1035-VIII. URL: http://zakon.rada.gov.ua/laws/show/1035-19

6. Guidelines on the rights and duties of the opposition in parliament. Geneva: Inter-Parliamentary Union. URL: http://www.ipu.org/splz-e/gabon.htm

7. Про Регламент Верховної Ради України: Закон України. *Відомості Верховної Ради України*. 2010. № 14-15; 16-17. Стор. 412. Ст. 133.

8. Про внесення змін до Регламенту Верховної Ради України: Закон України. *Голос України*. 2010. № 194. – (16 жовтня). URL: https://zakon.rada.gov.ua/laws/show/2600-17#Text

9. Шаранич С.С. Порівняльний аналіз функціонування парламентської більшості (коаліції) в європейських країнах. *Наук. вісн. Ужгород. нац. ун-ту. Сер.: Право*. 2012. Вип. 19. С. 65-71.

10. Процедурні керівні принципи щодо прав та обов'язків опозиції в демократичному парламенті (2008): Резолюція ПАРЄ 1601. URL: http://w1.c1.rada.gov.ua/pls/mpz2/docs/753_1601_Opozytsija_rezoljutsija.htm

11. Report of the Venice Commission "On the role of the opposition in a democratic parliament", adopted 15.11.2010. URL: https://www.venice.coe.int/-webforms/documents/default.aspx?pdffile=CDL-AD(2010)025-e

12. Меморандум про взаєморозуміння між Верховною Радою України та Європейським Парламентом про спільні рамки парламентської підтримки та підвищення інституційної спроможності від 3 липня 2015 року. *Голос України*. 2015. № 118. – (4 липня). URL: https://zakon.rada.gov.ua/laws/show/n0002001-15#Text

13. Комунікаційна стратегія Верховної Ради України на 2017 – 2021 роки: Розпорядження Голови Верховної Ради України від 21.11.17 р. № 486. URL: https://zakon.rada.gov.ua/laws/show/v0486004-17

14. Стратегія електронного парламентаризму на 2018 – 2020 роки: Розпорядження Голови Верховної Ради України від 05.07.18 р. № 278 URL: https://zakon.rada.gov.ua/rada/show/278/18-%D1%80%D0%B3#Text

15. Про внесення змін до Регламенту Верховної Ради України щодо вдосконалення електронної форми документообігу у Верховній Раді України: Закон України від 16.01.20 р. № 469-IX. *Відомості Верховної Ради України*. 2020. № 34. С. 5. Ст. 236. URL:https://zakon.rada.gov.ua/rada/show/469-20#n2

16. Про внесення зміни до пункту 3 розділу II "Прикінцеві та перехідні положення" Закону України "Про внесення змін до Регламенту Верховної Ради України щодо вдосконалення електронної форми документообігу у Верховній Раді України": Закон України від 13.07.20 р. № 758-IX. *Відомості Верховної Ради України*. 2020. № 48. Ст. 429.

17. Про внесення зміни до пункту 3 розділу II "Прикінцеві та перехідні положення" Закону України "Про внесення змін до Регламенту Верховної Ради України щодо вдосконалення електронної форми документообігу у Верховній Раді України": Закон України від 26.01.21 р. № 1132-IX. *Відомості Верховної Ради України*. 2021. № 12. Ст. 100.

18. Войнова Е.О. Електронна демократія як форма політичної комунікації. URL: //fpps.onua.edu.ua/index.php/2012-03-29-12-56-21/35-2012-04-03-14-46-53

19. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 08.11.17 р. № 797-р. *Офіційний вісник України*. 2017. № 92. С. 75. Ст. 2803. URL: https://zakon.rada.gov.ua/rada/show/797-2017-%D1%80#Text

20. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України. *Офіційний вісник України*. 2017. № 78. С. 109. Ст. 2402. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text

21. Електронний парламент України: досвід створення: наукове видання / за заг. ред. С.О. Довгого. Київ: Логос, 2015. 452 с. С. 9.

22. Рекомендації Комітету міністрів Ради Європи Rec(2004)15 "Електронне урядування" 4.Recommendation Rec(2004)15 Electronic governance ("E-governance") (Committee of Ministers of the Council of Europe). *Official Journal*. <https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Key_documents/ Rec(04)15_en.pdf>

23. Recommendation CM/Rec(2009)1 on electronic democracy (e-democracy) (Committee of Ministers). *Official Journal*. <https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Recommendation_CM_Rec2009_1_en_PDF.pdf>

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

УДК 342.6/355.6

ПШЕНИЧНИЙ В.О., аспірант ДНУ ІБП НАПрН України.

МАТЕРІАЛЬНА ВІДПОВІДАЛЬНІСТЬ У СФЕРІ ДЕРЖАВНОЇ ОХОРОНИ УКРАЇНИ

Анотація. *В даній статті, на основі сучасних правових підходів регулювання правових відносин в процесі становлення України як правової держави, її інтегрування в європейську спільноту, здійснення реформування державних структур, досліджується питання стану функціонування нинішнього інституту матеріальної відповідальності військовослужбовців Управління державної охорони України, акцентується увага на існуючих недоліках функціонування даного виду юридичної відповідальності.*

Ключові слова: *державна охорона, військовослужбовці, інститут матеріальної відповідальності, коефіцієнт кратності, цивільні особи.*

Summary. *In this article, on the basis of modern legal approaches to regulating legal relations in the process of Ukraine's formation as a rule of law, its integration into the European community, reforming state structures, the issue of the state of functioning of the current institution of material responsibility of servicemen of the State Security Department of Ukraine is investigated, attention is focused on the existing shortcomings in the functioning of this type of legal liability.*

Keywords: *state protection, military personnel, institute of material responsibility, multiplicity factor, civilians.*

Аннотация. *В данной статье, на основе современных правовых подходов регулирования правовых отношений в процессе становления Украины как правового государства, ее интеграции в европейское сообщество, осуществление реформирования государственных структур, исследуется вопрос состояния функционирования нынешнего института материальной ответственности военнослужащих Управления государственной охраны Украины, акцентируется внимание на существующих недостатках функционирования данного вида юридической ответственности.*

Ключевые слова: *государственная охрана, военнослужащие, институт материальной ответственности, коэффициент кратности, гражданские лица.*

Постановка проблеми. У сучасному врегулюванні нормами закону сфери матеріальної відповідальності військовослужбовців за шкоду, задану державі, є питання щодо стану урегульованості згаданої сфері в окремо взятих суб’єктів згаданих відносин, зокрема в Управлінні державної охорони України (далі – УДО України). Зважаючи на те, що забезпечення безпеки об’єктів і суб’єктів державної охорони здійснюється як громадянами, які відбувають військову службу, яка є державною службою особливого характеру, так і залученими до зазначеного громадянами, які перебувають на цивільній державній службі, на нашу думку існує доцільність у здійсненні наукового аналізу нинішнього стану вирішення даного питання, оскільки існують певні особливості у вирішенні згаданої проблеми. Насамперед, це обумовлюється правовими відносинами, що виникають, змінюються та припиняються між громадянами та державою у процесі забезпечення ними державної охорони щодо безпеки її об’єктів та суб’єктів.

Однієї із завдань правової науки в умовах сучасного розвитку України як правової держави та євроінтеграційних процесів, проведення в державі ряду реформ, включаючи сектор безпеки і оборони, є необхідність в: уточненні переліку суб’єктів юридичної відповідальності за вчинення відповідного виду правопорушення; наповнення реальним змістом конституційного принципу щодо рівності усіх перед законом.

Метою статті є визначення стану матеріальної відповідальності у сфері державної охорони України.

Виклад основного матеріалу. Національний суверенітет і безпека вважаються одними із найважливіших чинників для життєдіяльності будь-якого суспільства. За останні десятиріччя ситуація навколо питання забезпечення національної безпеки докорінно змінилася. Старі види загроз національній безпеці (військові конфлікти) значно ослабли. Водночас глобалізація втратила свій імідж, поступившись такому небезпечному періоду, який можна назвати періодом насилля.

Зазначене випливає з того, що поряд із старими загрозами національній безпеці з'явилися нові, так звані асиметричні загрози, в деякій мірі ще більш небезпечні: тероризм; гібридні війни; екологічні, техногенні, соціальні, продовольчі та енергетичні виклики і загрози, що вимагають консолідації зусиль та зміцненню зв'язків між державами, сприяють новому баченню та виробленню концепції безпеки світовому співтовариству.

Ще в недалекому минулому вважалося, що значення питання забезпечення національної безпеки знижується, оскільки це був об'єктивний процес руху світового співтовариства до загального миру. Проте загальновідомі трагічні події, що відбулися у світі впродовж останніх років, докорінно змінили погляди на зазначене вище питання.

Національна політика безпеки, вироблення засад якої є пріоритетом парламенту, прийняття на її основі державних рішень, суттєво впливають на стан і забезпечення внутрішньої та зовнішньої безпеки держави. Впровадження політики національної безпеки передбачає участь багатьох державних та недержавних органів та організацій, а також громадян. Як зазначається у [1]: "При цьому дуже важливо, щоб держава розробила всеохоплюючу стратегію національної безпеки з урахуванням усіх її аспектів та учасників. Такий підхід допоможе реагувати на загрози багатобічно і в повному обсязі. Так звані нові ризики, такі як тероризм і міжнародна злочинність, особливо потребують узгоджених дій, оскільки боротьба з цими загрозами передбачає залучення багатьох учасників: військових, міністерства фінансів, поліції, прикордонних військ, розвідувальних служби і т.д.".

Нині значно змінилися участь та роль людей, які мають пряме відношення до забезпечення безпеки різних об'єктів. З огляду на зазначене, є важливим, щоб національна політика у сфері безпеки відображала погляди людей щодо важливості та необхідності її забезпечення, поєднувала у собі головні цінності і принципи, пов'язані з безпекою, а держава забезпечувала їх реалізацію та пильно охороняла від посягань.

Одним із механізмів, що призначений для сприяння стабільного, безперервного, ефективного та надійного функціонування суб'єктів забезпечення безпеки, є інститут матеріальної відповідальності за заподіяну шкоду. Являючись одним із самостійних видів юридичної відповідальності, матеріальна відповідальність за трудовим правом є обов'язком однієї із сторін трудового договору (працівника або власника чи уповноваженого ним органу) відшкодувати іншій стороні шкоду, заподіяну внаслідок винного, протиправного невиконання або неналежного виконання трудових обов'язків у встановленому законодавством розмірі і порядку [2]. Як видно з наведеного, матеріальна відповідальність суб'єктів в трудовому праві є двосторонньою, взаємною.

Інститут матеріальної відповідальності має важливе значення для вирішення питання належного виконання військовослужбовцями УДО України військово-службових обов'язків, а також для забезпечення збереження матеріальних цінностей суспільства як в цілому, так і для вирішення питання збереження технічних та інших засобів забезпечення безпеки зокрема. На зазначене у своїх наукових дослідженнях звертав увагу український науковець Корж І.Ф. [3].

Держава забезпечує військовослужбовців УДО України необхідною зброєю, бойовою та спеціальною технікою, іншим військовим майном та грошовими коштами. Всі ці цінності є матеріальною основою боєздатності та боєготовності УДО України, а тому підлягають всебічній охороні та збереженню.

У процесі здійснення заходів здійснення державної охорони питання, пов'язані з необхідністю гармонізації військово-службових відносин, бережливого ставлення до державного майна, яке використовується (застосовується) для вирішення зазначеного вище завдання, а також з необхідністю запобігання посягань на державну власність, його розкрадання, пошкодження, незаконного використання, погіршення або зниження його цінності, набули особливої актуальності.

Особливості, які притаманні інституту військової служби в УДО України, суттєво вплинули на сутність та характер матеріальної відповідальності. На відмінну від трудового права, вона спочатку мала односторонній характер, тобто, не була взаємною для її суб'єктів, оскільки передбачала лише відповідальність одного з них – військовослужбовця. Водночас, ця ситуація змінилася після запровадження контракту про проходження військової служби, положення якого передбачають взаємну відповідальність суб'єктів згаданих правовідносин.

Згідно з чинним законодавством, за шкоду заподіяну майну держави, яке використовується для забезпечення безпеки об'єктів та суб'єктів державної охорони, застосовується матеріальна відповідальність. Так, положенням чинного на сьогоднішній день Закону України від 03.10.19 р. № 160-IX [4] визначаються підстави та порядок притягнення військовослужбовців та деяких інших осіб до матеріальної відповідальності за шкоду, завдану державному майну, у тому числі військовому майну, майну, залученому під час мобілізації, а також грошовим коштам, під час виконання ними службових обов'язків. Згаданий Закон України було прийнято на заміну Положенню, затвердженому Постановою Верховної Ради України від 23.06.95 р. № 243/95-ВР [5], норми якого не відповідали вимогам Конституції України (п. 22, ч. 1, ст. 92) про те, що "виключно законами України визначаються засади цивільно-правової відповідальності; діяння, які є злочинами, адміністративними чи дисциплінарними правопорушеннями, та відповідальність за них" [6].

Прийняті в Україні концептуальні та програмні документи, а також нормативно-правові акти у сфері державної охорони дали поштовх до реформування та подальшого розвитку як згаданої сфери, так і суб'єктів її забезпечення. Поряд з військовослужбовцями, повноцінними учасниками у здійсненні заходів забезпечення об'єктів та суб'єктів державної охорони нині є і цивільні особи – службовці, працівники за трудовим договором. Так, згідно зі статтею 20 Закону України "Про державну охорону органів державної влади України та посадових осіб" від 04.03.98 р. № 160/98-ВР – "працівники Управління державної охорони України, функціональні обов'язки яких не пов'язані безпосередньо із здійсненням державної охорони щодо органів державної влади України, забезпеченням безпеки посадових осіб та об'єктів, визначених цим Законом, у разі їх залучення до здійснення державної охорони користуються правами, що надаються військовослужбовцям Управління державної охорони України відповідно до пунктів 1, 2, 4, 5 статті 18 цього Закону. У зазначених випадках на них поширюються права і гарантії, передбачені для військовослужбовців Управління державної охорони України" [7].

Для вирішення відповідних завдань у сфері державної охорони згадані категорії громадян, так само як і військовослужбовці, використовують державне майно (зброю, спеціальні техніку та обладнання тощо). Однак, цивільні особи не є такими ж суб'єктами матеріальної відповідальності у згаданій сфері, як військовослужбовці. За

шкоду, заподіяну державі під час виконання ними службових обов'язків, згадана категорія осіб відповідає згідно з трудовим законодавством, тобто, вони є суб'єктами матеріальної відповідальності за трудовим чи службовим правом. Законодавець не передбачив відповідальність цієї категорії осіб у згаданих випадках, тому у Законі України від 03.10.19 р. № 160-IX [4] утворена певна правова прогалина, насамперед, щодо кратності відшкодування за вчинену шкоду. Перелік озброєння, зброї та боєприпасів до неї, нестача або розкрадання яких відшкодовується винними особами у кратному співвідношенні до їх вартості, визначається Кабінетом Міністрів України [8].

Так, в Законі України "Про державну службу" від 10.12.15 р. № 889-VIII [9] відсутні спеціальні нормативно-правові положення про кратність відшкодування державними службовцями матеріальних збитків, які вони спричинили державному органу під час виконання ними своїх службових обов'язків. Водночас, незважаючи на зазначене, згідно з положенням Глави 3 вказаного Закону України, передбачена можливість притягнення до матеріальної відповідальності державних службовців за шкоду, заподіяну фізичним та юридичним особам (що включає і орган, в якому проходять службу) незаконними рішеннями, діями чи бездіяльністю, насамперед, в добровільному порядку чи в порядку зворотної вимоги (регресу) у розмірі та порядку, визначених законом.

Зазначимо, що для цивільних осіб трудовим законодавством передбачено обмежену і повну матеріальну відповідальність. Разом з тим, згідно зі статтею 135-3 Кодексу законів про працю України від 10.12.91 р. № 322-VIII [10], законодавством може бути встановлено окремий порядок визначення розміру шкоди, що підлягає покриттю, в тому числі у кратному обчисленні, заподіяної підприємству, установі, організації розкраданням, умисним зіпсуттям, недостачею або втратою окремих видів майна та інших цінностей, а також у тих випадках, коли фактичний розмір шкоди перевищує її номінальний розмір.

Матеріальна відповідальність за своєю правовою природою є різновидом цивільно-правової відповідальності. Водночас вони мають певні відмінності, яка полягає у їхніх призначеннях і функціях. Матеріальна відповідальність має правовідновний характер, виконуючи компенсаційну функцію, і передбачає повернення витрат (заподіяної шкоди) суб'єкту правовідносин, тобто повне відновлення його прав, хоча і не завжди має повну, а має обмежену матеріальну відповідальність. Компенсаційна функція передбачає повернення витрат, які не викликані правопорушенням, заподіянням шкоди, тобто забезпечує лише часткове повернення витрат. Зазначена функція у цивільній сфері не притаманна матеріальній відповідальності у воєнній сфері за шкоду, вчинену військовослужбовцями, і яка передбачає компенсування шкоди у кратному розмірі.

У свою чергу, цивільно-правова відповідальність носить правовідновний, відшкодувальний та штрафний характер (стягнення пені, неустойки, штрафу), а також наявність деліктної, позадоговірної санкції – упущеної вигоди.

Матеріальна відповідальність невідривно пов'язана із суспільними правовідносинами, що започатковуються, розвиваються та припиняються у сфері державної охорони та регулюються нормами різних галузей права, тобто визначається відповідною галузевою природою порушеного обов'язку в згаданих правовідносинах. Так військово-службові правовідносини, що започатковуються між державою та громадянами України при їх вступі на військову службу, а також між військовослужбовцями у процесі проходження військової служби, регулюються нормами військового законодавства, яке є органічною складовою такої галузі права, як адміністративне. Державно-службові правовідносини, що започатковуються між державою та громадянами України при їх вступі на державну (цивільну) службу, а також між державними службовцями у процесі проходження цивільної служби, теж регулюються нормами адміністративного права.

Тим самим, можна констатувати різну галузеву належність матеріальної відповідальності у сфері державної охорони, що, у свою чергу, дозволяє стверджувати про функціонування матеріальної відповідальності як родового поняття (складається з різних галузевих видів). Враховуючи зазначене вище, можна стверджувати про дискримінаційну ситуацію, що склалася як у сфері державної охорони – зокрема, так і в секторі безпеки і оборони – в цілому, щодо різного підходу до матеріальної відповідальності військовослужбовців і цивільних осіб за завдану державі одну і ту ж саму шкоду: для військовослужбовців – обмежену, повну та підвищену із застосуванням кратності, для цивільних – повну або обмежену.

Як зазначалося вище, законодавством може бути встановлено окремий порядок визначення розміру шкоди, що підлягає покриттю, в тому числі у кратному обчисленні, заподіяної підприємству, установі, організації розкраданням, умисним зіпсуттям, недостачею або втратою окремих видів майна та інших цінностей, а також у тих випадках, коли фактичний розмір шкоди перевищує її номінальний розмір. Так, згідно із Законом України "Про визначення розміру збитків, завданих підприємству, установі, організації розкраданням, знищенням (псуванням), недостачею або втратою дорогоцінних металів, дорогоцінного каміння та валютних цінностей" від 06.06.95 р. № 217/95-ВР передбачено, що покриття працівником завданих матеріальних збитків здійснюється із застосуванням коефіцієнтів 2 і 3 [11]. Кратність розраховується у Порядку, затвердженому Кабінетом Міністрів України від 22.01.96 р. № 116 [12].

Частина 3 статті 6 Закону України від 03.10.19 р. № 160-IX [4] передбачає підвищену матеріальну відповідальність військовослужбовців та прирівняних до них осіб у кратному співвідношенні до вартості такого майна, але не більше десятикратного розміру. Перелік озброєння, зброї та боєприпасів до неї, нестача або розкрадання яких відшкодовується винними особами у кратному співвідношенні до їх вартості, визначається Кабінетом Міністрів України.

Згадана нерівність не відповідає положенням статті 24 Конституції України, згідно з якою "громадяни мають рівні конституційні права і свободи та є рівними перед законом. Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками" [6]. Ця проблема, як і деякі інші, так і залишилась не до кінця врегульованою законодавцем в остаточній редакції закону.

Висновки.

З огляду на викладене, зазначимо, що питання матеріальної відповідальності за шкоду, завдану державі у сфері державної охорони, потребує відповідного корегування.

Найсуттєвішим аспектом згаданої проблеми, що потребує врегулювання нормами закону, на нашу думку, є – необхідність усунення дискримінаційного, неконституційного положення щодо непропорційного застосування матеріальної відповідальності у частині застосування коефіцієнта кратності до військовослужбовців та до цивільних осіб.

Використана література

1. Парламентський контроль за сферою безпеки: принципи, механізми і практичні аспекти. – (Міжпарламентський союз/Женевський центр демократичного контролю за збройними силами). *Інтертехнологія.* Київ, 2003. С.23.

2. Трудове право України: підручник / за ред. Н.Б. Болотіної, Г.І. Чернишової. Київ: Знання, 2001. 564 с.

3. Корж І.Ф. Проблеми функціонування інституту матеріальної відповідальності у сфері національної безпеки. *Вісник Львівського університету. Серія юридична.* 2009. Вип. 48. С. 189-196.

4. Про матеріальну відповідальність військовослужбовців та прирівняних до них осіб за шкоду, завдану державі: Закон України від 03.10.19 р. № 160-IX. URL: https://zakon.rada.gov.ua/laws/show/160-20#Text (дата звернення: 27.01.2021).

5. Про затвердження Положення про матеріальну відповідальність військовослужбовців за шкоду, заподіяну державі: Постанова Верховної Ради України від 23.06.95 р. № 243/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/243/95-%D0%B2%D1%80#Text (дата звернення: 28.01.2021).

6. Конституція України: Закон України від 28.06.96 р. №254 к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

7. Про державну охорону органів державної влади України та посадових осіб: Закон України від 04.03.98 р. № 160/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/160/98-%D0%B2%D1%80#Text (дата звернення: 27.01.2021).

8. Про затвердження переліку озброєння, зброї та боєприпасів до неї, нестача або розкрадання яких відшкодовується винними особами у кратному співвідношенні до їх вартості: Постанова Кабінету Міністрів України від 15.07.20 р. № 604. URL: https://zakon.rada.gov.ua/laws/show/604-2020-%D0%BF#n9 (дата звернення: 27.01.2021).

9. Про державну службу: Закон України від 10.12.15 р. № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text (дата звернення: 27.01.2021).

10. Про затвердження Кодексу законів про працю України: Закон України від 10.12.91 р. № 322-VIII. URL: https://zakon.rada.gov.ua/laws/show/322%D0%B0-08#Text (дата звернення: 27.01.2021).

11. Про визначення розміру збитків, завданих підприємству, установі, організації розкраданням, знищенням (псуванням), недостачею або втратою дорогоцінних металів, дорогоцінного каміння та валютних цінностей: Закон України від 06.06.95 р. № 217/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/217/95-%D0%B2%D1%80#Tex (дата звернення: 29.01.2021).

12. Про затвердження Порядку визначення розміру збитків від розкрадання, нестачі, знищення (псування) матеріальних цінностей: Постанова Кабінету Міністрів України від 22.01.96 р. № 116. URL: https://zakon.rada.gov.ua/laws/show/116-96-%D0%BF#Text (дата звернення: 29.01.2021).

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

До відома читачів

Перелік статей,
опублікованих у журналі ІНФОРМАЦІЯ І ПРАВО у 2021 р.

№ з/п	Назва статті	Автор(и)	№ журналу, стор.
Інформаційне право			
1	Аберація нормативно-правової інформації	Корж І.Ф.	1(36)/2021, с. 9-16
2	Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми	Брижко В.М., Пилипчук В.Г.	1(36)/2021, с. 17-28
3	Кіберсталкінг: відображення у національному законодавстві	Карєв І.Ю., Фурашев В.М.	1(36)/2021, с. 29-34
4	Свобода інформації: концептуальні підходи у міжнародному праві	Забара І.М.	1(36)/2021, с. 35-44
5	Тексти, музика, зображення, що створюються штучним інтелектом: до визначення моделі правової охорони	Капіца Ю.М.	1(36)/2021, с. 45-54
6	Інформаційне насильство, інформаційна маніпуляція та пропаганда: поняття, ознаки та співвідношення	Самчинська О.А., Фурашев В.М.	1(36)/2021, с. 55-65
7	Удосконалення законодавства щодо дистанційного навчання в умовах карантину	Сандул В.С., Старова С.Б.	1(36)/2021, с. 66-72
8	Цифрова людина як філософська проблема	Дзьобань О.П.	2(37)/2021, с. 9-19
9	Законодавче забезпечення та особливості локалізації персональних даних: кращі практики зарубіжного досвіду	Красніков С.А.	2(37)/2021, с. 20-27
10	Правові засади протидії мові ворожнечі: ретроспективний огляд та аналіз перспектив	Головко О.М.	2(37)/2021, с. 28-38
11	Парламентський контроль у сферах духовності і культури: безпековий аспект	Корж І.Ф.	3(38)/2021, с. 9-20
12	Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією	Маляренко В.І.	3(38)/2021, с. 21-27
13	Інституційне забезпечення процесів протидії російській інформаційній експансії та пропаганді в сучасному світі	Панченко О.А.	3(38)/2021, с. 28-34
14	Реформування правової системи України під впливом міжнародного права	Маньгора В.В.	3(38)/2021, с. 35-40
15	Інформаційна культура особистості: сутність поняття	Беланюк М.В., Уханова Н.С.	3(38)/2021, с. 41-49
16	Правові аспекти захисту інформації з обмеженим доступом в Україні	Ковальов К.Є.	3(38)/2021, с. 50-58
17	Амбівалентність функціонування публічної влади в Україні	Корж І.Ф.,	4(39)/2021, с. 9-21
18	Інформаційна революція: соціоантропологічні та світоглядні трансформації	Дзьобань О.П., Жданенко С.Б.	4(39)/2021, с. 22-34
19	Правовий статус та характеристика цифрової людини	Радутний О.Е.	4(39)/2021, с. 35-51
20	Модальність правової визначеності у сфері захисту та безпеки приватності персональних даних	Брижко В.М.	4(39)/2021, с. 52-69

43	Протидія тероризму: досвід ЄС	Білан І.А.	2(37)/2021, с. 67-73
44	Удосконалення загальнодержавної системи боротьби з тероризмом	Поліщук С.М.	2(37)/2021, с. 74-80
45	Державна безпека України в сучасних умовах: проблеми компетенції державних органів	Гордієнко С.Г., Доронін І.М.	2(37)/2021, с. 81-92
46	Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект	Горун О.Ю.	2(37)/2021, с. 93-102
47	Засади інституціонально-функціонального забезпечення кібербезпеки в сучасних умовах	Гуржій С.В.	2(37)/2021, с. 103-114
48	Щодо концепції організаційно-технічної моделі кіберзахисту	Мануілов Я.С.	2(37)/2021, с. 115-122
49	Особливості кримінально-правової охорони державної таємниці за законодавством США	Пономаренко О.А.	2(37)/2021, с. 123-128
50	Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення	Поляков О.М.	2(37)/2021, с. 129-138
51	Сучасний досвід США у сфері забезпечення кібербезпеки	Стежко С.М., Шевченко Т.О.	2(37)/2021, с. 139-144
52	Забезпечення цифрового суверенітету в умовах геополітичного протиборства: кращі практики зарубіжного досвіду	Калайда Ю.П.	2(37)/2021, с. 145-154
53	Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки	Григоренко В.А.	2(37)/2021, с. 155-161
54	Імпортозаміщення програмного забезпечення як важлива складова посилення кібербезпеки держави	Шевченко В.П.	2(37)/2021, с. 162-169
55	Особливості законодавчого забезпечення економічної безпеки України	Правдюк А.Л.	2(37)/2021, с. 170-182
56	Інституційне забезпечення створення кібервійськ в Україні	Фица В.М.	3(38)/2021, с. 109-114
57	Вимоги правоохоронних органів ЄС щодо законного перехоплення інформації в електронних комунікаційних мережах	Кокіза С.В., Степанов В.А.	3(38)/2021, с. 115-120
58	Кримінологічний аналіз загроз правам і свободам людини в інформаційному просторі під час карантину у зв'язку з пандемією CoVID-19	Батиргареєва В.С.	3(38)/2021, с. 121-131
59	Роль профілювання наркотичих засобів, психотропних речовин та прекурсорів у протидії їх незаконному обігу	Кучинська І.В.	3(38)/2021, с. 132-138
60	Загрози терористичного характеру закордонним дипломатичним установам України	Скулиш Є.Д., Баліцький В.В.	3(38)/2021, с. 139-148
61	Удосконалення системи боротьби з тероризмом: досвід США	Бохенко В.М.	3(38)/2021, с. 149-154
62	Особливості правового режиму забезпечення інформаційної безпеки України, зумовлені Конституцією України	Борисов О.	3(38)/2021, с. 155-161
63	Актуальні питання щодо вживання терміносполук у висновках експерта (за матеріалами експертиз відео-, звукозапису)	Ковальчук Н.А., Леонов Б.Д.	3(38)/2021, с. 162-167
64	Правові аспекти реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт в сфері забезпечення національної безпеки держави	Алексеєва О.А.	3(38)/2021, с. 168-175

65	Огляд новел вітчизняного законодавства у сфері забезпечення кібербезпеки (на прикладі стратегії кібербезпеки України на 2021 – 2025 роки)	Мануілов Я.С.	4(39)/2021, с. 38-105
66	Актуальні питання оцінювання ризиків кіберзагроз: аналіз зарубіжного досвіду	Панченко О.А.	4(39)/2021, с. 106-112
67	Кібербезпека як важливий фактор забезпечення життєдіяльності вітчизняної енергетичної галузі	Стежко С.М., Фица В.М.	4(39)/2021, с. 113-120
68	Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак	Цяпа С.М.	4(39)/2021, с. 121-128
69	Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект	Жеребець О.М.	4(39)/2021, с. 129-134
70	Застосування принципів міжнародного права у сфері забезпечення міжнародної безпеки	Бєлєвцева В.В.	4(39)/2021, с. 135-140
71	Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю	Гуцалюк М.В.	4(39)/2021, с. 141-147
72	Проблеми забезпечення захисту кібепростору від діяльності терористичних організацій	Озерчук І.М.	4(39)/2021, с. 148-154
73	Організаційно-правові засади посилення спроможностей держави у сфері забезпечення кібероборони	Красніков С.А.	4(39)/2021, с. 155-161
74	Сучасні загрозливі тенденції використання Telegram-каналів на шкоду державним інтерсам	Гуржій С.В.	4(39)/2021, с. 162-169
75	Можливості блокчейн-технологій у розслідуванні кримінальних правопорушень, вчинених в кіберпросторі	Калайда Ю.П.	4 (39)/2021, с. 170-178
76	Становлення та розвиток правового регулювання обігу віртуальних активів	Новицький В.Я., Фица В.М.	4(39)/2021, с. 179-186
77	Диверсифікація як кодифіковано-цифрова система адміністративно-правового управління: міжінфраструктурне забезпечення інформаційного капіталу	Лісовська Ю.П.	4(39)/2021, с. 187-192
78	Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу	Таран О.В., Гавловський В.Д.	4(39)/2021, с. 193-201
Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"			
79	Правове забезпечення конституційних прав і свобод: адміністративно-правовий аспект	Косілова О.І.	1(36)/2021, с. 151-158
80	Інформаційна культура особистості: сутність і зміст	Уханова Н.С.	1(36)/2021, с. 159-166
81	Захист трудових прав осіб рядового і начальницького складу органів внутрішніх справ України, звільнених зі служби через скорочення штатів внаслідок ліквідації міліції	Ірха Ю.Б.	1(36)/2021, с. 167-177
82	Дослідження історії кодифікації українського права А. Яковлівим	Маньгора Т.В.	1(36)/2021, с. 178-183
83	Історико-правові передумови здійснення реформи децентралізації публічної влади в Україні	Антонюк О.М.	2(37)/2021, с. 183-190
84	Правосвідомість як основа механізму забезпечення гендерної рівності в Україні	Піковська Т.В.	2(37)/2021, с. 191-197
85	Нормативно-правове забезпечення реалізації політичних прав громадян України: сучасний стан, проблеми та перспективи розвитку	Косілова О.І.	3(38)/2021, с. 176-183

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

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).*

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада НДІІП НАПрН України 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

№ 4(39)/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.