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(47)/2023

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.
DOI: https:// .....

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(47)/2023

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 candidate of sciences, Doctor of Philosophy – Ph.D. 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.
DOI: https:// .....

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * * *

З М І С Т

Інформаційне право

Цифрова трансформація

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. 21.6. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ПП "Фенікс".
65009, м. Одеса, вул. Зоопаркова, буд. 25. Свідоцтво суб'єкта видавничої справи серія ДК № 1044 від 17.09.2002 р.

Рекомендовано до друку Вченою радою ДНУ ІІБП НАПрН України, протокол № 12 від 30.11.23 р.

TABLE OF CONTENTS

Informative Law

Digital transformation

Informative and National Safety

Recommended for publication by the IISL of the NALS of Ukraine, protocol No. 12 dated 30.11.23

Інформаційне право

УДК 001.92:316.324.8::34

ПИЛИПЧУК В.Г., *доктор юридичних наук, професор*, академік Національної академії правових наук України, директор ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-3754-4592.

ТЕОРЕТИЧНІ ТА ІСТОРИКО-ПРАВОВІ ЗАСАДИ ТРАНСФОРМАЦІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В СУСПІЛЬСТВО ЗНАНЬ

Анотація. *У статті висвітлюється генезис наукових досліджень і розробок з питань теорії інформації і знань, історичні, філософські та правові аспекти становлення інформаційного суспільства та його трансформації у суспільство знань.*

Ключові слова: *інформація, знання, інформаційне суспільство, цифрове суспільство, суспільство знань.*

Summary. *The article highlights the genesis of scientific research and development on the theory of information and knowledge, historical, philosophical and legal aspects of the formation of the information society and its transformation into a knowledge society*

Keywords*: information, knowledge, information society, digital society, knowledge society.*

Постановка проблеми. На межі XX – XXI століть людство стало свідком третьої з часу свого існування інформаційної революції. Дві попередні полягали в поширенні писемності та винаході друкарства, а третя була пов’язана зі створенням електронно-обчислювальних машин та упровадженням інформаційних (цифрових) технологій в усі сфери життєдіяльності людини, суспільства, держави та міжнародної спільноти. Ці обставини стали визначальними у процесі інформатизації та подальшого розвитку суспільних відносин.

Усвідомлення нетотожності знання й інформації, історичності інформації щодо знання, переорієнтація з інформації на знання були викликані неоднозначністю глобальних інформаційно-комунікаційних процесів, наслідками яких поряд з техніко-технологічним та економічним зростанням стали нові форми інформаційної залежності, несвободи та нерівності. Сучасні держави та суспільства опинилися захоплені процесами “гіперіндустріалізації”, а інформаційні (цифрові) процеси – відносинами маніпулювання, тотального комерційного обміну тощо, у результаті чого актуалізувалися загрози об’єктивному знанню.

Нову ситуацію щодо зростання обсягів і швидкостей трансльованої інформації за відсутності можливостей її повноцінної рецепції й декодування опрацьовував І. Валлерстайн [1]. На його думку, якість знань у сучасному суспільстві істотно погіршилася, а інформація перетворилася на “ексформацію”.

Термін “ексформація” є протилежним термінові “інформація” і означає надмірність повідомлення, визначену способом його передачі, цілями продукування інформації та її контентом. Домінування “ексформації” створює семантичний хаос внаслідок великої кількості змістів, які не розшифровуються споживачем.

Глобальна доступність інформації, Інтернет, світові інформаційні програми тощо стали засобом об’єднання різних складових, що створило ситуацію “нерозшифрованих

сенсів", зручну для здійснення маніпуляцій. Зі збільшенням кількості інформації, як свідчить аналіз, відбуваються зменшення і деградація сенсу. Апелюючи до бажань і чуттєвих імпульсів, власники інформації грають сенсом, перекручують факти, підміняють реальності, породжують ситуацію нісенітниці, а населення перетворюється на суспільство "нічогонезнайок".

Нині вже цілком усвідомленою є необхідність коригування концепції інформаційного суспільства, в рамках якої знання й інформація часто трактувалися як синоніми. З'явилася реальна потреба у стимулюванні виробництва й поширенні знання, пошуку нових правил і етичних норм, а також трансформації сучасного інформаційного суспільства в суспільство знань.

Результати аналізу наукових публікацій. Вчені наприкінці XX ст. дійшли висновку, що глибинною трансформацією, яка нині відбувається, є становлення і розвиток сучасного суспільства як суспільства знань. Про прихід *knowledge economy* і *knowledge society* пишуть в англомовних виданнях; про рух до *Wissemgesellschaft* – в німецькомовних; франкомовні автори критично обговорюють концепт *capitalisme cognitif*. Соціальна думка відкрила перспективу входження в суспільство знань. Проте місце останнього в історичній стадіальності мислиться різними авторами по-різному. Заслуговують на увагу й висновки про те, що з'ясування особливої ролі знання було обумовлено свого роду ностальгією європейського суспільства за цінностями епохи Просвітництва [2; 3].

Загалом, як свідчить аналіз наукових здобутків, в ході суспільних трансформацій людство випробувало різноманітні та досить сильні інформаційні потрясіння, спричинені релігійними війнами, великими географічними відкриттями, винаходом друкарського верстата, виникненням книгодрукування тощо. Внаслідок цього розпочалося формування нових соціально-етичних норм та суспільних цінностей, а одним із найважливіших завдань було проголошене перетворення інформації в знання та створення суспільства знань.

Метою статті є висвітлення актуальних теоретичних, історичних та правових питань трансформації інформаційного суспільства в суспільство знань, як майбутнього цивілізаційного виміру людства.

Виклад основного матеріалу. В епоху античної філософії Сократ, Платон, Аристотель вперше порушили питання про специфіку знання і його відмінність від професійних знань-умінь. Перший підсумок цих роздумів затвердив уявлення про переваги теоретичного знання над практичним, протилежність знання думці, а також загального знання – знанню, втіленому у практичні навички. Почав складатися новий ідеал освіченості громадян, в якому загальний інтерес або інтерес соціального цілого, загальна суспільна навичка, затьмарили переваги оволодіння приватними ремеслами. У Аристотеля ми знаходимо соціальне розрізнення теоретичної освіченості й спеціальної підготовки. На його думку, якщо людина загальним чином освічена й судить про будь-які речі, а "знаюча" – як досвідчена лише в своєму ремеслі, то краще бути загальним чином освіченою, аніж такою, що "знає як".

У період розвитку старогрецької філософії поняття знання представлене двома лініями (умовно – платонівською й аристотелівською). Сократ, а потім – Платон і платоніки вважали єдиною функцією знання самопізнання і самозростання людини за допомогою оволодіння нею знаннями. Опоненти Сократа – софісти вперше випробували прагматично спрямовану версію знання, вбачаючи мету знання у досягненні людиною успіху за допомогою забезпеченої знанням діяльності. Ця проблематика мала місце й у подальших наукових дискусіях. В результаті сформувалася певна парадигма, яка

зумовлює сучасне розуміння знання, його місце та роль у розвитку інформаційного суспільства та формуванні суспільства знань.

Знання створює підстави для прогностичної діяльності й тривалого (стратегічного) планування. На відміну від інформації, воно надає можливість робити прогнози, виявляти причинно-наслідкові зв'язки та ухвалювати рішення стосовно подальших дій.

Знання також служить підставою для конкретної соціальної дії, будучи при цьому універсальним. Широко відомим є афоризм Ф. Бекона: *scientia est potentia* який означає: "знання – сила". Термін "потенція" характеризує силу знання, його можливість змінювати фрагменти дійсності. Знання актуалізується, коли люди вдаються до перевірки нових гіпотез, що відкидають минулі стереотипи знань. Саме усвідомлення різнотипності фундаментального й прикладного знання виявилося надзвичайно важливим для формування розуміння соціальної природи знання як наочної основи концепції суспільства знань.

Один із основоположників концепції суспільства знань П. Дракер [4] звернув увагу на те, що епохальна подія перетворення капіталізму на цілісну соціальну систему супроводжувалася радикальними змінами концепції знання. Раптово зі сфери свідомості, співвіднесеної зі сферою буття, знання перетворилося на діяльнісний ресурс, споживчу послугу, суспільний товар та у визначальний чинник виробництва. Це дозволило Дракеру вести мову про створення нової економічної системи на основі знання.

Згідно зі слушними оцінками Дракера історичні події відбуваються в результаті дії низки незалежних один від одного обставин і процесів. У той же час він вважав, що є один найважливіший елемент – радикальна зміна значення знання, яка відбулася в Європі у XVIII столітті. У цей час формується поняття технології як знання особливого роду. До складу цього терміну входять: *techne* ("секрети ремесла") і – *логія* (за Дракером – "організоване, систематизоване, цілеспрямоване знання"). Дракер дійшов висновку, що всі суспільні трансформації XIX – XX ст. відбувалися саме під впливом зміни функцій знання.

В ході *першого етапу* знання використовувалося для розробки знарядь праці, виробничих технологій і видів готової продукції, що означало початок промислової революції.

Протягом *другого етапу* (1880 – 1945 рр.) виникли знання про трудову діяльність людини. Результатом його застосування стала революція у продуктивності праці.

Третій етап характеризується *"застосуванням знань до сфери знання",* що, за Дракером, стало поштовхом до революції у сфері управління в галузі економіки та створення економічної системи на основі знання.

Таким чином, був зроблений висновок про нові функції знання, що зростається з технологіями і змінює свою соціальну природу.

Як зазначалося, у науковій літературі подекуди ототожнюються інформація і знання або під інформацією розуміється один з різновидів знання. Існують контексти, коли відмінності знання й інформації справді виявляються несуттєвими.

Цю проблему розглядає А. Ракітов [5], відзначаючи, що інформація сама по собі не дає підстав для соціальних дій та не володіє регулятивним сенсом. Для того, щоб деяка одиниця інформації стала формою знання, необхідно, щоб на підставі змісту цього повідомлення було можливо проводити деякі системно зв'язані операції, які володіють характеристиками певного напряму діяльності. Одиниці інформації самі по собі не стимулюють людських рішень і діяльності. Даний критерій змістовних відмінностей між знанням та інформацією є умовним і відносним. Одиниця знання, навпаки, може

бути перетворена на змістовне знання, що мотивує людину до дій. Цю послідовність правил Ракітов називає регулятивною системою, яка забезпечує процес переходу від знання до дії. Звичну бінарну позицію "знання – діяльність" пропонується замінити на "знання – правила – діяльність".

Термін *"знання"* в новому соціальному контексті вимагає й нової інтерпретації. На рівні буденної свідомості продовжує залишатися достатнім визначення знання як правильного бачення світу, як дійсного знання. Стає актуальним недооцінений раніше взаємозв'язок знання й незнання. Наука не тільки створює знання, але одночасно проблематизує відсутність знання, а брак знання стає джерелом соціальних суперечностей.

Другий напрям актуалізації *знання* в сучасних умовах – це підвищення цінності неформалізованих, непрофесійних, особистих знань. Як справедливо вважає Андре Горц, інформатизація підвищила в ціні непіддатливе формалізації знання, засноване на персональному досвіді (що включає кмітливість, здатність до переорієнтації, самоорганізації, комунікації тощо) [6].

Способи вкладання індивідом знання цього типу у свою працю наперед не визначені, і Горц говорить про самовіддачу й мотивацію. Праця в "економіці знань" не піддається вимірюванню в одиницях часу – не згаяний на роботу час, а мотивація і особисті знання працівника стають найважливішими чинниками створення вартості.

Як відомо, науковий аналіз поняття "особисті знання" було здійснено англійським вченим Майклом Полані [7], який переглянув пріоритет деперсоніфікованого наукового знання, що задовольняє критерію об'єктивності, на користь стихії персонального знання. М. Полані мав намір всебічно врахувати той факт, що акти пізнання здійснюються особою і носять глибоко особистий характер. Поняття "особисті знання" нині широко використовується в теорії управління та протиставляється "спеціальному знанню".

Проведений аналіз дозволяє зробити такі попередні оцінки:

1) основою соціальної сфери є знання. Знання не ідентичне інформації, яка є лише інструментом знання;

2) одним із напрямів актуалізації цінності знання при переході до суспільства знань є визнання соціальної значущості неформалізованого, особистого знання. Способи оволодіння особистим знанням залишаються невизначеними і значною мірою належать стихії повсякденності;

3) суспільство з ринковою економікою свідомо орієнтується на постановку й вирішення інноваційних задач, що потребують саме новітніх знань (наукоємних виробництв, економічних і соціальних проектів тощо). Іншими словами, сучасний етап розвитку суспільства характеризується тенденціями орієнтованості на суспільство знань.

Прийнято вважати, що ідея суспільства знань набула поширення наприкінці XX ст. Цей факт найчастіше пов'язують з іменами П. Дракера, Н. Штера, Т. Сакайї. Однак, як справедливо зазначає В. Копилов, ґенеза цієї ідеї сягає своїм корінням більш ранньої історії, хоча самого поняття "суспільство знань" у ті часи, дійсно, ще не було. Проте, саме так в історії філософії було з багатьма поняттями та ідеями, зокрема, з ідеєю правової держави. Концепт Платона про філософа на троні також певною мірою можна вважати зародженням ідеї суспільства знань [8].

Важливою віхою стала опублікована 2005 року всесвітня доповідь ЮНЕСКО *"До суспільства знань"* [9]. У цій доповіді було поставлене завдання перенести центр досліджень з інформаційного суспільства на суспільство знань, що саме по собі не

сформується в інформаційному та в будь-якому іншому суспільстві, оскільки зростання обсягу інформації зовсім не обов'язково детермінує збільшення обсягу знань та зміну його соціальної ролі й місця. Необхідно, аби засоби збору, обробки, осмислення та споживання інформації також були адекватні завданню продукування і використання знань для розвитку людського суспільства в усіх сферах. При цьому, поняття "суспільство знань" було запропоновано інтерпретувати в ширшому соціальному контексті із залученням філософських, психологічних, етичних, аксіологічних, культурологічних та інших параметрів.

Сам факт прийняття вказаної доповіді ЮНЕСКО підтвердив актуальність та необхідність розбудови суспільства знань. Тобто, ідея суспільства знань була переведена з розряду утопічного ідеалу до реальних перспективних моделей соціальної організації.

Поняття і концепт *"суспільство знань"* в категоріальний апарат соціальної філософії ввів П. Дракер у роботі "Посткапіталістичне суспільство", опублікованій у 1993 р. в США. Він розрізняє поняття "посткапіталістичне суспільство" та "суспільство знань" і зазначає, що нині ще не сформовано суспільство знань, а лише формується економіка знань.

П. Дракер не єдиний, хто констатував підвищення ролі знання в житті суспільства і насамперед матеріального виробництва. Досить згадати Ф. Бекона, А. Сен-Сімона або К. Маркса, не кажучи вже про сучасників П. Дракера – представників так званого технологічного детермінізму XX ст. від Т. Веблена і Дж. Бернхема до численних сучасних теорій "нового індустріалізму" Дж. Гелбрейта та його послідовників, "постіндустріалізму" Д. Белла та його послідовників, "постфордизму" Р. Райха, "інформаційного капіталізму в мережному суспільстві" М. Кастельса, "постмодернізму" Ж. Бодрійяра та його послідовників, "суспільства корпоративного, споживчого капіталізму" Г. Шиллера, "рефлексивної модернізації" Е. Гідденса, "гнучкої спеціалізації" Л. Харшхорна, "публічної сфери" Ю. Хабермаса, "інформаційного суспільства" Е. Массуди та ін., які так чи інакше вже концептуалізували ідею пріоритетної ролі знання в економічному житті сучасного суспільства.

У 1994 р. канадський дослідник Альберто Ніко Штер опублікував першу монографію "Суспільство знань" [10]. При цьому, вчений наполягає на тому, що термін "постіндустріальне суспільство" слід замінити на термін "суспільство знань". Під *суспільством знань* він розумів *суспільство, в якому переборено розбіжності дискурсів науки, технології, культури та соціуму*, а також вбачав у ньому нову соціальну реальність, яку характеризував такими основними ознаками: *а) посилення значення фундаментальної науки як безпосередньої продуктивної сили; б) зростання ролі знання як засади індивідуальних та колективних дій; в) поява політичної економії знання; г) підвищення статусу експертів та експертних груп* тощо.

В цілому, як видається, можна стверджувати, що загальний концепт "суспільства знань" сформувався на початку 1990-х років, тобто не набагато пізніше формування теорії інформаційного суспільства. У зв'язку з цим, Є. Наумкіна цілком слушно зауважує, що *"усвідомлюючи глибокі суперечності і загрози в розвитку інформаційного суспільства, мислителі стали активно досліджувати інші виміри нового соціального порядку. Наслідком такого пошуку стало формування на межі століть концепції суспільства знань"* [11].

Однак, варто зауважити, що нині поняття "суспільство знань" ще не зайняло належного місця у філософській та правовій науці, хоча сам цей концепт не викликає суттєвих заперечень. Навіть після опублікування згаданої доповіді ЮНЕСКО "До

суспільства знань", так званої "наукової революції" в контексті формування суспільства знань ще не відбулося.

Загалом, як свідчить аналіз наукових здобутків, ***суспільство знань розглядається*** *як:*

а) вищий ступінь інформаційного суспільства;

б) сучасний етап розвитку інформаційного суспільства;

в) суспільство, що приходить на зміну інформаційному суспільству.

Низка дослідників вважає *концепції інформаційного суспільства, постіндустріального суспільства і суспільства знань* змістовно близькими. Те, що якісні соціальні зміни в сучасному світі обумовлені функціонуванням у ньому інформації та знання, – це очевидний факт, який демонструє, з їхньої точки зору, "споріднений" характер теорій. Тобто між інформаційним суспільством, постіндустріальним суспільством і суспільством знань ними не виявляються нездоланні перешкоди, що дозволяють проводити жорсткі демаркаційні лінії.

Протилежна точка зору щодо суспільства знань, як альтернативи інформаційному суспільству, актуалізувалася порівняно недавно. Інформаційне (цифрове) суспільство мислилося як техноцентристське, а *суспільство знань робить акцент на нових якостях людської особистості, на інтелектуальних і креативних здібностях людини, які стають безпосередньою продуктивною силою*. При цьому, інноваційні процеси виробництва й упровадження наукових знань є головним джерелом ефективності. У такому сенсі людська особистість постала як основна рушійна сила суспільного й економічного прогресу.

Загалом, низка авторів констатують, що нині існують тільки попередні версії *теорії суспільства знань*. Серед наукових праць, присвячених аналізу цієї проблеми, можна виокремити матеріали, зосереджені на змісті документів ЮНЕСКО стосовно суспільства знань та присвячені аналізу й упорядкуванню сукупності представлених там ідей. Друга група досліджень виконана відповідно до методології позитивізму і звертається до реальних характеристик сучасного суспільства.

У цьому контексті, ***суспільство знань*** розглядається як:

– ***ідеал***, або *нормативна модель*, до якої реальним суспільствам запропоновано свідомо прагнути, відповідним чином перебудувавши цілі й завдання державної політики;

– ***об'єктивна тенденція трансформації суспільства,*** що динамічно розвивається та послідовно проходить такі стадії: *постіндустріальне суспільство, інформаційне суспільство, суспільство знань*.

Для більш повного осмислення поняття "суспільство знань" також варто *позначити певні історичні етапи його концептуалізації*, зокрема:

1) суспільство знань, як слушно зазначає Д. Єфременко, має коротку історію, але довгу передісторію. При цьому, як зазначалося, категорія "знання" досить легко проектується на платонівську "ідеальну державу", на "Нову Атлантиду" Ф. Бекона, на "Місто Сонця" Т. Кампанелли, на ноосферу В. Вернадського тощо. Витоки концепції суспільства знань криються в теоріях інформаційного та постіндустріального суспільства, де аналізується кардинальна зміна соціальних функцій інформації і знання, а також у галузях історичних, філософських, соціологічних наук, які досліджують проблеми просвітництва і розвитку суспільства;

2) проблема знання, як одного з чинників виробництва, опинилася в центрі дискусій другої половини XX ст. Процес посилення ролі науки і знань в поєднанні з модернізацією й нелінійним розглядом суспільства датується початком 1960-х років.

Ф. Махлуп, який аналізував економіку наукових досліджень і засобів розповсюдження науково-технічної інформації, підкреслював їх значення, що зростає, об'єднавши їх загальним терміном "індустрія знань" [12]. Висновки Ф. Махлупа були підтримані американською громадськістю і покладені в основу обґрунтування концепції інформаційного суспільства;

3) термін *"суспільство знань"* в контексті організації влади й системи управління в умовах підвищення суспільної ролі знань у 1960-х роках також використав політолог Р. Лейн, який розглядав вплив наукових знань на сфери економіки і політики [13]. Одним із перших спробував осмислити нову соціальну ситуацію й виразно прописав остаточне завершення ери індустріалізму Даніель Белл, який не протиставляв інформацію і знання, а згадував їх поряд, підкреслюючи цінність науково-теоретичних знань, і прогнозував зростання їх ролі в суспільстві нового типу, що формується;

4) з середини 1990-х рр. почало широко використовуватися поняття *"цифрове суспільство"*. Д. Тапскотт, характеризуючи цей етап суспільної еволюції та орієнтуючись саме на знання, виокремлює такі *основні ознаки цифрового суспільства*: цифрова форма представлення об'єктів; віртуалізація виробництва; інноваційна природа виробництва; інтеграція, конвергенція, "безпосередність" (усунення посередників) тощо [1];

5) в сучасних публікаціях в контексті *цифрової трансформації* та *формування суспільства знань* часто визнається кризовий стан науки, зокрема, в Україні. Як свідчать результати аналізу, зазначене потребує кардинального перегляду державної політики та ролі державних органів щодо забезпечення пріоритетного розвитку наукової і науково-технічної діяльності. Потребує також вирішення проблема комплексного розвитку відповідних фундаментальних і прикладних досліджень, у тому числі, у сфері законодавства і права, оскільки розбудова суспільства знань також потребує належного правового забезпечення. З цього приводу заслуговують на увагу й підтримку оцінки [15], що ***трансформуючись в суспільство знань, Україна може стати однією з процвітаючих країн світу та явити новий спосіб державного устрою й життя, випередивши інші держави, навіть не наздоганяючи їх***.

Висновки.

1. Застосування логіки досліджень хвильового суспільного розвитку, а також аналіз історичних процесів на теренах України дають змогу виокремити такі основні ***історико-правові періоди розвитку суспільства*** на українських землях:

– аграрне суспільство *(почало формуватися майже 7,5 тисяч років тому, з часів розвиненої аграрної цивілізації – т. зв. "трипільської культури" – та фактично існувало до другої половини XX століття);*

– індустріальне суспільство *(почало зароджуватися у XVIII столітті та було остаточно сформовано в колишній УРСР у другій половині XX століття);*

– інформаційне суспільство *(почало формуватися наприкінці XX століття в умовах незалежної України, а нині перебуває у стадії цифрової трансформації)*.

2. З погляду права сутність інформаційного суспільства була визначена 1993 року Комісією Європейського Союзу: *"Інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку"* [16]. За результатами проведеного аналізу наукових здобутків в інформаційній сфері видається за можливе запропонувати дещо інший підхід стосовно визначення цього терміну, зокрема:

Інформаційне суспільство – це історична стадія розвитку людини, суспільства, держави та міжнародної спільноти, для якої характерні:

– зростання ролі інформації, знань та інформаційно-комунікаційних технологій в усіх сферах життєдіяльності;

– збільшення кількості людей, зайнятих виробництвом інформаційних ресурсів, технологій, продуктів і послуг, зростання їх ролі у валовому внутрішньому продукті;

– поширення процесу інформатизації за всіма функціональними напрямами інформаційної діяльності;

– формування національного і глобального інформаційного простору для задоволення потреб в інформаційних ресурсах, продуктах і послугах;

– збереження, розвиток та поширення в інформаційних мережах національних культурних, духовних і моральних цінностей;

– забезпечення безпеки людини і громадянина, суспільства, держави та міжнародної спільноти в інформаційній сфері.

3. Стрімке впровадження в соціально-економічну сферу новітніх інформаційних (цифрових) технологій *(Інтернету речей, Хмарних технологій, Великих Даних, штучного інтелекту* тощо*)* поряд з позитивними здобутками створило також реальні загрози захисту прав, свобод і безпеки людини в інформаційній сфері, а також *виникнення проблеми врегулювання безпрецедентних можливостей сучасного Інтернет-середовища традиційними (“доцифровими”) юридичними нормами і практиками*, базованими на традиційному уявленні про межі й засоби забезпечення приватності життя людини.

При цьому, проблеми захисту і правового забезпечення інформаційної безпеки в умовах розв’язаної рф *інформаційної війни* проти України та інших держав світу залишаються вкрай актуальними, оскільки застосування інформаційної зброї, інформаційних та психологічних операцій може призводити до спричинення реальної шкоди життю і здоров’ю людини, втрати території країни без застосування збройної сили, а також завдавати колосальних збитків суспільству і державі. Водночас, як видається, розбудова суспільства знань сприятиме подоланню інформаційної агресії та насилля.

4. Сучасний стан розвитку суспільства дозволяє розглядати інформаційне суспільство *(information society, digital society, electronic society)* як етап переходу до нового перспективного стану свого соціально-економічного й науково-технічного розвитку – до ***суспільства знань*** *(knowledge society)*. У ньому головним джерелом існування й розвитку, основним ресурсом функціонування та рушійною силою прогресивних перетворень стануть знання, які накопичило і продовжуватиме накопичувати людство та які ефективно будуть використовуватися практично усіма підсистемами суспільства для розв’язання своїх повсякденних і перспективних завдань.

Загалом, за нашими оцінками, *суспільство знань – вищий ступінь розвитку суспільства, збагаченого духовним та інтелектуальним потенціалом людства*. За таких умов знання сприяють розвитку продуктивних сил, рухають економіку, морально вдосконалюють суспільство. Саме знання стають джерелом багатства й успіху громадян, закладів, підприємств, установ та організацій, місцевих громад, регіонів і країни в цілому.

Сьогодні немає сумніву, що XXI століття має стати століттям знань та всебічного інтелектуального розвитку людини, а отже необхідно вирішувати принципово нову глобальну проблему, пов’язану з трансформацією інформаційного суспільства в суспільство знань та підготовкою людства до життя та діяльності в цілком нових умовах майбутнього світу.

Використана література

1. Валлерстайн И. После либерализма ; пер. с англ. М.М. Гурвица и др. – Едиториал УРСС, 2003. С. 139.

2. Бехманн Г. Общество знання – краткий обзор теоретических поисков. *Вопросы философии.* 2010. № 2. С. 113-126.

3. Кушерець В.І. Аналіз знання як стратегічного ресурсу трансформації суспільства (світоглядно-методологічний аспект): автореф. дис. ...д-ра філос. наук: 09.00.03. Київ, 2003. 41 с.

4. Дракер П. Посткапиталистическое общество. *Новая постиндустриальная волна на западе: Антология*. – Academia, 1999. С. 67-100.

5. Ракитов Л.И. Регулятивный мир : знание и общество, основанное на знаниях. *Вопросы философии.* 2005. № 5. С.84-85.

6. Горц А. Нематериальное: знание, стоимость и капитал ; пер. с фр. и нем. М. Сокольской]. – Изд. дом Государственного ун-та – Высшей школы экономики, 2010. 206 с.

7. Полани М. Личностное знание: на пути к посткритической философии ; пер. с англ. общ. ред. В.А. Лекторского, В.И. Аршинова. – Прогресс, 1985. 344 с.

8. Копилов В.О. Суспільство знання – категоризація ідеї. *Вісник Національної юридичної академії України імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія* ; редкол. А. П. Гетьман та ін. – Харків: Право, 2011. № 8. С. 45-46.

9. К обществам знания: всемирный доклад ЮНЕСКО 2005. URL : http//unesdoc.unesco.org

10. Ster N. Knowledge Societies. – L., 1994. 234 p.

11. Наумкина Е.А. Від інформаційного суспільства до суспільства знань: освітній аспект: зб. наук. праць *Філософські науки*. Суми: СДПУ ім. А.С. Макаренка, 2009. Вип. 1. С. 32.

12. Махлуп Ф. Производство и распространение знаний в США. – Прогресс, 1966. 463 с.

13. Lane R. The decline of politics and ideology in a knowledgeable society. *American sociological rev*. N.Y., 1966. Vol. 31. № 5. P. 620-670.

14. Тапскотт Д. Электронно-цифровое общество: плюсы и минусы эпохи сетевого интеллекта ; пер. с англ. И. Дубинского, под ред. С. Писарева. Київ: ITN Пресс : Рефл-бук, 1999. 403 с.

15. Ткачук В.В. Інформатизація освіти як чинник формування інноваційно-інформаційного суспільства в Україні (філософський аналіз): автореф. дис. ...канд. філос. наук: 09.00.10. Київ, 2010. 18 с. (С. 11).

16. Брижко В. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних: наук. посібник / В. Брижко, М. Швець. Кн. 2. Київ: ТОВ "Пан Тот", 2006. С. 444-448.

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

УДК 316.485.25::316(477):351.86

БЕБИК В.М., *доктор політичних, кандидат психологічних наук, професор,*
професор Українського державного університету ім. М. Драгоманова,
голова Всеукраїнської асоціації політичних наук.

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ, ПСИХОЛОГІЧНИХ ТА ГІБРИДНИХ ВІЙН

Анотація. *В статті сформулювало основні категорії теорії інформаційно-комунікаційних, психологічних та гібридних війн. В умовах формування глобального інформаційного суспільства інформаційна сфера стає віртуальним театром військових дій, в якому здійснюється жорстка боротьба за контроль над суспільною свідомістю (загальною, груповою, індивідуальною). В цих умовах потрібно по-новому подивитися на базові категорії та характеристики інформаційного суспільства, переосмислити поняття інформаційного простору і часу, які знаходяться під впливом дії сучасних інформаційно-комунікаційних технологій, віртуалізації реального простору і часу, маніпулятивних соціально-психологічних впливів та руйнівних технологій інформаційно-комунікаційних військ.*

Ключові слова: *інформаційне суспільство, інформаційно-комунікаційна війна, психологічна війна, гібридна війна, інформаційно-комунікаційні війська.*

Summary. *The article formulates the main categories of the theory of information and communication, psychological and hybrid wars. In the context of the formation of a global information society, the information sphere is becoming a virtual theater of war, in which a fierce struggle for control over public consciousness (general, group, individual) is being waged. In these circumstances, it is necessary to take a fresh look at the basic categories and characteristics of the information society, to rethink the concept of information space and time, which are influenced by modern information and communication technologies, virtualization of real space and time, manipulative socio-psychological influences and destructive technologies of information and communication troops.*

Keywords: *information society, information and communication warfare, psychological warfare, hybrid warfare, information and communication troops.*

Постановка проблеми. Будь-яка наукова теорія потребує формулювання базових категорій і характеристик феномену, що досліджується. Формування глобального інформаційного суспільства та його національних і регіональних моделей спонукає нас по-новому подивитися на поняття і сутність інформаційно-комунікаційних, психологічних та гібридних війн, які, на жаль, стали однією з характерних ознак вказаного вище інформаційного суспільства, що активно глобалізується під впливом сучасних інформаційно-комунікаційних, соціально-політичних та соціально-психологічних технологій.

Метою статті є формулювання базових категорій і характеристик інформаційно-комунікаційних, психологічних і гібридних війн, поняття і типології інформаційно-комунікаційних військ, узагальнення досвіду діяльності аналітичних служб, розвідки і контррозвідки в умовах інформаційно-комунікаційних, психологічних та гібридних війн.

Виклад основного матеріалу. Перед розглядом особливостей ведення інформаційно-комунікаційних, психологічних та гібридних війн в умовах формування глобального інформаційного суспільства, на нашу думку, варто використати типологію

теорій інформаційного суспільства, виокремлену В. Пилипчуком і О. Дзьобанем [10, с. 276-277], на основі якої ми пропонуємо вказані вище теорії інформаційного суспільства поділити на наступні типи теорій:

- технологічні (з точки зору використання науково-технологічних інновацій);
- економічні (враховуючи зростаючу економічну цінність інформації);
- людських ресурсів (в контексті збільшення зайнятості в інформаційно-технологічному секторі);
- просторово-мережеві (з урахуванням поширення масштабів інформаційно-комунікаційних мереж);
- гуманітарні (на основі підвищення рівня інформатизації освітньо-культурної сфери);
- політичні (в контексті використання е-демократії, е-парламенту, е-урядування, е-суду);
- цивілізаційні (через зростання пливу інформаційно-комунікаційних технологій на цивілізаційні зміни у суспільстві) тощо.

Використовуючи вказану вище типологію теорій інформаційного суспільства (яка не є закінченою і остаточно сформованою), ми все-таки вже можемо рухатися вперед і вдосконалювати, власне, саме базове поняття інформаційного суспільства.

Отже, ***інформаційне суспільство*** *це – історична форма організації суспільства, побудована на інтегральному і тотальному використанні інформаційно-комунікаційних технологій, ресурсів та структур, програмно-технічних засобів, мульти-медійних і мережевих технологій, електронних засобів масової комунікації та сукупного інтелектуального капіталу* [4, с. 61].

На основі розуміння цих базових рис інформаційного суспільства ми можемо сформулювати поняття ***інформаційної війни*** *як форми ведення інформаційного протиборства між різними суб'єктами (державами, неурядовими, економічними та ін. структурами), яка передбачає проведення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони і захисту власної інформаційної безпеки* [12, с. 101-103].

Якщо ж взяти до уваги, що космічно-філософське розуміння інформаційної війни (наприклад, у формі ентропійної чи генетичної війни) є значно ширшим за сучасне технологічно-прикладне розуміння цього терміну, ми можемо запропонувати звужене розуміння поняття інформаційно-комунікаційної війни з праксеологічної (мережево-технологічної) точки зору.

Інформаційно-комунікаційна війна *це – спеціалізована форма військово-комунікаційних дій в інформаційно-комунікаційному просторі (глобальному, національному, ворожому) з метою:*

а) формування та здійснення бажаних (суб'єктами інформаційно-комунікаційної війни) змін у глобальній суспільній свідомості;

б) руйнування інформаційно-комунікаційної сфери ворога та його суспільної свідомості;

в) захисту власної інформаційно-комунікаційної сфери та національної суспільної свідомості.

В даному контексті ми повинні розуміти, що вплив на суспільну свідомість в таких випадках здійснюється з обох боків віртуальної лінії фронту в інформаційно-комунікаційній сфері – на рівні соціуму, соціальних груп та індивідів.

Зрозуміло також, що подібне протистояння має бути одночасно спрямованим на:

а) захист системи власної державної та національної безпеки;

б) руйнування ворожої системи державної та національної безпеки.

При цьому ми маємо чітко розуміти, що державна безпека це – безпека держави (в інституціонально-функціональному розумінні), а національна безпека це – безпека нації (в етно-культурному розумінні).

Державна безпека – це безпека державних структур (військових, економічних, політичних, соціальних, промислово-технологічних, енергетичних, комунікаційних та інших структур), без яких держава не може існувати як системне, самодостатнє і кероване утворення.

Національна безпека – це фізична і гуманітарна безпека нації (мовно-культурної, освітньо-наукової, релігійно-міфологічної, соціально-психологічної та інших гуманітарних сфер суспільства), без яких не може існувати нація як етнічно-територіально суверенна інтегральна спільнота.

В умовах формування глобального інформаційного суспільства, його цивілізаційно-регіональних та національних моделей, інформаційно-комунікаційна війна (у вузькому розумінні) – це, перш за все, війна в цифровому інформаційно-комунікаційному просторі.

В цьому зв’язку варто було б згадати слова Еріка Девіса: “Цифровий світ, який лежить перед нами, – це … «гібрид», перехрестя кодів і масок, алгоритмів і архетипів, науки і симулякрів. Вибухова міфологія кіберпростору, крім того, є проявом цифрового анімізму, який просочується скрізь технокультурні кордони наукової парадигми” [5, с. 278-279].

Іншими словами, інформаційно-комунікаційна війна – це війна впливів (руйнівних або формуючих) на суспільну свідомість методами кодування/перекодування, маніпуляції інформацією та використання інформаційно-комунікаційних технологій для передачі належним чином “упакованої” комунікатором інформації.

Втім, ми не можемо погодитися з Е. Девісом в контексті його віри в “цифровоий” анімізм, позаяк анімізм це – віра в те, що все в природі (фізичні об’єкти, люди, тварини, рослини) мають свою душу.

Не факт, до речі, що душа є цифровою, а не аналоговою. Нагадаємо, що на перших етапах розвитку комп’ютерної техніки аналогові ЕОМ успішно конкурувати з цифровими, особливо в управлінні технологічними процесами на виробництві та у військовій (ракетно-космічній) сфері.

Водночас, не варто й забувати про те, що наші предки з неоліту і античного світу (шумери/сівери/кімери/копти) вирили, що каміння та глина мають душу. А жерці (брахмани та друїди) вірили, що душу мають також і тварини та рослини. Скіфи (кельти і саки), елліни Прадавньої України вірили в те, що душу мають озера, річки і джерела. Не даремно ж провідні річки України носять ім’я богині води Дани – Дніпро, Дунай, Дністер, Дон, Сіверський Донець [3].

Практично всі глобальні релігії світу переконані в існуванні безсмертної душі, до речі, не обов’язково людської. Наприклад, буддисти вірять в реінкарнацію душ в залежності від карми і дхарми. Якщо колись ти був кшатрієм (царем) чи брахманом (жерцем), але недостойно себе поводив, в наступному житті ти можеш бути гадюкою чи жабою.

Варто також згадати, що слово релігія (*religio* – лат.) означає – зв’язок людини з богом, по суті – *комунікацію*, яка в інформаційно-комунікаційному контексті означає – *обмін інформацією*.

Загалом, інформаційне суспільство та інформаційно-комунікаційні війни, на наш погляд, потрібно досліджувати системно, з урахуванням методології філософських, політичних, соціологічних, психологічних, інформаційно-комунікаційних та техніко-технологічних наук.

Скажімо, з філософських наук ми можемо взяти *концепцію глобальної космічної мережі Індри*, яка письмово була оформлена в надрах філософії дзен-буддизму (7 – 8 ст. н.е.), хоча сам буддизм на той час вже мав понад тисячолітню історію (з 6 ст. до н.е.).

В рамках даної концепції вважалося, що в небесному домі великого бога Індри (його царство, за ведійськими міфами, знаходилося між Сонцем і Полярною зіркою) існує дивним чином підвішена мережа, яка безкінечно розповсюджується в усі боки світу [19].

В кожному квадраті цієї упорядкованої мережі, як констатує Френсіс Кук, "...якийсь винахідник" повісив по одній яскравій перлині. Розміри цієї космічної мережі – безкінечні, відповідно, вказані перлини також безкінечні по числу [15, с. 2].

В кожній перлині вказаної космічної мережі, на думку філософів китайської школи Хуань (дзен-буддизм, 7 – 8 ст. н.е.), віддзеркалюються перлини з інших квадратів. Цей процес взаємного віддзеркалення перлин (фактично – обмін інформацією) є постійним. В наслідок цього, кожна перлина є джерелом цілого і живиться цілим, і є безкінечною мережею з безкінечною кількістю одиниць, що підтримують і визначають одна одне [5, с. 445].

Ось так, на основі "Сутри про велич квітки" (авторство якої приписують скіфському пророку Будді), буддійські філософи описують глобальну космічну мережу бога Індри, структура якої дивовижним чином нагадує глобальну інформаційно-комунікаційну мережу Інтернет, яка виникла в другій половині XX ст. – через 2.5 тис. років після виникнення буддизму!

В буддизмі ця глобальна космічна мережа є чітко структурованою і взаємозалежною. Але ж звідки і чому тоді ми спостерігаємо глобальний інформаційний хаос та інформаційно-комунікаційні війни? Можливо, тому, що інформаційний хаос існував ще до того інформаційно-комунікаційного впорядкування небесного (читай – космічного) простору Індри?

Логічної відповіді, принаймні, на даний момент ми не маємо. Тим більше, що буддизм і даосизм не визнають існування бога-творця. Вони вважають, що всесвіт був завжди. То ж виходить, що космічний інформаційний хаос та мережа Індри теж існували завжди і ми можемо припустити, що вони є невід'ємними частинами одного цілого – Космосу?

Але ж свідки тоді колосальне забруднення глобального інформаційного простору шкідливою і не потрібною (на наш погляд) інформацією? Чому і звідки беруться інформаційні війни? Як розпізнати інформацію істинну і фальшиву, особливо, в соціальних мережах?

Ось цей стан розгубленості досить яскраво характеризує Луїс Уайтлі Страйбер: "Я опинився на мінному полі. Реальні документи, які здаються фальшивими. Фальшиві документи, котрі виглядають як справжні. Величезна кількість "безіменних джерел". Я дрейфував скрізь марево цієї неймовірної історії" [16, с. 229].

Втім, панікувати не варто, оскільки фрагментарність і дискретність отримуваної нами з різних джерел інформації, цілком логічне пояснюється використанням соціально-психологічних та інформаційно-комунікаційних маніпуляцій на свідомому, підсвідомому та несвідомому рівнях.

Попри все, глобальна “інформаційна мозаїка”, на наш погляд, явно чи латентне підпорядковується певним “правилам гри” в рамках структурованих інформаційних потоків, в яких системно використовуються мозаїчні технології маніпуляцій.

Мозаїчні технології маніпуляцій це – маніпуляційні інформаційно-комунікаційні та соціально-психологічні технології, які використовуються інформаційно-комунікаційними військами противника, що систематично і цілеспрямовано “вистрілюють” в інформаційному просторі і часі належним чином “упаковані” і скомпоновані повідомлення (фейки, факти, комбінації фейків-фактів).

Ці повідомлення, на перший погляд, можуть бути зовсім інформаційне, не пов’язаними між собою. Але більш глибокий аналіз дозволяє розпізнати їх латентний зв’язок між собою на основі “психологічних якорів”, які підсвідомо і несвідомо збирають ці мозаїки-пазли в індивідуальній, груповій та суспільній свідомості в світоглядну картину світу, запрограмовану і викривлену маніпуляторами.

Якщо ми раптом і не маємо у своїй свідомості повного набору тих мозаїк-пазлів, дещо ми можемо (на основі засвоєного базового комплекту мозаїк-пазлів) домислити й самі. Отже, психологічний механізм – такий самий, як і в технологіях паблік рилейшнз: ми, начебто, робимо власні висновки, але насправді ці “власні висновки” нам вже майстерно запрограмували інформаційні війська противника.

Ось таким чином і формуються умови для спрямованих інформаційних впливів, у тому числі деструктивних і руйнівних, які є маніпулятивно-технологічною основою для ведення інформаційних, а на основі останніх – і гібридних війн.

Основою для вказаних вище впливів і маніпуляцій стала кібернетична теорія Норберта Вінера, який занадто ідеалізував комп’ютерні системи, бази даних, програмно-технічне забезпечення, які, на його думку, спроможні подолати хаос і ентропію (як міру хаосу і невизначеності).

Норберт Вінер в цьому зв’язку писав: “За допомоги управління і зв’язку ми завжди боремося з тенденцією природи до деградації організованого і руйнування усвідомленого” [17, с. 17]. Втім, ця “наукова” містика [5], на наш погляд, не коректне ставити знак рівності між природою і суб’єктом інформаційно-комунікаційної війни, який намагається зруйнувати інформаційно-комунікаційну сферу і суспільну свідомість об’єкта інформаційної війни.

Проте, це не заважає нам вважати, що природа, створена богом-творцем чи шляхом самонародження і самоорганізації, намагається таким чином зберегти природній інформаційний баланс, захищаючи саму себе, як кажуть програмісти, “від дурня”, що своїми недолугими і не професійними діями може зруйнувати інформаційний порядок Всесвіту.

В цьому випадку кібернетика з її штучним інформаційно-комунікаційним простором і віртуальним часом може вважатися своєрідним інформаційно-генетичним відхиленням від одвічного інформаційного порядку Всесвіту.

Цей підхід має рацію в межах релігій, які сповідують єдинобожжя (християнство, іудаїзм, іслам) і передбачають існування бога-творця. В буддизмі (скіфо-арійська релігія) і даосизмі (етнічна релігія хань) немає поняття бога-творця, оскільки ці релігійні доктрини передбачають, що Всесвіт ніхто не створював, оскільки він існував завжди.

Зрозуміло, що будь-яка релігійно філософська доктрина по своїй суті є ірраціональною і неоднозначною з точки зору логіки раціоналізму. І тому дещо парадоксальною виглядає описаний в буддизмі процес створення безкінечної мережі Індри, яка “колись була підвішена” і має безкінечну кількість перлин в кожній своїй секції, що віддзеркалює в собі інші перлини (чи не дзеркальні сервери? – *від Авт.*). Така

ось інформаційно-комунікаційна матриця Всесвіту, в якій кожен елемент взаємодіє через електромагнітну комунікацію (світло) і є, по суті, космічним першоаналогом сучасного Інтернету.

Концепції інформаційної війни створили методологічне підґрунтя для дослідників, які виокремили такий різновид інформаційної війни, як ***мережева війна*** – форма ведення війни, коли її учасники застосовують мережеві доктрини, стратегії, технології та структури, організаційно адаптовані до реалій сучасного інформаційного суспільства [12, с. 106-109].

Завдання мережевої війни:

1. досягнення інформаційної переваги (знищення засобів та систем розвідки, центрів обробки інформації та управління, засобів радіо- і теле-перехоплення сигналів);

2. завоювання переваги у повітрі (шляхом знищення та виведення з ладу систем протиповітряної оборони противника);

3. поступове знищення залишених без інформації та управління засобів ураження противника (авіації, ракетних комплексів, артилерії, бронетехніки);

4. остаточне знищення осередків спротиву противника (піхоти, вогневих точок, блок-постів).

В умовах ведення інформаційно-комунікаційних та гібридних війн важливе значення має ***радіоелектронна війна***, яка полягає у використанні електромагнітної енергії і засобів спрямування випромінюваної енергії (електромагнітного спектру частот) з метою здійснення безпосереднього впливу на живу силу противника та його техніку.

***Різновиди радіоелектронної війни*:**

- *електронну атаку* (випромінювання на особовий склад та технічні засоби ППО і радіолокації, удари по радіолокаційній зброї противника, використання електронних фальшивих цілей);
- *електронний захист* (спеціальні системи захисту власних засобів радіоелектронної війни: захисних екранів та укриттів, резервних систем перепрограмування);
- *радіоелектронний моніторинг* (пошук та ідентифікація цілей, визначення розташування, перехоплення, ліквідація загроз).

***Елементи радіоелектронної війни*:**

- *радіорозвідка* (збір, обробка, аналіз, оцінка розвідувальних даних);
- *радіотехнічна розвідка* (виявлення джерел електромагнітного випромінювання);
- *радіоелектронна контррозвідка* (забезпечення захисту, безпеки і таємності використання радіоелектронних систем та засобів) [12, с. 113-116].

Переходячи до аналізу ролі розвідки в інформаційно-комунікаційних війнах варто відзначити, що розвідка відіграє визначальну роль в будь-якій війні, оскільки своїм головним завданням має видобування, переробку та аналітичну оцінку й інтерпретацію отриманої інформації.

Свого часу один із генералів УСС (Управління стратегічних служб) США, яке потім було реорганізоване в ЦРУ (Центральне розвідувальне управління), Вашингтон Плетт писав: "…Розвідка виправдовує своє існування, постачаючи інформацію. Інформація є "чистим доходом" розвідки, що передається до інших державних органів і виправдовує зусилля розвідувальних органів" [11, с. 34].

Розвідка збирає інформацію всіма доступними методами: офіційними каналами, агентурним шляхом, аналізом відкритих джерел інформації: мас-медіїв, книг, журналів, соціальних мереж тощо.

В умовах формування інформаційного суспільства, безумовно, особливу роль відіграє ***електронна розвідка***, яка використовує дані космічних супутників, авіаційної, сухопутної та морської розвідок, випромінювання бойової та іншої техніки, перехоплень відео та аудіо сигналів, електронної пошти, електронних платежів, повідомлень у соцмережах, запитів у пошукових системах тощо.

Інформаційно-комунікаційна війна, як ми вже відзначали раніше, є спеціалізованою формою військових дій в інформаційному просторі та суспільній свідомості, що детермінує важливу роль в цих процесах соціально-психологічних чинників і визначає потребу у використанні терміну *психологічна війна.*

Наприклад, Михайло Требін вважає, що ***психологічна війна*** це – сукупність різних форм, методів і засобів впливу на людину з метою зміни в бажаному напрямі її психологічних характеристик (поглядів, думок, ціннісних орієнтацій, настроїв, установок, мотивів, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому [12, с. 110-113].

Відповідно до такого методологічного підходу виокремлюють і типологію *маніпулятивних впливів на людську психіку*:

1. інформаційно-психологічний (пропагандистський) вплив;
2. психогенний (фізичний вплив на мозок або інформаційно-шоковий вплив на свідомість);
3. психоаналітичний вплив на підсвідомість (терапевтично або з використанням гіпнозу);
4. нейролінгвістичний вплив (нейролінгвістичне програмування);
5. психотропний вплив (парапсихологічний або екстрасенсорний - з використанням психо-генераторів, біолокаційних установок, хіміко-біологічних засобів стимулювання певних психологічних реакцій);
6. психотропний вплив (вплив на психіку з використанням спеціалізованих медичних препаратів, хімічних та біологічних речовин).

Попри все це, ми вважаємо, що терміни *інформаційної війни* та *психологічної війни*, не зважаючи на свій інформаційно-комунікаційний зв'язок, є різними категоріями.

На наш погляд, ***психологічна війна*** *– це спеціалізована форма інформаційно-комунікаційних та фізико-хімічних впливів на суспільну свідомість, яка використовує різні форми, методи і засоби впливу на психіку людей з метою зміни в бажаному напрямі їх психологічних характеристик і соціальних норм.*

Розглядаючи суспільну свідомість як специфічний театр військових дій в рамках інформаційних і психологічних війн ми можемо виокремити *стратегічну, оперативну та тактичну психологічну війну*.

Визначившись з термінами інформаційно-комунікаційна та психологічна війна, цілком логічне розпочати використання термінів: *інформаційно-комунікаційні війська* та *психологічні війська*.

Інформаційно-комунікаційні війська – це суб'єкти інформаційно-комунікаційної діяльності, які здійснюють руйнівні та маніпулятивні впливи на противника:

- інформаційний простір, суспільну свідомість, інтелектуальний капітал, культуру, мову, релігію;
- структури держави (органи влади, прокуратуру, суди);
- силові структури (армію, поліцію, спецслужби);
- фінансово-економічну сферу, критичну інфраструктуру (енергозабезпечення, зв'язок, системи охорони здоров'я, системи соціального захисту) та ін. [4, с. 88-89].

Психологічні війська – це структури, які здійснюють психологічну війну проти противника, використовуючи руйнівні та маніпулятивні впливи на суспільну свідомість (соціум, соціальні групи, індивідів).

Виходячи з головних завдань психологічних військ ми можемо виокремити наступні психологічні впливи на суспільну свідомість противника, які здійснюються *структурами психологічних військ*:

- інформаційно-пропагандистські, нейролінгвістичні, окультні (через ЗМІ);
- психогенні / інформаційно-шокові (через ЗМІ);
- психоаналітичні (через дистанційний (ЗМІ) або безпосередній гіпноз);
- психотропні / парапсихологічні (через психо та біолокаційні генератори);
- психотропні / медичні (через хіміко-біологічні препарати);
- психотропні (через медичні препарати, хімічні та біологічні речовини) [4; 12; 13].

ХХІ століття породило ще один важливий термін, який потрапив вже до словників і підручників: *гібридна війна*, яка розглядається як форма воєнних дій із залученням до конфлікту різнорідних за складом, засобами, рівнем і характером підготовки озброєних сил… Щоб перемогти у гібридній війні треба мати найсучасніші збройні сили, силові структури, що здатні до проведення антитерористичної боротьби, удосконалені та захищені засоби інформаційної боротьби [12, с. 98-99], хоча ці проблеми досліджувалися, наприклад, китайськими мислителями ще в 10 – 13 ст. [8, с. 123].

Проте, військово-політична практика сьогодення корегує змістовне визначення терміну гібридна війна, зокрема, з урахуванням специфіки rozzійсько-української війни та інших війн ХХІ століття.

Гібридна війна *– форма військових дій, яка системно використовує варіативні комбінації інформаційно-комунікаційних та психологічних військ, сил спеціальних операцій, розвідки, спеціальних служб та традиційних військ (сухопутних, морських, космічно-повітряних та ін.).*

Варто відзначити, що в сучасних умовах традиційні війська, з геополітичних, стратегічних і тактичних міркувань, використовуються в обмежених масштабах. А інформаційно-комунікаційні війська, психологічні війська, сили спеціальних операцій, розвідувальні та контррозвідувальні служби залучаються системно і регулярно.

Наостанку варто відзначити, що теоретико-методологічні засади ведення інформаційно-комунікаційних, психологічних та гібридних війн мають надзвичайно важливе практичне значення, особливо, в умовах формування глобального інформаційного порядку та еволюції системи Нового світового порядку.

Використана література

1. Асеевский, А. ЦРУ: шпионаж, терроризм, зловещие планы: москва: Политиздат, 1985. 271 с.

2. Бебик В., Куйбіда В. Депутатська діяльність у системі публічного врядування: навч. посіб. Київ: НАДУ, 2017. 372 с.

3. Бебик В. Тисячолітня Україна: доісторичні цивілізації та глобальні релігійно-політичні доктрини: навчально-методичний посібник. Київ-Ужгород. 2012. 280 с.

4. Глобальні інформаційні, психологічні та гібридні війни: загрози та протидії: кол. моногр. / за заг. ред. В. Бебика та Н. Мякушко. Київ: Талком, 2023. 260 с.

5. Дэвис Э. Техногнозис: миф, магия и мистицизм в информационную эпоху / пер. с англ. С. Кормильцева, Е. Бачининой, В. Харитонова: екатеринбург: Ультра. Культура, 2008. 480 с.

6. Інформаційно-комунікаційна демократія: монографія / ред. кол. Довгий С.О., Лісничий В.В., Бебик В.М., Радченко О.В. – (Інститут телекомунікацій і глобального інформаційного простору НАН України). С.: Вид. СВС Панасенко І.М., 2015. 420 с.

7. Калакура Я.С., Рафальський О.О., Юрій М.Ф. Ментальний вимір української цивілізації. Київ: Генеза, 2017. 560 с.

8. Лапина З.Г. Учение об управлении государством в средневековом Китае: москва: Главная редакция восточной литературы, 1985. 383 с.

9. Піпченко Н.О. Соціальні медіа у структурі зовнішньої політики провідних міжнародних акторів: монографія. Київ: Центр вільної преси, 2014. 224 с.

10. Пилипчук В.Г.; Дзьобань О.П. Інформаційне суспільство: філософсько-правовий вимір : монографія. Ужгород: ТОВ "ІВА", 2014. 282 с.

11. Плэтт В. Стратегическая разведка. Основные принцип: москва: Издательский дом "Форум". 1997. С. 34.

12. Політологічний енциклопедичний словник / уклад.: Л.М. Герасіна, В.Л. Погрібна, І.О. Поліщук та ін. ; за ред. М.П. Требіна. Харків: Право, 2015. 816 с.

13. Психиатрический энциклопедический словарь / Й.А. Стоименов, М.Й. Стоименова, П.Й. Коева и др. Київ: МАУП, 2003. 1200 с.

14. Сенченко М., Сенченко О., Гастинщиков В. Мозкові центри країн світу. Київ: ДП Вид. дім "Персонал", 2016. 278 с.

15. 36 стратагем / пер.з кит. В. Урусова, О. Николишина. Харків: Фоліо, 2016. 223 с.

16. Cook, Frencis. Hua-yen Buddhism. University Park, Penn.: Pensylvania State University Press, 1977. P. 2.

17. Strieber, Whitley. Communion. New York ; Avon, 1987. P. 229.

18. Wiener, Norbert. The Human Use of Human Beings. New York : Doubleday Anchor Books, 1954. P. 17.

19. The Hindu World / Ed. By S. Mittal, G. Thursby. New York; London : Routledge, 2004. 658 p.

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

УДК 342.7:32/33

КОРЖ І.Ф., *доктор юридичних наук, с.н.с.,* заступник керівника наукового центру електронного парламенту та правової інформації ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-0446-5975.

ПРАВА ЛЮДИНИ ТА КОРУПЦІЯ, ЯК ПРОЯВ ЇХ ПОРУШЕННЯ

Анотація. *В статті досліджується питання стану запровадження та дотримання загальновизнаних правових принципів та норм міжнародного права у сфері основоположних прав і свобод людини в Україні. Зазначено, що під правами людини потрібно розуміти визначальні засади правового статусу особи, які належать їй від самого народження, є природними і невідчужуваними, без яких людина не може існувати як повноцінна суспільна істота, а тому вони є необхідним елементом громадян, суспільства і правової держави. В основі концепції прав людини лежать дві основні цінності – людська гідність і рівність. Визначаються та формалізуються права людини насамперед міжнародним правом, яке включає в себе ряд базових міжнародно-правових актів, як то: Загальна декларація прав людини; Європейська Конвенція про захист прав людини і основоположних свобод та протоколи до неї; Хартія основних прав Європейського Союзу. Україна, яка зазначила свій подальший розвиток у напрямку інтеграції в ЄС, формалізувала права своїх громадян у прийнятій в 1996 році Конституції, в якій закріплена ціла низка як традиційних, так і нових гарантій прав та свобод людини та громадянина, які дозволяють кожному громадянину обирати вид своєї поведінки, користуватися економічними й соціально-політичними свободами та соціальними благами як в особистих, так і в суспільних інтересах. Підкреслено, що утвердження в Україні прав людини як вищої соціальної цінності ускладнюється низкою чинників, що визначається головним чином низькою правовою культурою як суспільного загалу, так і державних службовців і підтверджується тим, що протягом багатьох років Україна займала одне з перших місць серед держав-членів Ради Європи за кількістю справ про порушення прав громадян, які перебували на розгляді в Європейському суді. Це вказує на існуючі проблеми в державі щодо правовиховання, правосвідомості, правової культури тощо громадян, які перебувають насамперед в органах публічної влади, і що виливається у прояві корупції, як правовому нігілізмі громадян. Особливої цинічності зазначене набуває у період ведення бойових дій проти російської агресії, про що свідчать непоодинокі повідомлення в мас-медіа. Такі прояви корупційних скандалів у Міністерстві оборони України, в цивільно-військових адміністраціях, в органах місцевого самоврядування, в інших державних органах країни свідчить про наявність глибокої політико-правової кризи в органах державного управління країни, наслідком відсутності програмних документів щодо здійснення державної кадрової політики, незадіювання правових механізмів боротьби з корупцією. Навіть Закон України "Про деолігархізацію" піддався нищівній критиці не лише з боку української громадськості, а й з боку "західної" спільноти. Підтвердженням актуальності та значущості необхідності вирішення в Україні проблеми корупції свідчить факт висунення нашим союзником США чітких умов подальшої підтримки України у її боротьбі з агресією та прагненням вступити до Європейського Союзу. Майбутній успіх України залежить від прискорення темпу реформ, що залишаються нереалізованими, та невідкладного виконання визначених пріоритетних перетворень в Україні.*

Ключові слова: *загрози, корупція, міжнародне право, права людини, основоположні права і свободи, справедливість.*

Summary. *This article examines the state of implementation and compliance with generally recognized legal principles and norms of international law in the field of fundamental human rights*

and freedoms in Ukraine. It is noted that human rights should be understood as the defining principles of a person's legal status, which belong to them from birth, are natural and inalienable, without which a person cannot exist as a full-fledged social being, and therefore they are a necessary element of citizens, society and the rule of law. The concept of human rights is based on two basic values – human dignity and equality. Human rights are defined and formalized primarily by international law, which includes a number of basic international legal acts, such as: Universal Declaration of Human Rights; European Convention on the Protection of Human Rights and Fundamental Freedoms and its protocols; Charter of Fundamental Rights of the European Union. Ukraine, which noted its further development in the direction of integration into the EU, formalized the rights of its citizens in the Constitution adopted in 1996, which enshrines a whole series of both traditional and new guarantees of human and citizen rights and freedoms, which allow each citizen to choose the type of his behavior, to use economic and socio-political freedoms and social benefits both in personal and public interests. It is emphasized that the establishment of human rights in Ukraine as the highest social value is complicated by a number of factors, which is mainly determined by the low legal culture of both the general public and civil servants and is confirmed by the fact that for many years Ukraine occupied one of the first places among the member states of the Council of Europe by the number of cases of violation of citizens' rights that were pending in the European Court. This indicates the existing problems in the state regarding legal education, legal awareness, legal culture, etc. of citizens who are primarily in public authorities, and which manifests itself in the manifestation of corruption, as legal nihilism of citizens. This becomes particularly cynical during the period of fighting against Russian aggression, as evidenced by numerous reports in the mass media. Such manifestations of corruption scandals in the Ministry of Defense of Ukraine, in civil-military administrations, in local self-government bodies, in other state bodies of the country testify to the presence of a deep political and legal crisis in the state administration bodies of the country, as a result of the lack of program documents on the implementation of state personnel policy, inactivity legal mechanisms to fight corruption. Even the Law of Ukraine "On De-Oligarchization" was subjected to devastating criticism not only from the Ukrainian public, but also from the "Western" community. Confirmation of the relevance and importance of the need to solve the problem of corruption in Ukraine is evidenced by the fact that our ally the USA put forward clear conditions for further support of Ukraine in its fight against aggression and aspiration to join the European Union. The future success of Ukraine depends on accelerating the pace of reforms that remain unimplemented and the immediate implementation of identified priority transformations in Ukraine.

Keywords: *threats, corruption, international law, Human Rights, fundamental rights and freedoms, justice.*

Постановка проблеми. Стан і рівень забезпечення прав людини завжди були актуальною проблемою як в колишніх СРСР та УРСР, так і в сучасній Україні, і мають складні аспекти її прояву. В Україні зазначена проблема тісно пов'язана з неналежним рівнем дотримання закріплених у Конституції України основоположних прав і свобод людини з боку держави та її органів, що знаходить свій вияв у труднощах реалізації згаданих прав і свобод, в недостатньому рівні їх захищеності від порушень та в гарантії їх поновлення.

Права людини в Україні пов'язуються насамперед із правовим статусом особи, що характеризується як юридичне закріплення правового положення людини і громадянина в сучасному суспільстві. А основу правового статусу людини і громадянина складають її права і свободи. Обравши свій подальший розвиток у сім'ї розвинутих економічно і політично країн Європи, Україна, відповідно до міжнародних зобов'язань, законодавчо врегулювала питання визначення та забезпечення основоположних прав і свобод у своїй Конституції та законах.

Водночас, як показує практика правового, політичного, соціального тощо життя в Україні, питання дотримання та забезпечення основоположних прав і свобод знаходяться ще на неналежному рівні. Зазначене підтверджується значною кількістю в Україні політичних, судових, мас-медійних тощо скандалів, а також "лідируючими" позиціями України в Європейському суді з прав людини за кількістю скарг громадян України до держави щодо порушення нею їхніх прав і свобод, а також невиконання рішень судів щодо їх поновлення.

Особливої гостроти в житті українського суспільства набули факти прояву корупції, яка, є негативним суспільним явищем, що проявляється в злочинному використанні службовими особами, громадськими і політичними діячами їх прав і посадових можливостей з метою особистого збагачення. Окрім того, що корупція створює загрози національній безпеці та демократичному розвитку держави, вона негативно впливає на всі сторони суспільного життя, підриває універсальні соціальні цінності, якими є права людини. У процесі прояву корупції здійснюється порушення основоположних прав і свобод людини у різних сферах життєдіяльності.

Корупція є одним із найбільш істотних факторів організованої злочинності, яка, у свою чергу, є одним із факторів, що негативно впливають на соціальну життєдіяльність, порушуючи права людини – на життя, свободу, благополуччя, особисту недоторканність тощо. Тим самим корупція є суттєвою перешкодою на шляху реалізації прав людини, до реалізації Українським народом свого прагнення жити в правовій, соціальній, демократичній державі.

Метою статті є, на підставі аналізу стану в Україні правового регулювання основоположних прав і свобод людини і громадянина відповідно до загальноприйнятих міжнародних принципів, вияснити та уточнити прогалини у даній сфері, оскільки аналіз стану та постійний моніторинг забезпечення прав людини в Україні, наукові дослідження зазначеного є дієвим способом встановлення реального стану справ у цій сфері, що дозволить своєчасно та ефективно реагувати на існуючі ризики та загрози.

Також передбачається розкрити сутність та стан в Україні нинішнього феномену "корупція", як факту прояву правового нігілізму, низького рівня правової культури у суспільстві, недостатнього рівня правового виховання в державі, та визначити рівень терпимості публічної влади щодо згаданого феномену з ціллю напрацювання відповідних пропозицій щодо напрямів та механізмів мінімізації негативного впливу корупції на українське суспільство.

Виклад основного матеріалу. Одним із здобутків нинішнього цивілізованого світу є міжнародна формалізація прав людини, тобто, вкладення в правові рамки комплексу природних і непорушних свобод і юридичних можливостей, що обумовлені фактом існування людини в цивілізованому суспільстві; іманентними можливостями людини поводитися відповідно до своїх свідомих волевиявлень та робити все, що не заборонено законом і не спричиняє невиправданої шкоди правам і свободі інших людей.

Під правами людини, як зазначено в науково-довідковій літературі, розуміються визначальні засади правового статусу особи. Права належать людині від народження, а тому є природними і невідчужуваними. Без цих прав людина не може існувати як повноцінна суспільна істота. Вони є необхідним елементом громадян, суспільства і правової держави [1, с. 710].

Першим міжнародно-правовим документом, що визначає та формалізує права людини, є Загальна декларація прав людини, прийнята у 1948 р. ООН [2], яка офіційно проголосила основні права і свободи людини. Декларація була проголошена як завдання, до виконання якого повинні прагнути всі народи і всі держави з тим, щоб кожна людина і

кожний орган суспільства, завжди маючи на увазі цю Декларацію, прагнули шляхом освіти сприяти повазі до цих прав і свобод і забезпеченню, шляхом застосування національних і міжнародних прогресивних заходів, загального і ефективного визнання і здійснення їх як серед народів держав-членів Організації, так і серед народів територій, що перебувають під їх юрисдикцією. Декларація передбачає, що всі люди народжуються вільними і рівними у своїй гідності та правах. Вони наділені розумом і совістю і повинні діяти у відношенні один до одного в дусі братерства.

Декларація має на меті забезпечити загальне та ефективне визнання і дотримання проголошених у ній прав, беручи до уваги те, що метою Ради Європи (РЄ) є досягнення тіснішого єднання між її членами і що одним із засобів досягнення цієї мети є забезпечення і розвиток прав людини та основоположних свобод.

Другим подібним міжнародно-правовим документом є Європейська Конвенція про захист прав людини і основоположних свобод (Європейська Конвенція з прав людини) [3] та протоколи до неї, яка була ратифікована Україною в 1997 році [4]. Договірні Сторони Конвенції повинні гарантувати кожному, хто перебуває під їх юрисдикцією, права і свободи, визначені в розділі I цієї Конвенції, що включає в себе:

– право на життя;
– заборона катування;
– заборона рабства і примусової праці;
– право на свободу та особисту недоторканість;
– право на справедливий суд;
– ніякого покарання без закону;
– право на повагу до приватного і сімейного життя;
– свобода думки, совісті і релігії;
– свобода вираження поглядів;
– свобода зібрань та об’єднання;
– право на шлюб;
– право на ефективний засіб юридичного захисту;
– заборона дискримінації.

Концепція передбачає певні відступи для Сторін під час війни або іншої суспільної небезпеки, яка загрожує життю нації, за умови, що вживані ними заходи не суперечать іншим зобов’язанням згідно з міжнародним правом.

Як зазначається в Раді Європи, права людини подібні до своєрідної броні: вони захищають нас; вони подібні до правил, оскільки кажуть нам, як можна поводитися; і вони подібні до суддів, тому що ми можемо до них волати. Вони абстрактні як емоції, і як емоції вони належать кожному і існують, що б навколо не відбувалося. Вони подібні до природи, тому що їх можна зневажати; і подібні до духу, тому що їх неможливо зруйнувати. Подібно до часу, вони однаково ставляться до всіх нас: багатим і бідним, старим і молодим, білим і чорним, високим і низькорослим. Вони пропонують нам повагу, і вимагають від нас ставитись з повагою до інших. Ми можемо іноді розходитися у визначенні доброти, істини та справедливості, але, зустрівшись із ними у житті, ми їх обов’язково дізнаємося [5].

Право – це вимога, про яку люди справедливо заявляють. Визнання прав людини означає визнання того, що кожній людині дано право вимагати дотримання таких положень: люди мають ці права, що б не говорилося і щоб не робили, тому що людина, так само, як і усі люди, також є людиною. Права людини притаманні кожній людині.

В основі концепції прав людини лежать дві основні цінності: перша – це людська гідність, а друга – рівність. Права людини можна розуміти як щось, що визначає базові

норми, необхідні для того, щоб жити з почуттям гідності, і їхня універсальність випливає з того, що принаймні в цьому всі люди рівні. Тому у Європейському Союзі (ЄС) з цих двох основних цінностей виводяться багато інших, і з їхньою допомогою точніше визначаються, як на практиці мають співіснувати люди та суспільства. Наприклад: ***Свобода***: оскільки людська воля становить важливу частину людської гідності. ***Примус*** робити щось усупереч нашому бажанню принижує людську особистість. ***Повага до інших:*** оскільки відсутність поваги до інших не дозволяє оцінити їхню індивідуальність та їхню людську гідність. ***Неприпустимість дискримінації:*** оскільки рівність людей у людській гідності означає, що ми можемо судити про права і можливості людей, з їх фізичних чи інших ознак. ***Терпимість***: оскільки нетерпимість свідчить про відсутність поваги до відмінностям, а рівність значить тотожність чи однаковість. ***Справедливість:*** оскільки люди, рівні у своїй приналежності до людського роду, заслуговують на справедливе ставлення. ***Відповідальність:*** оскільки повага до прав інших людей передбачає відповідальність кожної людини за її дії та вимагає від неї зусиль, спрямованих на реалізацію її прав та прав усіх людей.

Права людини невід'ємні, неподільні, взаємозалежні та взаємопов'язані. Вони виступають у ролі мінімальних стандартів, які застосовуються до всіх людей; кожна держава чи суспільство мають право встановлювати та застосовувати більш високі або більш специфічні стандарти.

Необхідно зазначити, що після прийняття Загальної декларації прав людини, у різних регіонах світу були розроблені власні системи захисту прав людини, які існують поряд із системою, створеною ООН. Дотепер існують регіональні установи захисту прав людини в Європі, Америці та Африці. В арабському світі та країнах Азіатсько-Тихоокеанського регіону (АСЕАН) також робляться кроки до інституційного закріплення регіональних стандартів прав людини. Але при цьому багато країн цієї частини світу також ратифікували основні договори та конвенції ООН, тим самим висловивши свою згоду з їхніми основними принципами і добровільно взяли на себе зобов'язання щодо дотримання міжнародного права стосовно прав людини.

Прихильність Європейського Союзу до захисту прав людини отримала новий імпульс з прийняттям Лісабонського Договору від 13 грудня 2007 року, який набув чинності 1 грудня 2009 року [6] та дав повне юридичне обґрунтування підготовленій у 2000 році Хартії основних прав Європейського Союзу [7]. Новий договір замінює Європейську Конституцію. Формально договір не є Конституцією – у ньому немає згадки про гімн чи прапор. Але документ зберіг всі ключові постанови про реформи, що були в первинному документі – Європейській конституції.

У Хартії викладено громадянські, політичні, соціальні та економічні права, яких зобов'язані дотримуватись як держави-члени, так і сам Європейський Союз. Європейський Суд з прав людини (ЄСПЛ) виступатиме проти будь-якого положення у законодавстві Євросоюзу, яке суперечить Хартії, та перевірить закони країн-членів ЄС на їхню відповідність Хартії, залишаючи за національними судами ухвалення рішень з повсякденних питань. Хартія поділяє права на шість "категорій": гідність, свобода, рівність, солідарність, громадянські права та справедливість. Категорія "гідність" гарантує право на життя та вводить заборону на тортури, рабство та смертну кару. Категорія "свобода" включає право на приватне життя, одруження, свободу думки та вираження думок, право зборів, право на освіту, право на працю, право мати власність та притулок. До "рівності" належать права дітей та людей похилого віку. Категорія "солідарність" включає соціальні права та права трудящих, право на справедливі умови праці, захист від необґрунтованого звільнення та доступ до медичної допомоги. До

“громадянських прав” входять свобода слова та свобода пересування, а категорія “справедливість” гарантує право на ефективні засоби правового захисту, справедливий судовий розгляд та презумпцію невинності.

Зазначимо, що правові механізми, створені для захисту різних сфер людських інтересів. У Європі, а також в Африці, Південній та Північній Америці, є суд, який розглядає скарги щодо порушення прав – Європейський Суд з прав людини. Навіть якщо скарги не підпадають під юрисдикцію Європейського Суду, то існують інші механізми, які дозволяють притягти держави до відповідальності за їхні дії та примусити їх до виконання своїх зобов’язань відповідно до угод про права людини. Людям легше від самого факту існування таких правових норм, навіть якщо не завжди є правові засоби, щоби примусити держави до їх виконання.

Як зазначають в ЄС, реалізувати права людини – це вміти долати перешкоди на цьому шляху:

- по-перше, деякі уряди, політичні партії чи кандидати у владу, діячі соціальної та економічної сфери, представники громадянського суспільства часто говорять “мовою прав людини”, але при цьому не беруть на себе зобов’язань захищати ці права. Іноді причиною цього є нерозуміння того, якими мають бути стандарти прав людини. В інших випадках йдеться про умисне зловживання та бажання виставити себе поборником прав людини та створити собі позитивний імідж в очах усього світу;
- по-друге, уряди, політичні партії та кандидати у владу, громадянські активісти можуть критикувати інших за порушення прав людини, але при цьому самі не дотримуються стандартів прав, а це називається політикою подвійних стандартів;
- по-третє, можуть бути випадки, коли права одних людей обмежуються для захисту прав інших. Іноді це може бути справедливо, оскільки права людини не безмежні, але, здійснюючи свої права, людина не повинна заважати іншим людям робити те саме. Проте, треба бути пильними і не допускати, щоб захист прав інших людей не став простим приводом для введення обмежень. Важливо, щоб моніторингом таких випадків займалися представники громадянського суспільства та незалежні судові органи;
- по-четверте, є приклади, коли захист прав однієї групи людей може спричинити обмеження прав інших, і це треба відрізняти від наведеного вище прикладу обмеження прав [5].

Україна, яка зазначила свій подальший розвиток у напрямку інтеграції в ЄС, формалізувала права своїх громадян у прийнятій в 1996 році Конституції [7]. У ній закріплена ціла низка як традиційних, так і нових гарантій прав та свобод людини та громадянина, які дозволяють кожному громадянину обирати вид своєї поведінки, користуватися економічними й соціально-політичними свободами та соціальними благами як в особистих, так і в суспільних інтересах. Цьому питанню присвячений “Розділ ІІ – Права, свободи та обов’язки людини і громадянина” Конституції України. Визначаючи права людини, Конституція України закріплює обов’язок кожного неухильно додержуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей. Незнання законів не звільняє від юридичної відповідальності (ст. 68 Конституції України).

В Конституції України можна виділити наступні групи прав людини:

– громадянські права, тобто можливості людей, що характеризують їх фізичне і біологічне існування, задоволення матеріальних, духовних та деяких інших потреб;

– політичні права, тобто можливості людини і громадянина брати участь у громадському і державному житті, вносити пропозиції про поліпшення роботи державних

органів, їх службових осіб і об'єднань громадян, критикувати недоліки в роботі, безпосередньо брати участь в різних об'єднаннях громадян;

– економічні права, тобто можливості людини і громадянина, які характеризують їх участь у виробництві матеріальних благ;

– соціальні права, тобто можливість людини і громадянина по забезпеченню належних соціальних умов життя;

– екологічні права, тобто можливість людини і громадянина мати безпечне екологічне середовище;

– культурні права, тобто можливості доступу людини до духовних цінностей свого народу (нації) та всього людства;

– сімейні права, тобто можливості людини і громадянина вільно розпоряджатися собою в сімейних правовідносинах:

а) невтручання в сімейне життя;

б) добровільне укладання шлюбу, рівні права і обов'язки у шлюбі і сім'ї;

в) право на державну охорону сім'ї, материнства, батьківства і дитинства;

г) право на рівність дітей незалежно від походження чи народження у шлюбі або поза шлюбом тощо.

Необхідно зазначити, що Конституція України декларує правовий характер Української держави (ст. 1). Розвиваючи ці програмні положення, ст. 3 Основного Закону проголошує людину та її права найвищою соціальною цінністю в Україні. При цьому права людини виступають детермінуючим критерієм, що визначає зміст і спрямованість діяльності держави. Закріплюється принцип відповідальності держави перед людиною за свою діяльність, а утвердження забезпечення прав та свобод людини визначається головним обов'язком держави.

Такі формально юридичні характеристики Української держави, носять, по суті, не стільки констатуючий, скільки програмний, цільовий характер, визначаючи напрям розвитку держави на перспективу. Разом із тим, є очевидним, що надмірна відірваність суспільних реалій від їх правової форми спричиняє нелегітимність влади в очах українських громадян. Влада, яка зневажає невідчужувані права, втрачає свою легітимність, врешті як втрачають легітимність і закони чи інші нормативні акти, видані нею.

Утвердження в Україні прав людини як вищої соціальної цінності ускладнюється низкою чинників. Чи не найважливіший із них – низька правова культура не лише суспільного загалу, але й багатьох державних службовців, у чиї посадові обов'язки безпосередньо входить захист порушених прав і попередження порушення інших прав. Однак ті, хто покликаний захищати правові цінності, часто використовують їх у суто риторичних цілях, своєю особистою поведінкою демонструючи зневагу до прав людини і пропонуючи суспільству приклад зразків поведінки, які заохочують його моральний розлад.

Важливо зазначити, що одночасно з прийняттям Конституції було необхідним створення механізму реалізації Основного Закону, у тому числі й щодо практичного втілення передбачених нею прав, свобод і обов'язків. При цьому під механізмом реалізації слід розуміти діяльність суб'єктів права, в результаті якої громадяни реально мають свободи, користуються правами та виконують обов'язки, та сукупність юридичних норм, які регулюють дану діяльність.

Механізм реалізації прав, свобод і обов'язків складається з гарантій їх забезпечення. Гарантії забезпечення прав, свобод і обов'язків людини і громадянина – це відповідні умови й засоби, які сприяють реалізації кожною людиною і громадянином закріплених

Конституцією України прав, свобод і обов'язків. Вони диференціюються на особисті, політичні, економічні, ідеологічні і юридичні.

Таким чином Конституція України приділяє особливу увагу питанню конституційного закріплення прав і свобод людини і громадянина. Це закономірно, адже права і свободи людини й громадянина в наш час стали загальновизнаною найвищою суспільною цінністю. Нині визнання та практичне здійснення прав і свобод людини і громадянина стало основним критерієм міри демократичності тієї чи іншої держави. Всі права людини і громадянина рівноцінні і взаємопов'язані і тому однаковою мірою повинні захищатися державою. Неприпустиме нехтування одними правами під приводом реалізації інших прав. Всі права людини і права громадянина повинні захищатися державою. З цією метою в Україні створені певні державні інститути. Гарантом права і свобод людини і громадянина є Президент України. Парламентський контроль за дотриманням конституційних прав і свобод людини і громадянина здійснює Уповноважений Верховної Ради України з прав людини. При недотриманні прав людини чи/та громадянина, кожен має право на захист. Одним із способів захисту є судовий захист, тобто право людини на звернення до суду за відновленням своїх прав та інтересів.

Необхідно зазначити, що до міжнародних механізмів реалізації прав, свобод і обов'язків, окрім зазначених вище актів, можна віднести:

– Міжнародний Пакт про громадянські і політичні права від 16.12.1966 р.;

– Міжнародний Пакт про економічні, соціальні і культурні права від 16.12.1966 р;

– Конвенція проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання від 10.12.1984 р.;

– Конвенція про ліквідацію всіх форм расової дискримінації від 21.12.1965 р. (ICERD);

– Конвенція ООН про подолання всіх форм дискримінації щодо жінок від 1979 р. (CEDAW);

– Конвенція ООН про права дитини від 20.11.1989 р. (UNCRC);

– Конвенція про права осіб з інвалідністю від 13.12.2006 р. (UNCRPD).

Європейський суд з прав людини є міжнародним органом, який за умов, визначених Конвенцією про захист прав людини та основоположних свобод, може розглядати заяви, подані особами, які скаржаться на порушення своїх прав.

Україна є стороною Конвенції про захист прав людини і основоположних свобод з 11 вересня 1997 року. Водночас протягом багатьох років Україна займала лідируючі місця серед держав-членів Ради Європи за кількістю справ, які перебували на розгляді в Європейському Суді. Порушення Україною Конвенції про захист прав людини і основоположних свобод, стосується зокрема, таких питань:

– невиконання або тривале виконання рішень національних судів;

– надмірна тривалість провадження досудового слідства у кримінальних справах і судового розгляду цивільних, кримінальних, господарських та адміністративних справ;

– незабезпечення права на належний судовий захист, неефективність розслідування кримінальних справ правоохоронними органами за скаргами на неналежне поводження з боку представників органів держави;

– порушення майнових прав;

– неналежні умови утримання та лікування осіб, які перебувають під вартою [8].

При цьому найбільша кількість скарг – 95 % – це невиконання судових рішень. Також тривалий розгляд справ у судах [9]. Як випливає з наведеного, основним порушником прав людини є державна влада, що вказує на існуючі проблеми в державі

щодо правовиховання, правосвідомості, правової культури тощо громадян, які перебувають в органах публічної влади.

Водночас необхідно зазначити, що щорічно державний бюджет України втрачає принаймні 450 мільярдів гривень через корупційні схеми. Цифра вражає сама по собі, але якщо до неї додати ще 500 мільярдів гривень потенційних інвестицій, яких наша країна не отримує через ті ж таки схеми, то матимемо ще один державний бюджет. Тобто ми могли б спокійно подвоїти наші видатки на оборону, охорону здоров'я, освіту та соціальне забезпечення, якби наша боротьба з корупцією була ефективною [10].

Оскільки на сьогоднішній день термін "корупційна схема" не має офіційного визначення, заслуговує на увагу науковий підхід до цього Ю.В. Орлова, який пропонує під його широким визначенням, згідно з яким дана схема є умовно самостійною формою прояву організованої злочинності у сфері економіки, розуміти стійкий, комплексний соціально-правовий феномен, що виражається у системній діяльності, алгоритмізованій послідовності дій щодо готування та безпосереднього вчинення корупційних злочинів як мети та/або засобу задоволення інтересів у сфері економічних відносин неправомірним способом з попереднім створенням юридичної бази прикриття чи без такого, але з використанням елементів механізму правового регулювання.

Однією з кримінологічно значущих властивостей корупційних схем є їх інституційне взаємопроникнення, що впливає на системну дисфункцію цілих галузей народного господарства, безпеки й обороноздатності країни [11].

Зазначимо, що згадане вище знаходить свій яскравий вираз у прояві корупції, як правовому нігілізмі, навіть у період ведення війни. Зараз це все виглядає надзвичайно цинічно, коли одні крадуть гроші, а інші жертвують своїм життям ради Вітчизни. А проявляється зазначене через:

– поставки державі товарів чи послуг за завищеними цінами через різноманітні "компанії-прокладки";

– завищення обсягів виконаних робіт, закупівлю на папері речей, яких не існує, які не поставляються державі тощо.

Так, у мас-медіа ходить інформація, надана Державною митною службою України, що Сили оборони України з початку 2023 року не отримали 653 партії вантажів, які при ввезенні в Україну були задекларовані, як гуманітарна допомога для військових. Серед цих товарів – пластини для бронежилетів, прилади нічного бачення, тепловізори, дрони та автомобілі. Випадків, коли українці бачать гуманітарні товари на полицях магазинів, дуже багато. Непоодинокі випадки, коли за кордоном українці отримують гуманітарну допомогу, а потім її продають. Є волонтери, які заробляють на добрій волі країн, що нам допомагають, і продають "гуманітарку" магазинам.

Неодноразові прояви корупційних скандалів у Міністерстві оборони України, в цивільно-військових адміністраціях, в органах місцевого самоврядування, в інших державних органах країни свідчать про наявність глибокої політико-правової кризи в органах державного управління країни, про відсутність належного рівня правосвідомості та правової культури як у політиків, так і у службовців публічної влади, а також про відсутність державної кадрової політики у державі та належної правової культури.

Зазначене вище підтверджується, і це знаходить своє вираження в публікаціях мас-медіа, постійним виникненням політичних і корупційних скандалів у суспільстві, при здійсненні призначень керівного складу правоохоронних органів, органів безпеки та в інші державні органи, а також в подальшій діяльності посадовців, яких було призначено з порушенням процедури. Україну регулярно накриває лавина інформаційних повідомлень про звільнення, висунення підозр у скоєнні корупційних дій і затримання чиновників із

різних державних відомств, зокрема митниці, податкової та Міністерства оборони. Прикладом зазначеного може слугувати корупційний скандал, пов'язаний із ігноруванням дії комендантської години у м. Києві, коли під час її дії працюють нічні ресторани і клуби (нічний клуб "Бохо"), а працівники поліції багато місяців не зважають на порушення та ігнорують виклики жителів, при цьому міністр МВС України розказує про свою безсилість навести належний порядок. Це явна ознака "кришування" корупційних дій з боку влади.

Зазначене не свідчить про здійснення активної антикорупційної боротьби у державі, а радше свідчить про вимушену реакцію правоохоронних органів на факти викриття зазначених корупційних дій представниками громадянського суспільства, яке все активніше проявляє нетерпимість до проявів цього правового нігілізму. Таким чином, фактично поширення корупції за своєю суттю є поширенням правового нігілізму, оскільки однією з основних її ознак є свідома неповага до права, його ігнорування і розрахунок на безкарність. Тим самим порушуються права інших громадян у різних сферах життєдіяльності.

Підтвердженням пасивності правоохоронних органів у боротьбі з корупцією є показники України у рейтингу Індексу сприйняття корупції Transparency International, в якому за 2022 рік Україна посідає 116 місце зі 180, з 33 балами, що всього на один бал позитивніше, ніж у 2021 році [12]. І цей результат – незважаючи на прийняття таких базових нормативних актів у сфері боротьби з корупцією, як:

– Закон України "Про засади державної антикорупційної політики на 2021-2025 роки", яким затверджено Антикорупційну стратегію на 2021 – 2025 роки, якою і визначаються дані засади [13];

– Постанова Кабінету Міністрів України "Про затвердження Державної антикорупційної програми на 2023 – 2025 роки" [14], метою якої є досягнення значного прогресу в запобіганні та протидії корупції, забезпечення злагодженості та системності антикорупційної діяльності всіх державних органів та органів місцевого самоврядування, а також належного процесу післявоєнного відновлення України;

– Закон України "Про запобігання загрозам національній безпеці, пов'язаним із надмірним впливом осіб, які мають значну економічну та політичну вагу в суспільному житті (олігархів)" ("Про деолігархізацію") [15], метою якого є подолання конфлікту інтересів, викликаного злиттям політиків, медіа та великого бізнесу, унеможливлення використання політичної влади для збільшення власних капіталів, забезпечення національної безпеки України в економічній, політичній та інформаційній сферах, захист конституційних прав та свобод громадянина, захист демократії, забезпечення державного суверенітету та уникнення випадків маніпулювання свідомістю громадян шляхом умисного спотворення інформації задля отримання доступу до ресурсів, що належать на праві власності Українському народові.

Необхідно зазначити, що Закон України "Про деолігархізацію" піддався нищівній критиці не лише з боку української громадськості, а й з боку "західної" спільноти. Так, Венеціанська Комісія рекомендувала відійти від "особистісного" підходу у питанні боротьби з олігархічним впливом, і зосередитися на системному підході запровадження заходів, покликаних унеможливити руйнівні наслідки олігархічного впливу для демократії, верховенства права і прав людини.

Європейська Комісія "За демократію через право" (Венеціанська Комісія) підкреслювала, що закон про деолігархізацію не можна втілювати у нинішньому вигляді. Про це йдеться у висновку Венеціанської Комісії, схваленому на пленарній сесії 9 – 10 червня 2021 року. Як зазначили її експерти – більшість країн запровадили

комплекс взаємопов'язаних законодавчих заходів – міжвідомчих, адміністративних, економічних та інших, аби запобігти руйнівним наслідкам для демократії, верховенства права і прав людини від зосередження в руках приватної особи значного впливу на економічне, політичне і громадське життя країни. До таких заходів може відноситися ефективна політика у питанні конкуренції, антикорупційні заходи і заходи для боротьби з відмиванням коштів, заходи для забезпечення плюралізму в медіа, правила фінансування політичних партій і виборчих кампаній. Замість того, аби відстоювати цей багатосекторальний, систематичний підхід, Україна обрала шлях боротьби з руйнівним впливом олігархізації через окремий "особистісний підхід" завдяки схваленні Закону "про олігархів", – йдеться у висновках [16].

Там же зазначено, що Закон складно узгодити з принципами політичного плюралізму і верховенства права, оскільки він має потенціал використання у політичних цілях. На даному етапі, як видається, поки суть наявного "особистісного підходу" не змінена, навіть значні правки до закону про олігархів не зможуть усунути неминучі розбіжності зі стандартами Ради Європи щодо прав людини, демократії і верховенства права. З цієї причини, Венеціанська Комісія приходить до висновку, що закон не має бути впровадженим у поточному вигляді і що треба дотримуватися "систематичного" підходу.

Венеціанська Комісія озвучила перелік рекомендацій для української влади. Зокрема, рекомендується юридично відкласти втілення даного Закону, здійснити поглиблений і всебічний аналіз наявних систематичних заходів та їхніх недоліків з точки зору структури, повноважень та координації. Однак Українська влада не прислухалася до висловлених порад і, як показала практика, Закон не досяг своєї мети. В Україні продовжують мати місце корупційні скандали, найбільшу нетерпимість до яких проявляє саме громадянське суспільство, тільки не публічна влада країни. Тим самим продовжуються прямі і опосередковані порушення прав громадян у різних сферах життєдіяльності.

Про актуальність та значущість вирішення в Україні проблеми корупції свідчить факт висунення нашим союзником США чітких умов подальшої підтримки України у її боротьбі з агресією та прагненням вступити до Європейського Союзу. Майбутній успіх України залежить від прискорення темпу реформ, вважають у Вашингтоні, й надали Києву список пріоритетних перетворень. До найбільш нагальних перетворень віднесено посилення Спеціалізованої антикорупційної прокуратури (САП) та низку кроків з посилення Національного антикорупційного бюро (НАБУ), до яких належить, наприклад, збільшення його штату до 300 осіб, посилення кримінальної спроможності НАБУ та збереження його незалежності. На реалізацію цих перетворень надається три місяці.

Також упродовж трьох місяців має бути відновлена вимога до розкриття інформації про активи та фінансову звітність, проведений незалежний, прозорий відбір нового голови Національного агентства з запобігання корупції (НАЗК) та завершений перезапуск Вищої ради правосуддя. На реформування судової гілки влади, Міністерства оборони та всіх силових відомств надається від трьох місяців до півтора року.

Окрім цього, перелік містить вимоги щодо реформування роботи наглядових рад державних підприємств "Укренерго" і "Нафтогазу", створення наглядової ради для нового "Укроборонпрому", корпоратизації "Енергоатому" [17].

Зазначені вимоги як актуальні питання суспільства не один рік стоять на порядку денного української держави щодо їх вирішення. Однак, прояву відповідної політичної волі з боку керівництва держави не видно до цього часу. Є надія, що під відповідним міжнародним тиском вони будуть вирішені найближчим часом.

Висновки.

Підсумовуючи висловлене вище, доцільно зазначити, що Україна у своєму подальшому розвитку впевнено крокує до єднання з сім'єю вільних, демократичних, економічно розвинутих європейських народів і прагне якнайшвидше влитися у "сім'ю" цих народів під назвою "Європейський Союз", хоча при цьому у своєму русі певним чином "шкутильгає".

Однією із найважливіших умов для реалізації зазначеного є впровадження в життя українського суспільства загальновизнаних принципів та правових норм європейського і міжнародного права, насамперед що регулюють основоположні права і свободи людини. Україна у даній сфері зробила багато, привівши свою Конституцію та законодавство в цілому до згаданих принципів, що вказує на бажання і невідворотність набраного Україною руху до ЄС.

Водночас, як це має місце і в інших пострадянських країнах, виконання зазначених принципів і правових норм в Україні бажає бути кращим і більш дієвим, про що свідчать значна кількість правопорушень у даній сфері, судових позовів з цих питань, а також звернень громадян до Європейського суду з прав людини щодо порушених їхніх прав, де Україна займає "лідируючі" позиції.

Найбільшим виразником згаданих вище порушень в Україні є високий рівень корупції, про що свідчать відповідні міжнародні показники індексу сприйняття корупції у різних країнах, за якими Україна перебуває в когорті негативних лідерів у Європі. Свідченням зазначеного є "антикорупційні вимоги" США, висунуті до України, як умови їхньої підтримки подальшої боротьби Українського народу проти російської агресії.

На нашу думку, лише завдяки активній позиції та наполегливості громадянського суспільства за підтримки представництв наших європейських та американських союзників в Україні, Український народ "примусить" публічну владу України виконати "домашнє завдання" у даній сфері, тобто проявити належну політичну волю для зазначеного.

Використана література

1. Юридична енциклопедія: в 6 т. / редкол. Ю.С.Шемшученко та ін. Київ: Укр. Енцикл., 2002. Т. 4: Н-П. 720 с.

2. Загальна декларація прав людини: прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 28.08.2023).

2. Європейська Конвенція про захист прав людини і основоположних свобод (Європейська Конвенція з прав людини) від 4 листопада 1950 року URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 28.08.2023).

3. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції: Закон України від 17.07.97 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/475/97-%D0%B2%D1%80 (дата звернення: 28.08.2023).

4. Что такое права человека? Совет Европы: пособие по образованию в области прав человека с участием молодежи. URL: https://www.coe.int/ru/web/compass/what-are-human-rights- (дата звернення: 28.08.2023).

5. Лісабонський договір 2007 року. URL: https://studies.in.ua/pravoes-shporu/2461-lsabonskiy-dogovr-2007-r.html (дата звернення: 28.08.2023).

6. Про основоположні права: Хартія Європейського Союзу від 1 грудня 2009 року. URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu (дата звернення: 28.08.2023).

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

8. Україна та Європейський Суд з прав людини. URL: https://coe.mfa.gov.ua/spivrobitnictvo /ukrayina-ta-yevropejskij-sud-z-prav-lyudini (дата звернення: 07.09.2023).

9. 95 % скарг до ЄСПЛ від українців стосуються невиконання судових рішень – Захаров. URL: https://www.radiosvoboda.org/a/devianosto-piat-vidsotkiv-skarg-do-yevrosudu-vid-ukrainsiv-sto suyutsia-nevykonannia-sudovyh-rishen/30962110.html (дата звернення: 07.09.2023).

10. Ю. Самаєва. Скільки країна щороку втрачає на схемах. URL: https://zn.ua/ukr/mac rolevel/koruptsijnij-kalkuljator.html (дата звернення: 07.09.2023).

11. Ю.В. Орлов. Корупційна схема: поняття та сутність: зб. тез доп. V Міжнар. Наук. практ. конф. *Кримінально-правові та кримінологічні засади протидії корупції*, м. Харків, 31 берез. 2017 р. / Харків. Нац. Ун-т внутр. справ ; Кримінол. Асоц. України. Харків: ХНУВС, 2017. 228 с. С. 138-140.

12. А. Андрійчук. Громадський контроль обмежений. Як війна впливає на рівень корупції в Україні. URL: https://www.radiosvoboda.org/a/indeksiv-spryynyattya-koruptsiyi-ukrayina/322489 30.html (дата звернення: 09.09.2023).

13. Про засади державної антикорупційної політики на 2021 − 2025 роки: Закон України від 20.06.22 р. № 2322-IX. URL: https://zakon.rada.gov.ua/laws/show/2322-20#Text (дата звернення: 09.09.2023).

14. Про затвердження Державної антикорупційної програми на 2023-2025 роки: Постанова Кабінету Міністрів України від 04.03.23 р. № 220. URL: https://zakon.rada.gov.ua/laws/show/220-2023-%D0%BF#Text (дата звернення: 09.09.2023).

15. Про запобігання загрозам національній безпеці, пов'язаним із надмірним впливом осіб, які мають значну економічну та політичну вагу в суспільному житті (олігархів): Закон України від 23.09.21 р. № 1780-IX. URL: https://zakon.rada.gov.ua/laws/show/1780-20#Text (дата звернення: 09.09.2023).

16. В. Саєнко. Венеціанська Комісія назвала аргумент проти закону "про деолігархізацію". URL: https://www.unian.ua/politics/venecianska-komisiya-nazvala-argument-proti-zakonu-pro-deoligar hizaciyu-12292110.html (дата звернення: 09.09.2023).

17. США висунули Україні чіткі умови підтримки. Що це означає? URL: https://www. dw.com/uk/dopomoga-v-obmin-na-reformi-comu-ssa-visunuli-ukraini-citki-umovi-pidtrimki/a-66 942465 (дата звернення 29.09.2023).

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

УДК 340:34.01+004

БАРАНОВ О.А., *доктор юридичних наук, професор,*
керівник наукового центру цифрової трансформації та права
ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0003-3233-6687.

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ ПРАВОВОГО СТАТУСУ РОБОТА ІЗ ШТУЧНИМ ІНТЕЛЕКТОМ

Анотація. *Технології штучного інтелекту екстенсивно поширюються у всьому світі, сьогодні вони використовуються практично у всіх сферах соціальної активності та демонструють вражаючі успіхи підвищення ефективності будь-якої діяльності. В умовах глобалізованого, складного, взаємопов'язаного та взаємозумовленого світу застосування штучного інтелекту має особливе значення для покращення процесу прийняття рішень, тотальне зниження якості яких стало основною причиною деградації цивілізації. Індустрії безперервно демонструють зростання разючих можливостей роботів з штучним інтелектом у різних сферах діяльності від особистого життя до управління державою. Одночасно експерти наголошують на наявності спектру загрозливих факторів, що супроводжують неконтрольоване поширення практичного застосування роботів із штучним інтелектом. Для усунення невизначеності наслідків масштабного використання роботів зі штучним інтелектом та амбівалентності у їх сприйнятті з боку суспільства необхідно терміново сформувати правове забезпечення процесів їх проектування, виробництва та застосування. Створення відповідного законодавства має ґрунтуватися на чіткому та однозначному визначенні правового статусу робота із штучним інтелектом, що потребує ретельного дослідження проблем визначення його суб'єктності та автономності, а також з'ясування пріоритетності застосування універсального чи спеціалізованого робота.*

Ключові слова*: штучний інтелект, робот, правовий статус, автономність, законодавство.*

Summary. *Artificial intelligence technologies are spreading extensively throughout the world, today they are used in almost all areas of social activity and demonstrate amazing success in increasing the efficiency of any activity. In a globalized, complex, interconnected and interdependent world, the use of artificial intelligence is of particular importance for improving the decision-making process, the total decline in the quality of which has become the main reason for the degradation of civilization. Industries are continuously demonstrating the growth of the amazing capabilities of artificially intelligent robots in various fields of activity from personal life to government. At the same time, experts note the presence of a range of threatening factors accompanying the uncontrolled spread of the practical use of robots with artificial intelligence. To eliminate the uncertainty of the consequences of the large-scale use of robots with artificial intelligence and the ambivalence in their perception by society, it is urgent to create legal support for the processes of their design, production and use. The creation of appropriate legislation should be based on a clear and unambiguous definition of the legal status of a robot with artificial intelligence, which requires a thorough study of the problems of determining its subjectivity and autonomy, as well as establishing the priority of using a universal or specialized robots.*

Keywords*: artificial intelligence, robot, legal status, autonomy, legislation.*

Постановка проблеми. Будь-які явища в суспільному житті не з'являються та не зникають зненацька. Завжди спостерігається діалектичний процес, який складається

з послідовних етапів: перший етап – поява певного поодинокого явища, другий етап – збільшення кількості випадків появи цього явища, третій етап – мотивоване поширення появи цього явища; четвертий етап – неконтрольоване (стихійне) поширення цього явища; п'ятий етап – повсюдна присутність цього явища. На одному з цих етапів виникає проблема правового регулювання суспільних відносин, пов'язаних з цим явищем. Саме таким чином розвивається процес появи технологій штучного інтелекту (далі – ШІ), сучасний стан, результати та перспективи застосування яких вимагають відповіді на питання правового регулювання суспільних відносин, пов'язаних з ними.

Каталізація зростання актуальності питання правового регулювання застосування ШІ обумовлена наявністю низки фундаментальних причин [38]: обмеженість когнітивних можливостей людини; наявність трьох цивілізаційних когнітивних протиріч; підвищення складності соціальних та інформаційних процесів у суспільному житті; тотальне та повсюдне зниження якості прийняття рішень; деградація цивілізації.

Наявність тісного зв'язку між якістю рішень та ефективністю когнітивних функцій людини обумовлює неухильне зростання вимог до змісту та якості останніх. Оскільки, ефективність когнітивних функцій людини має відповідати сучасному надскладному середовищу існування цивілізації, то дедалі більше людей усвідомлюють природні обмеження своїх когнітивних можливостей та докладають зусиль щодо їх творчого подолання [12].

Чому саме виникає така пильна увага до когнітивних функцій людини? Про це свідчать, наприклад такі факти: при прийнятті стратегічних рішень на високому рівні ми знаходимо докази недостатності когнітивних можливостей людини у зв'язку з використанням Великих Даних, проблемами з когнітивними упередженнями та когнітивним перевантаженням [22]; необхідна наявність конкретних когнітивних здібностей, які люди мають використовувати, щоб впевнено приймати рішення і навіть пояснювати свої наміри чи поведінку [28]; когнітивна гнучкість (тобто здатність узгоджувати тип когнітивної обробки з типом наявної проблеми) дозволяє особам досягти значно кращої ефективності прийняття рішень [21]; моделі прийняття рішень, засновані на принципах послідовної вибірки та накопичення до певного порогу почали відігравати центральну роль у нейронауці прийняття рішень [5]; здатність експертів приймати інтуїтивні рішення сильно залежить від їхніх когнітивних навичок обробки інформації, які дозволяють відсіювати нерелевантні сигнали, зберігаючи відповідні сигнали [24].

Цивілізаційні когнітивні протиріччя людства може бути нейтралізовано завдяки застосуванню досягнень четвертої промислової революції [38]. Наприклад, перше цивілізаційне когнітивне протиріччя людства було нівельовано завдяки винаходу комп'ютера. Друге цивілізаційне когнітивне протиріччя людства ефективно нівелювалось завдяки широкому використанню комп'ютерних технологій (цифрових технологій) в процесі комп'ютеризації, інформатизації, розвитку інформаційного суспільства та постіндустріального розвитку. Третє когнітивне протиріччя людства може бути нівельовано завдяки широкому використанню технологій Інтернету речей, центральною складовою яких є ШІ.

Потужним маркером стратегічної важливості ШІ для майбутнього цивілізації є те, що за останні 5 років понад 60 розвинених держав прийняли або розробляють національні стратегії розвитку та використання ШІ [34]. Так відбувається тому, що застосування роботів із ШІ створює реальні умови для подолання третього когнітивного протиріччя людства, забезпечення оперативного прийняття оптимальних рішень із залученням будь-якого обсягу різноманітних знань та інформації, різкого підвищення ефективності різноманітної діяльності.

Одночасно, невирішеність проблеми правового забезпечення застосування роботів з ШІ створює потужний бар'єр на шляху їх широкого використання в різноманітних сферах соціальної активності. До основної актуальної проблеми формування правового забезпечення застосування робота із ШІ відноситься проблема визначення його правового статусу.

Метою статті є визначення суб'єктності або об'єктності робота із ШІ, умов визнання автономності робота із ШІ та пріоритетності застосування універсального чи спеціалізованого робота із ШІ.

Виклад основного матеріалу.

І. Робот із ШІ – це суб'єкт чи об'єкт правовідносин?

Проблема правового регулювання застосування роботів з ШІ має давню історію, яка починається з розквітом автоматизації різноманітних процесів, що відбувалися у минулому столітті. У свій час з'ясувалось, що результати деяких автоматизованих процесів, які здійснювались без безпосереднього впливу людей, мали юридичні наслідки для юридичних та фізичних осіб, як суб'єктів права. Це створювало враження, що певні юридично значущі дії, які здійснювались в інтересах певних суб'єктів права, відбувались автоматично без участі людей. Цей факт став причиною виникнення дискусій щодо проблеми визначення юридичного статусу для систем автоматизації [1].

Сучасні уявлення про значення та особливості застосування роботів з ШІ, як наступного покоління розвитку ідей автоматизації діяльності людини, можна звести до двох основних пануючих груп, зміст яких є визначальним щодо встановлення їх правового статусу.

1. ***Робот – інструмент (об'єкт).*** Роботи – це своєрідні інструменти, які люди використовують для підвищення ефективності своєї певної праці в процесі реалізації діяльності. У такому випадку, робот з ШІ в процесі свого функціонування не взаємодіє із людьми та слугує лише ***для забезпечення*** реалізації суспільних відносин *традиційними суб'єктами – юридичними або фізичними особами*.

Правовий статус робота із ШІ у такому випадку є аналогічним правовому статусу раба в Римський імперії як *знаряддя виробництва – "знаряддя, що говорить"* [42].

2. ***Робот – суб'єкт***. Автономні роботи із ШІ можуть виступати "стороною" в суспільних відносинах при реалізації певної діяльності, в яких інша сторона – це традиційні суб'єкти. Чому роботи можуть бути стороною відносин? Тому, що вони автономно, незалежно від людей можуть самостійно оцінювати стан оточуючого світу, дії інших суб'єктів, за результатами цієї оцінки самостійно формувати або змінювати загальну або локальну мету та зміст своїх дій, самостійно приймати рішення щодо своєї діяльності. А також тому, що їх діяльність може відбуватись в умовах неповної визначеності, тобто коли вони діють в умовах впливу непередбачуваних мінливих обставин. У такому випадку роботи із ШІ розглядаються як людиноподібні суб'єкти, які здійснюють людиноподібні дії в процесі відносин з традиційними суб'єктами. Якщо дії традиційних суб'єктів в таких відносинах підлягають правовому регулюванню, то логічно припустити, що робот з ШІ, який є іншою стороною суспільних відносин, також має бути суб'єктом цих правовідносин.

Отже, якщо робот з ШІ в процесі свого функціонування взаємодіє або з традиційними суб'єктами, або з іншими роботами із ШІ ***задля реалізації*** суспільних відносин, здійснення яких має відбуватись згідно із встановленими правилами, то він має дотримуватись цих правил.

Таким чином, узагальнюючи, можна констатувати, що склалися дві полярні концепції щодо правового регулювання застосування роботів:

– перша – робот з ШІ не може бути суб'єктом права, оскільки він може *використовуватись лише для забезпечення реалізації* суспільних відносин традиційним суб'єктом суспільних відносин;

– друга – робот з ШІ може бути суб'єктом права, оскільки він бере участь в *реалізації* суспільних відносин як сторона цих відносин.

Прихильники першої концепції принципово не допускають можливості виконання роботами із ШІ ролі суб'єктів суспільних відносин, оскільки вони вважають, що:

– недосконаліть сучасного рівня розвитку технологій ШІ не дозволяє визнати їх самостійними суб'єктами права [32];

– досі існують хибні уявлення, засновані на помилковій думці про те, що втілення ШІ має якості юридичної особи [19];

– на сучасному науковому етапі штучно розумна істота не може вважатися суб'єктом права під страхом характеристики інструменталізму [11].

Прихильники другої концепції, які підтримують ідею визнання робота із ШІ учасником суспільних відносин, а значить визнання суб'єктом права, базуються на наступних міркуваннях:

– концептуально правова система надає можливість визнання правосуб'єктності з цивільними правами штучних агентів [9];

– роботи мають можливості приймати *самостійні* рішення або іншим чином самостійно взаємодіяти з третіми особами [14];

– існує можливість виконання *автономним ШІ* різних правових ролей в певних суспільних відносинах, тобто можна констатувати гетерогенність юридичного статусу ШІ [25];

– ШІ здатний здобувати інформацію про навколишнє середовище та осмислювати її, щоб діяти *раціонально та автономно* навіть у невизначених ситуаціях [10];

– якщо системи ШІ наближаються до точки, коли вони не відрізняються від людей, вони повинні мати право на статус, порівнянний із фізичними особами [8];

– машини (штучний інтелект – *Авт*.) у своїй діяльності не страждають від невідповідності "я" самому собі [16], що якраз є бажаним для випадку правового регулювання їх застосування.

Виходячи зі змісту дискусій, можна сформулювати три гіпотези, які концентровано відображають основний зміст різних наукових підходів до оновлення або реформування систем права та законодавства з огляду на необхідність правового регулювання застосування роботів із ШІ. Це такі гіпотези:

1) *роботи є об'єктом суспільних відносин*, а значить мають бути об'єктом правовідносин;

2) *роботи є суб'єктом суспільних відносин*, а значить мають бути суб'єктом правовідносин;

3) *роботи можуть бути як об'єктом, так і суб'єктом* суспільних відносин, а значить можуть бути як об'єктом, так і суб'єктом правовідносин.

Перші дві гіпотези виглядають як альтернативні, тому між їх прихильниками точаться багаторічні жваві та безкомпромісні дискусії. Але реальне життя не може бути поділено на дві автономні частини: або чорне, або біле. Є багато проявів інших варіантів реалізації життєвих ситуацій, коли щось в одному випадку виконує роль позитивного фактору а в іншому – роль негативного. Проблема полягає в тому, що при використанні

термінів “робот” та “штучний інтелект”, не завжди береться до уваги зміст їх дефініцій. Оскільки учасники дискусій, як правило, спираються на власне уявлення змісту дефініцій цих термінів, то у більшості випадків дискусії ставали безкомпромісними.

Якщо взяти до уваги дефініції, що були обґрунтовано запропоновані в роботах [35; 36], то стає зрозумілою можливість для одного і того ж робота із ШІ виконувати свою роль як об’єкта, так і суб’єкта суспільних відносин. Основним водорозділом щодо якісного поділу ролей робота із ШІ як об’єкта або як суб’єкта є наявність або відсутність автономності його поведінки.

Отже, будемо додтримуватись третьої гіпотези та визнавати ролі робота-інструмента та робота-суб’єкта не як альтернативні, а як ситуаційні в залежності від властивостей та характеристик їх системи когнітивних функцій, локалізованих для конкретних умов та вимог їх застосування. Локалізація не потребує відповідної адаптації запропонованих дефініцій термінів “робот” та “штучний інтелект” внаслідок їх універсальності.

Таким чином, пропонуємо вважати, що робот з ШІ може виконувати роль як робота-інструмента (об’єкта), або як робота-суб’єкта в залежності від ситуаційної доцільності та ефективності їх застосування в тій чи іншій ролі.

В сучасному світі спостерігаємо випадки, кількість яких щодня наростає лавиноподібно, коли роботи із ШІ приймають участь в реалізації суспільних відносин, в яких іншою стороною є традиційні суб’єкти права. Зазвичай у такому випадку в суспільних відносинах ***робот з ШІ замінює певний тип традиційного суб’єкта – фізичну або юридичну особу.*** При заміні традиційного суб’єкта робот із ШІ має бути також незалежним та автономним у своїй поведінці. Конкретний тип традиційного суб’єкта, якого замінює робот з ШІ, визначається особливостями здійснення конкретної діяльності в умовах певної галузі соціальної активності, соціального статусу, соціальної ролі та посади.

Завдяки вражаючим когнітивним можливостям ШІ забезпечується висока ефективність реалізації суспільних відносин, яка може значно перевищувати їх ефективність, коли в них беруть участь лише традиційні суб’єкти. Такий ефект від застосування роботів з ШІ спостерігається в багатьох сферах соціальної активності, що відкриває великі перспективи для стрімкого розширення спільної соціальної діяльності традиційних суб’єктів та роботів з ШІ.

Отже, якщо учасником певних суспільних відносин, які регулюються нормами права, з однієї сторони є традиційний суб’єкт як суб’єкт права, а з іншої – робот з ШІ, то останній має бути суб’єктом права. Більш того, задля забезпечення ефективності реалізації суспільних відносин робот з ШІ має мати такі ж самі суб’єктивні права, юридичні обов’язки та відповідальність як традиційний суб’єкт, якого він замінює при здійсненні конкретної діяльності.

Протягом останніх десятиліть послідовно дедалі потужніше поширюється думка щодо необхідності створення законодавчої бази забезпечення широкого застосування технологій ШІ. Тому для сучасних умов вже актуальне наступне: справжнє питання полягає в тому, щоб визначити, як змінити закон, а не чи потрібно його змінювати [1]; законодавці повинні переглянути існуючу законодавчу базу та адаптувати її до мінливих потреб суспільства [7], потрібні оновлені дискусії, оскільки постануть нові унікальні дилеми для закону та наших суспільних цінностей [26].

Але для будь-якої зміни (вдосконалення чи навіть реформування) систем права та законодавства кардинально важливим є питання можливості визнання робота із ШІ

суб'єктом права. Для обґрунтування відповіді на це питання підведемо підсумок розуміння сучасної ситуації застосування роботів з ШІ:

– людина при здійсненні конкретної діяльності має реалізовувати певні суб'єктивні права та виконувати юридичні обов'язки, які визначаються нормами права, тобто вона є суб'єктом права;

– людина має мати систему *галузевих, спеціальних та індивідуальних* когнітивних функцій з певним нормативним рівнем розвитку необхідним та достатнім для здійснення певної конкретної діяльності;

– наявність системи *галузевих, спеціальних та індивідуальних* когнітивних функцій з певним нормативним рівнем розвитку дозволяє людині мати відповідну *галузеву, спеціальну та індивідуальну* правосуб'єктність, правоздатність, дієздатність та деліктоздатність;

– практика свідчить про те, що робот із ШІ застосовується або для заміни традиційного суб'єкту, який здійснює конкретну діяльність в умовах певної галузі соціальної активності, соціального статусу, соціальної ролі та посади, або для підвищення ефективності праці традиційного суб'єкта на певних етапах його конкретної діяльності;

– робот з ШІ при заміні традиційного суб'єкта, який здійснює певну конкретну діяльність, має мати систему *галузевих, спеціальних та індивідуальних* когнітивних функцій з певним нормативним рівнем розвитку, а також *галузеву, спеціальну та індивідуальну* правосуб'єктність, правоздатність, дієздатність та деліктоздатність такі ж самі як і традиційний суб'єкт, якого він замінює.

Важливі висновки:

– якщо робот з ШІ застосовується для підвищення ефективності праці традиційного суб'єкта на певних етапах його конкретної діяльності, то він має бути ***об'єктом правовідносин****;*

– якщо робот з ШІ застосовується для заміни традиційного суб'єкта при здійсненні конкретної діяльності, яка регулюється нормами права в умовах певної галузі соціальної активності, соціального статусу, соціальної ролі та посади, то він має бути ***суб'єктом правовідносин***.

ІІ. Визнання автономності штучного інтелекту.

В межах даного дослідження будемо розглядати поняття автономії робота із ШІ у предметно орієнтованій площині – юридичній, уникаючи зайвих як загально наукових, так і технічних аспектів цього явища.

Цивілізаційна місія цифрових трансформацій як всеохоплюючого процесу впровадження досягнень четвертої промислової революції в частині цифрових технологій, зокрема найбільш важливого та потужного засобу нейтралізації обмеження когнітивних можливостей людини – технології ШІ [37].

Отже, приходимо начебто до парадоксального висновку: задля підвищення якості життя людства інтелектуальну (когнітивну) працю людини потрібно замінити на більш ефективну інтелектуальну (когнітивну) працю ШІ. Але подібна заміна праці людей не вперше відбувається в історії людства. Досить згадати появу плугу, станків, автомобілів, тракторів, екскаваторів і багато, багато іншого, що дозволило замінити обмежену за можливостями фізичну працю людей на більш ефективну працю механізмів. Зрозуміло, що використання ШІ не може бути беззаперечним, воно має бути обґрунтовано доцільністю, раціональністю та ефективністю заміни когнітивної праці людини. Таке обґрунтування має враховувати особливості когнітивної праці при здійсненні тієї чи іншої конкретної діяльності.

До основних особливостей Homo sapiens відноситься можливість самостійного, незалежного від інших, прийняття рішень як результату функціонування системи когнітивних функцій мозку. Самостійність та незалежність прийняття рішень, усвідомлення наслідків реалізації прийнятих рішень, розуміння впливу реалізації рішень на власне майбутнє та майбутнє інших мають абсолютне значення для визнання автономності людини як суб'єкта права. В юридичній конотації все це охоплюється такою правовою категорією як дієздатність.

Існує думка, що автономного суб'єкта чи агента як такого не існує, автономія швидше повинна розглядатися як результат відносин, які уможливлюють автономні процеси [3]. На перший погляд, це заперечує можливість як людини, так і робота із ШІ мати таку властивість як автономність. Дійсно, на прийняття рішень традиційним суб'єктом відносно певних ситуацій або процесів впливає поведінка інших суб'єктів, дотичних до цих процесів. Також на зміст рішень, що приймаються, впливають: стан оточуючого середовища (політичного, соціального, економічного, бізнесового, наукового, громадського тощо), який є результатом діяльності певної спільноти людей; думки різноманітних експертів та суспільних авторитетів; зміст продукції ЗМІ тощо. Тобто уявляється, що в умовах сучасного взаємопов'язаного та взаємообумовленого світу при прийнятті рішень не може бути повної, абсолютної автономності людей.

Насправді все відбувається не зовсім так прямолінійно. В реальності, ***людина завжди отримує зовнішню інформацію*** про ситуації, процеси, поведінку інших, стан оточуючого середовища, думки тощо. В подальшому, внаслідок реалізації метакогнітивного процесу за певними алгоритмами ***людина обробляє необхідну зовнішню та внутрішню інформацію, яка зберігається у мозку людини,*** з врахуванням мети, цінностей та особистих обставин життєдіяльності людини. Результатом обробки інформації є зміст рішення або декількох варіантів рішення, яке приймає людина. Багатоваріантне рішення буде потребувати додаткового етапу обробки інформації, можливо із залученням додаткової інформації та знань, задля обрання найкращого варіанту.

Отже, приходимо до наступного висновку: зміст зовнішньої інформації дійсно формується за участю та під впливом інших людей, але її обробка поряд з обробкою внутрішньої інформації, тобто формування змісту рішення відбувається завдяки індивідуальному та автономному метакогнітивному процесу мозку людини.

Таким чином, ***автономність людини*** *– це здатність до самостійного отримання та оброблення інформації, усвідомленого прийняття рішень та їх реалізації, здійснення певних дії або діяльності для досягнення заданої цілі.*

Власне така властивість людини як автономність є базовою ознакою її дієздатності. З врахуванням думки різних вчених [39 – 44], запропонуємо наступне визначення: ***дієздатність –*** *це реальна персоніфікована здатність суб'єкта правовідносин своїми діями усвідомлено та самостійно (автономно) реалізовувати суб'єктивні права та виконувати юридичні обов'язки.*

У звіті COMEST серед основних властивостей робота зазначається автономність, в сенсі здатності "думати" для себе і приймати власні рішення для впливу на навколишнє середовище, без прямого зовнішнього контролю [33]. Автономність робота із ШІ передбачає, що він буде навчатись з минулого досвіду, самостійно модифікувати свої алгоритми, тому їх поведінка не буде цілком передбачуваною.

Автономні системи (роботи із ШІ – *Авт.*) відіграватимуть важливу роль у багатьох додатках у різноманітних сферах, включаючи космічну, морську, повітряну, польову, дорожню та сервісну робототехніку [20]. Роботи із ШІ потенційно можуть надати багато

економічних переваг, наприклад, для гірничодобувної промисловості завдяки зниженню витрат, ефективності та підвищенню продуктивності, зменшення впливу небезпечних умов на працівників, безперервного виробництва та підвищення безпеки [17]. З іншого боку, автономні системи дозволять споживачам зменшити або навіть зовсім не витрачати зусиль щодо вибору певного товару або послуги [2].

Існує безліч підходів для розуміння природи автономних систем та рівня їхньої автономії – від самих широких філософських поглядів на автономність людини до вузькоспеціалізованих проявів автономності окремих технічних систем [15]. Проте, не вистачає чіткої таксономії автономних систем та чіткого набору офіційних визначень, наприклад, військової автономії [13].

Стверджується, що вільне та різноманітне використання терміну "автономний" у робототехніці фактично позбавило цю галузь важливої концепції, яка, по суті, така ж, як ми знаходимо її в біології, філософії, етиці та праві [31]. Сутність цієї концепції полягає в принциповій можливості людини самостійно та усвідомлено діяти і реалізовувати свої наміри. Фактично, ця концепція є підґрунтям одного з базових положень юриспруденції – визначення дієздатності фізичної особи.

Таким чином, вирішення проблеми визначення автономності має важливе значення для вирішення як загальної проблеми регулювання застосування робота із ШІ, так і окремої проблеми визначення його правового статусу.

Наведемо найбільш типові варіанти визначень автономного робота із ШІ як такого, що:

– може відчувати світ і вибирати дію, специфічну для свого поточного контексту [4];

– здатен приймати рішення та реалізовувати їх у зовнішньому світі незалежно від зовнішнього контролю чи впливу [14];

– здатен приймати рішення в реальному часі в непередбачуваних умовах для виконання поставленого завдання, призначеного людиною, та адаптуватися до навколишнього середовища [18].

Звертають увагу на те, що правове становище ШІ залежить від певних аспектів його автономності від людини, наприклад, таких як наявність [25]: суб'єктності (у тому числі – автономність як інтелектуального агенту); самореферентності у самонавчанні, самостійності у прийнятті рішень; когнітивної та адаптаційної автономності; просторово-кінетичної автономності.

Звідси випливає, що найбільш важливими властивостями для забезпечення автономності робота із ШІ в умовах невизначеності є самостійність (незалежність від людей): сприйняття та оброблення інформації про оточуюче середовище, прийняття та реалізація рішень, самонавчання, адаптування до змін, просторово-кінетичне переміщення об'єктів у просторі, досягнення заданої цілі тощо.

В подальшому будемо спиратись на визначення, яке було обґрунтовано раніше [38]: ***автономність робота з ШІ*** *– це здатність в умовах невизначеності до самостійного без участі людини оброблення інформації, прийняття рішень та їх реалізації, здійснення певних дії або діяльності для досягнення заданої цілі.*

Міністерство транспорту США визначає шість рівнів автоматизації робомобілей, починаючи від відсутності автоматизації водіння (рівень 0) до повної автоматизації водіння (рівень 5) [27]. В даному випадку термін автоматизація, що означає заміну людини як водія на автоматичний пристрій (робот з ШІ), виступає синонімом терміну "автономність". Від рівня автоматизації залежить рівень автономності робота з ШІ. З огляду на це, можна передбачити, що особливості правового регулювання

застосування робота з ШІ будуть залежати від рівня автономності інформаційного перетворення, прийняття рішень та їх реалізації.

Європарламент звертає увагу на те, що бажано визначити статус найскладніших *автономних* роботів як електронних осіб у випадках, коли роботи прийматимуть самостійні рішення чи іншим чином самостійно будуть взаємодіяти з третіми особами [14]. Оскільки закони, які б враховували автономність, ще не прийняті, то ця невизначеність створює бар'єри на шляху просування в реальне життя широкого спектру ефективних роботів з ШІ [23].

Дехто висловлює впевненість, що поява автономних роботів з ШІ, які є незалежними від людей, не тільки малоймовірна, але ймовірно небажана [29]. В той же час, інноваційне підвищення ефективності робота із ШІ, зокрема, завдяки застосуванню у майбутньому квантових комп'ютерів чи використанню покращених алгоритмів глибокого навчання, відкриває гарні перспективи щодо забезпечення режиму реальної автономності роботів. Роботів з реальною автономністю з нетерпінням очікують в багатьох сферах соціальної активності, наприклад, в медицині [23]. Але в цьому випадку, необхідно проводити ретельні наукові розвідки щодо юридичних наслідків збільшення автономності роботів з ШІ.

Таким чином, широке використання можливостей феномену автономності обмежується невирішеністю певних правових проблем, наприклад, проблем визначення правового статусу автономного робота із ШІ, встановлення співвідношення між рівнем автономності та рівнем дієздатності суб'єкта права, захисту прав споживачів, визначення відповідальності тощо.

Важливі висновки:

– автономність традиційного суб'єкта є необхідною умовою реалізації ним суб'єктивних прав та виконання юридичних обов'язків в процесі здійснення конкретної діяльності;

– автономність робота із ШІ є необхідною умовою для заміни традиційного суб'єкта в конкретній діяльності.

ІІІ. Про пріоритетність застосування універсального чи спеціалізованого робота із ШІ.

В сучасному світі наростають випадки, кількість яких щодня збільшується, коли роботи із ШІ беруть участь в реалізації суспільних відносин, в яких іншою стороною є традиційні суб'єкти. Йдеться про звичайні суспільні відносини, але в яких традиційний суб'єкт (фізична або юридична особа) замінюється на робота з ШІ.

Оскільки, робот із ШІ має еквівалентно замінювати певний традиційний суб'єкт, який здійснює конкретну діяльність в умовах певної галузі соціальної активності, соціального статусу, соціальної ролі та посади, то він має бути здатним в конкретних правовідносинах:

– здійснювати конкретну діяльність еквівалентно тому як її має здійснювати традиційний суб'єкт;

– здійснювати конкретну діяльність автономно та незалежно;

– реалізовувати суб'єктивні права та виконувати юридичні обов'язки еквівалентно тому як це має здійснювати традиційний суб'єкт;

– виконувати загальні вимоги законодавства, які є дотичними до цих правовідносин, еквівалентно тому як їх має виконувати традиційний суб'єкт.

Отже, якщо учасником правовідносин з однієї сторони є традиційний суб'єкт як суб'єкт права, а з іншої – робот з ШІ, то останній має бути суб'єктом права. Задля забезпечення ефективності реалізації правовідносин робот з ШІ має мати такі ж самі

суб'єктивні права, юридичні обов'язки та відповідальність як традиційний суб'єкт, якого він замінив при здійсненні конкретної діяльності.

Основний методологічний недолік багатьох сучасних правових досліджень полягає в тому, що апріорі робот з ШІ сприймається як цілісна та закінчена універсальна даність за аналогією з людиною. Багато суддів розуміли поняття "робот" як певну аналогію людини, маючи на увазі їх зовнішню схожість [6]. Таке сприйняття базується на популярній *концепції людиноподібності робота із ШІ*, яка, вочевидь, отримала поширення з одного боку завдяки багаточисельним футуристичним бестселерам, а з іншого – завдяки недостатності ґрунтовних знань щодо принципів, закономірностей та особливостей проектування, створення, впровадження, експлуатації та застосування ШІ.

Відповідно до *концепції людиноподібності роботів з ШІ* уявляється, що всі без виключення роботи мають бути або роботом-андроїдом, або з певного етапу розвитку науки та техніки – андроїдом, які у всьому подібні (аналогічні) людині [35]. При цьому вважається, що для будь-яких випадків застосування властивості та показники системи когнітивних функцій, а також фізичні характеристики виконавчих пристроїв роботів з ШІ є *універсальними (однаковими*).

Тобто йдеться про стратегію застосування так званого ***універсального робота із ШІ як еквівалентної заміни людини при здійсненні будь-якої конкретної діяльності в будь-якої галузі соціальної активності***. Універсальність означає, що будь-який робот з ШІ, як і будь-яка людина, має можливість здійснювати будь-яку діяльність в будь-який час, а також те, що для будь-яких видів та типів роботів з ШІ показники їх інтелектуальних властивостей є універсальними.

Отже, ***універсальний робот з ШІ*** *– це робот з ШІ із певним нормативним рівнем розвитку системи когнітивних функцій та опорно-рухової виконавчої системи, який є необхідним та достатнім для здійснення будь яких видів та типів діяльності в умовах будь-якої галузі соціальної активності, соціальної роли, соціального статусу та посади.*

В дійсності, стратегія застосування універсального робота із ШІ має значні недоліки.

По-перше, створення "універсального" робота із ШІ представляє собою надскладне завдання для великої спільноти фахівців з різних областей науки та практики, виконання якого можна очікувати протягом довгих десятиліть. В той же час, мотивація продовження цієї складної роботи очевидна. Вважається, що завдяки вражаючим когнітивним можливостям ШІ забезпечується висока ефективність його діяльності, яка може значно перевищувати ефективність діяльності традиційних суб'єктів. Тому у майбутньому очікується великий синергетичний ефект від застосування універсальних роботів з ШІ в багатьох сферах соціальної активності, що відкриває великі економічні та інші перспективи для покращення якості життя землян.

По-друге, ми є свідками того, що протягом відносно невеличкого відрізку часу процес розвитку роботів із ШІ практично має поступово повторити процес еволюційного розвитку Homo sapiens. Причиною поступовості є обмеження можливостей науки та техніки щодо потенційного наближення властивостей та показників як системи когнітивних функцій, так і виконавчих пристроїв робота із ШІ до персоніфікованих інтелектуальних та фізичних можливостей людини.

Йдеться про природній поступовий процес збільшення розуміння, поглиблення та накопичення знань про: принципи та закономірності нейробіологічних алгоритмів функціонування мозку людини; особливості реалізації окремих когнітивних функцій мозку; якісні та кількісні характеристики реалізації простих, складних та метакогнітивних функцій, а також методи та способи їх спостереження і вимірювання; розуміння ролі та

взаємовпливу окремих когнітивних функцій мозку, зокрема таких як емоції, почуття гідності, свідомість, розуміння, усвідомлення та самоусвідомлення в процесі детермінації поведінки людини тощо. Всі ці знання є необхідними для максимально ідентичного модулювання процесу розвитку та функціонування інтелекту людини, що є вкрай важливим для виконання завдання щодо створення "універсального" робота із ШІ.

По-третє, реалізація процесу моделювання функціонування інтелекту як повної сукупності когнітивних функцій людини суттєвим чином залежить від рівня розвитку науки, техніки та технологій. Йдеться насамперед, про математичні методи обробки Великих Даних, програмування, машинного навчання, про комп'ютерну техніку, телекомунікації, робототехніку, електроннику, мікроелектроніку, механіку, мікромініатюризацію виконавчих пристроїв тощо.

По-четверте, можна стверджувати, що можливості окремих зразків робота із ШІ лише поступово наближаються до персоніфікованих інтелектуальних та фізичних можливостей людини. Йдеться про персоніфіковані можливості людини, які є необхідними для здійснення конкретної діяльності в умовах певної галузі соціальної активності, її соціального статусу, соціальної ролі та посади.

Саме тому, як в сучасних умовах, так і протягом майбутніх десятиліть мейнстрімом буде застосування так званого *спеціалізованого робота із ШІ* для заміни традиційного суб'єкта, який здійснює конкретну діяльність. Здійснення конкретної діяльності обумовлює необхідність для традиційного суб'єкта мати лише конкретні персоніфіковані інтелектуальні та фізичні можливості відповідно до конкретної галузі соціальної активності, соціального статусу, соціальної ролі та посади.

Визнання к*онцепції людиноподібності робота із ШІ* зумовлює впевненість в тому, що універсальний робот з ШІ з можливостями, аналогічними універсальним можливостям людини, потенційно здатний здійснювати будь-яку діяльність.

Постає питання: чи потрібно на практиці, щоб кожен робот з ШІ був універсальним при заміні традиційних суб'єктів, які здійснюють конкретну діяльність? Кожна людина, яка здійснює конкретну діяльність, має мати релевантну саме цій діяльності конкретну систему *загальних, галузевих, спеціальних та індивідуальних* когнітивних функцій з певним нормативним рівнем розвитку. Штучний інтелект, робота із ШІ має імітувати лише конкретну персоніфіковану систему когнітивних функцій відповідного традиційного суб'єкта, якого він замінює при здійсненні конкретної діяльності. Тобто маємо однозначну відповідь: робот з ШІ при заміні традиційного суб'єкта, який здійснює конкретну діяльність, не має бути універсальним, оскільки останній має таку систему когнітивних функцій, зміст та обсяг наявних знань, навичок, вмінь та досвіду які набагато перевершують потреби необхідні для здійснення конкретної діяльності.

Отже, стає цілком очевидною хибність стратегії заміни традиційного суб'єкта при здійсненні конкретної діяльності на універсального робота із ШІ, який би мав можливість реалізовувати всю безмежну різноманітність діяльності, праці та суспільних відносин.

Крім того, зроблений висновок підтверджується наступними важливими міркуваннями економічного плану.

По-перше, у випадку застосування універсального робота із ШІ виникає необхідність завантаження до нього неосяжного обсягу знань, навичок, вмінь та досвіду дотичних до всіх можливих випадків його застосування, а також необхідність його озброєння універсальними виконавчими пристроями, які забезпечать здійснення будь-якого виду та типу діяльності. Все це потребує значних техніко-технологічних ресурсів, а значить – значних економічних витрат як в процесі створення, так і в процесі експлуатації універсального робота із ШІ.

По-друге, стратегія створення універсального робота є надзвичайною економічно неефективною. Це пояснюється тим, що левова частка наявних ресурсів, потужностей та можливостей універсального робота не буде використана в процесі заміни традиційного суб'єкта, який здійснює конкретну діяльність. Дійсно, вельми абсурдною виглядає пропозиція використати універсальний робот з ШІ для заміни продавця продовольчими товарами або портьє в готелі тощо. Тобто впровадження стратегії застосування універсального робота із ШІ для заміни традиційного суб'єкта, який здійсню конкретну діяльність, закономірно породжує нерозв'язну проблему повернення інвестицій.

По-третє, для здійснення конкретної діяльності у випадку спеціалізованого робота із ШІ можна застосувати набагато більше техніко-технологічних ресурсів ніж у випадку універсального робота із ШІ.

Висновок: будь-який спеціалізований робот з ШІ завжди буде мати набагато кращі показники якості здійснення конкретної діяльності, ніж універсальний робот з ШІ. Справедливість цього висновку підтверджується характерною особливістю розвитку цивілізації, яка полягає в тому, що діалектично суспільна та індивідуальна діяльність традиційних суб'єктів закономірно розвивалася шляхом постійного розширення та поглиблення спеціалізації.

Таким чином, при заміні традиційного суб'єкта робот з ШІ має бути не універсальним, а *спеціалізованим роботом з ШІ*, наявні ресурси, потужності та можливості якого є повністю релевантними до умов здійснення конкретної діяльності.

Робот із ШІ будемо називати спеціалізованим, якщо він буде застосуватись для заміни традиційного суб'єкта, який здійснює конкретну діяльність. Отже, ***спеціалізований робот з ШІ –*** *це робот з ШІ із певним рівнем розвитку спеціалізованого набору когнітивних функцій та спеціалізованої опорно-рухової системи, який є необхідним та достатнім для здійснення конкретної діяльності.*

Для конкретних типів діяльності в умовах конкретної галузі соціальної активності, соціального статусу, соціальної ролі та посади спеціалізованому роботу із ШІ необхідно буде "опанувати" набагато менший обсяг необхідних знань, навичок, вмінь та досвіду ніж у випадку універсального робота. Це означає значну економію необхідних організаційних, трудових, фінансових, виробничих, інтелектуальних та матеріальних ресурсів, які мають бути витрачені для заміни традиційного суб'єкта на робота із ШІ при здійсненні конкретної діяльності. Саме тому сучасна практика впровадження повсюдно сконцентрована на точковій заміні традиційного суб'єкта на спеціалізованого робота із ШІ, що дозволяє зробити процес їх створення значно ефективнішим, економічним, простішим та швидшим.

Так наприклад, у 2022 – 2023 роках відбувається бум розроблення та масового використання універсальних систем ШІ як генеративних, так і на основі великих мовних моделей. Але вже наприкінці 2023 року практично всі великі розробники такі як OpenAI, Google, Anthropic, DeepMind тощо, а також всі маленькі компанії та стартапи зосередили зусилля на створенні предметно-орієнтованих (спеціалізованих) систем ШІ [30]. Предметна орієнтація полягає в тому, що створюються чат-боти, які спрямовані на певну спеціалізовану роботу із конкретними видами тексту, зображення, малюнками, відео, об'єктами тощо.

З огляду на значні проблеми економічного, організаційного, технологічного, безпекового та юридичного характеру виявляється слушним визнати раціональність стратегії створення та впровадження *спеціалізованих роботів з ШІ*, орієнтованих на заміну конкретних традиційних суб'єктів в конкретних типах діяльності та робочих місць. Відповідно проблема визначення правового статусу роботів з ШІ має

вирішуватись за принципом від простого до складного, від одиничного до загального для кожного виду і типу варіативної частини правосуб'єктності (правоздатності та дієздатності) певних типів традиційних суб'єктів. У такому випадку, задля забезпечення ефективності реалізації суспільних відносин обсяг та зміст правосуб'єктності, правоздатності, дієздатності та деліктоздатності спеціалізованого робота з ШІ не має мати ніяких відмінностей від правосуб'єктності правоздатності, дієздатності та деліктоздатності традиційних суб'єктів (суб'єктів права), яких він замінює.

Таким чином, пропонуємо один з основних принципів, який маємо покласти в основу *загальної концепції визначення правового статусу робота із ШІ*: ***заміна традиційного суб'єкта в правовідносинах має відбуватись завдяки застосуванню лише спеціалізованого робота із ШІ.***

У такому випадку, при здійсненні правових досліджень завжди бажано уявляти спеціалізованого робота із ШІ, як такого, що має такі ж самі персоніфіковані показники рівня розвитку системи когнітивних функцій та обсяг суб'єктивних прав, юридичних обов'язків і відповідальності, які має традиційний суб'єкт, якого він замінює в межах конкретної діяльності.

Сутність цього принципу полягає в тому, що в подальшому завжди будемо розглядати застосування робота як заміну традиційного суб'єкта, який є учасником конкретних правовідносин. У такому випадку природно залишаємо за межами правової науки дослідження причин, які обумовлюють необхідність заміни традиційного суб'єкта. Це пояснюється тим, що дослідження таких причини є предметом інших наукових дисциплін, більш того, вони за своєю природою є різноманітними, багатофакторними та локалізованими для конкретних видів і типів діяльності традиційних суб'єктів.

Доречно зауважити, що заміна одного суб'єкта іншим при реалізації певних суспільних відносин є рутинним явищем в житті суспільства. Одні політики змінюють інших на посаді президента, міністра або голови парламенту, одні фахівці замінюють інших на посаді вчителя, лікаря, на робочому місці водія трамвая, продавця, будівельника тощо. Всі ці заміни суб'єктів в межах певних соціальних ролей, соціальних статусів та посад в ідеалі мають безшовними, тобто відбуватись без перепон. Безшовна заміна означає заміну без погіршення показників ефективності та результативності сумісної діяльності суб'єктів, що забезпечується завдяки наявності відповідної сукупності норм права, суб'єктивних прав та юридичних обов'язків, які детермінують їх поведінку.

Важливі висновки:

– *в умовах здійснення конкретної діяльності застосування спеціалізованого робота із ШІ є набагато ефективнішим ніж застосування універсального робота із ШІ;*

– *в умовах здійснення конкретної діяльності традиційний суб'єкт може бути замінений лише на спеціалізованого робота із ШІ як робота-суб'єкта;*

– *спеціалізований робот з ШІ має мати такі ж самі суб'єктивні права, юридичні обов'язки та відповідальність як традиційний суб'єкт, якого він замінює.*

Використана література

1. Allen, Tom, and Robin Widdison. 1996. Can computers make contracts. *Harv. JL & Tech.* 9: 25.

2. André, Q. at el. 2018. Consumer choice and autonomy in the age of artificial intelligence and big data. *Customer needs and solutions.* 5: 28-37.

3. Bächle, T.C. 2023. The age of machine autonomy? Digital society blog. URL: https://www.hiig. De/publication/the-age-of-machine-autonomy/3

4. Bryson, J. and A. Winfield, 2017. Standardizing Ethical Design for Artificial Intelligence and Autonomous Systems. *Computer.* 50(5): 116-119.

5. Busemeyer, J. et al. 2019. Cognitive and Neural Bases of Multi-Attribute, Multi-Alternative, Value-based Decisions. *Trends in Cognitive Sciences.* 23: 251-263.

6. Calo, Ryan. 2016. Robots as legal metaphors. *Harvard Journal of Law & Technology*. 30 (1): 209-237.

7. Čerka, Paulius, Jurgita Grigienė and Gintarė Sirbikytė. 2015. Liability for damages caused by artificial intelligence. *Comput. Law Secur*. Rev. 31: 376-389.

8. Chesterman, S. 2020. Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly.* 69(4): 819-844.

9. Chopra, Samir, and Laurence White. 2004. Artificial agents-personhood in law and philosophy. *ECAI.* 16.

10. Cugurullo, F. 2020. Urban artificial intelligence: From automation to autonomy in the smart city. *Frontiers in Sustainable Cities.* 2: 38.

11. Divino, S. and R. Magalhães. 2021. What is it like to be an artificial intelligence? Nagel's view from nowhere and artificial intelligence as subject of law. *Direito Público.* 18.100.

12. Dresler, M. et al. 2019. Hacking the Brain: Dimensions of Cognitive Enhancement. *ACS Chemical Neuroscience.* 10: 1137-48.

13. Edmonds, Jeffrey at el. 2021. *Artificial Intelligence and Autonomy*. Center for Naval Analyses.

14. European Parliament. 2017. Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. 16 February.

15. Formosa, Paul. 2021. Robot autonomy vs. human autonomy: Social robots, artificial intelligence (AI), and the nature of autonomy. *Minds and Machines.* 31.4: 595-616.

16. Hildebrandt, M. 2020. The Artificial Intelligence of European Union Law. *German Law Journal.* 21(1): 74-79.

17. Hyder, Z., Siau, K., and F. Nah. 2019. Artificial intelligence, machine learning, and autonomous technologies in mining industry. *Journal of Database Management (JDM)*, 30(2): 67-79.

18. Karnow, Curtis EA. 2016. The application of traditional tort theory to embodied machine intelligence. *Robot Law*. 51-77.

19. Kemp, R. 2021. Legal Aspects of Artificial Intelligence (v. 3.0).

20. Kunze, L at el. 2018. Artificial Intelligence for Long-Term Robot Autonomy: A Survey. *IEEE Robotics and Automation Letters*. 3 (4): 4023-4030.

21. Laureiro-Martínez, D, Brusoni, S. 2018. Cognitive flexibility and adaptive decision-making: Evidence from a laboratory study of expert decision makers. *Strat Mgmt J*. 39:1031-1058.

22. Merendino, A. et al. 2018. Big Data, big decisions: The impact of big data on board level decision-making. *Journal of Business Research.* 93: 67-78.

23. Mezrich, J.L. 2022. Is artificial intelligence (AI) a pipe dream? Why legal issues present significant hurdles to AI autonomy. *American Journal of Roentgenology*. 219(1): 152-156.

24. Okoli, J. and Watt, J. 2018. Crisis decision-making: the overlap between intuitive and analytical strategies. *Management Decision.* 56(5): 1122-1134.

25. Ponkin, I. and A. Redkina. 2018. Artificial Intelligence from the Point of View of Law. *Vestnik Rossiiskogo universiteta druzhby narodov*. 22 (1): 91-109.

26. Rodrigues, Rowena. 2020. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology.* 4.

27. Sae International. 2018. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *SAE international.* 4970(724): 1-5.

28. Sahu, A, R. Padhy and A. Dhir. 2020. Envisioning the Future of Behavioral Decision-Making: A Systematic Literature Review of Behavioral Reasoning Theory. *Australasian Marketing Journal.* 28: 145-159.

29. Sawyer, B. D. at el. 2021. Human factors and ergonomics in design of a 3: automation, autonomy, and artificial intelligence. *Handbook of human factors and ergonomics.* 1385-1416.

30. Shelby Hiter. 2023a. What Is a Large Language Model? *eWeek*, June 6, 2023. URL: https://www.eweek.com/artificial-intelligence/large-language-model

31. Smithers, T. 1997. Autonomy in Robots and Other Agents. *Brain and Cognition.* 34: 88-106.

32. Surden, Harry. 2019. Artificial intelligence and law: An overview. *Georgia State University Law Review.* 35: 19-22.

33. UNESCO. 2017. Report of COMEST on robotics ethics. World Commission on the Ethics of Scientific Knowledge and Technology.

34. Van R. et al. 2022. AI Watch – National strategies on Artificial Intelligence: A European perspective. European Union / OECD.

35. Баранов О. 2018. Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом. *Інформація і право*. 4: 46-70.

36. Баранов О. 2023. Визначення терміну "штучний інтелект. *Інформація і право*. 1: 32-49.

37. Баранов О. 2023. Цивілізаційна місія цифрових трансформацій. *Інформація і право*. 3(46): 25-41.

38. Баранов О.А. 2022. Трансформація: соціальна & цифрова & правова: монографія. Т. 1. Порятунок цивілізації: економіка результату. Видавничий дім "Гельветика".

39. Гусарєв С. Та інші. 2017. Теорія держави та права. Освіта України.

40. Зайчук, О., Оніщенко Н. 2006. Теорія держави і права. Юрінком Інтер.

41. Козюбра М. та інші. 2015. Загальна теорія права. Ваіте.

42. Підопригора О.А., Харитонов Є.О. 2009. Римське право. Юрінком Інтер.

43. Скакун О. Ф. 2014. Теорія права і держави. Алерта.

44. Цвік М. та інші. 2009. Загальна теорія держави і права. Право.

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

УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор,* професор НА СБ України.
ORCID: https://orcid.org/0000-0003-0069-3727.

ВПЛИВ МІЖНАРОДНИХ ПРОЦЕСІВ РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА ІНФОРМАЦІЙНЕ ПРАВО УКРАЇНИ

Анотація. *У статті здійснено аналіз впливу міжнародних процесів регулювання штучного інтелекту на інформаційне право України. Відзначено, що принципи регулювання штучного інтелекту мають знайти відображення у інформаційному праві України. З огляду на документи ООН, G7, ЄС, США, Китаю зроблено висновок що процес розробки уніфікованого міжнародного регулювання ШІ є складним й імовірно триватиме роками, оскільки деякі країни виступають за розробку всеосяжної міжнародної конвенції, інші вважають, що це призведе до надмірного регулювання і зашкодить інноваціям. На підставі аналізу існуючого законодавства в Україні (Концепція розвитку штучного інтелекту в Україні, План заходів з реалізації Концепції розвитку ШІ в Україні на 2021 – 2024 роки) зроблено висновок, що воно не повною мірою відображає світові тенденції регулювання ШІ. Україна має долучатися до світової практики запровадження етичних правил і правового регулювання використання ШІ з метою захисту прав людини, забезпечення безпеки ШІ-систем, прозорості для громадськості їх створення, підзвітності розробників. Запропоновано розробити проект Закону України "Про створення і використання штучного інтелекту в Україні", а також розпочати науково-практичну дискусію щодо створення уповноваженого державного органу/комісії з контролю і нагляду за використанням ШІ в Україні. У новому законодавстві України щодо ШІ варто врахувати досвід ЄС та США, а також відповідно до Кодексу поведінки для організацій із розробки передових систем ШІ, врегулювати питання використання різноманітних заходів внутрішнього та незалежного зовнішнього тестування ШІ, публічного повідомлення про можливості, обмеження та сфери належного і неналежного використання систем ШІ, обміну інформацією та звітуванням про інциденти серед організацій, що розробляють системи ШІ тощо.*

Ключові слова*: штучний інтелект, інформаційне право, міжнародне регулювання, персональні дані, кібербезпека.*

Summary. *The article is devoted to the international regulation on artificial intelligence influence on the Information Law of Ukraine. It was noted that the principles of regulation of artificial intelligence should be reflected in the Information Law of Ukraine. Based on the documents of the UN, G7, EU, USA, China, it was concluded that the process of developing a unified international regulation of AI is complex and will probably last for years, as some countries are in favor of developing a comprehensive international convention, while others believe that this will lead to excessive regulation and harm innovations. Based on the analysis of the existing legislation in Ukraine (Concept for the Development of Artificial Intelligence in Ukraine, Action Plan for the Implementation of the Concept for the Development of AI in Ukraine for 2021 – 2024), it was concluded that it does not fully reflect global trends in AI regulation. Ukraine should join the global practice of introducing ethical rules and legal regulation of the use of AI in order to protect human rights, ensure the safety of AI systems, transparency for the public, accountability of developers. The new legislation of Ukraine on AI should take into account the experience of the EU and the USA, as well as, in accordance with the Code of Conduct for organizations developing advanced AI systems, regulate the use of various measures of internal and independent external testing of AI, public notification of opportunities, limitations and areas of proper and improper use of AI systems, information sharing and incident reporting among organizations developing AI systems, etc.*

Keywords*: artificial intelligence, Information Law, international regulation, personal data, cybersecurity.*

Постановка проблеми. Правові механізми використання штучного інтелекту (далі – ШІ) поступово розробляються в Україні та інших державах світу. ШІ має широкий спектр застосувань в економіці [1] та соціумі [2]. ШІ використовується і буде використовуватися для автоматизації завдань, які в даний час виконуються людьми, наприклад, обробка даних, обслуговування клієнтів і виробництво; розробка нових продуктів і послуг, наприклад, для розробки самокерованих автомобілів та медичних діагностичних систем; управління ризиками, наприклад, ризиками кредиту, ланцюгів поставок і ризиками кібератак, розробки нових методів лікування, а також для діагностики та прогнозування захворювань, персоналізації навчання, а також для створення нових навчальних матеріалів тощо. За данимидосліджень до 2030 року ШІ може додати до світової економіки до $15,7 трильйона США [3].

Фактичне використання в Україні програм ШІ, які нерідко несуть ризики для персональних даних, захисту інших видів інформації з обмеженим доступом, а також для інших конституційних прав громадян, вимагає аналізу теоретико-правових основ міжнародного регулювання ШІ та його впливу на інформаційне право України.

Результати аналізу наукових публікацій свідчать про те, що подібні питання регулювання нових інформаційних технологій були предметом досліджень багатьох українських учених, а саме В.В. Остроухова, В.М. Панченко, С.Г. Петрова, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, Т.Ю.Ткачука, О.М. Юрченка та інших.

Зарубіжними вченими досліджуються питання меж регулювання ШІ [4]. Останніми роками проблемамШІ приділяли увагу дослідники з огляду на розробку відповідних механізмів в ЄС [5], Китаї [6], а також з точки зору мінімізації ризиків для прав громадян [7; 8].

Однак у цілому питання впливу міжнародних процесів регулювання ШІ на інформаційне право Українибуло предметом наукових досліджень лише фрагментарно.

Метою статті є розкриття впливу міжнародних процесів регулювання штучного інтелекту на інформаційне право України.

Виклад основного матеріалу. Законодавство України визначає ШІ так: організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [9].

У сучасних комп’ютерних науках існує багато підходів до визначення ШІ. У цій роботі будемо використовувати таке визначення поняття ШІ – це системи, які створені для навчання на досвіді, розпізнавання закономірностей і прийняття рішень на основі аналізунавколишнього середовища та здійснення дій з певним ступенем автономності для досягнення конкретних цілей, які зазвичай потребують людського інтелекту.

Існуючі сучасні системи ШІ можуть бути суто програмними, які діють у віртуальному світі (наприклад, голосові помічники, програмне забезпечення для аналізу зображень, пошукові програми, системи розпізнавання мови та обличчя), або вбудованими в апаратні пристрої (наприклад, роботи, автономні автомобілі, дрони або програми Інтернету речей).

На 2023 рік, за даними багатьох рейтингів, державами-лідерами розвитку і використання ШІ є США і Китай. Відповідно до Звіту про цифрову економіку 2021 р. Конференції ООН з торгівлі та розвитку [10], на США і Китай разом припадає 94 % всього фінансування стартапів ШІ за останні п’ять років, 70 % найкращих світових

дослідників ШІ та майже 90 % ринкової капіталізації найбільших у світі цифрових платформ. Ці держави виділяються за такими показниками, як: інвестиції у дослідження і розробки ШІ, розробка і впровадження технологій ШІ, підготовка кадрів у галузі ШІ, правове і регуляторне середовище для розвитку ШІ.

Потужна наукова базав галузі ШІ, пов'язана з технологічними компаніями (Google, Microsoft, Amazon, IBM, Nvidia, OpenAI)і значними інвестиціями у дослідження і розробки у США поєднується з активнимдержавним інвестуванням у розвиток ШІ, зокрема, через програму Агентства передових оборонних дослідницьких проєктів США [11].

У Китаї уряд виділяє значні кошти на дослідження і розробки ШІ, а також створює правове і регуляторне середовище для розвитку цієї технології. П'ять китайських технологічних компаній, у тому числі BaiduInc і SenseTimeGroup 31 серпня 2023 року запустили для громадськості свої чат-боти з ШІ після отримання схвалення уряду, оскільки уряд Китаю прагне розширити використання таких чат-ботів в умовах конкуренції з США [12].

ООН має значний вплив на екосистему ШІ. Ще у 2020 році Координаційна рада керівників системи ООН (CEB) та її керівники високого рівня Комітету з програм (HLCP) створили міжвідомчу робочу групу з питань ШІ (IAWGAI), спільно очолювану ITU та ЮНЕСКО [13].

Нещодавно ООН створило спеціальну групу експертів з питань ШІ (High-Level AdvisoryBody, HLAB) для вивчення потенційних ризиків та переваг ШІ та розробки рекомендацій щодо його регулювання, перше засідання якої (групи) відбулося у жовтні 2023 року [14].

Однак, процес розробки міжнародного регулювання ШІ є складним й імовірно триватиме роками, оскільки деякі країни виступають за розробку всеосяжної міжнародної конвенції, інші вважають, що це призведе до надмірного регулювання і зашкодить інноваціям.

У 2021 році оприлюднено Рекомендації ЮНЕСКО щодо етики ШІ [15], які пропонують принципи розвитку правового регулювання ШІ для всіх країн світу. У Рекомендаціях 2023 року ЮНЕСКО наголосила на необхідності схвалення урядами навчальної програми ШІ для шкільної освіти, професійно-технічної та вищої освіти [16].

Всесвітня організація охорони здоров'я у 2021 році оприлюднила доповідь щодо ШІ в галузі охорони здоров'я, яка спрямована на використання ШІ для покращення охорони здоров'я людей [17].

Основними напрямами правового регулювання ШІ у демократичних зарубіжних державах і в ЄСє права людини на приватність, свободу слова та рівність, безпечне використання ШІ, зокрема запобігання злочинним діям та іншим негативним наслідкам використання ШІ, відповідність етичним принципам, зокрема принципу справедливості та принципу недискримінації.

ЄС працює над розробкою законодавчого регулювання ШІ. До кінця 2023 року ЄС остаточно введе в дію Акт про штучний інтелект (Artificial Intelligence Act, AI Act) [18], який визначатиме основні принципи для розробки та використання ШІ: безпечності, справедливості, підзвітності та прозорості. Варто відзначити, що Рада Європи ще у 2018 році схвалила Етичну хартію використання ШІ в судових системах і їхньому середовищі [19].

У США Національний інститут стандартів і технології (National Institute of Standards and Technology, NIST) у січні 2023 року оприлюднив Рамку управління

ризиками ШІ [20]. У 2023 році була розроблена дорожня карта для національних досліджень ШІ [21].

30 жовтня 2023 року Президент США підписав Указ про безпечний, захищений і надійний ШІ (Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, далі – Указ) [22], який встановлює нові стандарти безпеки та захисту ШІ, захищає конфіденційність громадян США, забезпечує захист їх прав, зокрема як споживачів та працівників, сприяє інноваціям та конкуренції.

Указ спрямований на гарантування домінування США в управлінні ризиками ШІ. Прийняттю Указу передувало добровільне зобов'язання 15 провідних компаній сприяти безпечному та надійному розвитку ШІ.

Указом введено серйозні адміністративно-наглядові повноваження уряду США:

вимоги до розробників найпотужніших систем ШІ ділитися результатами своїх тестів на безпеку та іншою важливою інформацією з урядом США. Компанії, які розробляють будь-яку базову модель, що становить серйозний ризик для національної безпеки, національної економічної безпеки або національної охорони здоров'я та безпеки, зобов'язані повідомляти федеральний уряд під час навчання моделі та повинні ділитися результатами всіх тестів;

Національний інститут стандартів і технологій США встановить суворі стандарти для масштабних випробувань, щоб забезпечити безпеку перед публічним випуском ШІ. Міністерства США також розглядатимуть загрози систем ШІ для критичної інфраструктури, а також ризики хімічної, біологічної, радіологічної, ядерної та кібербезпеки. Агентства, які фінансують проєкти в галузі наук про життя, встановлять стандарти як умову федерального фінансування, для забезпечення належного скринінгу та управління ризиками, пов'язаними із ШІ;

Міністерство торгівлі США розробить рекомендації щодо автентифікації контенту та нанесення водяних знаків, щоб чітко маркувати контент, створений ШІ. Федеральні агентства будуть використовувати ці інструменти, щоб американцям було легко дізнатися, що повідомлення, які вони отримують від уряду, є автентичними, і стануть прикладом для приватного сектора і урядів у всьому світі.

Вважаємо, що подібну можливість технологічно і юридично доцільно впровадити в Україні для маркування автентичних правдивих повідомлень у контексті протидії російськимдезінформаційним кампаніям.

Зазначеним Указом започатковано розробку Меморандуму про національну безпеку, який регулюватиме подальші дії щодо ШІ у сфері безпеки і буде розроблений Радою національної безпеки та керівником апарату Білого дому. Меморандум гарантуватиме, що військове та розвідувальне співтовариство США безпечно, етично та ефективно використовуватиме ШІ у своїх місіях, а також спрямовуватиме дії на протидію військовому використанню ШІ супротивниками.

Указ також спрямований на наступні ініціативи:

прийняття законодавства про конфіденційність даних громадян США, особливо дітей;

прискорення розробки та використання методів збереження конфіденційності, які дозволяють навчати системи ШІ, зберігаючи при цьому конфіденційність навчальних даних;

підсилення криптографічних інструментів збереження конфіденційності громадян;

подолання алгоритмічної дискримінації щодо розслідування порушень громадянських прав, пов'язаних з ШІ;

використання ШІ при призначенні покарання, умовно-достроковому звільненні, триманні під вартою, прогнозуванні злочинності тощо;

відповідальне використання ШІ в охороні здоров'я, наприклад для розробки ліків, та для трансформації освіти, зокрема персоналізованого навчання в школах;

пом'якшення шкоди та максимізації переваг ШІ для працівників, посилення федеральної підтримки працівників, які стикаються з перебоями в роботі, зумовленими ШІ;

пілотний проект National AI Research Resource, який надасть дослідникам ШІ і студентам доступ до ресурсів і даних ШІ, а також гранти на дослідження ШІ;

міжнародну співпрацю та правозахисну діяльність із розгортання ШІ за кордоном для вирішення глобальних проблем.

Приклади правового регулювання розробки і використання ШІ є й в інших державах. Так, Китай з 15 серпня 2023 року увів у дію Тимчасові заходищодо управління службами генеративного ШІ [23]. Парламент Франції нещодавно схвалив широкомасштабне використання відеоспостереження в реальному часі на основі ШІ як частину закону про безпеку Олімпійських ігор 2024 року [24].

На міждержавному рівні також приймаються рішення щодо регулювання ШІ. Зокрема, 30 жовтня 2023 МЗС Японії оприлюднило заяву лідерів G7 щодо Хіросімського процесу з питань ШІ[25], а вже 1-2 листопада 2023 року у Великій Британії була підписана Декларація Блечлі (The Bletchley Declaration) [26] країн-учасниць Саміту з безпеки ШІ (AI Safety Summit). Зазначимо, що Україна була однією із 29 держав-учасниць Саміту.

Кодекс поведінки для організацій з розробки передових систем ШІ [27] як частина Хіросімського процесу з ШІ передбачає такі принципи і заходи:

використання різноманітних заходів внутрішнього та незалежного зовнішнього тестування,наприклад червоні команди (red-teaming), з метою виявлення ризиків та вразливих місць. Розробники повинні прагнути забезпечити можливість відстеження щодо наборів даних, процесів і рішень, прийнятих під час розробки ШІ системи;

виявлення та пом'якшення вразливостей, а також інцидентів та моделей нецільового використання після розгортання, включаючи розміщення на ринку;

публічне повідомлення про можливості, обмеження та сфери належного і неналежного використання передових систем ШІ для забезпечення достатньої прозорості;

обмін інформацією та звітуванням про інциденти серед організацій, що розробляють передові системи ШІ, включаючи промисловість, уряди, громадянське суспільство та наукові кола;

встановлення та розкриття політики управління розробників ШІ та організаційних механізмів для реалізації цих політик відповідно до підходу, що ґрунтується на оцінці ризику;

інвестування і впровадження надійних засобів контролю безпеки, включаючи фізичну безпеку, кібербезпеку та засоби захисту від внутрішніх загроз протягом усього життєвого циклу ШІ;

розробка та розгортання надійних механізмів автентифікації вмісту та походження ШІ контенту, а також застереження користувачам, про те, що вони взаємодіють з ШІ;

інвестування в дослідження, які підтримують покращення безпеки та довіри до ШІ;

пріоритет розробці передових систем ШІ для вирішення найбільших у світі викликів, зокрема, кліматичної кризи, глобальної охорони здоров'я та освіти, цифрової грамотності;

розробка міжнародних технічних стандартів;

управління якістю введення даних і захист персональних даних та інтелектуальної власності.

Усі перелічені документи мають бути використані в Україні, де наразі відсутній спеціальний закон про ШІ. Однак, деякі правові норми, які опосередковано регулюють використання ШІ, містяться в Законі України "Про захист персональних даних", Законі України "Про авторське право і суміжні права" та Законі України "Про електронні комунікації" тощо.

У 2020 році Кабінет Міністрів України схвалив Концепцію розвитку штучного інтелекту в Україні, яка передбачає розробку та впровадження національного законодавства про ШІ. Для досягнення мети Концепції у сфері оборони, наприклад, передбачено забезпечити використання технологій ШІ у системах:

командування та управління;

озброєння та військової техніки;

збору та аналізу інформації під час ведення бойових дій;

аналізу/розвідки, підтримки проведення розвідувальних заходів, обробки картографічної інформації;

протидії кіберзагрозам у сфері оборони, що базуються на застосуванні технологій ШІ, у тому числі таких, що дозволяють швидко виявити кібератаки, попереднє сканування та наступне уникнення шкідливих кодів або сканування підозрілих моделей поведінки, а не конкретного коду;

імітаційного та когнітивного моделювання бойової обстановки;

когнітивного аналізу спроможностей військових підрозділів [9].

План заходів з реалізації Концепції розвитку ШІ в Україні на 2021 – 2024 роки, затверджений розпорядженням Кабінету Міністрів України від 12.05.21 р. № 438-р. [28] зокрема передбачає:

впровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню;

розроблення системи показників для оцінки стану інформаційної безпеки з використанням технологій ШІ тощо.

Використання ШІ має значний потенціал для відновлення України після російської війни проти України, зокрема для визначення масштабів руйнувань (аналізу супутникових знімків і даних з дронів), оцінки збитків, планування відновлення (враховуючи обмежені ресурси та нагальні потреби), реконструкції (будівництва, ремонту та очищення) тощо.

Однак, наразі існують певні ризики для України у сфері ШІ, зокрема можливості використання ШІ для порушення прав громадян України, крадіжки даних, шахрайства тощо, використання рф ШІ для поширення дезінформації, пропаганди або кібератак, залежність України від іноземних технологій, нерівномірний розподіл вигод від розробки і використання ШІ, трансформація техно-ШІ в біо- та психо-розробки.

Безумовно, Україна має долучатися до світової практики запровадження етичних правил і правового регулювання використання ШІ з метою захисту прав людини, забезпечення безпеки ШІ-систем, прозорості для громадськості їх створення, підзвітності розробників. Доцільно розпочати науково-практичну дискусію щодо створення уповноваженого державного органу/комісії з контролю і нагляду за використанням ШІ в Україні.

Зважаючи на зазначені ризики, а також з урахуванням того, що Україна може стати експортером послуг ШІ, що сприятиме створенню нових робочих місць та стимулювати

економічний розвиток, доцільно розробити проект Закону України “Про створення і використання ШІ в Україні”.

Насамкінець зазначимо, що Міжнародна академія інформації здійснює заходи іззапровадження експертного оцінювання технологій ШІ та інших ІТ програм, розроблених українськими фахівцями, на відповідність законодавству ЄС щодо ШІ з 2024 року, а також сприяння українським стартапам ШІ у виході на зарубіжні ринки з метою зменшення тенденції використання ІТ трудових ресурсів без належного внеску в бюджет України.

Висновки.

Підсумовуючи викладене, зазначимо, що міжнародні процеси регулювання ШІ мають знайти відображення у інформаційному праві України. На підставі аналізу документів ООН, G7,ЄС, США, Китаю зроблено висновок що процес розробки уніфікованого міжнародного регулювання ШІ є складним й імовірно триватиме роками, оскільки деякі країни виступають за розробку всеосяжної міжнародної конвенції, інші вважають, що це призведе до надмірного регулювання і зашкодить інноваціям.

До кінця 2023 року ЄС остаточно введе в дію Акт про штучний інтелект (Artificial Intelligence Act, AI Act), який визначатиме основні принципи для розробки та використання ШІ і, безумовно, матиме вплив на розробників ШІ з України.

Існуюче в Україні законодавство (Концепція розвитку штучного інтелекту в Україні, План заходів з реалізації Концепції розвитку ШІ в Україні на 2021 – 2024 роки) не повною мірою відображає світові тенденції регулювання ШІ. Україна має долучатися до світової практики запровадження етичних правил і правового регулювання використання ШІ з метою захисту прав людини, забезпечення безпеки ШІ-систем, прозорості для громадськості їх створення, підзвітності розробників. Доцільно розробити проект Закону України “Про створення і використання штучного інтелекту в Україні”, а також розпочати науково-практичну дискусію щодо створення уповноваженого державного органу/комісії з контролю і нагляду за використанням ШІ в Україні.

У новому законодавстві щодо ШІ варто врахувати досвід ЄС та США, а також відповідно до Кодексу поведінки для організацій із розробки передових систем ШІ, врегулювати питання використання різноманітних заходів внутрішнього та незалежного зовнішнього тестування ШІ, публічного повідомлення про можливості, обмеження та сфери належного і неналежного використання систем ШІ, обміну інформацією та звітуванням про інциденти серед організацій, що розробляють системи ШІ тощо.

Перспективами подальших наукових пошуків визначаємо питання суб’єктно-об’єктного складу, а також адміністративно-наглядових повноважень державних органів України щодо розробників систем ШІ.

Використана література

1. Assessing the Economic Impact of Artificial Intelligence. URL: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-ISSUEPAPER-2018-1-PDF-E.pdf

2. AI and the Future of Work Post-Covid. https://hai.stanford.edu/sites/default/files/2021-05/HAI_Industry-Brief_AI-and-the-Future-of-Work-Post-Covid_1.pdf

3. PwC’s Global Artificial Intelligence Study: Exploiting the AI Revolution. URL: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

4. De Almeida, P.G.R., dos Santos, C.D. &Farias, J.S. Artificial Intelligence Regulation: a framework for governance. Ethics InfTechnol 23, 505-525 (2021). URL: https://doi.org/10.1007/s10676-021-09593-z

5. Justo-Hanani, R. The politics of Artificial Intelligence regulation and governance reform in the European Union. Policy Sci 55, 137-159 (2022). URL: https://doi.org/10.1007/s11077-022-09452-8

6. Roberts, H., Cowls, J., Morley, J. et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI &Soc 36, 59-77 (2021). URL: https://doi.org/10.1007/s00146-020-00992-2

7. C. Fernández-Aller et al. An Inclusive and Sustainable Artificial Intelligence Strategy for Europe Based on Human Rights. *IEEE Technology and Society Magazine.* Vol. 40, no. 1. Pp. 46-54. March 2021, doi: 10.1109/MTS.2021.3056283.

8. E. D. Gibbons. Toward a More Equal World: The Human Rights Approach to Extending the Benefits of Artificial Intelligence. *IEEE Technology and Society Magazine.* Vol. 40, no. 1. Pp. 25-30, March 2021, doi: 10.1109/MTS.2021.3056295

9. Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

10. Digital Economy Report 2021. URL: https://unctad.org/system/files/official-document/der2021 _overview_en_0.pdf

11. Creating breakthrough technologies and capabilities for national security. URL: https://www.darpa.mil

12. China lets Baidu, others launch ChatGPT-like bots to public, tech shares jump. URL: https://www.reuters.com/technology/baidu-among-first-win-china-approval-ai-models-bloomberg-news-2023-08-30

13. High-Level Advisory Body on Artificial Intelligence. URL: https://www.un.org/techenvoy/ai-advisory-body

14. UN Secretary-General launches AI Advisory Body on risks, opportunities, and internationalgovernance of artificial intelligence. URL: https://www.un.org/sites/un2.un.org/files/231025_press-release-aiab.pdf

15. Recommendation on the Ethics of Artificial Intelligence. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455

16. Guidance for generative AI in education and research. UKR: https://unesdoc.unesco.org/ark:/48223/pf0000386693

17. WHO issues first global report on Artificial Intelligence (AI) in health and six guiding principles for its design and use. URL: https://www.who.int/news/item/28-06-2021-who-issues-first-global-report-on-ai-in-health-and-six-guiding-principles-for-its-design-and-use

18. EU AI Act: first regulation on artificial intelligence. URL: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

19. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EURO PE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf

20. Artificial Intelligence Risk Management Framework (AI RMF 1.0). URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

21. Strengthening andDemocratizingtheU.S. Artificial Intelligence Innovation Ecosystem. An Implementation Plan for a National Artificial Intelligence Research Resource. URL: https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf

22. President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence

23. Interim Measures for the Management of Generative Artificial Intelligence Services. URL: https://www.chinalawtranslate.com/en/generative-ai-interim

24. ‘All-out assault on privacy’: France is first EU country to legalise AI-driven surveillance. URL: https://www.brusselstimes.com/430820/all-out-assault-on-privacy-france-is-first-eu-country-to-legalise-ai-driven-surveillance

25. G7 Leaders' Statement on the Hiroshima AI Process. URL: https://www.mofa.go.jp/ecm/ec/page5e_000076.html

26. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

27. Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System. URL: https://www.mofa.go.jp/files/100573471.pdf

28. План заходів з реалізації Концепції розвитку ШІ в Україніна 2021– 2024 роки. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text

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

УДК 32.019.51:323.28:323.2(477)

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

КІБЕРТЕРОРИЗМ: ІНФОРМАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *У статті висвітлені інформаційно-правові аспекти кібертероризму. На підставі аналізу підходів, вироблених зарубіжними і вітчизняними вченими, визначено суттєві ознаки кібертероризму, критерії його відмежування від суміжних понять. Аналізуються кіберінциденти та основні цілі кібертерористів у кіберпросторі України. Міститься правовий аналіз як нормативних актів України у сфері інформаційної безпеки, так і міжнародно-правових актів у цій сфері. Проаналізовано новації в законодавстві окремих зарубіжних країн у сфері боротьби з кібертероризмом. Запропоновано авторське визначення кібертероризму. На базі аналізу зарубіжного досвіду у сфері боротьби з тероризмом пропонуються зміни до Закону України "Про боротьбу з тероризмом", а також законодавства про кримінальну відповідальність за акти кібертероризму.*

Ключові слова*: тероризм, кібертероризм, кіберпростір, інформаційні технології, інформаційне насильство, кримінальна відповідальність.*

Summary*. The article covers the informational and legal aspects of cyberterrorism. On the basis of the analysis of approaches developed by foreign and domestic scientists, essential signs of cyberterrorism. Cyber incidents and the main goals of cyber terrorists in Ukrainian cyberspace are analyzed. It contains a legal analysis of both regulatory acts of Ukraine in the field of information security and international legal acts in this area. Innovations in the legislation of certain foreign countries in the field of combating cyberterrorism are analyzed. The author's definition of cyberterrorism as a type of terrorist activity, which is carried out using cyberattacks in cyberspace, is proposed. Based on the analysis of foreign experience in the field of combating terrorism, amendments are proposed to the Law of Ukraine "On Combating Terrorism", as well as to the legislation on criminal liability for acts of cyberterrorism.*

Keywords*: terrorism, cyberterrorism, cyberspace, information technologies, information violence, criminal liability.*

Постановка проблеми. Кібертероризм є серйозною загрозою для світової спільноти поряд з ядерною, бактеріологічною і хімічною зброєю. Світовий досвід свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні мережі та організації віддаленої кібератаки на інформаційні ресурси жертви [1, с. 42-43]. Очевидно, що актуальність цієї загрози буде зростати і надалі в ході розвитку і поширення інформаційно-телекомунікаційних технологій.

Рівень загрози кібертероризму проти України стрімко зростає в умовах неприкритої агресії рф проти України з лютого 2022 року. Особливо помітне зростання кількості кіберінцидентів і кібератак на державні інформаційні ресурси та об'єкти

критичної інфраструктури України з боку російських хакерів. Від початку повномасштабної війни (і станом на середину листопада 2022 року) на українську енергетику було здійснено понад 1,2 млн. кібератак [2].

Результати аналізу наукових публікацій. Теоретичні аспекти протидії кібертероризму досліджували Лабенко Л.В. [3], Бураєва Л.А. [4], Банк Р.О. [5], Діордіца І.В. [6], Пилипчук В.Г., Дзьобань О.П. [7] та ін.

Особливості кібертероризму як одного із способів інформаційної війни висвітлені у працях Почепцова Г.Г. [8], Коршунова В.О. [9], Леонова Б.Д. [10], Рижова І.М. [11], Яцик Т.П. [12] та ін.

Істотний внесок у дослідження кібертероризму як засобу введення інформаційної війни в умовах глобалізації та розвитку кіберпростору здійснили зарубіжні вчені, серед яких можна виділити роботи Д. Белла [13], Е. Тоффлера [14], Б. Хофмана [15], А. Шміда [16] та ін.

Проте серед науковців і практичних фахівців у сфері інформаційних технологій немає єдиних підходів до визначення поняття "кібертероризм", його суттєвих ознак. Існують також розбіжності поглядів щодо форм і різновидів такого тероризму.

Метою статті є удосконалення на базі аналізу вітчизняного і зарубіжного досвіду у сфері інформаційної безпеки визначення кібертероризму, а також внесення пропозицій з встановлення кримінальної відповідальності за його суспільно небезпечні прояви.

Виклад основного матеріалу. Закон України "Про боротьбу з тероризмом" не містить визначення терміну "кібертероризм". Цей Закон згадує поняття "технологічний тероризм", під яким слід розуміти кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру (ст. 1) [17]. Наведене визначення охоплює різні різновиди тероризму і не збігається з дефініцією кібертероризму, який, виходячи з наведеного визначення, вбачається одним з проявів технологічного тероризму.

Закон України "Про основні засади забезпечення кібербезпеки України" визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1) [18]. Проте, ст. 1 Закону України "Про боротьбу з тероризмом" не згадує такий прояв терористичної діяльності у кіберпросторі.

Стратегія інформаційної безпеки [19] визначає основні напрями забезпечення інформаційної безпеки України. Серед них згадується протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів (Стратегічна ціль 1).

Стратегія національної безпеки України [20] основним завданням розвитку системи кібербезпеки визначає гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури (п. 52), а серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів виділяє активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та

кібератакам. У Стратегії згадується інформаційна “зброя”, яку застосовує рф для поширення міжнародного тероризму у кіберпросторі [10, с. 73-74].

Міжнародний тероризм, зокрема в кіберпросторі, згадує також Стратегія забезпечення державної безпеки (затверджена Указом Президента України від 16 лютого 2022 року № 56) [21]. Ця Стратегія одним з об’єктів забезпечення державної безпеки називає кібербезпеку.

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, реалізація якої здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. З цією метою Указом Президента України від 26 серпня 2021 року № 447/2021 затверджено Стратегію кібербезпеки України [22].

У цій Стратегії зазначається, що 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. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [22].

Глобального масштабу набуває використання кіберпростору терористичними організаціями. У Розділі 1 Стратегії кібербезпеки України зазначається, що пріоритетними цілями кібертероризму залишаються 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 [22]. Кіберінциденти здійснюються через інформаційно-телекомунікаційні системи, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади.

Аналіз нормативно-правових актів у сфері боротьби з тероризмом свідчить про те, що кібертероризм розглядається як одне з основних джерел загроз національній та міжнародній кібербезпеці, а його визначення на рівні закону згадує кіберпростір як сферу застосування терористичної діяльності.

Зауважимо, що визначення кібертероризму не містять міжнародні правові акти, серед яких виділяються Конвенція Ради Європи про запобігання тероризму (2005 р.), Конвенція про кіберзлочинність (2001 р.). Наслідком ратифікації остатнньої став Закон України “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” від 23 грудня 2004 року, відповідно до якого в Розділі 16 “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” викладені у новій редакції статті 361, 362, 363 Кримінального кодексу та встановлена відповідальність за статтями 361-1, 361-2 та 363-1 цього Кодексу [23, с. 256].

Аналіз різних підходів, викладених у зазначених актах, дає підстави для висновку, що кібертероризм є частиною або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму [5, с. 112]. Деякі дослідники вважають, що кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища – тероризму [6]. Більшість вчених вважає, що інформаційний тероризм як явище за змістом охоплює прояви кібертероризму.

На доктринальному рівні це поняття досліджувалося як вченими, так і практичними фахівцями у сфері інформаційних технологій. На думку зарубіжних дослідників, кібетероризм є різновидом кібератак на комп’ютерні системи.

Центр стратегічних і міжнародних досліджень визначає кібертероризм як використання комп'ютерних мережевих інструментів для припинення функціонування критичних об'єктів національної інфраструктури (зокрема, енергетичних, транспортних, урядових), або для примусу або залякування уряду або цивільного населення [24].

З точки зору американського професора У. Тафойа, кібертероризмом є залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об'єктів критичної інфраструктури або знищення інформації [25].

Визначення кібертероризму міститься й в роботах вітчизняних вчених.

На думку Діордіци І.В., термін "кібертероризм" є синтезом понять "кібербезпековий простір" та "тероризм" [6]. Для кібертероризму характерним є використання комп'ютера як інструмента злочину та існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину [6].

Пилипчук В.Г. та Дзьобань О.П. вважають, що кібертероризм – це навмисна, політично вмотивована атака на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійснені з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій [4].

Схожого підходу дотримується В.В. Топчій, на думку якого під кібертероризмом слід розуміти навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [26].

Залежно від злочинної мети та використання інструментів (засобів) її досягнення від кібертероризму слід відрізняти медіа-тероризм, під яким розуміють зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, сприяння вчиненню теракту). Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо [5, с. 114].

Основною ознакою кібертероризму є кібератаки, які здійснюються у кіберпросторі. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" під кібератакою слід розуміти спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [18].

Об'єктами таких атак є інформація, програми, комп'ютери, локальні та глобальні мережі. З-поміж властивостей інформаційного насильства виділяється: несиловий, ідеальний характер, вихід за межі фізичних закономірностей; не лінійність; порушення закону збереження речовини й енергії, кумулятивний характер, можливість бурхливого зростання інформації; широке розповсюдження; можливість ідеального клонування; нелокалізованість у часі; опосередкований характер і прихованість впливу; віртуальний

характер впливу; можливість фіксування; селективність; легкість доступу, злому інформаційних систем [27].

Україна зазнає кібератак різної потужності, починаючи ще з 2014 року.

Однією із наймасштабніших за наслідками була кібератака з поширення вірусу NotPetya, який 27 червня 2017 р. атакував численні комп'ютерні системи українських державних і комерційних установ. За підрахунками спеціалістів Microsoft та ESET, кібератака зачепила щонайменше 65 країн. Встановлено, що першою й основною (якщо не єдиною) метою кібератаки була саме Україна. За попередніми підрахунками, у результаті атаки на території України станом на 7 липня 2017 р. було виведено з ладу до 10 % приватних, урядових і корпоративних комп'ютерів [28].

Ще до повномасштабного вторгнення рф в лютому 2022 року експерти з кібербезпеки прогнозували збільшення проявів кібертероризму в Україні. З початку неприкритої агресії рф Україна стала об'єктом чисельних кібератак, які охопили державні установи, приватні організації та громадян. У 2022 році рф втричі збільшила кількість таких атак на Україну[29].

Однак, якщо раніше вони були спрямовані здебільшого на військові цілі, то в умовах війни суспільно небезпечні хакери спрямовані на критичну інфраструктуру, яка зазнає кібератак [29].

Збільшення кібератак на критичну інфраструктуру України викликає занепокоєння у країн ЄС та НАТО, які теж можуть стати об'єктами кібератак. Світова тенденція сучасності – кожна країна динамічно працює над інституційними засадами протидії кібертероризму, навіть в певних випадках у форматі створення кібервійськ [30, с. 148].

В даному контексті доречно розглянути досвід окремих зарубіжних країн – союзників України у сфері боротьби з кібертероризмом.

Так, кримінальне законодавство Франції значно розширило межі відповідальності за злочинні прояви тероризму в кіберпросторі. У КК Франції у 2016 р. було криміналізоване створення сайтів терористичної спрямованості за межами Франції. У гл. 25 кн. 4 КПК Франції визначено особливу процедуру, що застосовується до справ організованої злочинності, у т.ч. тероризму, зміст якої полягає, зокрема, у встановленні спеціальних складів судів і оперативно-розшукових команд.

Парламент Франції також затвердив положення про створення паризького суду, що спеціалізуватиметься на боротьбі з кіберзлочинністю [31].

КК ФРН не містить визначення тероризму. У КК ФРН передбачено посилену відповідальність за злочини, що вчиняються організованими об'єднаннями. До них слід віднести такі: створення злочинних об'єднань (ст. 129), створення терористичних об'єднань (ст. 129-а), тяжкі випадки торгівлі людьми (ст. 181), геноцид (ст. 220-а), викрадення людини (ст. 234), насильницьке переміщення громадян за межі країни (ст. 234-а). До проявів терористичної діяльності у ФРН, зокрема, відносять: заподіяння шкоди територіальній цілісності, порушення зовнішньої чи внутрішньої безпеки держави; порушення конституційних засад; заподіяння шкоди військам НАТО, розміщеним на території ФРН.

Федеральним законом передбачено створення спільних файлів поліції та розвідувальних служб щодо осіб, підозрюваних у здійсненні терористичної діяльності. Мова йде про створення так званих "файлів антитерору", в рамках яких відбувається обмін інформацією між правоохоронними органами та службами ФРН [32, с. 35].

Закон ФРН від 25 грудня 2008 р. розширив повноваження кримінальної поліції щодо впровадження спеціальних програм у комп'ютери осіб, підозрюваних у причетності до діяльності терористичних організацій [33]. Цей Закон мав профілактичну мету: відстеження терористів-одинаків.

24 червня 2016 р. в ФРН прийнято Закон “Про заходи з протидії тероризму”, яким передбачається: запровадження більш жорстких правил реєстрації власників передплаченого зв’язку; організація автоматизованого обміну даними між національними спецслужбами та правоохоронними органами, а також із спецслужбами іноземних держав; збільшення термінів зберігання відповідної інформації; зменшення з 16 до 14 років мінімального віку громадян, за якими дозволено здійснювати стеження [34].

Також у 2016 р. внесено зміни до Закону ФРН “Про Федеральну розвідувальну службу” (BND), якими розширюються її повноваження. 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 [34].

Норми про відповідальність за кібертероризм містить федеральне законодавство США. Відповідно до положень Патріотичного закону США 2001 р. федеральне кримінальне законодавство розрізняє поняття *“*кібертероризм”. Так, згідно зі ст. 814 цього Закону, положення якої доповнюють § 1030 “Шахрайство та пов’язана з ним діяльність щодо комп’ютерів” Розділ 18 Зведеного закону США, поняття “кібертероризм” охоплює різні кваліфіковані форми хакерства (в тому числі й ті, що спричиняють матеріальні збитки на суму, яка становить $5 тис. і більше), заподіяння шкоди захищеним комп’ютерним мережам громадян, юридичних осіб та урядових установ, включаючи шкоду медичному обладнанню, “фізичну шкоду якій-небудь особі”, “загрозу громадському здоров’ю та безпеці”, “шкоду, що завдана комп’ютерній системі, яку використовує урядова установа для відправлення правосуддя, організації національної оборони чи забезпечення національної безпеки” (покаранням за це є штраф та/або тюремне ув’язнення на строк до 20 років) [32, с. 371]. Отже, у США (на рівні федерації) введено поняття “кібертероризм”, а також встановлено кримінальну відповідальність за його злочинні прояви.

Викладене свідчить про необхідність удосконалення на законодавчому рівні поняття “кібертероризм”, а також встановлення кримінальної відповідальності за вчинення терористичного акту з використанням кібертероризму. До речі, стаття 7.2.4. проекту КК України передбачає відповідальність за терористичний акт, згідно з якою винною визнається, зокрема, особа, яка з метою залякати населення або дестабілізувати діяльність органу державної влади, органу місцевого самоврядування, міжнародної організації, представництва іноземної держави чи юридичної особи, або примусити їх вчинити яку-небудь дію чи утриматися від її вчинення: захопила, утримувала, знищила або пошкодила об’єкт критичної інфраструктури чи його устаткування, необхідне для функціонування цього об’єкта, або порушила його належне функціонування; незаконно втрутилася в роботу інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мережі [33].

Висновки.

Аналіз викладених підходів свідчить про те, що основою кібертероризму є кібератаки, які вчинюються у кіберпросторі або з його використанням. Ці атаки спрямовані на залякування населення або дестабілізацію діяльності органу державної влади, органу місцевого самоврядування, міжнародної організації, представництва іноземної держави чи юридичної особи з метою примусити їх вчинити яку-небудь дію чи утриматися від її вчинення.

Під кібертероризмом слід розуміти терористичну діяльність, яка здійснюється із застосуванням кібератак у кіберпросторі або з його використанням. Таку діяльність

доцільно визначити в ст. 1 Закону України “Про боротьбу з тероризмом”, а серед ознак терористичного акту (ст. 258 КК України) слід передбачити його вчинення у формі кібертероризму. Одним із варіантів вирішення порушеного питання є доповнення частини 2 ст. 258 КК України після слів “групою осіб” словами “або вчинені шляхом кібератаки”. Заходи з протидії кібертероризму доцільно передбачити в Концепції боротьби з тероризмом в Україні та Плані заходів з її реалізації.

Вважаємо, що реалізація запропонованих змін сприятиме боротьбі з проявами кібертероризму в Україні.

Використана література

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

2. Російські хакери посилюють кібератаки на цивільні цілі, щоб тероризувати українців. – (Посадовець АНБ). URL: https://lb.ua/society/2023/01/12/542313_rosiyski_hakeri_posilyuyut.html

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

4. Бураева Л.А. Информационный терроризм как угроза национальной безопасности российской федерации. URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoy-federatsii/viewer

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

6. Діордіца І.В. Поняття та зміст кібертероризму. URL: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu

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

8. Почепцов Г.Г. Информационные войны. – (Серия: Образовательная библиотека); москва: Рефл-бук, 2001. 576 с.

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

10. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. № 2(37)/2021. С. 72-79.

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

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

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

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

15. Хоффман Б. Терроризм – взгляд изнутри ; пер. с анг. Е. Сажина; москва: Ультра. Культура, 2003. 252 с.

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

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

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

19. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.21 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n2

20. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

21. Стратегія державної безпеки: Указ Президента України від 16.02.22 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5

22. Стратегія кібербезпеки безпеки України: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

23. Макаренко Є.А., Рижиков М.М., Ожеван М.А. Міжнародні інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. 916 с.

24. James A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/02 1101_risks_of_cyberterror.pdf

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

26. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf

27. Дзьобань О.П. Насильство інформаційне. Енциклопедія соціогуманітарної інформології. Київ: Видавничий дім "Гельветика", 2020. Т. 1. С. 151-155.

28. Інформаційна безпека та кібербезпека держави: аналітична доповідь до Щорічного послання Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України в 2017 році". Київ: Національний інститут стратегічних досліджень, 2017. С. 47-56.

29. Victor Zhora. State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned. 2022. URL: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

30. Білан І.А. Особливості застосування шкідливого програмного забезпечення спецслужбами країни-агресора. *Інформація і право*. № 2(45)/2023. С.139-152.

31. Франція посилала боротьбу з тероризмом. URL: https://www.ukrinform.ua/rubric-world/1995413-francia-posilila-borotbu-z-terorizmom.html

32. Романовский Г.Б. Противодействие терроризму в Германии: законодательные новеллы. *Наука. Общество. Государство.* – (Электронный научный журнал), 2019. Т. 7. № 4 (28). С. 33-39. URL: http://esj.pnzgu.ru ISSN 2307-9525

33. Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundes kriminalamt / dejure.org. URL: https://dejure.org/BGBl/2008/BGBl._I_S._3083

34. Іноземний досвід протидії тероризму: висновки для України: аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini

35. Савченко А.В. Порівняльний аналіз кримінального законодавства України та федерального кримінального законодавства США: дис. …док-ра юрид. наук. 12.00.08. Київ: Акад. МВС України 2007. 614 с.

36. Проект Кримінального кодексу України за станом на 22 трав. 2023 року). URL: https://ewcriminalcode.org.ua/upload/media/2023/05/22/kontrolnyj-tekst-proektu-kk-22-05-2023.pdf

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

УДК 34(477.83)+341.123:659.1(477.83)

КРАСНОСТУП Г.М., *кандидат юридичних наук, старший науковий співробітник*

ПРАВОВЕ РЕГУЛЮВАННЯ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ ЖУРНАЛІСТІВ ТА ІНШИХ МЕДІА-УЧАСНИКІВ В УКРАЇНІ

Анотація. *Стаття присвячена дослідженню питання правового регулювання статусу, засад діяльності та відповідальності журналістів та інших медіа-учасників в Україні, у тому числі в контексті правового режиму воєнного стану. Особливу увагу у статті приділено п'ятирічній кампанії Ради Європи щодо безпеки журналістів та доцільності переформатування сторінки, присвяченої Україні, та розподілу попереджень на сайті Платформи Ради Європи із захисту журналістики та безпеки журналістів. Стаття базується на аналізі правового поля, наукових джерел, законодавства та практичних прикладів з вітчизняної та світової практики. Висновки дослідження сприяють кращому розумінню ролі та впливу фіксерів, блогерів та інших медіа-учасників у ситуаціях воєнного стану, а також визначенню можливих шляхів покращення правового регулювання їхньої діяльності з урахуванням необхідності забезпечення інформаційної безпеки.*

Ключові слова*: журналіст, професійна діяльність журналістів, фіксер, блогер, медіа-учасник, медіа-актор.*

Summary. *The article is dedicated to the examination of legal regulation concerning the status, principles of operation, and responsibilities of journalists and other media actors in Ukraine, including within the context of the legal framework in the martial law conditions. Special attention in the article is given to the five-year campaign by the Council of Europe regarding journalist safety and the reformatting of the Ukraine-related section and the distribution of alerts on the Council of Europe Platform for the Protection of Journalism and Journalists website. The article is based on an analysis of the legal framework, scholarly sources, legislation, and practical examples from domestic and international practices. The research findings contribute to a better understanding of the role and impact of fixers, bloggers, and other media actors in situations of a state of war, as well as to identifying possible ways to improve the legal regulation of their activities while considering the need to ensure information security.*

Keywords: *journalist, journalistic profession, fixer, blogger, media participant, media actor.*

Постановка проблеми. Сьогодні в усьому світі з'явилася тенденція, коли кожен користувач мережі Інтернет, конкуруючи з медіа, можуть масово поширювати інформацію до необмеженого кола осіб. При цьому, створюється певний контент, який миттєво поширюється серед знайомих, друзів, незнайомих осіб, колег і друзів незнайомих осіб. Такий ланцюжок може бути схожим на морську хвилю, а може у дуже стислий період у часі стати справжнім інформаційним цунамі.

На тлі сучасних змін у суспільно-політичному ландшафті, особливо в умовах правового режиму воєнного стану, соціальні мережі та онлайн-платформи стають місцем інтенсивної комунікації, де активно розгортається діяльність блогерів та інших медіа-учасників. Статус блогера, фіксера та інших медіа-учасників, їхні засади діяльності та відповідальність набувають особливого значення у цих умовах, адже їхні публікації можуть впливати на суспільну думку, ставлення громадян до подій та рішень державної влади. При цьому, у контексті правового режиму воєнного стану виникають численні питання, пов'язані з необхідністю забезпечення свободи вираження поглядів, доступу до інформації та необхідністю захисту інформаційної безпеки.

Результати аналізу наукових публікацій. У своїх наукових працях проблемні питання захисту професійної діяльності журналістів досліджують такі вітчизняні науковці: З.В. Григорова, А.А. Данько-Сліпцова, М.Ю. Наумова, Я.В. Нечипорук та інші. Окремо хочу виділити колег-практиків, які внесли вагомий внесок у правове регулювання діяльності журналістів, а саме: Р.Б. Головенко, І.Є. Розкладай, А.Ф. Сафаров, Т.С. Шевченко, А.О. Черевко. Разом з цим, потребує додаткового дослідження та висвітлення питання правових аспектів визначення статусу інших медіа-учасників, засад їх діяльності та відповідальності.

Метою статті є удосконалення правового регулювання статусу, засад діяльності та відповідальності журналістів та інших медіа-учасників в Україні, у тому числі в контексті правового режиму воєнного стану.

Виклад основного матеріалу. Поставлена проблема вимагає детального аналізу та систематизації правових, соціологічних та етичних аспектів діяльності журналістів, фіксерів, блогерів та інших медіа-учасників під час правового режиму воєнного стану, що робить її актуальною та важливою для подальших досліджень. З огляду на невизначеність та розвиток нових засобів комунікації, а також змін у правовому полі, розуміння ролі та відповідальності фіксерів, блогерів та інших медіа-учасників є важливим кроком до забезпечення належної інформаційної безпеки, правопорядку та захисту прав громадян під час надзвичайних ситуацій.

З огляду на наведене, сьогодні потребує особливої уваги питання правового регулювання визначення статусу "інших медіа-учасників", засад їх діяльності та відповідальності, у тому числі під час правового режиму воєнного стану.

Закон України "Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста" розрізняє два поняття "журналіст" та "особи, що прирівнюються до журналістів". Так, статтею 1 вказаного Закону передбачено, що журналіст – творчий працівник суб'єкта у сфері медіа, який професійно збирає, одержує, створює, редагує, поширює і забезпечує підготовку інформації для медіа. Статус журналіста підтверджується документом, виданим суб'єктом у сфері медіа, професійною чи творчою спілкою журналістів. Документ, що підтверджує статус журналіста, має містити найменування та вид медіа, його ідентифікатор у Реєстрі суб'єктів у сфері медіа або найменування професійної чи творчої спілки, фото, прізвище, ім'я та по батькові журналіста, номер документа, дату видачі і строк його дії, підпис особи, яка видала документ [1].

Частиною другою статті 15 вказаного Закону передбачено, що до журналістів для цілей цієї статті, статей 12 і 13 Закону прирівнюються кіно- і телеоператори, режисери та інші працівники суб'єктів у сфері медіа, якщо вони за необхідності входять до складу відряджених творчих груп. Таким чином, Закон передбачає прирівняння цих осіб лише в частині стажу роботи, охорони праці, відрядження журналістів (статті 12, 13 та 15 Закону).

Одним із зобов'язань України, що випливає з її членства в Раді Європи, є, зокрема, обов'язок забезпечувати належне виконання рішень Європейського Суду з прав людини.

Згідно з частиною першою статті 46 Конвенції про захист прав людини і основоположних свобод та статтею 2 Закону України "Про виконання рішень та застосування практики Європейського суду з прав людини" рішення Європейського Суду є обов'язковими для виконання [2].

Під виконанням рішення Європейського Суду слід розуміти виплату відшкодування, а також вжиття державою додаткових заходів індивідуального характеру, спрямованих на усунення конкретного порушення, визначеного в рішенні Європейського Суду, та заходів

загального характеру, спрямованих на усунення підстав для надходження до Європейського Суду аналогічних заяв проти України у майбутньому.

Наразі під посиленим наглядом Комітету міністрів Ради Європи (далі – Комітет) Рішення Європейського Суду з прав людини у справі "Гонгадзе проти України" (заява № 34056/02) від 8 листопада 2005 р. [3], яке стосується порушення статті 2 Конвенції у зв'язку з відсутністю ефективного розслідування викрадення та смерті журналіста, статті 3 Конвенції з огляду на принизливе поводження з вдовою журналіста органами досудового розслідування, а також порушення статті 13 Конвенції у зв'язку з відсутністю ефективних засобів правового захисту та компенсації.

Справа про зникнення пана Гонгадзе привернула увагу багатьох міжнародних організацій. Вона розглядалась у контексті свободи засобів масової інформації в Україні, стан якої вже протягом декількох років критикувався на міжнародному рівні.

Відповідно до статті 1 Закону України "Про виконання рішень та застосування практики Європейського Суду з прав людини" виконання рішення Європейського Суду передбачає, крім виплати справедливої сатисфакції, вжиття додаткових заходів індивідуального та загального характеру.

Заходами загального характеру відповідно до статті 13 Закону є заходи, спрямовані на усунення зазначеної в рішенні проблеми, зокрема шляхом внесення змін до чинного законодавства та практики його застосування.

На практиці за загальним правилом остаточне рішення Європейського Суду передається Комітету, який здійснює нагляд за його виконанням. Наразі рішення у справі "Гонгадзе проти України" залишається невиконаним. У рішенні Комітету, ухваленому на 1390-му засіданні від 3 грудня 2020 р., делегати повторно висловили стурбованість щодо "вузького" визначення поняття "журналіст" в Кримінальному кодексі України, ще раз наголосили, що органи влади, відповідно до Конвенції, зобов'язані застосовувати ініціативний підхід в питаннях, що стосуються погроз та злочинів проти осіб, які реалізують своє право на свободу вираження поглядів, незалежно від їх офіційного професійного статусу. Також делегати закликали органи влади внести зміни до законодавства, відповідно до стандартів Ради Європи, зокрема, відповідно до Рекомендації Комітету державам-членам стосовно захисту журналістики і безпеки журналістів та інших медіа-учасників (CM/Rec(2016)4), не обмежуючи захист тих, хто офіційно визнаний журналістами.

У Рекомендаціях CM/Rec(2016)4 державам-членам щодо захисту журналістики й безпеки журналістів та інших працівників медіа Комітет зазначив про те, що тривожним і неприйнятним є те, що журналісти й інші медіа учасники в Європі все частіше стають об'єктами погроз, утисків, переслідувань, залякувань, безпідставного позбавлення волі, фізичних нападів, катувань і навіть убивств через проведення ними розслідувань, висловлення власної думки чи висвітлення певних тем, особливо коли це стосується зловживання владою, корупції, порушень прав людини, злочинної діяльності, тероризму та фундаменталізму.

Ця тривожна ситуація не обмежується професійними журналістами й іншими працівниками традиційних медіа. Як зазначають Європейський суд з прав людини та багато інших міждержавних органів, у тому числі ООН у своєму Плані дій щодо безпеки журналістів і проблеми безкарності, Комітет з питань прав людини, національних меншин і міжнаціональних відносин у своєму Загальному коментарі № 34, визначення працівників медіа розширилося в результаті появи нових форм медіа цифрової ери. Воно охоплює тих, хто робить внесок у громадське обговорення та хто веде журналістську діяльність або виконує функції громадського контролю.

У Додатках до Рекомендацій Комітет дав вказівку державам-членам забезпечити комплексну законодавчу базу, яка надасть змогу журналістам та іншим медіа учасникам брати участь у громадських обговореннях ефективно та без остраху. “Законодавча база, в тому числі положення кримінального права, які стосуються захисту фізичної та моральної цілісності особи, повинна ефективно впроваджуватись, насамперед через адміністративні механізми та визнання особливої ролі журналістів та інших медіа-учасників в демократичному суспільстві”. Крім того, Комітет привернув увагу, що актуальний технологічний розвиток змінив традиційне середовище медіа, як це описано, зокрема в CM/Rec (2011)7, стосовно нового визначення медіа, що привело до виникнення нових концепцій медіа та нового розуміння динамічної екосистеми медіа. Відповідно до пункту 9 Додатку до Рекомендацій розвиток інформаційних та комунікаційних технологій спрощує участь у суспільному обговоренні для все більш широкого та розмаїтого спектру суб’єктів. Тому Європейський Суд з прав людини неодноразово зазначав, що окремі особи, організації громадянського суспільства, інформатори та вчені, на додачу до професійних журналістів та медіа, можуть значним чином сприяти суспільному обговоренню і таким чином відігравати роль, подібну чи рівноцінну тій, яку традиційно відіграють інституалізовані медіа та професійні журналісти.

У Рекомендаціях Комітет проаналізував визначення журналістики іншими міжнародними організаціями, зокрема, Комітет з прав людини ООН також зазначив, що журналістика – це діяльність, яку веде широке коло осіб, у тому числі професійні журналісти на умовах постійної зайнятості, аналітики, блогери й інші особи, які самостійно публікують інформацію будь-якого типу у друкованих виданнях, мережі Інтернет чи деінде [4]. Генеральна Асамблея ООН також визнала, що журналістика постійно розвивається і включає здобутки інституцій медіа, окремих осіб і низки організацій, які шукають, одержують або надають інформацію чи ідеї будь-якого типу як онлайн, так і офлайн і таким чином сприяють суспільному обговоренню. Згідно з Планом дій ООН щодо безпеки журналістів та проблеми безкарності захист журналістів не повинен обмежуватися особами, які офіційно визнані журналістами, він поширюється на інших осіб, зокрема працівників медіа громад й громадянських журналістів та інших осіб, які можуть використовувати нові медіа як засіб звернення до своєї аудиторії.

Комітет покладає обов’язок на державу гарантувати справжню свободу кожній особі, яка перебуває під її юрисдикцією, і убезпечити журналістів й інших учасників медіа від необґрунтованих арештів, незаконних затримань або умисних зникнень.

Мова йде про гарантування безпеки й захисту журналістів та інших учасників медіа є передумовою для їх можливості ефективно брати участь у суспільному обговоренні. Постійні залякування, погрози і насильство щодо журналістів та інших учасників медіа у поєднанні з нездатністю притягнути до відповідальності винних у скоєнні таких правопорушень породжують страх і мають ефект стримування для свободи вираження поглядів і суспільного обговорення. Крім того, Європейська Комісія за демократію через право (Венеціанська Комісія) у своєму Звіті за 2015 рік про демократичний нагляд за сигналами розвідувальних органів в частині здійснення правоохоронними органами або органами безпеки масового перехоплення даних зазначила, що журналісти є групою, яка потребує особливого захисту, оскільки пошук їхніх контактів може виявити їхні джерела (і ризик виявлення може бути потужною перешкодою для викривачів). Згідно зі звітом, професію журналіста було нелегко визначити, оскільки неурядові організації також формували громадську думку, і навіть блогери могли претендувати на такий самий захист. У світлі викладеного, особи, які

здійснюють функцію громадського контролю шляхом збирання та поширення суспільно необхідної інформації на невизначене коло осіб, проте не мають відповідного статусу, повинні користуватися належним правовим захистом з урахуванням стандартів Ради Європи. Крім того, відповідно до частин першої – другої статті 13 згаданого Закону заходи загального характеру вживаються з метою забезпечення додержання державою положень Конвенції, порушення яких встановлене Рішенням, забезпечення усунення недоліків системного характеру, які лежать в основі виявленого Судом порушення, а також усунення підстави для надходження до Суду заяв проти України, спричинених проблемою, що вже була предметом розгляду в Суді. Заходами загального характеру є заходи, спрямовані на усунення зазначеної в Рішенні системної проблеми та її першопричини, зокрема: внесення змін до чинного законодавства та практики його застосування. Тобто, виконання рішення "Гонгадзе проти України" потребує приведення національного законодавства у відповідність до стандартів Ради Європи в частині поширення гарантій захисту на осіб, які формально не набули статусу журналіста та не пов'язані трудовими відносинами зі медіа.

З огляду на наведене, підпунктом 8 пункту 2 Рекомендацій парламентських слухань на тему: "Безпека діяльності журналістів в Україні: стан, проблеми і шляхи їх вирішення", схвалених Постановою Верховної Ради України від 14.01.20 р. № 456-IX, Верховній Раді України рекомендовано привести у відповідність до європейських стандартів визначення понять "журналіст" та "журналістська діяльність", виключивши ознаку систематичності такої діяльності, з метою охоплення захистом і тих осіб, які несистематично займаються журналістикою і зазнали втручання у свою журналістську діяльність, та уникнення необхідності доведення протиправного наміру перешкоджання журналістській діяльності [5].

Привертаємо увагу до того, що зазвичай в рекомендаціях та документах можуть використовуватися різні терміни залежно від контексту та мети тексту. Так, терміни "медіа-учасники" та "медіа-актори" можуть бути використані в контексті рекомендацій Ради Європи про журналістів. Вони означають приблизно одне й те саме, а саме: осіб або організації, які беруть участь у медіа-просторі і впливають на інформаційне середовище.

У наукових колах та документах Ради Європи використовують наступні поняття:

журналісти (journalists) – загальний термін, який може використовуватися для опису всіх осіб, що працюють у журналістській сфері;

медіа-професіонали (media professionals) – термін, який, на нашу думку, підкреслює професіоналізм журналістів та інших осіб, які працюють у медіа;

працівники журналістики (journalistic workers) – словосполучення може бути використане для акцентування робочого аспекту журналістики;

медіа-практиканти (media practitioners) – словосполучення, що підкреслює активну працю журналістів медіа-сфері;

журналістська громадськість (journalistic community) – поняття, що вказує на журналістів як частину спільноти, що займається журналістською діяльністю;

медіа-представники (media representatives) – словосполучення може бути використане для акцентування представницького характеру журналістів у суспільстві.

На нашу думку, поняття "медіа-учасники" є більш формальним та нейтральним виразом, тоді як "медіа-актори" може бути сприйнятий більш неформальним чи спільним словом. Отже, на практиці можна використовувати будь-який з цих термінів у залежності від контексту та власних стилістичних уподобань.

На думку Головенка Р.Б. вплив блогів уже в деяких аспектах конкурує з впливом медіа. Попри те статус блогерів залишається розмитим, значною мірою через об'єктивні причини. Адже зараз більша частина громадян є користувачами Інтернету й створює певний контент, додає в друзі всіх без розбору – не завжди просто визначити, коли користувач з великою кількістю друзів чи підписників у соцмережах набуває медійного впливу, характерного для блогера зараз більша частина громадян є користувачами Інтернету й створює певний контент, додає в друзі всіх без розбору – не завжди просто визначити, коли користувач з великою кількістю друзів чи підписників у соцмережах набуває медійного впливу, характерного для блогера [6].

У Національному класифікаторі України ДК 003:2010 "Класифікатор професій", затвердженому наказом Держспоживстандарту України від 28.07.10 р. № 327 (зі змінами), передбачено професійне угруповання "Письменники, редактори та журналісти" (код 2451.2), до якого вміщені не тільки професійні назви робіт зі словом "журналіст" (наприклад, "Журналіст", "Журналіст мультимедійних видань засобів масової інформації"), а й інші назви, пов'язані з журналістською діяльністю "Коментатор", "Кореспондент", "Оглядач", "Політичний оглядач", "Редактор" тощо [7].

Також назви посад журналістського спрямування можна визначити згідно з Переліком посад журналістів державних і комунальних суб'єктів у сфері медіа, які прирівнюються до посад керівних працівників, спеціалістів секретаріату (апарату) відповідного державного органу або органу місцевого самоврядування, затвердженим Постановою Кабінету Міністрів України від 28.12.16 р. № 1038 (у редакції постанови Кабінету Міністрів України , яка набере чинності 31 березня 2024 р.) "Про умови оплати праці журналістів державних і комунальних суб'єктів у сфері медіа" [8]. Професійні назви посад, передбачені у наведеному Переліку, відповідають назвам Класифікатора професій. Крім цього, посади режисерів (код 2455.2), телеоператорів (код 3132) та інших працівників суб'єктів у сфері медіа можуть бути прирівняні до журналістів за умовами і нормами статей 12, 13 та 15 Закону України "Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста" у випадку, якщо вони за необхідністю входять до складу відряджених творчих груп.

Європейський підхід щодо врегулювання статусу "інших медіа-учасників" також полягає у використанні більш широкого поняття. Рекомендації Комітету CM/Rec(2016)4 "Про захист журналістики та безпеку журналістів та інших медійних суб'єктів" разом з журналістами використовують поняття "інші медіа-актори" або "інші медійні суб'єкти". Разом з цим, у пункті 37 цих Рекомендацій зазначено, що "свавільне використання адміністративних заходів, таких як реєстрація та акредитації блогерів, користувачів Інтернету тощо" розглядається у негативному значенні [9].

Щодо правового регулювання статусу фіксерів, блогерів та інших медіа-учасників та порядку їх діяльності в Україні зазначаємо.

Чинне національне законодавство не містить визначення термінів "фіксер" і "блогер". Водночас привертаємо увагу до усталеної практики нормопроектування, відповідно до якої не потребують пояснень загальновживані терміни, що застосовуються у праві в тому ж значенні, що й у побуті.

На законодавчому рівні поняття "блогер" не визначено у більшості країн світу. Термін "блогер" є більш суб'єктивним і відноситься до людей, які створюють і публікують власний контент в мережі Інтернет на різних платформах, таких як веб-блоги, соціальні медіа, YouTube тощо. Визначення цього терміну може бути включено до внутрішніх правил конкретних платформ.

На нашу думку, ***блогер*** *– це особа, яка публікує власні коментарі, записи, відео, фотографії тощо в мережі Інтернет, зазвичай на своєму веб-сайті або в інших онлайн-платформах, з метою висловлювання своїх думок, ідей, коментарів, а також спілкування з аудиторією.* При цьому, слід враховувати, що сьогодні блогерами можуть бути навіть діти молодшого шкільного віку.

Фіксер *– це особа, яка надає допомогу журналістам або іншим медіа учасникам з метою організації їх роботи на віддалених локаціях, зазвичай в районах конфліктів (бойових дій) або інших складних ситуаціях.* Зазвичай фіксер допомагає журналістам та іншим представникам медіа забезпечити доступ до інформації, знаходить контакти та перекладає, вирішує логістичні питання тощо.

Фіксери та блогери за національним законодавством можуть добровільно зареєструватися як суб'єкти у сфері онлайн-медіа. Разом з цим, згідно з частиною третьою статті 16 Закону України "Про медіа" особа, яка регулярно поширює масову інформацію під своїм редакційним контролем через власні облікові записи на платформах спільного доступу до інформації, має право добровільно зареєструється як суб'єкт у сфері онлайн-медіа в порядку, передбаченому статтею 63 цього Закону [10].

В експертному середовищі постає запитання, чи отримує такий зареєстрований блогер статус журналіста? Головенко Р.В. вважає, що це залежить від сфери правовідносин і від того, яке законодавче визначення до них застосовується. Наприклад, у Кримінальному кодексі України примітка до ст. 345-1 визначає: "Під професійною діяльністю журналіста в цій статті… слід розуміти систематичну діяльність особи, пов'язану зі збиранням, одержанням, створенням, поширенням, зберіганням або іншим використанням інформації з метою її поширення на невизначене коло осіб через друковані засоби масової інформації, телерадіоорганізації, інформаційні агентства, мережу Інтернет". Тобто, гіпотетично блогер має вважатися журналістом за цим визначенням (як і його помічники, асистенти тощо, якщо такі є), хоча на практиці правоохоронцями визнаються за журналістів переважно ті, хто поширює інформацію через зареєстроване державою медіа [6].

Але існують і протилежно інші позиції з порушеного питання у наукових колах. Так, Нечипорук Я.В. вважає, що хоч діяльність блогера і полягає у збиранні і поширенні інформації у мережі Інтернет, однак ототожнювати блогерську діяльність з журналістською не варто, адже блогери здійснюють її не як професію, а скоріше реалізовують право на інформацію таким чином [11, с. 173].

Згідно з пунктом 11 частини першої статті 8 Закону України "Про правовий режим воєнного стану" в Україні або в окремих її місцевостях, де введено воєнний стан, військове командування разом із військовими адміністраціями (у разі їх утворення) можуть самостійно або із залученням органів виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування запроваджувати та здійснювати регулювання роботи медіа [12].

З метою об'єктивного висвітлення подій, забезпечення інформування населення та світової спільноти про воєнні злочини, які вчиняються російською федерацією в ході її широкомасштабної збройної агресії проти України, а також попередження витоку інформації з обмеженим доступом, запобігання поширенню представниками засобів інформації (у тому числі іноземними) та публічними особами, до думки яких прислуховується громадськість (лідери думок, блогери тощо) відомостей, розголошення яких може призвести до обізнаності противника про дії Збройних Сил України та інших складових сил оборони, негативно вплинути на хід виконання завдань за призначенням під час дії правового режиму воєнного стану, Головнокомандувачем Збройних Сил

України видано наказ від 0303.22 р. № 73 “Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборону та представниками засобів масової інформації на час дії правового режиму воєнного стану”. Цим наказом “блогерів” прирівняно до представників медіа, тим самим поширено на них:

- алгоритм роботи з акредитованими представниками засобів масової інформації під час дії правового режиму воєнного стану;
- порядок акредитації представників засобів масової інформації під час дії правового режиму воєнного стану;
- правила роботи представника засобу масової інформації у районі ведення бойових дій.

Привертаємо увагу до того, що таке правове регулювання не поширюватиметься на фіксерів у разі, якщо вони є фрілансерами та працюють самостійно без оформлення трудових відносин із певним суб’єктом у сфері медіа.

Крім цього, 30 травня 2023 р. було внесено зміни до Закону України “Про рекламу”, які наберуть чинності 2 жовтня 2023 р., згідно з якими можна вести мову про правове регулювання в Україні “поширення реклами блогерами”. Так, Закон не містить визначення поняття “блогер”, але визначає користувацький контент як інформацію, (у тому числі користувацьке відео), що створюється та/або поширюється особами на платформах спільного доступу до відео та на платформах спільного доступу до інформації (Facebook, Instagram, LinkedIn) або з використанням електронних комунікацій (Messenger, Viber, Telegram). Якщо такий контент створений блогерами на замовлення, то він має маркуватись відповідно до прописаних у законі норм. У протилежному випадку блогери нестимуть відповідальність.

Окремої уваги потребує правове регулювання притягнення журналістів, фіксерів, блогерів та інших медіа-учасників до відповідальності за порушення законодавства зазначаємо.

Статтею 17 Закону України “Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста” врегульоване питання відповідальності за посягання на життя і здоров’я журналіста, інші дії проти нього та відповідальність журналіста за завдану ним моральну (немайнову) шкоду, а стаття 24 Закону України “Про інформацію” врегульовує питання щодо заборони втручання в професійну діяльність журналістів і медіа.

Щодо відповідальності на практиці є свої особливості, адже поширювача інформації, якщо це не зареєстроване медіа чи якась відома особа, далеко не завжди легко можна ідентифікувати. Частина блогерів не підписується своїм іменем або використовує псевдонім (це нікому не заборонено, хоча окреме таке право виписане лише для журналістів). Звісно, що важче ідентифікувати блогера, який пише тексти, ніж того, хто записує відео за власною участю чи розміщує в блозі фото зі своїм зображенням [6].

24 лютого 2022 р. Верховною Радою України було прийнято декілька законів України про внесення змін до Кримінального кодексу України за поширення незаконного контенту, зокрема до статті 111-1 “Колабораційна діяльність”, статті 114-2 “Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану”, статті 436-2 “Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти

України, глорифікація її учасників” та статті 435-1 “Образа честі і гідності військовослужбовця, погроза військовослужбовцю”.

Вказані статті встановлюють відповідальність осіб, у тому числі фіксерів, блогерів та інших медіа-учасників, за поширення забороненої інформації, передбаченої відповідним складом злочину.

Разом з цим, велику актуальність мають існуючі правові механізми захисту журналістів та інших медіа-учасників, особливо під час правового режиму воєнного стану.

Одним із стратегічних завдань Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28.12.21 р. № 685/2021, є забезпечення дотримання свободи вираження поглядів, доступу до інформації, а також захист професійної діяльності журналістів [13].

Журналісти та інші медіа учасники відіграють важливу роль у захисті демократичного та плюралістичного суспільства, і Європейський Суд з прав людини визнає їх “сторожовими псами громадськості”. Тим не менш, журналісти дедалі частіше стають жертвами різного роду нападів, що заважають їхній повсякденній роботі, починаючи від фізичного та психологічного насильства і закінчуючи онлайн-погрозами, переслідуваннями та залякуваннями.

Цей “клімат” тиску на журналістів є давньою проблемою, яка стосується все більшої кількості держав-членів Ради Європи, і тому вимагає високого рівня політичної уваги та невідкладних дій.

Слід привернути увагу до того, що у 2015 році Радою Європи у співпраці з відомими міжнародними неурядовими організаціями, що працюють у сфері свободи слова та об’єднаннями журналістів, було створено Платформу Ради Європи для сприяння захисту журналістики та безпеки журналістів (далі – Платформа), яка на сьогодні має 15 партнерів: Європейська федерація журналістів, Міжнародна федерація журналістів, Асоціація європейських журналістів, Article 19, Репортери без кордонів, Комітет захисту журналістів, Index on Censorship, Міжнародний інститут преси, Міжнародний інститут безпеки новин, Rory Peck Trust, European Broadcasting Union, PEN International, European Center for Press and Media Freedom, Free Press Unlimited і Justice for Journalists Foundation.

7 березня 2023 р. Платформа опублікувала свій щорічний звіт “Війна в Європі та боротьба за право на репортажі” [14]. Звіт написано партнерськими організаціями Платформи, коаліцією п’ятнадцяти неурядових організацій та асоціаціям журналістів, що займаються свободою медіа. У ньому аналізуються ключові сфери законодавства, політики та практики, що впливають на свободу медіа та безпеку журналістів у Європі, і визначаються дії, необхідні для покращення ефективного захисту журналістів.

Відповідно до Міжнародного гуманітарного права та Міжнародного права з прав людини, російська федерація як окупаційна влада несе повну відповідальність та дотримання прав людини та основних свобод на тимчасово окупованих територіях України (в тому числі окупованих з лютого 2014 р.).

25 січня Європейський Суд з прав людини оголосив перше рішення (щодо прийнятності скарги, тобто підсудності справи ЄСПЛ) у міждержавній справі проти росії через окупацію нею частини східних областей України [15]. Таке рішення юридично підтверджує за росією статус окупанта з 2014 р. та визначає часові й територіальні рамки доведеної окупації. Тому, на Платформі має бути чітко зазначено, що Україна не має відповідати за попередження, пов’язані з агресією російської федерації.

Все це підштовхнуло нас до думки, що слід переформовувати сторінку, присвячену Україні в частині розподілу попереджень на сайті Платформи.

На основі зазначеного вище, 4 жовтня 2023 р. під час неформальної зустрічі з партнерами Платформи було запропоновано розглянути можливість розподілу усіх попереджень на дві категорії, залежно від джерела загрози:

- попередження, пов'язані з агресією російської федерації (Alerts related to the aggression of the russian federation). Ця категорія може включати підкатегорію, пов'язану з агресією російської федерації на тимчасово окупованих територіях;
- попередження, не пов'язані з агресією російської федерації (Alerts not related to the aggression of the russian federation).

Водночас вважаємо, що Україна має докладати всіх можливих зусиль для розслідування відповідних злочинів та притягнення винних осіб до відповідальності.

5 жовтня 2023 р. Радою Європи розпочато п'ятирічну загальноконтинентальну кампанію з безпеки журналістів під гаслом "Журналісти мають значення", яка спрямована на покращення безпеки журналістів та інших медіа акторів і захист свободи медіана на всьому континенті, а також на підвищення обізнаності про роль журналістів.

Генеральний секретар Ради Європи Марія Пейчинович Бурич сказала: "Майже неможливо уявити справжню демократію без різноманітних і незалежних медіа, які діють як "сторожові пси громадськості" та генерують публічні дебати. За допомогою кампанії ми прагнемо допомогти урядам захистити журналістів, щоб вони могли виконувати свою роботу без зайвого втручання, без залякувань і насильства та виконувати свою важливу роль у суспільстві" [16].

Головною метою кампанії є покращення умов безпеки, в яких працюють журналісти та інші медіа учасники по всій Європі, зокрема шляхом ухвалення та впровадження національних планів дій щодо захисту журналістів та посилення правових та інституційних стандартів. Іншими важливими цілями кампанії є встановлення ефективних засобів правового захисту на національному рівні для боротьби з порушеннями свободи медіа, покращення розслідування злочинів проти журналістів та забезпечення належного покарання винних. Ця кампанія головним чином орієнтована на журналістів, прес-ради, організації, що сприяють і захищають свободу медіа, суддів, прокурорів, правоохоронних органів, державних службовців, політиків, громадянське суспільство та заклади освіти, але вона також охопить широкі кола громадськості.

Як очікується, кампанія триватиме до кінця 2027 року, спрямована на протидію загрозам свободи преси в Європі, що відображається у зростанні випадків насильства та залякування журналістів та безкарності правопорушників.

Висновки.

В умовах сучасних змін у суспільно-політичному середовищі, особливо в умовах війни, соціальні мережі та Інтернет-платформи стають основними майданчиками комунікації та інформаційного взаємодії. Зростання ролі фіксерів, блогерів та інших медіа-учасників, як активних учасників цього процесу, підкреслює актуальність обговорюваної проблематики.

Законодавство інших країн частіше регулює окремі аспекти діяльності блогерів та інших медіа-учасників, такі як авторське право, реклама, захист даних тощо, але сам термін "блогер" не завжди має юридичне визначення.

Правове регулювання статусу та діяльності фіксерів, блогерів та інших медіа-учасників в Україні є актуальним з огляду на необхідність:

1) захисту їх професійної діяльності (поширення суспільно необхідної інформації);

2) притягнення їх до відповідальності за поширення забороненої законом інформації (стаття 28 Закону України “Про інформацію”, стаття 36 Закону України “Про медіа”, Законом України “Про державну таємницю” у разі допуску в установленому порядку відповідної особи до секретної інформації).

При цьому, гарантування безпеки й захисту журналістів та інших медіа-учасників є передумовою для їх можливості ефективно брати участь у суспільному обговоренні.

З огляду на наведене, потребує внесення змін у Законі України “Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста” в частині перегляду понять “журналіст” та “особи, що прирівнюються до журналістів”.

Забезпечення свободи слова та захист національної безпеки в умовах правового режиму воєнного стану в Україні є двома важливими цілями під час удосконалення правового регулювання діяльності журналістів, блогерів, фіксерів та інших медіа-учасників. Необхідність дотримання цього балансу полягає у створенні ефективного правового механізму, який б забезпечував свободу вираження думок, але водночас запобігав поширенню дезінформації та забороненої законом інформації, що може шкодити національній безпеці.

Використана література

1. Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста : Закон України від 23.09.97 р. № 540/97-ВР. *Відомості Верховної Ради України*. 1997. № 50. Ст. 302. URL: https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text

2. Про виконання рішень та застосування практики Європейського Суду з прав людини: Закон України від 23.02.06 р. № 3477-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 260. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text

3. Рішення Європейського Суду з прав людини у справі “Гонгадзе проти України”, заява № 34056/02 від 08.11.05 р. URL: https://minjust.gov.ua/files/general/2023/03/27/20230327181034-40.pdf

4. Isabel Wiseler-Lima Report on the protection of journalists around the world and the European Union’s policy on the matter (2022/2057(INI)). URL: https://www.europarl.europa.eu/doceo/document/A-9-2023-0206_EN.html?fbclid=IwAR25yz1P7ma-S90qPswrsOndx79YfBnZGBSEW6UaMOqXNw-UyMA9B1uHGaE

5. Про Рекомендації парламентських слухань на тему: “Безпека діяльності журналістів в Україні: стан, проблеми і шляхи їх вирішення”: Постанова Верховної Ради України від 14.01.20 р. № 456-IX. *Відомості Верховної Ради України*. 2020. № 29. Ст. 205. URL: https://zakon.rada.gov.ua/laws/show/456-IX#Text

6. Головенко Р.Б. Правовий статус блогерів в Україні: аналіз ЗМІ. URL: https://imi.org.ua/monitorings/pravovyj-status-blogeriv-v-ukrayini-analiz-imi-i53699

7. Національний класифікатор України ДК 003:2010 “Класифікатор професій”: наказ Держспоживстандарту України від 28.07.10 р. № 327. URL: https://ips.ligazakon.net/document/FIN5940J

8. Про умови оплати праці журналістів державних і комунальних суб’єктів у сфері медіа: Постанова Кабінету Міністрів України від 28.12.16 р. № 1038. URL: https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-postanovy-kabinetu-ministriv-ukrainy-vid-28-hrudnia-2016-r-1038-915-250823

9. Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors. – Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers’ Deputies. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9

10. Про медіа: Закон України від 13.12.22 р. № 2849-IX URL: //https://zakon.rada.gov.ua/laws/show/2849-20#Text

11. Нечипорук Я.В. Правовий статус блогера. *Юридичний електронний науковий журнал*. 2022. № 9/2022. С. 172-176. URL: http://lsej.org.ua/9_2022/41.pdf

12. Про правовий режим воєнного стану: Закон України від 12.05.15 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

13. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.21 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

14. War in Europe and the Fight for the Right to Report: Media freedom in Europe in 2023 – Partners' annual report. URL: https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680aa75e3

15. Україна vs росія: юридична боротьба в ЄСПЛ за притягнення країни-агресорки до відповідальності за порушення прав людини. URL: https://minjust.gov.ua/news/ministry/ukraina-vs-rosiya-yuridichna-borotba-v-espl-za-prityagnennya-kraini-agresorki-do-vidpovidalnosti-za-porushen nya- prav-lyudini

16. Journalists matter : Council of Europe launches campaign for the safety of journalists. URL: https://www.coe.int/en/web/freedom-expression/-/-journalists-matter-council-of-europe-launches-campaign-for-the-safety-of-journalists

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

УДК 347.4

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

ПРАВОВА ОХОРОНА КОМП'ЮТЕРНИХ ПРОГРАМ ЯК ОБ'ЄКТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Анотація. *У статті висвітлено поняття "комп'ютерна програма" та визначено сутність правової охорони комп'ютерних програм як об'єктів права інтелектуальної власності. Досліджено норми зарубіжного та вітчизняного законодавства з питань правової охорони комп'ютерних програм як об'єктів права інтелектуальної власності. З'ясовано, що у багатьох країнах світу комп'ютерні програми визнаються об'єктами як авторської, так і патентної охорони, якщо виконуються всі умови патентоспроможності (новизна, винахідницький рівень, промислова придатність). Розкрито проблеми правової охорони комп'ютерної програми як об'єкта авторського права за допомогою режиму комерційної таємниці. Проаналізовано питання юридичної відповідальності за порушення охорони комп'ютерних програм як об'єктів права інтелектуальної власності. Визначено доцільність застосування комплексного підходу до охорони комп'ютерних програм як об'єкту права інтелектуальної власності.*

Ключові слова*: комп'ютерна програма, інтелектуальна власність, авторське право, патент, програмне забезпечення.*

Summary. *The article highlights the concept of "computer program" and defines the essence of legal protection of computer programs as objects of intellectual property law. Foreign and domestic legislation regarding the legal protection of computer programs as objects of intellectual property law has been studied. It has been found that in many countries of the world, computer programs are recognized as objects of both copyright and patent protection, if all conditions of patentability (novelty, inventive step, industrial applicability) are met. The problems of legal protection of a computer program as an object of copyright using the trade secret regime are revealed. The issue of legal responsibility for violation of the protection of computer programs as objects of intellectual property law is analyzed. The expediency of applying a comprehensive approach to the protection of computer programs as an object of copyright has been determined.*

Keywords: *computer program, intellectual property, copyright, patent, software.intellectual property, official work, protection of copyright objects, official duties, creative activity.*

Постановка проблеми. У зв'язку з бурхливим розвитком інформаційних технологій, розширенням меж функціонального використання комп'ютерних програм виникає необхідність у їх належній правовій охороні. Вибір ефективної системи правової охорони комп'ютерних програм в Україні є предметом постійних дискусій у колах практикуючих юристів у зв'язку з тим, що такі програми є досить складним та комплексним об'єктом, окремі елементи якого можуть охоронятись різними інститутами права інтелектуальної власності [1]. Ускладнюють ситуацію відсутність уніфікованого понятійного апарату в цій сфері, а також те, що законодавство України містить численні прогалини та суперечності у сфері регулювання прав інтелектуальної власності на об'єкти інтелектуальної власності. Зміни до законодавства, серед яких,

зокрема, Закон України "Про авторське право і суміжні права" від 01.12.22 р. № 2811-IX, зумовлюють потребу подальшого дослідження правової охорони комп'ютерних програм. Проблема такої охорони є надзвичайно актуальною для світового співтовариства.

Результати аналізу наукових публікацій. Питання правової охорони комп'ютерних програм як об'єктів права інтелектуальної власності висвітлено у працях відомих вітчизняних вчених. Серед таких робіт можна назвати праці І. Ващинця [2], В. Дмитришина [3], Д. Жуванова [4], Канарик Ю.С. [5], З. Пічкурова, С. Петренка [6], Щербини Є.М. [7] та інших. Проте залишається не вирішеною низка питань щодо належної правової охорони комп'ютерних програм

Разом з тим констатується недостатній рівень наукової розробленості цієї проблеми в Україні. Не применшуючи теоретичну і практичну значимість проведених досліджень цієї теми, варто зазначити, що вони не вичерпують усіх аспектів проблеми правової охорони комп'ютерних програм як об'єкта інтелектуальної власності. Звертаючи увагу на період проведених досліджень зазначених авторів, потрібно вказати, що у них не враховано останні зміни у законодавстві у сфері охорони об'єктів інтелектуальної власності. Крім того, залишаються малодослідженими низка питань захисту таких інформаційних продуктів як об'єкта комерційної таємниці.

Викладене зумовлює актуальність і необхідність подальшого дослідження правової охорони комп'ютерних програм як об'єкта інтелектуальної власності.

Метою статті є висвітлення проблем правової охорони комп'ютерних програм як об'єктів права інтелектуальної власності, а також визначення шляхів щодо удосконалення такої охорони в контексті оптимізації законодавства у галузі права інтелектуальної власності.

Виклад основного матеріалу. Ефективність правової охорони комп'ютерних програм як об'єктів права інтелектуальної власності значною мірою залежить від правильного розуміння її сутності. Серед вчених немає єдності підходів щодо визначення сутності поняття "комп'ютерна програма".

Універсальний словник-енциклопедія визначає комп'ютерну програму як низку команд для комп'ютера, що становлять запис алгоритму однією з мов програмування [8].

На думку А. Музики і Д. Азарова, комп'ютерна програма є різновидом комп'ютерної інформації. Вона обов'язково містить певні відомості й одночасно є побудованою за особливими правилами, є сукупністю "зрозумілих" комп'ютеру даних (символів, кодів, сигналів, команд), яка забезпечує функціонування та керування комп'ютерними системами та/або телекомунікаційними мережами, виконання ними певних завдань[9, с. 86].

В. Дмитришин вважає, що "комп'ютерна програма" – це створений творчою діяльністю фізичної особи набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, втілений на носіях будь-якого виду (електронних, паперових) для використання в автоматичних пристроях для обробки інформації або іншому обладнанні, що базується на цифровій техніці з метою приведення його у дію для досягнення певної мети або результату [3, с. 16].

Відповідно до ст. 1 Цивільного кодексу України (далі – ЦК України) – комп'ютерна програма – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [10].

Слід зазначити, що поряд з терміном “комп’ютерна програма” отримали поширення терміни “програмне забезпечення”, “програмний продукт”, які є подібними за змістом. Людина при написанні програми для комп’ютера оперує поняттями, що виражаються за допомогою команд алгоритмічної мови [4].

Таким чином, програма містить алгоритм, написаний зрозумілою людині мовою (вихідний код). Комп’ютер може оперувати лише поняттями, вираженими лише у формі чисел (об’єктний код) [4]. Програма може бути записана у текстовому вигляді на мовах програмування, подана у графічному вигляді за допомогою блок-схем, занесена до пам’яті обчислювальної системи у вигляді електричних сигналів або збережена на носіях інформації у вигляді файлу.

Значимість комп’ютерних програм на сьогоднішній день зростає, вони є засобом створення, впровадження і розвитку новітніх технологій в різних галузях. Стрімкий розвиток комп’ютерних програм випереджає нормативно-правову базу, яка має здійснювати регулювання [1].

Спроби пошуку оптимального варіанту щодо визначення правової охорони змісту комп’ютерних програм тривають давно.

Фахівці з права інтелектуальної власності пропонували декілька варіантів охорони даних об’єктів за допомогою:

- засобів авторського права;
- засобів права промислової власності (патент);
- спеціальних режимів (режим конфіденційної інформації або промислових секретів).

Законодавство України у сфері інтелектуальної власності визначає комп’ютерні програми виключно як об’єкти авторського права. Так, ст. 420, ч. 2 ст. 433 ЦК України визначає комп’ютерні програми об’єктами авторського права [10]. Відповідно до ст. 18 ЦК України комп’ютерні програми охороняються як літературні твори [10]. Така охорона поширюється на комп’ютерні програми незалежно від способу чи форми їх вираження.

Водночас, згідно з ч. 3 ст. 8 Закону “Про авторське право і суміжні права” така правова охорона поширюється тільки на форму вираження твору і не поширюється на будь-які ідеї, теорії, принципи, методи, процедури, процеси, системи, способи, концепції, відкриття, навіть якщо вони виражені, описані, пояснені, проілюстровані у творі. Це означає, що в Україні охороняються авторським правом лише форми виразу комп’ютерних програм [11]. Технологічний процес обробки даних, так званий алгоритм, який доречно було б зарахувати до об’єктів права інтелектуальної власності, нині захистити проблематично, хоча така проблема є майже в кожної країни.

Враховуючи, що авторським правом охороняється лише форма вираження, слід зазначити, що при захисті комп’ютерної програми таким чином має значення код, а не ідея, концепція, принципи [1]. У такому разі можна, змінивши, наприклад, оформлення програми, але не змінюючи її суть, одержати зовсім новий об’єкт охорони. При цьому не можна вважати порушенням використання різними авторами у своїх розробках стандартизованого для певної мови програмування фрагмента вихідного тексту програми, який уперше був використаний іншим розробником, оскільки такий фрагмент є об’єктом, що не охороняється [1].

Забезпечуючи охорону комп’ютерних програм нормами авторського права, законодавець неминуче стикається з проблемами, зумовленими специфікою комп’ютерної програми, як об’єкта, що охороняється, оскільки в ній принцип роботи (алгоритм) має безумовний пріоритет над формою вираження (алгоритм, викладений

мовою програмування і представлений у вигляді вихідного тексту або об'єктного коду). Основне значення для комп'ютерної програми має її функціональність, яка зумовлюється алгоритмом, а написання програми на тій чи іншій мові програмування, тобто представлення її в тій чи іншій формі, може бути не важливим для користувача. Забезпечуючи охорону форми твору, авторське право об'єктивно не захищає алгоритм, що лежить в його основі. Тобто якщо запозичити алгоритм самої програми, то це не буде вважатись порушенням авторських прав, що є абсолютно неправильним [12].

Авторське право на твір виникає внаслідок факту його створення. Для виникнення і здійснення авторського права не вимагається реєстрація твору чи будь-яке інше спеціальне його оформлення, а також виконання будь-яких інших формальностей, автор не повинен доводити своє авторство в силу дії "презумпції авторства" [13, с. 97]. Строк охорони комп'ютерної програми як одного з об'єктів авторського права відповідно до Закону України "Про авторське право та суміжні права" триває протягом життя автора та 70 років після його смерті [11].

Як ми бачимо, правова охорона комп'ютерних програм за національним законодавством здійснюється за допомогою інституту авторського права, що відповідає вимогам Бернської Конвенції про охорону прав на літературні і художні твори. Відповідно до цієї Конвенції, до якої Україна приєдналася і з 25 жовтня 1995 р. стала її членом, а також згідно з п. 4 ст. 433 ЦК України та ст. 18 Закону України "Про авторське право та суміжні права" – комп'ютерні програми охороняються як літературні твори. Стаття 18 цього Закону у відповідності з міжнародними конвенціями, учасницею яких на сьогодні є Україна, встановлює, що комп'ютерні програми охороняються як літературні твори незалежно від способу чи форми їх вираження [11].

Нині практично в усіх країнах світу комп'ютерна програма охороняється авторським правом [1].

Протягом 1980-х рр. у США, Великобританії, Франції, Японії та інших країнах світу були прийняті зміни до законодавства про охорону авторських прав, що забезпечують захист програмного забезпечення.

Натомість у багатьох країнах комп'ютерні програми визнаються й об'єктами патентної охорони, якщо виконуються всі умови патентоспроможності (новизна, винахідницький рівень, промислова придатність). Насамперед йдеться про ті випадки, коли комп'ютерна програма є частиною технологічного процесу, технічного пристрою тощо й сумісно з ними може бути визнана об'єктом патентної охорони [13, с. 97].

Наприклад, у Сполучених Штатах Америки, зважаючи на високий рівень розроблення численних програмних продуктів, поряд із авторсько-правовою охороною комп'ютерних програм діє й патентно-правова охорона. За статистичними даними приблизно 30 тисяч патентів, виданих у різні роки Європейським патентним відомством, належать до комп'ютерних програм [4].

Прихильники охорони комп'ютерних програм за допомогою засобів права промислової власності зазначали, що комп'ютерні програми не завжди носять літературний чи художній характер, оскільки режиму охорони підлягає лише форма вираження. Дійсно, вважати комп'ютерну програму літературним твором є не зовсім логічним.

Закон України "Про охорону прав на винаходи і корисні моделі" визначає винахід (корисну модель) як результат інтелектуальної діяльності людини в будь-якій сфері технологій. Відповідно до п. 1.2 "Правил розгляду заявки на винахід та заявки на корисну модель", винахід – це технологічне (технічне) вирішення, що відповідає умовам

патентоздатності, а корисна модель – нове й промислово придатне конструктивне виконання пристрою [15].

Відповідно до ст. 459 та 460 ЦК України, ч. 2 ст. 6 Закону України "Про охорону прав на винаходи і корисні моделі", до об'єктів винаходу належать продукт (пристрій, речовина, штам мікроорганізмів, культура клітин рослини і тварини тощо), процес (спосіб), а до об'єктів корисної моделі – пристрій або процес (спосіб). Комп'ютерна програма може отримати правову охорону як винахід за умови, якщо вона: 1) є результатом інтелектуальної діяльності людини; 2) є технологічним (технічним) рішенням у будь-якій сфері технологій; 3) відповідає умовам патентоздатності, а саме має ознаки новизни, винахідницького рівня та є промислової придатності [1].

Хоча комп'ютерна програма як така не є технічним рішенням, тому не відповідає критеріям патентоздатності, вона може отримати правову охорону у складі технічних рішень, в яких використовується. За певних обставин алгоритм роботи комп'ютерної програми може отримати охорону шляхом отримання патенту на корисну модель або винахід як спосіб (процес) [1].

Патент на винахід дозволяє захистити змістовий бік програмного забезпечення, патентна охорона поширюється на сутність, утілену в алгоритмі, яка є основною ідеєю програми (якщо вона відображена в істотних ознаках формули винаходу) і запобігає її несанкціонованому використанню.

У Законі України "Про охорону прав на винаходи і корисні моделі" прямо не зазначено про патентоздатність комп'ютерних програм, що дає сподівання на певні можливості щодо часткового врегулювання цього питання нормами патентного права і в Україні [15; 13, с. 97].

Ще одним з можливих шляхів правової охорони комп'ютерних програм є спеціальний режим – режим конфіденційної інформації.

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (ст. 505 ЦК України) [10].

Статтею 420 ЦК України визначено, що комерційна таємниця є одним з об'єктів інтелектуальної власності. Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором (ч. 2 ст. 506 ЦК України) [10].

Ознаки комерційної таємниці, що властиві їй в силу самої сутності об'єкту, обумовлюють особливі умови надання об'єкту правової охорони: відсутність загальновідомості, відсутність загальнодоступності, оборотоздатність, відсутність потреби реєстрації об'єкту [15]. Відсутність загальновідомості полягає в тому, що інформацією володіє обмежене коло осіб, хоча й не обов'язково одна особа. Особи, які допущені до таємниці, повинні бути зобов'язані не розголошувати їх. Володілець виключних прав на інформацію, яка становить комерційну таємницю, вправі вживати заходів для збереження конфіденційності інформації, різновидами яких є: 1) посадові інструкції, які містять обов'язок дотримуватись комерційної таємниці; 2) трудовий договір (контракт) з працівниками, їхній обов'язок утримуватись від передачі цих

відомостей третім особам, повідомляти контрагентів, що певні відомості складають комерційну таємницю [15].

Право роботодавця пропонувати працівникам підписувати угоду про нерозголошення комерційної таємниці має бути передбачено в Статуті підприємства, колективному, трудовому договорі. Перед тим як взяти з працівників підписку про нерозголошення відомостей, що становлять комерційну таємницю, слід здійснити певні процедури: видати наказ по підприємству про встановлення комерційної таємниці (в державній установі за рішенням керівника комерційна таємниця може бути віднесена до конфіденційної інформації); затвердити перелік відомостей, що становлять комерційну таємницю (з урахуванням переліку відомостей, що не становлять комерційної таємниці, передбаченому постановою Кабінету Міністрів України від 09.08.93 р. № 611); додати умову про нерозголошення до посадових інструкцій та довести їх до відома працівників під розписку; затвердити форму зобов'язання (договору) про нерозголошення інформації, що є комерційною таємницею. Зобов'язання про нерозголошення інформації може бути оформлене як записом безпосередньо в тексті трудового договору (контракту), так і у вигляді окремого договору – договору (контракту) про нерозголошення конфіденційної інформації чи комерційної таємниці, приписи якого залишаються чинними в межах строку дії цього договору і після припинення трудових відносин доки така інформація є актуальною.

У разі розголошення працівником інформації, що становить комерційну таємницю, ці документи становитимуть юридичну основу для притягнення до відповідальності та відшкодування заподіяного збитку [4].

Кримінально караними визнаються умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності (ст. 231 КК України) [5]. Незаконне розголошення або використання в інший спосіб особою у своїх інтересах інформації, яка стала їй відома у зв'язку з виконанням службових повноважень, визнається адміністративним проступком (ст. 172-8 КУпАП).

Незаконне використання комерційної таємниці потребує доведення. До речі, українські суди дедалі частіше почали розглядати справи щодо захисту конфіденційної інформації та пов'язані з цим спори. Так, ТОВ (позивач) звернувся до суду і вказав, що його співробітниця, з якою був підписаний договір про нерозголошення відомостей, у період перебування на лікарняному здійснила несанкціонований доступ через корпоративну поштову систему до інформації, що містить комерційну таємницю, з подальшим розголошенням такої інформації компанії-конкуренту, з яким відповідач вступив у трудові відносини. Працівниця стверджувала, що інформацію не розголошувала, а в систему зайшла через цікавість. Суди всіх інстанцій, в тому числі Верховний суд у постанові від 28.12.19 р. у справі №752/5775/16-ц, погодилися з тим, що факт входження в корпоративну систему відповідача зі свого домашнього комп'ютера за допомогою власного пароля ще не свідчить про використання комерційної таємниці та про будь-які порушення прав позивача [17].

Слід зазначити, що інформація може бути визнана державною таємницею, а охорона комп'ютерних програм як об'єктів інтелектуальної власності, що містять секретну інформацію, проводиться з дотриманням вимог Закону України "Про державну таємницю". Ст. 8 цього Закону встановлює, що до державної таємниці відноситься інформація у сфері економіки, науки і техніки про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних

зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України [16]. Отже, така інформація може набути статусу державної таємниці, але суб'єктом прав на цю інформацію може бути як фізична чи юридична особа, так і держава. За загальним правилом майнові права на результати дослідження, що фінансувались з бюджету належать виконавцям, і лише у випадку віднесення до держтаємниці вказані права належать державі [18, с. 57]. Аналіз спеціального законодавства у сфері інтелектуальної власності з метою виявлення окремих норм щодо охорони таких об'єктів свідчить, що єдиним законодавчим актом, який містить такі норми є Закон України "Про охорону прав на винаходи і корисні моделі", а відтак засекречування інших об'єктів, крім винаходів і корисних моделей, не передбачено [18, с. 57]. Розголошення державної таємниці щодо названих об'єктів тягне за собою відповідальність за ст. 328 КК України.

У провідних країнах світу комерційна таємниця має розвинену систему правової охорони. Так, у більшості юрисдикцій США комерційна таємниця охороняється законами (42 штати та Округ Колумбія прийняли ту чи іншу версію Уніфікованого Закону про комерційну таємницю (Uniform Trade Secrets Act) 1979 року) [15]. Існує також значна кількість законів про кримінальну відповідальність за незаконне заволодіння комерційною таємницею, основним з яких є Федеральний Закон про економічний шпіонаж 1996 року. Виділяють такі чотири основні елементи режиму комерційної таємниці в США: 1) це повинна бути "обмежена інформація", тобто інформація, яку можна відрізнити від загальновідомих знань та навичок; 2) елемент "секретності" – інформація не є добре відомою або такою, яку можна легко отримати; 3) інформація повинна мати економічну цінність, що полягає у наданні певної конкурентної переваги; 4) володілець повинен вжити розумних зусиль для того, щоб зберегти інформацію в таємниці [15].

Одним з можливих засобів захисту комерційної таємниці в США та Великобританії є Угоди NDA (CA).Йдеться про угоди про нерозголошення (non-disclosure agreement or confidentiality agreement), які пов'язує сторони зобов'язаннями конфіденційності в межах цивільних та трудових відносин. Така угода може бути односторонньою або взаємною. В першому випадку вони слугують запобіганню витоку інформації, отриманої під час перемовин, і тим самим спрямовані на запобігання потенційним збиткам. В другому випадку має місце захист як правило торгівельних чи виробничих секретів [19].

Висновки.

Правова охорона комп'ютерних програм як об'єкта інтелектуальної власності зумовлює потребу застосування різних підходів захисту комп'ютерних програм:

1) традиційний захист комп'ютерної програми як об'єкта авторського права у межах якого перевагами визнаються простота та доступність охорони: авторське право не потребує ніяких додаткових дій, реєстрація не є обов'язковою; авторське право поширюється як на всю програму, так і на її окремі частини; строк дії захисту авторським правом досить значний і на практиці значно перевищує строк технічної експлуатації комп'ютерної програми; доведення порушення авторського права та визначення розміру компенсації за таке порушення, як правило, є менш складним [1];

2) захист комп'ютерної програми нормами патентного права (за умови, коли програма є складником корисної моделі або винаходу і виконує певну функцію в межах цього технічного рішення) [13, с. 98] допомагає захистити сутність, функції, алгоритм, інтерфейс комп'ютерної програми, її внутрішнє наповнення; дає виключне право

власності на саму ідею (якщо вона відображена в істотних ознаках формули винаходу) і запобігає її несанкціонованому використанню;

3) використання можливостей правового режиму охорони комп'ютерних програм за допомогою комерційної таємниці дозволяє: обрати простіший та менш витратний (порівняно, наприклад, із захистом об'єктів промислової власності) спосіб охорони комерційно цінних результатів інтелектуальної діяльності шляхом поширення режиму комерційної таємниці; забезпечити безстрокову охорону конфіденційної інформації [1]. Перевагою захисту комп'ютерної програми за допомогою інституту комерційної таємниці є те, що такий спосіб охорони не передбачає повного розкриття інформації третім особам [1]. В цьому контексті рекомендується включати норму про нерозголошення комерційної таємниці в трудовий договір (контракт) як керівника підприємства, так й інших співробітників, а до їх посадових інструкцій додати умову про нерозголошення такої таємниці.

Можливим є укладання окремих договорів про нерозголошення комерційної таємниці з працівниками підприємства, що визнається одним з ефективних засобів захисту комерційної таємниці в провідних країнах світу (США, Великобританії, Швейцарії, ФРН).

Крім цього, вбачається за доцільне впроваджувати на підприємствах комплекс заходів з організації захисту комерційної таємниці, визначивши перелік відомостей, які становлять комерційну таємницю підприємства. Корисним є проведення тренінгів з працівниками, оскільки сам факт визначення статусу комерційної таємниці та конфіденційності й підписання документів ще не гарантує, що працівники усвідомили свої обов'язки з інформаційної безпеки.

Враховуючи викладене, вважаємо, що найбільш доцільним є застосування комплексного підходу до охорони та захисту своїх прав на комп'ютерні програми. Такий підхід узгоджується з чинним законодавством України, підсилює рівень захищеності та створює умови для відновлення порушених прав і притягнення порушника до юридичної відповідальності.

Використана література

1. Грушевська Н. Правова охорона комп'ютерних програм: як правовласнику захистити свої права. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske - pravo/pravova-ohorona-kompyuternih-program-yak-pravovlasniku-zahistiti-svoyi-prava.html

2. Ващинець І. Особливості правової охорони прав інтелектуальної власності на комп'ютерні програми. URL: https://legalactivity.com.ua/index.php?option=com_content&view=article&id=649%3A081013-11&catid=80%3A3-1013&Itemid=99&lang=ru

3. Дмитришин В., Березанська В. Інтелектуальна власність на програмне забезпечення в Україні. Київ: "Вірлен", 2005. 304 с.

4. Жуванов Д., Стогний Е. Яку форму охорони обрати для комп'ютерної програми? URL: http://www.inventa.ua/content.php?l=17&p=103

5. Канарик Ю.С., Сергієнко Б.Б. Правова охорона комп'ютерних програм як об'єктів права інтелектуальної власності. *Правові горизонти*. 2019. Вип. 19 (32). С. 31-35.

6. Петренко С.А. Правова охорона комп'ютерної програми як об'єкта інтелектуальної власності: шляхи розвитку. URL: http://irbisbuv.gov.ua/cgibin/irbis64r_81/cgiirbis_64.exe?C21COM=2&I21DBN=ARD&P21DBN=ARD&Z21ID=&Image_file_name=DOC/2010/10psavsr.zip&IMAGE_FILE_DOWNLOAD=1

7. Щербина Є.М., Гетьман Я.В. Проблемні питання правової охорони комп'ютерних програм як об'єктів авторського права. *Право і суспільство*. 2018. № 6. С. 58-62.

8. Комп'ютерна програма. Словопедія. URL: https://web.archive.org/web/20141129025158; http://slovopedia.org.ua/29/53407/18909.html

9. Музика А., Азаров Д. Про поняття злочинів у сфері комп'ютерної інформації. *Право України*. 2003. № 4. С. 86-89.

10. Цивільний кодекс України: Закон України від 16.01.03 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

11. Про авторське право та суміжні права: Закон України від 01.12.22 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#n855

12. Пушкіна О.В., Тодорошко Т.А., Мамонова Ю.Г. Захист прав інтелектуальної власності на комп'ютерні програми: прогалини у праві, рекомендації щодо їх усунення та досвід інших країн світу. *Актуальні проблеми вітчизняної юриспруденції*. Спецвипуск, 2019. С. 65-68.

13. Канарик Ю.С., Козирь А.А. Актуальніпитання охорони комп'ютерних програм в Україні. *Юридичний електронний журнал*. 2020. № 7. С. 96-98.

14. Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.93 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text

15. Комерційна таємниця: правова природа та підходи до регулювання. URL: https://parlament.org.ua/2004/05/13/komertsijna-tayemnitsya-pravova-priroda

16. Про державну таємницю: ЗаконУкраїни від 21.01.94 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

17. Юлія Габрук. Охорона конфіденційної інформації та комерційної таємниці: як? що? навіщо? URL: https://ur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/ohorona - konfidenciynoyi-informaciyi-ta-komerciynoyi-taemnici-yak-shcho-navishcho.html

18. Москалюк Н.Б. Особливості правового статусу держави як суб'єкта права інтелектуальної власності на секретні винаходи і корисні моделі. *Юридичний електронний журнал*. 2016. № 4. С. 54-58.

19. Швець Б. Угоди про нерозголошення (NDA) в деяких закордонних системах. Англія. США. Швейцарія. ФРН. URL: https://yur-gazeta.com/dumka-eksperta/ugodi-pro-nerozgoloshennya-nda-v-deyakih-zakordonnih-sistemah-angliya-ssha-shveycariya-frn.html

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

УДК 347.77

МАНЬГОРА Т.В., *кандидат юридичних наук,* доцент кафедри права Вінницького Національного аграрного університету.
МОГИЛЕВИЧ А., магістр Вінницького Національного аграрного університету.

ТОРГОВЕЛЬНА МАРКА, ЯК ОБ'ЄКТ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Анотація. *В статті проаналізовано історичну ретроспективу зародження та становлення торговельних марок. Поняття інтелектуальної власності як самостійної правової категорії виникло у другій половині XIX століття, а також було визнано необхідність у юридичному захисті знаків індивідуалізації товару і товаровиробника. В українському законодавстві використовуються різні терміни, такі як "знак для товарів і послуг", "торговельна марка", "торговельний знак" і т. д., що викликає певні ускладнення в інтерпретації та застосуванні відповідних правових норм. На основі положень чинного законодавства та наукових доробків різних авторів було сформовано авторське визначення поняття "торговельна марка", окреслено його ознаки та ключові функції. З'ясовано, що законодавство України не наводить вичерпного переліку позначень, які можуть бути зареєстровані як торговельні марки. Замість цього, в законодавстві встановлюється загальний принцип "розрізняльної здатності". На практиці така абстрактність є негативним явищем, оскільки не дає особам, що бажають зареєструвати торговельну марку чітких критеріїв відповідності. Досліджено процедуру реєстрації торговельної марки. Відповідно особа, яка бажає зареєструвати певне позначення як торговельну марку, звертається до Національного органу інтелектуальної власності і подає заявку на реєстрацію. Робиться висновок, що свідоцтво на торговельну марку є офіційним документом, що підтверджує виключні права заявника на використання торговельного знака щодо конкретних товарів або послуг, зазначених у ньому.*

Ключові слова: *торговельна марка, інтелектуальна власність, Національний орган інтелектуальної власності, знак, свідоцтво, право власності.*

Summary. *The article analyzes the historical retrospective of the origin and development of trademarks. The second half of the nineteenth century saw the emergence of intellectual property as an independent legal category, and the need for legal protection of marks of individualization of goods and producers was recognized. It is established that Ukrainian legislation uses various terms, such as "mark for goods and services", "trademark", "trade mark" etc. This is a negative aspect, as it may cause certain misunderstandings and complications in the interpretation and application of the relevant legal provisions. Based on the provisions of current legislation and scientific works of various authors, the author formulates the definition of the concept of "trademark", and outlines its features and key functions. It is established that Ukrainian legislation does not provide an exhaustive list of designations which may be registered as trademarks. Instead, the legislation establishes the general principle of "distinctiveness". In practice, such abstraction is a negative phenomenon, since it does not provide persons wishing to register a trademark with clear criteria of compliance. The author analyzes the trademark registration procedure. According to this procedure, a person wishing to register a certain designation as a trademark applies to the National Intellectual Property Authority and files an application for registration. The author concludes that a trademark certificate is an official document confirming the applicant's exclusive rights to use a trademark in respect of specific goods or services specified therein.*

Keywords: *Trademark, intellectual property, National Intellectual Property Authority, mark, certificate, property right.*

Постановка проблеми. В даний час в умовах науково-технічного прогресу та глобалізації зростає кількість пропонованих споживачеві товарів. Для успішного здійснення підприємницької діяльності виробнику необхідно виділити свою продукцію з множини однорідних товарів різних виробників. Цю проблему покликані вирішити засоби індивідуалізації, одним із яких є торговельна марка (далі – ТМ).

Основним призначенням ТМ відповідно до Цивільного кодексу України є індивідуалізація товарів юридичних осіб або індивідуальних підприємців. Будучи візитною карткою для покупця, частиною корпоративного стилю, найбільш яскравою складовою будь-якого підприємства, що запам'ятовується, ТМ дозволяє легко ідентифікувати продукцію конкретного виробника, основні напрямки його діяльності, модні тенденції в дизайні, тощо у період розробки ТМ.

Торговельна марка – динамічно розвивається, як засіб індивідуалізації, що заслуговує на серйозну увагу з точки зору його правового регулювання. У світі число реєстрованих ТМ безперервно зростає. ТМ становлять значну частину активів великих українських та міжнародних компаній. Збільшення кількості реєстрацій ТМ породжує велику кількість суперечок, пов'язаних, зокрема, з виникненням численних колізій прав на різні об'єкти інтелектуальної власності. Насправді має місце існування різних, часом навіть суперечних одна одній, правових позицій. Такий стан речей вказує на необхідність удосконалення законодавчо встановленого механізму вирішення спорів, який, з низки причин, далеко не у всіх випадках є чітко визначеним.

Сучасні потреби правового регулювання ТМ вимагають модернізації з метою забезпеченості та сприятливості реалізації суб'єктами своїх виняткових прав. У зв'язку з цим об'єктивна необхідність проведення комплексного дослідження ТМ як засобу індивідуалізації є досить актуальною в даний час.

Метою статті є визначення історичних, теоретичних та практичних аспектів запровадження та дії торговельної марки, як об'єкта права інтелектуальної власності.

Виклад основного матеріалу. Використання ТМ та клейм на території України налічує багатовікову історію. Ще за часів Київської Русі майстри використовували маркування для позначення своїх виробів та ідентифікації своєї майстерності.

Гончари були одними з перших, хто почав використовувати ТМ в Україні. Гончарські вироби часто маркувалися спеціальними символами, знаками або клеймами, що дозволяло розпізнати виробника та його продукцію. Згодом, використання ТМ розповсюдилося серед представників інших професій, таких як ковалі, столяри, ювеліри та інші ремісники. Маркування виробів допомагало ідентифікувати виробника, відрізняти його вироби від інших та гарантувати якість. Ця практика залишалася актуальною і в подальших періодах історії України, включаючи часи Речі Посполитої, Австро-Угорщини, Польської та радянської держав. Використання ТМ продовжувалося, надаючи можливість ідентифікувати виробника та забезпечувати якість товарів.

Беручи до уваги те, що території України історично входили до складу тих чи інших держав, можемо відзначити, що перше офіційне згадування про ТМ зустрічається в російському законодавстві XVII століття. У 1667 році був прийнятий "Новоторговий Статут", який встановлював правила щодо внутрішньої і зовнішньої торгівлі. Згідно з цим статутом, висувалася вимога позначати певні товари клеймом, щоб відрізняти російські товари від іноземних. Клеймо також свідчило про сплату мита [1, с. 16].

У 1774 році був прийнятий "Статут про промисловість", який передбачав обов'язкове клеймування всіх російських товарів спеціальними фабричними або заводськими знаками. Це сприяло ідентифікації виробника та його продукції, а також забезпечувало контроль якості [2, с. 129].

В подальшому, були прийняті ряд законів, що регулювали охорону прав на ТМ. У 1830 році був прийнятий Закон "Про товарні клейма", який вимагав власників певних видів виробництва, таких як суконні фабрики, паперові фабрики та інші, мати спеціальні клейма для позначення своїх виробів. Це сприяло ідентифікації виробників і забезпеченню визнання їх продукції.

Останнім дореволюційним актом, що стосувався торговельних марок, був закон "Про товарні знаки" від 26 лютого 1896 року. Цей закон залишався чинним до Жовтневої революції. Однак після революції всі підприємства були націоналізовані, і потреба в торговельних марках втратила свою актуальність.

В період непу (Нової економічної політики) в СРСР відбулося відродження торговельних марок. У 1922 році було прийнято декрет "Про товарні знаки", який став основоположним законодавчим актом у галузі охорони прав на торговельні марки. Протягом наступних років, у СРСР було прийнято ряд законодавчих актів, спрямованих на регулювання торговельних марок і знаків обслуговування.

У 1936 році був прийнятий закон про обов'язкове нанесення "виробничої марки" на продукцію. Ця марка слугувала ідентифікаційним знаком підприємства-виробника і наносилася на вироби.

У 1965 році СРСР ратифікував Паризьку конвенцію про охорону промислової власності та Мадридську угоду про міжнародну реєстрацію товарних знаків. Це сприяло встановленню міжнародних стандартів у галузі охорони ТМ [3, с. 8].

У 1991 році був прийнятий Закон СРСР "Про товарні знаки і знаки обслуговування", який передбачав багато нововведень в системі охорони торгових марок. Проте, розпад СРСР унеможливив набрання цим законом законної сили, оскільки кожна новостворена незалежна держава почала формувати власне законодавство щодо ТМ.

Першим законодавчим актом в Україні, що регулює використання і охорону товарних знаків, було "Тимчасове положення про правову охорону об'єктів промислової власності та раціоналізаторських пропозицій в Україні", затверджене 18 вересня 1992 року [4]. Це положення стало важливим кроком у створенні правової бази для охорони товарних знаків в Україні.

У 1993 році був прийнятий закон "Про охорону прав на знаки для товарів і послуг" [5]. Цей закон надав правовий механізм для реєстрації та охорони товарних знаків відповідно до вимог національного законодавства.З цього часу почалася сучасна епоха ТМ в Україні.

Відповідно до статті 492 Цивільного кодексу України, ТМ може бути будь-яке позначення або комбінація позначень, які є придатними до вирізнення товарів або послуг, вироблених або наданих однією особою, від товарів або послуг, вироблених або наданих іншими особами. Такими позначеннями можуть бути слова, літери, цифри, зображувальні елементи, комбінації кольорів та інші елементи, які дозволяють вирізнити товари або послуги однієї компанії від інших. Важливо, щоб така марка достатньо відрізнялася та була індивідуальною, щоб виділятися на ринку та ідентифікувати конкретного виробника чи постачальника [6].

Відсутність єдиного терміну в українському законодавстві для позначення об'єктів, пов'язаних з інтелектуальною власністю, як "знак для товарів і послуг", "торговельна марка", "торговельний знак" тощо, створює певні складнощі.

Використання різних термінів є проблемою правової техніки і може бути розглянуто як недолік законодавства. Відсутність єдиного терміну ускладнює єдність та уніфікацію правових норм, а також може створювати плутанину в юридичній практиці.

Та незважаючи на використання різних термінів, їх зміст та концепція в основному співпадають, і вони використовуються для позначення об’єкта інтелектуальної власності, який використовується для ідентифікації товарів і послуг конкретного виробника чи постачальника.

ТМ є об’єктами промислової власності і використовуються як засіб індивідуалізації учасників цивільного обороту, зокрема виробників та продукції, яку вони виробляють. Вони дозволяють ідентифікувати конкретного виробника чи постачальника товарів і послуг і відрізняти їх від інших учасників ринку [7, с. 83].

Для розкриття змісту поняття ТМ та її функцій, окрім норм права, слід також звернутись до теоретичних джерел. Аналіз наукової літератури підтверджує інтерес багатьох учених до цього поняття.

Так, визначення ТМ, надане О. Марушевою, передає наступну сутність: ТМ є позначенням, що може включати слова, літери, цифри, зображувальні елементи, комбінації кольорів та інші символи або їх комбінації. Вона має на меті відрізняти товари або послуги одних суб’єктів (правовласників) від однорідних товарів або послуг інших суб’єктів. Правовласник ТМ має виключні права на використання цього позначення, надання дозволу третім особам на його використання і захист від незаконного використання третіми особами [8, с. 215].

На думку Ф. Котлера, ТМ є ім’ям, терміном, знаком, символом, малюнком або їх поєднанням, призначеним для ідентифікації товарів або послуг одного продавця або групи продавців та для відрізнення їх товарів або послуг від товарів і послуг конкурентів [9].

Зазначене визначення підкреслює два ключові аспекти ТМ – ідентифікацію та диференціацію. Воно вказує, що марка служить для ідентифікації товарів або послуг конкретного продавця або групи продавців, що означає встановлення їх унікальності і розпізнаваності. Крім того, марка використовується для диференціації або відрізнення товарів або послуг від аналогічних товарів і послуг, що надаються конкурентами. Ця диференціація може бути досягнута за допомогою ім'я, знаку, символу, малюнка або їх поєднання.

Автор також зазначає, що сама диференціація між ТМ та конкуренцією є обов’язковою умовою необхідності ТМ. Це означає, що марка має створювати відмінність від товарів і послуг, пропонованих конкурентами, і виокремлювати продавця чи групу продавців з ринкової конкуренції.

Аналіз визначень ТМ, які містяться в літературі та нормативно-правових актах, дійсно дозволяє виділити низку істотних ознак, що відрізняють її від інших засобів індивідуалізації та результатів інтелектуальної діяльності, зокрема це:

1) Нематеріальний характер. ТМ є нематеріальним об’єктом, що виявляється у формі позначення, символу, знаку чи їх поєднання, які ідентифікують товари або послуги.

2) Комерційна цінність. ТМ має велике значення для бізнесу, оскільки її використання дозволяє підвищити впізнаваність продукту чи послуги, збільшити конкурентоспроможність і позиціонувати їх на ринку.

3) Інформаційний зміст. ТМ несе інформацію про походження товару або послуги, виробника чи продавця, їх якість, характеристики, асоціації, що допомагають споживачам зробити вибір.

4) Розрізняльна здатність. Однією з головних функцій ТМ є забезпечення розрізнення товарів або послуг одних суб’єктів від однорідних товарів або послуг інших суб’єктів. Вона дозволяє впізнавати і відрізняти товари та послуги, які мають певну марку, від товарів та послуг інших виробників чи продавців.

Правову природу ТМ визначають виконувані нею функції,оскільки напрямки законодавчого регулювання значного обсягу питань щодо правової охорони досліджуваних об’єктів залежать саме від того змісту, який вкладається в поняття функції ТМ.

Так, ТМ виконує функцію ідентифікації, оскільки вона дозволяє споживачам легко впізнавати конкретного виробника чи постачальника товарів чи послуг, з якими вони мають позитивний досвід або до яких вони мають довіру. Така ідентифікація може базуватися на логотипі, назві, символічних елементах або комбінації цих факторів [10, с. 23].

Крім того, ТМ виконує функцію вирізнення, допомагаючи розділити товари та послуги одного виробника від товарів та послуг конкурентів на ринку. Вона дозволяє виробнику позиціонувати свої продукти як унікальні, відрізняючи їх від аналогічних товарів і послуг інших учасників ринку.

З цього приводу слушними є твердження, Г.Ф. Шершеневича, який висловлював думку, що споживачі, оцінюючи якість товарів певного походження, часто знаходять їх за допомогою відмітних ТМ. Згідно з Г.Ф. Шершеневичем, що більшу популярність має певний товар, то більше інших торговців мають спокусу використовувати цю ТМ, щоб привернути до себе частину споживачів шляхом введення їх в оману [7, с. 84].

Розвиток ринку товарів та послуг призводить до розширення функцій ТМ. Крім основної функції ідентифікації та вирізнення товарів або послуг одного виробника від інших, ТМ також виконують інші функції, що становлять комплекс функцій. Існує різноманітність поглядів щодо функцій ТМ [11, с. 92], тому ми проаналізувавши наукові положення, окреслили наступні функції ТМ:

1. Розрізняльна функція. ТМ допомагає розрізнити товари або послуги одного виробника від товарів або послуг інших виробників.

2. Інформативна функція. ТМ містить інформацію про виробника, постачальника або характеристики товару, що допомагає споживачам приймати рішення про покупку.

3. Рекламна функція. ТМ може виконувати рекламну роль, привертаючи увагу споживачів та підтримуючи відповідний образ товару чи бренду.

4. Охоронна функція. ТМ дозволяє виробнику або продавцю захистити свої права на використання марки та запобігти незаконному використанню або підробці.

5. Гарантійна функція. ТМ може служити як гарантія якості або походження товару, спонукаючи споживачів довіряти конкретній марці та пов’язувати її зі стандартами якості.

6. Психологічна функція. ТМ може створювати певну психологічну асоціацію, викликаючи в споживача певні емоції, інтерес або лояльність до бренду.

Наступним варто відзначити те, що ні Закон України “Про охорону прав на знаки для товарів та послуг” [5], ні Цивільний кодекс України [6] не наводять вичерпного переліку позначень, які можуть бути зареєстровані як ТМ. Однак обидва законодавчі акти встановлюють обов’язкову вимогу до позначень, які заявляються на реєстрацію як знаки для товарів і послуг – вони повинні мати розрізняльну здатність. Це означає, що позначення повинні бути придатними для вирізнення товарів чи послуг одного суб’єкта від інших суб’єктів.

Згідно з чинним законодавством України, умовні позначення різних форм відображення, такі як звукові, світлові, кольорові чи їх поєднання, можуть бути зареєстровані як знаки для товарів і послуг. Однак, реєстрація таких знаків залежить від технічної можливості їх внесення до Реєстру та оприлюднення інформації про їх реєстрацію. Національний орган інтелектуальної власності (далі – НОІВ) вирішує

питання реєстрації цих знаків з урахуванням таких технічних обмежень та вимог до проведення реєстраційних процедур [12, с. 32].

Класифікація позначень ТМ на традиційні і нетрадиційні є одним із підходів, запропонованих В. Крижною. Згідно з цією класифікацією, традиційні позначення включають візуально сприймаючі словесні та зображувальні елементи, а також комбіновані позначення, що поєднують словесні та зображувальні елементи. Вони є традиційними, оскільки використовуються з самого початку для вирізнення товарів і послуг.

Нетрадиційні позначення, згідно з цією класифікацією, з'явилися пізніше і мають особливості порівняно зі словесними та зображувальними позначеннями. Вони поділяються на візуальні та невізуальні. Візуальні нетрадиційні позначення можуть мати незвичайну форму, кольори, фігури тощо. Невізуальні нетрадиційні позначення можуть включати звукові елементи, запахи, текстури, характеристики товару, а також інші елементи, що не мають візуального вияву [13, с. 45-49].

За формою свого відображення знаки для товарів і послуг можуть бути словесні, зображувальні, об'ємні, комбіновані тощо.

Словесні знаки для товарів і послуг є одним із видів позначень і ТМ. Вони представляють собою оригінальні слова, словосполучення і фрази. Словесні знаки набули значної популярності через їх високу ефективність. Вони легко запам'ятовуються, зручні для реклами і легко помітні. Часто вони мають особливий смисловий зміст і вдалий звучання, що сприяє виникненню приємних асоціацій у споживачів.

Словесні знаки для товарів і послуг можуть бути дуже різноманітними. У минулому часто обиралися імена відомих людей, героїв художніх творів, міфологічних персонажів, назви тварин, птахів, рослин, дорогоцінних каменів, природних явищ, небесних тіл, географічних об'єктів тощо. Використання словесних знаків, похідних з давніх мов або штучно утворених слів (неологізмів), також є поширеним [16, с. 196].

У сучасних умовах також часто використовуються словесні знаки, що пов'язані з фірмовими найменуваннями комерційних організацій. Деякі словесні знаки можуть складати суттєві елементи фірмових найменувань. Також словосполучення і короткі фрази можуть бути зареєстровані як словесні знаки, при цьому охороняється не лише саме слово чи словосполучення, а й їхнє шрифтове рішення.

Зображувальні знаки для товарів і послуг представляють собою різноманітні візуальні елементи, такі як значки, малюнки, орнаменти, символи, зображення тварин, птахів, предметів і т.д. Вони можуть бути створені на основі відомих пам'яток історії та культури, архітектурних споруд, географічних об'єктів, народних орнаментів, а також можуть відображати зовнішній вигляд юридичної особи або продукції, яку вона пропонує на ринку [15, с. 47].

Досить поширеними є абстрактні зображення і різноманітні символи. Успіх зображувальних знаків для товарів і послуг визначається їхньою простотою, помітністю, ефектністю та можливістю використання на різних матеріалах. Важливо, щоб такі знаки були легкі для сприйняття і мали сильне смислове навантаження. Натомість, складні й перевантажені зайвими деталями знаки зазвичай є менш ефективними.

Об'ємні знаки для товарів і послуг є зображеннями, які мають тривимірну форму. Вони включають в себе довжину, висоту і ширину знака. Об'ємний знак може бути створений на основі оригінальної форми самого виробу або його упаковки. Наприклад, це може бути унікальна форма мила, свічки, пілюлі або оригінальна форма пляшки для напою.

Важливо зазначити, що об'ємний знак не повинен просто повторювати зовнішній вигляд виробу. Він має містити якийсь новий елемент або особливість, що робить його відрізняючим. Форма виробу, яка використовується як об'ємний знак, повинна бути оригінальною і спроможною виділити товар конкретного виробника серед подібних товарів на ринку [16, с. 197].

Один з найвідоміших прикладів об'ємного знаку для товару є оригінальна форма пляшки Coca-Cola. Форма пляшки стала візуальною ідентифікацією бренду і надзвичайно впізнаваною серед споживачів. Це є прикладом успішного використання об'ємного знаку для товару.

Комбіновані знаки для товарів і послуг є поєднанням словесних і зображувальних елементів. Це можуть бути комбінації малюнка і слова, малюнка і букв, малюнка і цифр, а також поєднання слів і цифр. В таких знаках словесні та зображувальні елементи співіснують і доповнюють один одного, створюючи єдину композицію.

Комбіновані знаки часто мають смислове навантаження, де слова і зображення взаємодіють, пояснюючи і доповнюючи один одного. Бажано, щоб словесна і зображувальна частини знаку утворювали єдину цілісність і були композиційно і сюжетно пов'язані між собою [15, с. 50].

Одним з найпоширеніших видів комбінованих знаків для товарів і послуг є етикетки. На етикетках часто поєднуються словесні та зображувальні елементи, де слова вказують на назву товару або бренду, а зображення доповнюють ілюстрацією або символікою, пов'язаною з товаром. Крім того, кольорове виконання етикеток також може мати значення для створення візуальної привабливості та відрізнення від інших товарів на полиці.

За ступенем популярності знаки для товарів і послуг розподіляються на звичайні та добре відомі (загальновідомі). Звичайними є будь-які нові позначення товарів, що відповідають усім критеріям охороноспроможності. Добре відомим знаком для товарів і послуг визнається таке позначення, яке знайоме широкому колу споживачів. Спір про те, чи є певний знак на території України добре відомим, вирішується судом. При цьому вирішальне значення має думка споживачів [16, с. 198].

Тобто, можемо коротко узагальнити, що вітчизняне законодавство не обмежується конкретним переліком позначень, які можуть бути зареєстровані як ТМ. Заявники мають широку свободу вибору знаків для реєстрації як ТМ, які можуть бути словесними, зображувальними, комбінованими, об'ємними, світловими та іншими видами знаків.

Для набуття права на ТМ, необхідно пройти процедуру реєстрації. Вона полягає в тому, що особа, яка бажає зареєструвати певне позначення як ТМ, звертається до НОІВ і подає заявку на реєстрацію.

До переваг реєстраційної системи набуття права власності на ТМ можемо віднести:

1) Фіксацію об'єкта правової охорони. Реєстрація ТМ є офіційним актом, який дозволяє закріпити правову охорону для певного позначення. Це означає, що власник марки має ексклюзивні права на використання цього позначення для вирізнення певних товарів або послуг.

2) Інформування інших осіб про права власника. Реєстрація ТМ є способом повідомлення іншим особам, таким як споживачі, виробники і т.д., про набуття власником виключних прав на певне позначення. Це здійснюється шляхом публікації про видачу свідоцтва на ТМ. Державна реєстрація знака в Реєстрі додає додаткову вагу і визнання його правового статусу.

3) Реєстрація ТМ є обов'язковою умовою для проведення міжнародної реєстрації ТМ на підставі Мадридської угоди про міжнародну реєстрацію знаків від 14.04.1891 р. [17, с. 216].

Отож, процедура реєстрація права на ТМ включає наступні кроки. Так, найперше, що має зробити особа, яка бажає отримати свідоцтво на ТМ, повинна подати заявку до НОІВ. Заявку може бути подано особисто або через представника у справах інтелектуальної власності або іншу довірену особу.

Заявка повинна стосуватися лише одного знаку. Вона повинна бути написана українською мовою і містити наступні елементи:

1. Заяву про реєстрацію знаку, в якій зазначається бажане зареєстроване позначення.

2. Зображення позначення, яке заявляється для реєстрації.

3. Перелік товарів і послуг, для яких заявник просить зареєструвати знак. Товари і послуги повинні бути груповані за Міжнародною класифікацією товарів і послуг для реєстрації знаків.

4. Зазначення заявника (заявників) та його (їх) адреси [18].

Якщо заявник бажає отримати охорону кольору або поєднання кольорів як розрізняльної ознаки свого знаку, він має виконати наступні вимоги:

- заявник повинен заявити про це і вказати в заяві конкретний колір або поєднання кольорів, охорону яких він просить;

- у заявці повинні бути подані кольорові зображення вказаного знаку.

При поданні заявки на реєстрацію ТМ, заявник повинен сплатити збір, розмір якого встановлюється з урахуванням кількості класів Міжнародної класифікації товарів і послуг для реєстрації знаків, якими охоплюються товари і послуги, зазначені в заявці [19].

З моменту подання заявки на реєстрацію ТМ особа набуває певних прав та можливостей:

1. Право пріоритету. Згідно зі статтею 4 Паризької конвенції про охорону промислової власності, особа, яка подала заявку на реєстрацію ТМ в одній країні-учасниці, має право пріоритету для подання подібної заявки в інших країнах-учасницях. Це означає, що протягом певного періоду (зазвичай 6 місяців) особа може подати подібну заявку в інших країнах і матиме пріоритет перед іншими заявниками, що подали подібні заявки пізніше [20].

2. Можливість подати міжнародну заявку. Згідно зі статтею 3 Протоколу до Мадридської угоди про міжнародну реєстрацію знаків, особа, яка подала заявку на реєстрацію ТМ в своїй країні, може подати міжнародну заявку для отримання міжнародного реєстраційного захисту своєї марки в різних країнах-учасницях Мадридської угоди. Це спрощує процес подання заявок у багатьох країнах шляхом подання єдиної міжнародної заявки [21].

Подача заявки на реєстрацію ТМ обмежує реєстрацію тотожної або схожої ТМ на ім'я іншої особи для таких самих або споріднених з ними товарів і послуг (п. 3 ст. 6 Закону України "Про охорону прав на знаки для товарів і послуг") [5].

Після подання заявки на реєстрацію ТМ проводиться її експертиза, яка включає дві основні складові: формальну експертизу та кваліфікаційну експертизу (експертизу по суті).

Формальна експертиза. Під час формальної експертизи перевіряються вимоги щодо відповідності заявки встановленим формальним вимогам та процедурним правилам. Це

включає перевірку правильності заповнення заявки, наявності всіх необхідних документів, відповідності розміру збору та інших адміністративних вимог.

Кваліфікаційна експертиза (експертиза по суті). Під час кваліфікаційної експертизи проводиться аналіз позначення, що заявляється, з метою визначення його відповідності вимогам щодо реєстрації ТМ. Експерти оцінюють, чи знак відповідає критеріям відновлюваності, розрізнюваності та незайнятості. Також вони перевіряють, чи не порушує заявка права третіх осіб [22, с. 144-145].

Після проведення експертизи можуть бути прийняті рішення про видачу свідоцтва на реєстрацію ТМ або відмову у реєстрації з підставами, які повинні бути обгрунтовані. У разі отримання відмови заявник може звернутися до НОІВ з клопотанням про перегляд рішення.

Видача свідоцтва на ТМ здійснюється НОІВ у місячний строк після державної реєстрації знака. Після отримання свідоцтва видається, процедура оформлення прав на ТМ вважається завершеною.

Свідоцтво на ТМ є офіційним документом, що підтверджує виключні права заявника на використання торговельного знака щодо конкретних товарів або послуг, зазначених у свідоцтві. Це означає, що заявник отримує ексклюзивні права на використання ТМ в комерційних цілях у відношенні визначених товарів або послуг, а також має можливість захищати свої права на марку в разі порушень інших осіб.

Зміст правових можливостей власника реєстрації позначення, а також межі їх здійснення ґрунтуються на основних принципах правової охорони ТМ, визначених міжнародними договорами та спрямованих на забезпечення бажаного балансу між приватними і державними інтересами, виключними правами і вільною конкуренцією.

Згідно з Угодою про торговельні аспекти прав інтелектуальної власності (TRIPS), права інтелектуальної власності, включаючи ТМ, вважаються приватними правами. Це означає, що власник ТМ має ексклюзивне право на використання цієї марки і може перешкоджати, забороняти або надавати дозвіл на використання марки іншим особам. Права на ТМ є абсолютними і виключними суб'єктивними правами, що означає, що власник марки має повне контроль над використанням марки. Інші особи не можуть використовувати ТМ, що охороняється в Україні, без дозволу власника прав на неї [23].

Суть права на використання ТМ полягає у можливості її необмеженого комерційного використання для позначення товарів чи послуг, які виробляються, реалізуються або надаються. Використання ТМ охоплює наступні дії:

1. Нанесення марки на товар. Це означає нанесення марки на сам товар, його упаковку, вивіску, етикетку, нашивку, бирку або інший предмет, пов'язаний з товаром.

2. Зберігання товару з нанесеною маркою: Власник марки може зберігати товар з нанесеною на нього маркою з метою його пропозиції для продажу.

3. Пропозиція для продажу, продаж, імпорт чи експорт: Власник марки має право пропонувати товар, на якому нанесена марка, для продажу, а також здійснювати його продаж, імпорт чи експорт.

4. Використання марки для послуг: Якщо марка зареєстрована для позначення послуг, власник марки може застосовувати її під час пропозиції та надання будь-яких зазначених послуг.

5. Використання марки в діловій документації, рекламі та в мережі Інтернет: Власник марки може використовувати марку в діловій документації, рекламних матеріалах, а також у доменних іменах в Інтернеті [24, с. 149].

Використання ТМ розглядається не тільки як право, але і як обов'язок власника прав на неї. Законодавство України передбачає можливість припинення дії прав на ТМ у

разі тривалого безперервного невикористання. Згідно зі статтею 18 Закону України “Про охорону прав на знаки для товарів і послуг”, права на ТМ можуть бути достроково припинені, якщо протягом трьох років підряд марка не використовувалася без обґрунтованої причини. Припинення дії прав на ТМ може бути повним або частковим [5].

Власник свідоцтва також має обов’язок добросовісно користуватися правами, що випливають із свідоцтва, згідно зі статтею 17 Закону України “Про охорону прав на знаки для товарів і послуг”. Крім того, допускається використання ТМ у формі, яка відрізняється від зареєстрованої лише окремими елементами, якщо це не змінює в цілому відмітності марки. Це означає, що деякі незначні зміни в марці можуть бути припустимими, якщо загальний характер та відмітні риси марки залишаються незмінними [5].

Варто відзначити, що особою, яка використовує ТМ, може бути як сам власник прав на марку, так і особа, якій такі права надані власником на підставі ліцензійного договору або ліцензії. Ліцензійний договір використовується для тимчасового надання права використання ТМ іншій особі (ліцензіату) власником марки (ліцензіаром) на певних умовах. Умови ліцензійного договору встановлюються сторонами і можуть включати вид ліцензії, платежі, розмір та порядок розрахунків, територію та термін дії договору та інші умови [25].

Однією з обов’язкових умов ліцензійного договору є забезпечення ліцензіатом певного рівня якості продукції, що маркується ТМ ліцензіара. Також ліцензіар має обов’язок здійснювати контроль якості такої продукції. Ці вимоги гарантують споживачам, що товари, позначені ТМ, відповідають певному стандарту якості. Якщо товари ліцензіата не відповідають встановленому стандарту якості, ліцензіар має право заборонити подальше маркування товарів переданою ТМ.

Також, власник свідоцтва на ТМ має виключне право забороняти іншим особам використовувати марку без його згоди в таких випадках:

1. Використання зареєстрованої марки щодо товарів і послуг, які зазначені в свідоцтві. Інші особи не мають права використовувати цю марку для тих самих товарів і послуг, які вказані в свідоцтві власника.

2. Використання зареєстрованої марки щодо товарів і послуг, які є спорідненими з тими, що зазначені в свідоцтві, якщо таке використання може ввести в оману стосовно особи, яка виробляє товари або надає послуги. Це означає, що інші особи не можуть використовувати марку для схожих товарів або послуг, якщо це може призвести до плутанини або оманливого сприйняття споживачами.

3. Використання позначення, яке схоже на зареєстровану марку, щодо товарів і послуг, які зазначені в свідоцтві, якщо таке використання може спричинити плутанину між цим позначенням і зареєстрованою маркою.

4. Використання позначення, яке схоже на зареєстровану марку, щодо товарів і послуг, які є спорідненими з тими, що зазначені в свідоцтві, якщо таке використання може ввести в оману стосовно особи, яка виробляє товари або надає послуги, або може призвести до плутанини між цим позначенням і зареєстрованою маркою [26, с. 92-94].

Власник прав на ТМ має право передати свої виключні майнові права на марку іншій особі, якщо це не суперечить законодавству та не вводить споживачів в оману. Передача прав на ТМ може здійснюватися шляхом укладання цивільно-правового договору, який може бути як платним, так і безоплатним.

Цим договором власник марки відмовляється від подальшого використання марки і передає всі свої права на марку набувачеві, який приймає на себе всі права та обов’язки,

пов’язані з власністю на ТМ. Цей процес називається відчуженням прав на ТМ. Проте існує обмеження, що передача прав на ТМ не допускається, якщо це може ввести споживачів в оману щодо товарів або послуг особи, яка виготовляє ці товари або надає зазначені послуги. Тобто передача марки не повинна спричинити плутанину або оманливе сприйняття споживачами. Це обмеження має на меті захистити споживачів від неправомірного використання марок та забезпечити їхню інформованість і безпеку при покупках.

Висновки.

Аналіз історичної ретроспективи показав, що ТМ з’явилася в епоху середньовіччя як реальна практика. У цей період виникла потреба в ідентифікації товарів та товаровиробників, а маркування продукції з допомогою знаків стало поширеним. Однак, відповідна правова категорія ТМ виникла значно пізніше.Справжній розвиток правового статусу ТМ відбувся у другій половині XIX століття. Цей період відзначився виникненням інтелектуальної власності як самостійної правової категорії, а також визнанням потреби у юридичному захисті знаків індивідуалізації товару і товаровиробника. Законодавство про ТМ було створено для регулювання правового статусу марок, їх реєстрації, використання та захисту.

В результаті аналізу визначень ТМ в національних нормативних актах, визначення її ознак та функцій сформулюємо своє авторське визначення.

Вважаємо, що під ТМ потрібно розуміти умовне позначення, яке має комерційну цінність у комерційному обороті і несе інформаційний зміст. ТМ може мати як абстрактну, так і конкретну розрізняльність, і вона призначена для індивідуалізації товарів.

Щодо видів ТМ, то вітчизняне законодавство не обмежує конкретним переліком позначення, які можуть бути зареєстровані як ТМ. Заявники мають широку свободу вибору знаків для реєстрації як ТМ, які можуть бути словесними, зображувальними, комбінованими, об’ємними, світловими та іншими видами знаків.

Набуття права на ТМ відбувається шляхом реєстрації марки відповідно до вимог законодавства про охорону прав на знаки для товарів і послуг в країні, де власник бажає отримати захист. Основним кроком у набутті права на ТМ є подання заявки на реєстрацію марки до відповідного органу інтелектуальної власності. Заявка повинна містити необхідну інформацію про марку, включаючи її зображення, опис товарів або послуг, які будуть позначені цією маркою, та інші вимоги, встановлені законодавством. Якщо заявка успішно пройшла реєстраційний процес і не має суперечностей, то власнику марки надається свідоцтво про реєстрацію. Це свідчення про те, що власник має право використовувати марку та захищати її від незаконного використання іншими особами.

Набуття права на ТМ дозволяє власнику використовувати марку у комерційній діяльності, включаючи маркування товарів або послуг, рекламу, продаж та інші дії. Також, власник має право забороняти іншим особам використовувати схожі марки або марки, які можуть спричинити плутанину серед споживачів щодо походження товарів або послуг.

Використана література

1. Мельник О.М. Правова охорона знаків для товарів і послуг в Україні (цивільно-правовий аспект): монографія. Ірпінь: Академія ДПС України, 2001. 137 с.

2. Козерацька О.В. Історичний аспект становлення торговельної марки як об’єкта інтелектуальної власності. *Науковий вісник Ужгородського національного університету: Серія:*

Право / гол. ред. Ю.М. Бисага. Ужгород: Видавничий дім "Гельветика", 2014. Вип. 28. Т. 1. С. 128-131.

3. Безух О.В. Захист від недобросовісної конкуренції у сфері промислової власності: автореф. дис. …канд. юрид. наук. Донецьк, 2001. 19 с.

4. Про Тимчасове положення про правову охорону об'єктів промислової власності та раціоналізаторських пропозицій в Україні: Указ Президента України від 18.09.92 р. № 479/92. URL: https://zakon.rada.gov.ua/laws/show/479/92#Text (дата звернення: 01.11.2023).

5. Про охорону прав на знаки для товарів і послуг: Закон України від 15.12.93 р. № 3689-XII. *Відомості Верховної Ради України (ВВР).* 1994. № 7. Ст. 36.

6. Цивільний кодекс України: Закон України від 16.01.03 р. № 435-IV. *Відомості Верховної Ради України (ВВР).* 2003. №№ 40-44. Ст. 356.

7. Романадзе Л. Поняття, функції та види торговельних марок. *Теорія і практика інтелектуальної власності.* № 5/2010. С. 82-88.

8.Марушева О.Г. Особливості визначення поняття торговельної марки. *Право і Безпека.* Харків, 2012. № 5. С. 214-217.

9. Kotler P., Jatusripitak S., Maesincee S. The Marketing of Nations: A Strategic Approachto Building National Wealth. NY: The Free Press, 1997. URL: http://mobiload.info/the-marketing66 4838.pdf

10. Ніколаєнко Л.І., Міняйло Л.А., Топільська Л.В. Знаки для товарів і послуг / за ред. В.Л. Петрова. Київ: Ін Юре, 1999. 116 с.

11. Кодинець А.О. Засоби індивідуалізації учасників цивільного обороту, товарів і послуг у цивільному праві України: дис. ...канд. юрид. наук: 12.00.03. Київ, 2006. 218 с.

12. Інтелектуальна власність та патентознавство: підручник / Н.О. Білоусова, Н.В. Гаврушкевич, М.А. Данильченко та ін. / за ред. проф. П.М. Цибульова та доц. А.С. Ромашко. – (НТУУ "КПІ" ім. Ігоря Сікорського). Київ: Вид-во "Політехніка", 2021. 374 с.

13. Крижна В. Види торговельних марок. *Теорія і практика інтелектуальної власності.* 2008. № 1(39). С. 44-51.

14. Самусь А. Класифікація торговельних марок у праві США та України: порівняльно-правовий аналіз. *Підприємництво, господарство і право*. 6/2018. С. 61-65.

15. Ромашко А.С. Торговельна марка: самостійний пошук, підготовка до реєстрації, моніторинг: навч. посіб. / А.С. Ромашко, О.М.Кравець. Київ: НТУУ "КПІ" ім. Ігоря Сікорського, 2016. 170 с.

16. Тараненко О.М. Види торговельних марок. *Науковий часопис НПУ імені М.П. Драгоманова*. *Серія 18: Економіка і право*. 2011. Вип. 16. С. 195-199.

17. Бошицький Ю.Л. Інтелектуальна власність в сучасній Україні – актуальні питання модернізації та правового регулювання. *Часопис Київського університету права*. 2013. № 1. С. 213-217.

18. Детальніше про торгові марки (товарні знаки) в Україні. – (Михайлюк, Сороколат і партнери). URL: https://www.msp-patent.com.ua/ua/torgovuje_marki.html#star01 (дата звернення: 03.11.2023).

19. Національна реєстрація торгової марки в Україні. – (Юстікон: юридична компанія). URL: https://justicon.ua/ua/service/nacionalnaa-registracia-torgovoj-marki-v-ukraine.html (дата звернення: 03.11.2023).

20. Паризька Конвенція про охорону промислової власності від 20 березня 1883 року: набула чинності для України 25 грудня 1991 р. № 995_123. URL: https://zakon.rada.gov.ua/ laws/show/995_123 (дата звернення: 04.11.2023).

21. Мадридська угода про міжнародну реєстрацію знаків: міжнар. док. від 14.04.1891 р. URL: http://zakon2.rada.gov.ua/laws/show/995_134 (дата звернення: 04.11.2023).

22. Разумова Г.В. Особливості реєстрації торговельної марки в Україні та зарубіжних країнах. *Приазовський економічний вісник*. 2019. Вип. 4(15). С. 142-147.

23. Угода про торговельні аспекти прав інтелектуальної власності: міжнар. док. від 15.04.1994 р. URL: https://zakon.rada.gov.ua/laws/show/981_018#Text (дата звернення: 05.11.2023).

24. Крат В. Торговельна марка як об’єкт права інтелектуальної власності. МЕН № 5 (95), 2017 р. С. 142-154.

25. Ліцензійний договір на торговельну марку в IT-індустрії. URL: https://go-advocate.com/litsenzijnyj-dohovir-na-torhovu-marku-v-it-industriji/ (дата звернення: 05.11.2023)

26. Киричук А.С., Топіна Я.Ю. Право інтелектуальної власності на торгову марку. *Економіка і суспільство.* Вип. № 13/2017. С. 89-95.

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

УДК 340.12:341.231.14

АНДРУЩЕНКО О.П., аспірантка кафедри філософії
Національного юридичного університету
імені Ярослава Мудрого.

ВПЛИВ ЦИФРОВІЗАЦІЇ НА ЦІННІСНІ ПРІОРИТЕТИ РОЗВИТКУ ПРАВ ЛЮДИНИ

Анотація. *Статтю присвячено впливу інформаційного суспільства на права людини. У сучасних умовах досліджено етапи еволюції інформаційних прав людини, які можна розглядати як самостійний комплекс прав, принципів, вимог, гарантій та механізмів захисту в рамках правоохоронної системи. Визначено, що на формування інформаційних прав впливає низка факторів, визначальним серед яких є інформатизація суспільного життя, що призводить до формування глобального інформаційного суспільства. Досліджено позитивні та негативні моменти впровадження цифрових трансформацій у повсякденне життя.*

Ключові слова: *права людини, інформатизація, інформаційні права людини, цифровізація, інформаційне суспільство.*

Summary. *The article is devoted to the influence of the information society on human rights. In modern conditions, the stages of the evolution of human information rights, which can be considered as an independent complex of rights, principles, requirements, guarantees and protection mechanisms within the framework of the law enforcement system, have been studied. It was determined that the formation of information rights is influenced by a number of factors, the most important of which is the informatization of public life, which leads to the formation of a global information society. The positive and negative aspects of the introduction of digital transformations into everyday life have been studied.*

Keywords: *human rights, informatization, human information rights, digitalization, information society.*

Постановка проблеми. Розбудова інформаційного суспільства супроводжується глобалізацією соціального простору, посиленням впливу інформації на усі сфери життя людини, розвиток кожного індивіда на основі знань та впровадження інноваційних технологій у суспільне виробництво та побут кожної людини. У сучасному світі інформація – це одна з головних рушійних сил розвитку та позитивних соціальних змін у суспільстві. Розвиток інформаційних технологій у глобальному середовищі привів до того, що у сучасному світі інформація стала ключовим поняттям, а інформаційний сектор – найбільш популярним.

Інформаційне суспільство суттєво змінює суспільні відносини, їх правове регулювання та деякі спільні цінності, породжує нові очікування та виклики. Використання технологічних інструментів здатне як вирішити, так і створити багато проблем. Такі інструменти можуть, серед іншого, сприяти утвердженню справедливості й рівності, підтримувати та розвивати демократію, а також забезпечувати прозорість, відкритість, контроль і взаємодію між публічною владою, індивідами та групами.

Результати аналізу наукових публікацій. Важливі аспекти впливу інформаційного суспільства на права людини висвітлюються багатьма вітчизняними вченими: Л. Климанська [1], Г. Луцишин [2], Ю. Размєтаєва [3], О. Данильян, О. Дзьобань [4], С. Матяж [5], А. Березянська [6] та інші. Водночас вплив цифровізації на ціннісні

пріоритети розвитку прав людини, з огляду на історично короткий час наукового опрацювання феномену цифровізації в цілому, все ще є малодослідженою темою в інфраструктурі життєдіяльності людства й процесах глобалізаційних змін.

Метою статті є уточнення основних аспектів впливу цифровізації на ціннісні пріоритети розвитку прав людини, появу інформаційних прав у сучасних умовах розвитку суспільства.

Виклад основного матеріалу. Уся історія людства є історією еволюції й трансформації самої організації життєдіяльності людських спільнот, міжособистісних та суспільно-владних взаємодій, відповідних тим чи іншим ноосферно-історичним умовам. Сучасна наука не надає однозначної відповіді на питання щодо часу та передумов формування засад інформаційного суспільства як стадії розвитку людської цивілізації. Однак наприкінці XIX – на початку XX ст. розпочинається трансформація технократичного суспільства в інформаційне, а питання правового регулювання інформації, встановлення меж такого регулювання стають принциповими для подальшого розвитку цивілізації. Саме в цей період з'являються перші філософські праці, що знаменують настання епохи, коли всі процеси суспільного життя будуть під контролем "інформаційного капіталу" (Е. Белламі, М. Вебер, Ю. Габермас, О. Шпенглер).

У середині XX ст. починає викристалізовуватися ціла концепція функціонування суспільства нового типу, основою якої є інформаційна діяльність як вид соціально-інтеграційної активності. І в XXI ст. з'являються нові типи інформаційних мереж, які відрізняються від традиційних ЗМІ минулого. У мережі Інтернет і віртуальних соціальних спільнотах починають діяти інші закони, цифрова мережа стає комфортним простором для більшості людей, які відчувають психологічний дискомфорт у реальному, фізичному середовищі. Однак формування інформаційного суспільства на рівні конкретних країн і регіонів відбувається різними темпами, має свою специфіку і в цілому має глобальний характер.

Зараз для нас настав саме такий час революційних перетворень, пов'язаних з переходом людства до наступної фази інформаційного суспільства – суспільства знань. Цей перехід позначається в повсюдних процесах оцифровки процедур і документів поточної діяльності, переведення значної їх частини в формат електронних сервісів, формування великих баз даних та оперування ними – поширенні феномена цифровізації в широкому його розумінні. У повній відповідності до послідовності алгоритму трансформації суспільно-владних відносин процеси цифровізації спочатку широко розповсюдилися в бізнесовому середовищі, швидко охопили медійно-комунікативну сферу й дедалі більше входять у простір державного управління й місцевого самоврядування.

Трансформація обумовлена розвитком інформаційного суспільства та поступовим переходом до суспільства знань, впливом цифровізації на всі суспільні процеси. Активне використання цифрових технологій у різних напрямках життєдіяльності зумовило постановку питання про необхідність і достатність прав і свобод людини і громадянина, та виокремило поняття цифрові права і свободи людини. Права і свободи людини виступають сьогодні одним з найважливіших орієнтирів розвитку концепції національної безпеки. Особисті права і свободи людини, як відомо, є невід'ємними від безпеки людини, суспільства і держави. За цих умов актуальною постає проблема пошуку балансу між захистом приватності, у тому числі інформаційної приватності життя людини, та потребами забезпечення національної безпеки взагалі й інформаційної безпеки зокрема. Інноваційність технологій викликає закономірні питання щодо правового регулювання таких правовідносин, потреби зміни та/або вдосконалення

механізмів забезпечення прав людини, а також виділення нових, які також можуть виступати об’єктом захисту.

Аналіз зв’язку між новими технологіями та правами людини є складним і вимагає попереднього розуміння певних компонентів. По-перше, існує еволюційний розрив між технічним прогресом і його правовим забезпеченням. Адаптація як національного, так і міжнародного законодавства до досягнень науки і техніки часто відбувається дуже повільно, і, як наслідок, законодавство не завжди може адекватно регулювати ситуації, спричинені технологічним розвитком. По-друге, зміни в технологіях свідчать про тенденцію розвитку нормативного регулювання на міжнародному рівні. Сучасні технології є продуктом цифровізації, і часто процес їх використання стає можливим завдяки телекомунікаційним системам і комп’ютерним мережам. Отже, права осіб можуть бути порушені діями осіб, які використовують такі технології, але знаходяться в інших юрисдикціях.

В умовах глобальної інформатизації суспільства та впровадження новітніх технологій важливим питанням є захист національних інтересів, забезпечення прав і свобод людини і громадянина не лише у відомих нам суспільних відносинах, але і в контексті нових викликів сучасного інформаційного впливу. Адже глобальне покриття мережі Інтернет, що забезпечує відкритість та доступність інформації, використання сучасних форм комунікаційних технологій, активне впровадження цифрових трансформацій у повсякденне життя має як позитивні, так і негативні моменти.

Що стосується позитивної сторони, то важливим елементом демократії є забезпечення рівного доступу та участі громадян, яких достатньо в інформаційному суспільстві. Наприклад, люди з обмеженими можливостями, які не можуть голосувати, залучаються до демократичного процесу за допомогою технічних засобів, таких як спеціальні машини для голосування або онлайн-вибори. Деякі технологічні інструменти дозволяють розпізнавати голос для тих, хто не може написати або роздрукувати петицію чи запит на публічний доступ. Водночас є питання щодо верифікації людей, безпеки використання даних, правильного підрахунку голосів, захисту від кібератак і шкідливих програм. Крім того, постає питання забезпечення всіх громадян технічними засобами та формування відповідних знань і навичок їх використання. Можна констатувати, що темпи розвитку цифрових технологій зумовлюють необхідність реалізації державної політики відповідно до сучасних вимог глобальної цифрової трансформації, що відбуваються у більшості державах світу. Більшість прогресивних, розвинених країн активно розвивають процеси впровадження е-демократії, е-урядування, е-комерції, е- туризму на основі сучасних цифрових технологій. Це є великим кроком на шляху до розвитку демократії, якомога повнішої реалізації прав громадян, зокрема на доступ до публічної інформації, державних послуг, послуг освіти, послуг у сфері культури.

О. Конюкова та С. Летунова наголошують, що “цифровізація покликана якісно змінити зміст державного управління, зокрема окремі процедури, стадії управлінського циклу, державні функції, їх склад та типи. Такі зміни мають привести до підвищення якості, результативності та ефективності органів державної влади та публічного управління, а також до забезпечення більшої обґрунтованості державного втручання з одночасним зменшенням загальної ролі держави в цілому” [7, с. 78]. Дійсно, революційні процеси широкого й системного застосування цифрових даних у системі органів публічного врядування докорінним чином змінюють якість державного та муніципального управління, постають ефективним інструментом вирішення соціально-політичних та економічних проблем.

Також характерною ознакою сучасної техногенної цивілізації є небачена для попередніх епох здатність до прогресу, швидке удосконалення існуючих технічних засобів і технологій та запровадження нових, у тому числі ІТ. Застосування у виробництві та побуті новітніх наукових знань та технологій потребує їх детального аналізу з метою систематизації за історичними, культурними та техногенними ознаками, а також в контексті їх впливу на розуміння загальнолюдських цінностей.

На думку С. Матяж і А. Березянської: "ціннісні орієнтації – це певна сукупність ієрархічно пов'язаних між собою цінностей, яка ставить людині спрямованість її життєдіяльності. Джерелом формування ціннісних орієнтирів є активність особистості, що визначає рівень прагнень та її орієнтацію у процесі діяльності на досягнення конкретних цілей" [5, с. 28]. Однак тривають дискусії щодо визначення ціннісних пріоритетів розвитку людства, бо у центрі уваги цінностей сучасного світу та європейської спільноти знаходиться людина, її права, добробут, здоров'я, освіта, правове виховання. Але в той же момент у світі відбуваються спади культури, девальвація цінностей, екології, гідності, справедливості, свободи і рівності в окремих країнах. У деяких випадках національні цінності підриваються, зобов'язання ігноруються, а права порушуються.

Дедалі більше дослідників демократії схиляються до думки, що стара форма демократії більше не підходить для суспільства, в якому дедалі більше людей отримують інформацію про різноманітні соціальні та політичні проблеми через доступ до інформаційних технологій. Демократична держава як інструмент, покликана сприяти інтересам суспільства, людей та впроваджувати в органи державної влади інформаційні та телекомунікаційні технології. Така держава отримує нові можливості для інформування громадян, врахування їх громадської думки з ключових питань, підвищення ефективності своєї роботи.

Цифрова революція вплинула на розвиток глобальної економіки та кардинально змінила її вектор розвитку в бік тотальної цифровізації усіх сфер як на макрорівні, так і на мікрорівні. Цифрові технології набули широкого використання в медицині, освіті, виробництві, фінансово-банківській справі, військово-промисловому комплексі, державному апараті та інших важливих секторах, які забезпечують національну безпеку країни. Як слушно зауважує науковець П. Богуцький: "Право на інформацію дедали більше набуває ознак одного з основних прав людини, а свобода електронних, цифрових комунікацій стає важливою для соціальних комунікацій, для реалізації можливостей кожної особи. Однак правове регулювання усього складного комплексу суспільних відносин, які виникають на основі електронних комунікацій, цифровізації суспільства, не є досконалим, не в усіх випадках супроводжує сам процес електронних комунікацій, не забезпечує ефективність цифрових змін, які дедалі більше набувають ознак революційних" [6, с. 45]. Отже, сучасний етап розвитку цифрових технологій полягає у трансформаційних змінах достатньо сформованої ціннісної системи світу.

Слід погодитися з Л. Климанською та Г. Луцишиною, які зазначають, що "розвиток інформаційних технологій, і насамперед, соціальних мереж, веде до послаблення інформаційної залежності пересічних громадян від традиційних ЗМІ та розширення діапазону доступних їм думок, в тому числі альтернативних; до появи у громадськості реальної можливості брати участь в обговоренні тих проблем, які турбують її найбільше; до посилення відкритості та транспарентності політики і політичних інститутів; до розширення меж взаємодії громадян з урядовими органами, що дає надію на те, що голос пересічного громадянина буде почутим; до виникнення нових, ефективних механізмів політичної мобілізації мас, які забезпечують оперативну

організацію та координацію дій політичних однодумців, підвищують шанси невеликих партій та представників політичних меншин, які отримують можливість звернення до широких масових аудиторій" [1, с. 143]. З цього приводу Ю. Размєтаєва стверджує, що "технології в інформаційному суспільстві не лише доповнюють і стимулюють розвиток демократії, а й впливають на оцінку демократичних процесів. Наприклад, їх можна використовувати для визначення ступеня демократичності режиму, зокрема за допомогою комплексних індексів демократії, які розраховуються авторитетними неурядовими організаціями. Розвиток технологій дозволяє поліпшити ці індекси, виключити грубі помилки під час вибірки, опрацювати величезний обсяг інформації, значно пришвидшити процес оцінювання. На додачу технології дозволяють відстежувати зміни в режимах, зокрема неочевидним способом. Наприклад, дають змогу перевірити, що змінилося в окремій країні після оголошеного реформування, чи дійсно публічною владою виконується або лише декларується рух до демократизації, відстежити тривожні й негативні зміни, отримати докази втручання до демократичних процесів тощо" [2, с. 107].

Власне, інформаційне суспільство є тим середовищем, у якому ефективно реалізуються цінності громадянського суспільства, це тип суспільства рівних можливостей, доступних для кожного.

Однак, не можна констатувати, що все однозначно і наслідки інформатизації є виключно позитивними. Глобальна інформатизація і нові інформаційні технології відкривають великі можливості в усіх сферах людської діяльності, але також породжують нові проблеми, пов'язані з інформаційною безпекою особистості, суспільства і держави. З цього приводу слушно зазначають О. Данильян та О. Дзьобань, що "надаючи органам влади тотальний доступ до широкої та конфіденційної інформації у поєднанні з наявністю ресурсів для її обробки та узагальнення, а також для формування інформаційного простору, інформатизація постає як потужний ресурс влади, що дає додаткові можливості соціального контролю, який ставить під загрозу особисті свободи громадян. У масштабах усього людства інформатизація стала інструментом глобалізації міжцивілізаційного конфлікту, дозволивши більш розвиненим та успішним в економічному плані країнам нав'язувати усьому світу свою систему цінностей. На рівнях індивідуальної та суспільної свідомості виявляється потужний інформаційно-психологічний вплив, що веде до політичної, економічної та культурної експансії розвинутих країн. Можливість такого впливу відкриває широкі перспективи для маніпулювання суспільною думкою, у зв'язку з чим "випливає" досить неприємний аспект інформатизації: під її впливом сучасне суспільство втрачає свою стійкість" [3, с. 18]. Отже, небезпечними для дотримання прав і свобод людини слід вважати такі інформаційні впливи, які загрожують дестабілізуючими, деструктивними, такими, що ущемляють інтереси особистості, суспільства й держави результатами.

Аналіз проблем сучасного інформаційного суспільства (локальні війни, небезпека ядерного конфлікту, зростання населення, енергетична криза, екологічні та медико-генетичні проблеми, поширення певних соціальних проблем та погіршення здоров'я людини і, як наслідок, бідність, самогубства, порушення психіки, алкоголізм, наркоманія, злочинність і роздробленість культури) дає підстави для висновку: земна цивілізація на межі тисячоліть вступила у фазу еволюційної кризи. Причинами кризи є дисбаланс між технологічною (зокрема, інформаційно-технологічною) складовою суспільного розвитку і духовним рівнем розвитку окремої людини та суспільства загалом [8, с. 21]. Спостерігаються домінування науки й інформаційних технологій,

інтелектуалізація багатьох сфер життя на фоні нерозуміння законів природи і вищого сенсу існування людини, зруйнування людиною своєї екологічної ніші.

Проблема цінностей в інформаційному суспільстві є викликом сьогодення, оскільки сьогодні існує нагальна потреба обґрунтування прав і свобод людини як суб'єкта права на отримання, використання та передачу інформації. Слід зазначити, що права і свободи людини певною мірою позанаціональні й позатериторіальні. Вони є загальнолюдськими, незалежними від ідеології, релігії та інших різновидів соціальних норм, тому повинні бути об'єктом міжнародно-правового регулювання. Конституція України 1996 року піднесла права і свободи людини і громадянина на якісно вищий рівень порівняно з попередньою Конституцією УРСР 1978 року. Вони закріплені й гарантовані Розділом ІІ Конституції України, причому права і свободи людини поставлені на перше місце. Це означає, що Україна відповідно до положень Міжнародного пакту про економічні, соціальні і культурні права, Міжнародного пакту про громадянські та політичні права, положень, що закріплені Загальною декларацією прав людини на конституційному рівні, ввела норми забезпечення прав і свобод людини [9].

Негативний ефект поєднання цінностей та інститутів демократії із цифровими технологіями також може проявлятися в таких аспектах, як прямі й опосередковані загрози для прав людини, вторгнення у приватність, вплив на ухвалення рішень і вільний вибір осіб у демократичних процесах, формування певної суспільної думки, радикалізація поглядів, успішне застосування елементів і прийомів інформаційної війни. Зазначені негативні ефекти можуть посилюватися через так званий "цифровий розрив".

Ю. Размєтаєва зазначає, що "цифровий розрив – це нерівність у доступі, навичках і способах використання інформаційно-комунікаційних технологій. Він також відображає соціальну й економічну нерівність у суспільстві. Деякі індивіди та групи можуть бути позбавлені можливості брати участь у супроводжуваних технологічними інструментами демократичних процесах через відсутність ресурсів (наприклад, обладнаних комп'ютерами приміщень), умінь і навичок (наприклад, невміння працювати із системами електронної верифікації особи), віку (наприклад, труднощі з освоєнням незвичних цифрових інструментів), ґендеру (наприклад, відсутність освітніх можливостей для жінок у певних суспільствах) тощо. Проблема цифрового розриву є не лише питанням доступу до технологій. Вона має три рівні: 1) проблема доступу до інформації, 2) проблема застосування правильних інструментів роботи з інформацією, 3) інформаційна сприйнятливість. Нарешті, цифровий розрив не зменшується, а навпаки, збільшується завдяки впровадженню деяких інновацій, а також через зміни у використанні інформаційно-комунікаційних технологій" [2, с. 107]. Отже, на перший погляд технології здаються нейтральним інструментом, але при ближчому розгляді багато з них мають як позитивні, так і негативні властивості чи застосування.

О. Андрієнко зазначив, що "процеси соціально-політичних трансформацій, що проходять у сучасному світі, зокрема у межах українського суспільства, є надзвичайно інтенсивними. Вони торкаються практично всіх сфер суспільного, політичного, економічного, культурного життя людей, але найбільш важливим є світоглядний вимір цих змін. У глобалізованій (або навіть "глокалізованій") реальності дедалі більш ефективно працює принцип "метелика". Цей принцип у даному випадку означає, що локальні зміни дедалі частіше набувають глобального характеру, оскільки світ сьогодні стає все більш цілісним завдяки бурхливому розвитку інформаційних технологій. В умовах потужних змін перед суспільством завжди постають проблеми світоглядного характеру, зокрема браку стабільної системи цінностей та орієнтирів, адже стан

постійних системних трансформацій, стан економічної невизначеності та соціальної дезорієнтації навіть психологічно є дуже важким для суспільної свідомості, що змушена переживати так звану “світоглядну кризу сучасності”. Ця криза є набагато глибшою, аніж та, що торкається фінансово-економічної галузі. Більше того, вона виступає однією з головних підвалин економічної кризи. Серед найбільш переконаних прибічників демократичного шляху суспільного розвитку останнім часом народився міф про те, що саме демократичний суспільний устрій найбільш повно відповідає біологічній природі людини, оскільки в ній закладено прагнення свободи. Демократичний устрій залишався до сьогодні кращим (хоча і не ідеальним) варіантом суспільного устрою, але він не здатний існувати без гармонійного балансу між особистісною свободою та інтересами суспільства і держави” [4, с. 96-97]. Тобто вітчизняні дослідники інформаційного суспільства звертають увагу на ті труднощі і ризики, з якими стикається сучасна людина.

Справедливо зазначає М. Хаустова, що “ідеологічною основою глобалізаційних процесів, є максимізація індивідуальної свободи, що відбивається в ідеології неолібералізму, згідно якої головне прагнення людини зводиться до досягнення високого рівня економічного, технологічного, політичного та інформаційного розвитку. Інструментом такого гуманітарного вияву є права людини та права народів як головні ціннісні характеристики тих умов їх життєдіяльності, які покликані забезпечити свободу, справедливість, гідність, ідентичність нації. Якщо будь-які аспекти глобалізації не витримують перевірки правами людини, слід однозначно визнати їх антигуманними” [10, с. 229]. У цих умовах актуальним є питання пошуку балансу між захистом приватного життя, в тому числі інформаційної таємниці життя людини, потребами захисту інформації та національною безпекою. Іншими словами, в умовах верховенства права та розвитку інформаційного суспільства обмеження прав людини, зокрема, у сфері інформації, мають бути визначені законодавчо. Ця проблема набула більшої актуальності в сучасних умовах цифрових трансформацій та запровадження надзвичайної ситуації, пов’язаної з карантином та обмежувальними заходами, а потім – з повномасштабним вторгненням, що дозволило виявити низку важливих питань, які потребують невідкладного вирішення.

Однак законодавча влада України увійшла у стрімкий етап суцільної діджиталізації усіх сфер суспільних відносин. Наприклад, 30 січня 2019 року було затверджено Засади реалізації органами виконавчої влади принципів державної політики цифрового розвитку [11], якими визначено окремі принципи реалізації державної політики цифрового розвитку, серед яких, зокрема, відкритість, прозорість, багаторазовість використання та орієнтованість на громадян (полягає в забезпеченні першочергового врахування потреб та очікувань громадян під час прийняття рішень щодо форм чи способів здійснення функцій держави) тощо. Згодом Кабінетом Міністрів України було затверджено Положення про Міністерство цифрової трансформації України [12] та Положення про Міжгалузеву раду з питань цифрового розвитку, цифрових трансформацій і цифровізації [13]. Надалі цифровізацію було визначено як процес впровадження цифрових технологій у всі сфери суспільного життя (частина перша статті 1 Закону України “Про Національну програму інформатизації” [14]). У період воєнного стану актуальним стало також питання підвищення рівня цифровізації сил безпеки та сил оборони України, про що було видано окрему Постанову Кабінету Міністрів України “Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану” [15].

Таким чином, розвиток та нормативне закріплення у різних сферах суспільного життя цифрових технологій актуалізує, зокрема необхідність оптимізації механізму реалізації конституційних прав людини і громадянина шляхом надання можливості їх здійснення, в тому числі й у цифровому форматі [16, с. 187]. Очікується також, що масова цифровізація усіх сфер суспільного життя значно спростить механізми забезпечення прав громадян. І якщо ще нещодавно потрібно було витратити значну кількість часу для реалізації окремих видів прав, то тепер реалізація більшості норм законодавства, створення та розірвання правовідносин стали оптимально доступними в смартфоні. Органи і установи державного апарату стали доступними і відкритими, систематично звітуючи в онлайн середовищі про свою діяльність. Здійснення громадського контролю за діяльністю органів держави стало можливим без прив'язки до місця твого перебування, чи країни знаходження.

Слід також зазначити, що нині потреби людини розмежовуються на соціально опосередковані, де індивід виступає як вільний член соціуму і демонструє соціально значущу відповідальну поведінку, та індивідуально опосередковані потреби, які визначаються виключно суб'єктивними прагненнями до самореалізації. Так, В. Андрущенко, Л. Горбунова, М. Култаєва, С. Пролєв та інші науковці стверджують, що сучасне суспільство, створюване глобалізацією і глобальним вільним ринком, характеризується переходом від раціональної утилітарної культури до змішаної глобальної культури; від політичної емансипації до політики "життєвого стилю"; від рівності до відмінностей; від організації, ієрархії до реорганізації, мереж; від фіксованої ідентичності до її плюралізації; від кінця ідеологій до варіації життєвих стилів і переконань [17]. Погодимося з думкою О. Бабкіної, що "сучасний стан правосвідомості українського суспільства характеризується глибокою внутрішньою суперечливістю, амбівалентністю, девіацією. Це пов'язано з процесами трансформації, що охопили всі виміри буття людини, поставили саму її в екстремальну ситуацію вибору власної позиції, пошуку ідентичних власній особистості цінностей та світоглядних орієнтирів. За короткий історичний період зруйнувалась вся система звичних правових і політичних уявлень, настанов, цінностей, норм і стереотипів, які визначали життя пересічної людини в попередню епоху. Суперечливість суспільних перетворень, нові економічні реалії разом з політичними технологічними, ідеологічними та інформаційними новаціями викликали певну правову та ціннісну дезорієнтацію в суспільстві, поставили питання політичної ідентифікації та самоідентифікації як суспільства в цілому, так і окремої особистості" [18, с. 8]. Тобто в умовах глобалізації відбувається низка змін щодо забезпечення безпеки людини та обмеження її прав. Це різке збільшення залежності рівня життя людей від інтересів транснаціональних компаній; зниження значення фактора регіональної обумовленості, що означає, що зміни в житті людини дедалі більше і частіше залежать від процесів, які знаходяться далеко від її місця проживання; зменшити роль національних кордонів, які втратили значення не лише для торгівлі, капіталу та інформації, а й для ідей, моральних норм, національної культури та цінностей; збільшення швидкості змін на ринках і технологіях, що сприяє прискоренню темпу життя та підвищенню рівня нестабільності в суспільстві.

Можна констатувати, що цифровізація є потребою часу, що трансформує державні процеси з метою ефективної взаємодії людини та держави, оскільки права людини є правовими можливостями, які необхідні для її життєдіяльності щодо задоволення її матеріальних, фізичних та духовних потреб. Цифрова трансформація визначається як соціальна трансформація на основі максимального використання цифрових технологій. До цифрових трансформацій схильні більшість звичних для громадян видів діяльності,

адже вже зараз цифрові технології стали базою для створення нових продуктів, цінностей та, відповідно, основою отримання конкурентних переваг на більшості ринків, що приводить до появи нових, унікальних систем і процесів з новою ціннісною сутністю. Йдеться, наприклад, про створення нових персональних приладів, цифрових моделей, застосування технологій Великих Даних (Big Data), Інтернету речей (Internet of Things), Хмарних обчислень" (Cloud Computing), нових методів аналізу даних і алгоритмів прийняття рішень, інших технологій цифровізації і роботизації, зорема штучний інтелект.

Висновки.

Кожен етап розвитку людських відносин у світі супроводжується певними змінами в соціальному, економічному, культурному та правовому житті, які безпосередньо впливають на сутність людини. Тому процес розвитку та реформування прав людини не припиняється й сьогодні.

На зміни людських цінностей вплинули глобальні фактори – перехід від індустріальної цивілізації до постіндустріальної. Ми спостерігаємо адаптацію всієї системи до глобального інформаційного простору. Технічні досягнення цивілізації, новітні технології змінили життя людства і відкрили нові можливості для кожного. Фундаментальною цінністю сьогоднішнього життя стала цінність індивідуального розвитку, суб'єктивної оригінальності, визнання індивідуальної унікальності.

Зміна суспільства пов'язана з розвитком інформаційного суспільства та поступовим переходом до суспільства знань, впливом цифровізації на всі суспільні процеси. Активне використання цифрових технологій у різних сферах життя призвело до питання про необхідність і достатність прав і свобод людини і громадянина. Внаслідок технологічних трансформацій змінилися спосіб життя сучасної людини та суспільства в цілому, що призвело до зміни системи цінностей та переорієнтації людини на психологічні, соціальні та моральні цілі.

Хоча новітні технології не можна вважати абсолютно нейтральними, їх слід розглядати в світлі економічного, соціального та політичного контексту, що розвивається. Оскільки технології постійно змінюються, їх вплив на життя людей і суспільства значною мірою залежить від їх формування під впливом багатьох факторів, головну роль серед яких, безумовно, відіграє правове регулювання. У зв'язку з цим підхід до забезпечення основних прав має бути пріоритетним. Однак і тут важливо враховувати, що такі права не залишаються незмінними, вони розвиваються, відображаючи розвиток суспільства, і переходять у сферу новітніх технологій.

Використана література

1. Климанська Л.Д., Луцишин Г.І. Парадокси інформаційної демократії. *Перспективи. Соціально-політичний журнал.* 2023. № 1. С. 142-152.

2. Размєтаєва Ю.С. Демократія, права людини та інтернет. *Право і суспільство*. 2020. № 1. С. 104-110.

3. Данильян О.Г., Дзьобань О.П. Інформатизація як атрибут інформаційного суспільства: від ретроспекції до сучасної рефлексії. *Інформація і право.* № 1(40)/2022. С. 9-20.

4. Андрієнко О.В. Постдемократія як відповідь на світоглядну кризу сучасності. *Наука. Релігія. Суспільство.* 2009. № 3. С. 96-100.

5. Матяж С.В., Березянська А.О. Класифікація цінностей та ціннісних орієнтацій особистості. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія"*. 2013. Т. 225. Вип. 213. С. 27-30.

6. Богуцький П. Цифрова трансформація соціальних комунікацій та національна безпека України: матеріали науково-практичної конференції *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*. Київ, 2020. С. 45-48.

7. Конюкова О., Летунов С. Роль цифровізації у державному управлінні. *Global & Regional Research.* 2019. № 1. 74-79.

8. Кушакова-Костицька Н.В. Інформаційне суспільство: інтегративний підхід. *Юридична психологія та педагогіка.* 2010. Вип.1 (7). С. 19-27.

9. Мельник К.Ю., Бабенко А.О. Проблеми юридичних гарантій трудових прав працівників при укладенні, зміні та розірванні трудового договору. URL: https://b-ok.org/book/3054810/ac7510 (дата звернення: 16.11.2023).

10. Хаустова М.Г. Права людини в епоху цифрових трансформацій під впливом глобалізаційних викликів: зб. тез доповідей ІІІ Всеукраїнської наукової конференції, присвяченої 60-річчю Хмельницького національного університету *Гармонізація законодавства України з правом Європейського Союзу*. Хмельницький: ХНУ, 2022. С. 229-234.

11. Деякі питання цифрового розвитку: Постанова Кабінету Міністрів України від 30.01.19 р. № 56. URL: http://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text (дата звернення: 16.11.2023).

12. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18.09.19 р. № 856. URL: http://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12 (дата звернення: 16.11.2023).

13. Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових трансформацій і цифровізації: Постанова Кабінету Міністрів України від 08.07.20 р. № 595. URL: http://zakon.rada.gov.ua/laws/show/595-2020-%D0%BF#Text (дата звернення: 16.11.2023).

14. Про Національну програму інформатизації: Закон України від 01.12.22 р. № 2807-IX. URL: http://zakon.rada.gov.ua/laws/show/2807-20#n191 (дата звернення: 16.11.2023).

15. Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану: Постанова Кабінету Міністрів України від 04.02.23 р. № 139. URL: http://www.kmu.gov.ua/npas/deiaki-pytannia-pidvyshchennia-rivnia-tsyfrovizatsii-s-a139 (дата звернення: 16.11.2023).

16. Костецька Т.А. Розвиток цифрової трансформації в Україні як умова забезпечення муніципальних прав і свобод.: збірник тез Міжнародної науково-практичної Інтернет-конференції *Діджиталізація та права людини*, м. Хмельницький, 30 берез. 2021 р. Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2021. С. 187-190.

17. Андрущенко В., Горбунова Л., Култаєва М., Пролєв С. Філософія і методологія розвитку вищої освіти України в контексті євроінтеграційних процесів. Київ: Педагогічна думка, 2011. 320 с.

18. Бабкіна О.В. Політико-правова культура демократичного типу: проблеми формування. *Науковий часопис Національного педагогічного університету імені М.П. Драгоманова.* 2011. Вип. 5. С. 5-10.

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

Цифрова трансформація

УДК 004.912

ЛАНДЕ Д.В., *доктор технічних наук, професор*, керівник Наукового центру інформатики і права ДНУ ІІБП НАПрН України,
завідувач кафедри НН ФТІ КПІ ім. Ігоря Сікорського.
ORCID: https://orcid.org/0000-0003-3945-1178.

ФОРМУВАННЯ СЕМАНТИЧНОЇ МАПИ ПОНЯТЬ В ГАЛУЗІ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ

Анотація. *У статті викладено методику формування моделі предметної області парламентського контролю у вигляді семантичної карти. Ця методика базується на використанні генеративних систем штучного інтелекту і програми аналізу і візуалізації мережевої інформації LegalGraph. Показано можливість формування семантичної карти предметної області, задачі, яка раніше потребувала залучення великих часових та людських ресурсів. Показано, як інтегруються засоби інтелектуальної текстової аналітики та аналізу і візуалізації мереж. Методика може застосовуватися для мережного аналізу інформації з будь яких предметних областей, побудови відповідних семантичних мап.*

Ключові слова: *семантична мережа, генеративний штучний інтелект, правова інформація, парламентський контроль, квазіієрархічна мережа, візуалізація.*

Summary. *The article presents a methodology for constructing a model of the subject area of parliamentary control in the form of a semantic map. This methodology is based on the use of generative artificial intelligence systems and the LegalGraph network information analysis and visualization program. It demonstrates the possibility of creating a semantic map of the subject area, a task that previously required significant time and human resources. It also shows how tools of intelligent text analysis and network analysis and visualization are integrated. This methodology can be applied to network information analysis in various subject areas and the creation of corresponding semantic maps.*

Keywords: *semantic network, generative artificial intelligence, legal information, parliamentary control, quasi-hierarchical network, visualization.*

Постановка проблеми. Останнім часом генеративні системи штучного інтелекту (далі – ГШІ), такі як ChatGPT (https://chat.openai.com), стають дедалі більш поширеними в різних галузях. Найпоширеніші застосування включають машинний переклад, резюмування текстів, створення різних рівнів обговорення, таких як формулювання питань до навчальних матеріалів. Великі можливості у виділенні основних концепцій та іменних сутностей роблять ChatGPT корисним у фактографічних системах, зокрема в медицині та економіці [1]. Звісно, інтелектуальні чати інтегруються з зовнішніми системами, такими як геоінформаційні [2], системи аналізу та візуалізації графіків і мереж [3]. Зокрема, в роботі [3] показано, як можна створювати мережі зв'язків між персонажами літературних творів і мережі в областях з відношеннями "загальне-часткове".

Такі системи ГШІ, як ChatGPT, зазвичай називають генеративними мовними моделями (GLM), великими мовними моделями (LLM) або просто мовними моделями (LM). Ці терміни широко використовуються в наукових і технічних колах для позначення систем, здатних генерувати текст на основі введення та контексту.

Основи та принципи таких систем, як ChatGPT, базуються на передових методах ШІ. Ці системи використовують глибоке навчання та моделі генерації мови для створення зрозумілих людині відповідей на текстові запити. Вони тренуються на великих обсягах даних, щоб зрозуміти контекст і створити відповідні та інформативні відповіді. Принципи роботи таких систем включають розуміння тексту, генерацію відповідей та покращення якості моделі за допомогою зворотного зв'язку та додаткового навчання.

Метою роботи є представлення нових можливостей обробки правової інформації із застосуванням систем генеративного штучного інтелекту, зокрема, ChatGPT, для вирішення задач побудови семантичних мап, семантичного індексування, аналізу та візуалізації, що дозволяє розглядати такі системи як корисний аналітичний інструмент в галузі права, зокрема, для здійснення парламентського контролю.

Виклад основного матеріалу. Ця стаття присвячена опису методики створення причинних мереж, отриманих шляхом багаторівневої декомпозиції поняття "Парламентський контроль" за допомогою системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою програми LegalGraph (https://bigsearch.space/legal.html). Створену мережу можна розглядати як семантичну карту, де кожен її вузол або зв'язок є гіперпосиланням, що веде до юридичної пошукової системи.

Парламентський контроль – це система, яка дозволяє парламентарям контролювати діяльність уряду. Ця система є важливою для забезпечення прозорості та підзвітності уряду перед народом [4]. Наведемо декілька причин актуальності застосування ГШІ при здійсненні парламентського контролю:

– *Ефективність*. ГШІ може автоматизувати багато завдань, які в даний час виконуються людьми, таких як моніторинг новин, аналіз даних та підготовка звітів. Це може звільнити час парламентарям для більш важливих завдань, таких як розробка законів та контроль за діяльністю уряду.

– *Прозорість*. ГШІ може використовуватися для створення нових інструментів, які підвищать прозорість діяльності уряду. Наприклад, ГШІ можна використовувати для створення чат-ботів, які можуть відповідати на запитання громадян про діяльність уряду.

– *Об'єктивність*. ГШІ може використовуватися для аналізу даних об'єктивно. Це може допомогти парламентарям приймати більш обґрунтовані рішення.

Звичайно, використання ГШІ у сфері парламентського контролю також пов'язане з деякими ризиками, такими як:

- *Зловживання ГШІ для поширення дезінформації*. ГШІ можна використовувати для створення фейкових новин або інших видів дезінформації, які можуть використовуватися для впливу на громадську думку або підриву довіри до уряду.

- *Непрозорість використання ГШІ*. Може бути важко зрозуміти, як ГШІ використовується для прийняття рішень, що може призвести до зниження довіри до парламенту.

Для того, щоб мінімізувати ці ризики, необхідно розробити чіткі правила та стандарти щодо використання ГШІ у сфері парламентського контролю. Ці правила повинні враховувати такі аспекти, як прозорість, відповідальність та справедливість.

Загалом, парламентський контроль на базі ГШІ має потенціал для революціонізації сфери парламентського контролю. Ця технологія може допомогти парламентарям бути більш ефективними та прозорими, а також може допомогти їм приймати більш обґрунтовані рішення.

Основна проблема, яка виникає при створенні семантичних карт, полягає в тому, що зазвичай для цього потрібні великі ресурси та залучення експертів. Звісно, існують

віддалені спроби автоматизованого створення каузальних мереж; однак запропонований підхід створення рою віртуальних експертів [5] може суттєво спростити і прискорити цей процес.

Формування семантичної мапи.

Прикладом моделі предметної області "Парламентський контроль", в якості якої можна представити мережевий масив даних, який буде зручним для обробки комп'ютером, є направлена зважена мережа термінів. Направлена зважена мережа термінів (Directed Weighted Network of Terms – DWNT, або просто мережа термінів) – це семантична модель предметної області, де мережі є ключові терміни (слова та словосполучення), що відповідають сутностям, назвам концептів предметної галузі, а ребра – семантичні зв'язки між цими термінами. Порівняння DWNT, отриманих для різних текстів, дає змогу визначити семантичну близькість відповідних текстів.

У даному випадку нас, наприклад, цікавить проблематика парламентського контролю, тому запросимо у сервісу ChatGPT декомпозувати це поняття і видати відомі їй часткові поняття, що складають суть парламентського контролю. Тобто. центральним вузлом майбутньої мережі має стати поняття "Парламентський контроль". Успішне відпрацювання такого запиту визначить другий рівень ієрархії – поняття пов'язані з парламентським контролем, відповідні часткові поняття. Після цього для кожного такого часткового поняття також здійснюється декомпозиція. Такий процес може тривати нескінченно, але в роботі зупинимося лише на трьох рівнях. Незважаючи на ієрархічне формування такої мережі, отримана мережа загалом не буде строго ієрархічною структурою, а скоріше близькою до неї квазіієрархічною. Деякі часткові поняття при декомпозиції різних понять можуть співпадати.

Найчастіше при використанні ГШІ сутності або пари сутностей (а саме це потребується при побудові мережевих структур) можнуть витягувати безпосередньо з навченої моделі системи. Запропонувавши ChatGPT відпрацювати деякий запит (промпт), отримаємо множину часткових понять первинного поняття. Промпт для виявлення сутностей – результатів декомпозиції основного поняття може мати такий вигляд:

Декомпозуйте поняття "парламентський контроль". Виведіть 10 сутностей, які разом утворюють це поняття. Інформацію (позначення сутностей) прошу виводити у вигляді переліку окремих коротких записів без додаткових пояснень

У результаті ГШІ видає відповідь такого вигляду:

1. Парламент
2. Контроль
3. Нагляд
4. Виконавча влада
5. Звітність
6. Вплив
7. Механізми
8. Комітети
9. Голосування
10. Співпраця.

Система ChatGPT може надати різні відповіді під час обробки тексту в різний час, і всі вони розумні з точки зору людської логіки. Кожну з цих відповідей можна сприйняти як відповідь штучного експерта. Узагальнивши відповіді багатьох таких експертів, можна отримати більш повну і точну відповідь. Тому наведений промпт можна задати системі декілька разів, запустивши тим самим "рой віртуальних агентів". Багаторазове виконання дозволяє отримати різні відповіді, багато з яких співпадуть. Із статистичного погляду, – це самі достовірні результати. У разі розгляду первинного поняття "Парламентський контроль", отримуємо такі поняття:

ПАРЛАМЕНТ
КОНТРОЛЬ
НАГЛЯД
ВИКОНАВЧА ВЛАДА
ЗВІТНІСТЬ
ВПЛИВ
МЕХАНІЗМИ
КОМІТЕТИ
ГОЛОСУВАННЯ
СПІВПРАЦЯ

Після виконання першого етапу – отримання результату декомпозиції, для кожного із отриманих часткових понять здійснюється подальша декомпозиція за допомогою промптів типу:

Декомпозуйте поняття "ВИКОНАВЧА ВЛАДА" виходячи із його функціональності як частини парламентського контролю. Виведіть **10** сутностей, які разом утворюють це поняття з погляду парламентського контролю. Інформацію прошу виводити у вигляді переліку окремих коротких записів у форматі "ВИКОНАВЧА ВЛАДА; сутність" без додаткових пояснень

При цьому система ChatGPT може допомогти отримати зміст CSV-файлу (поля, розділені точкою з комою), а саме:

ВИКОНАВЧА ВЛАДА; ВИКОНАННЯ ЗАКОНІВ
ВИКОНАВЧА ВЛАДА; РЕГУЛЮВАННЯ ГАЛУЗЕЙ ГОСПОДАРСТВА
ВИКОНАВЧА ВЛАДА; РОЗРОБКА ТА ВИКОНАННЯ БЮДЖЕТУ
ВИКОНАВЧА ВЛАДА; ЗОВНІШНІ СПРАВИ
ВИКОНАВЧА ВЛАДА; НАЦІОНАЛЬНА БЕЗПЕКА
ВИКОНАВЧА ВЛАДА; ПРИЗНАЧЕННЯ ГРОМАДСЬКИХ СЛУЖБОВЦІВ
ВИКОНАВЧА ВЛАДА; ГУБЕРНАТОРИ (У ФЕДЕРАЛЬНИХ СИСТЕМАХ)
ВИКОНАВЧА ВЛАДА; АДМІНІСТРАТИВНІ РІШЕННЯ
ВИКОНАВЧА ВЛАДА; КОНТРОЛЬ ЗА БЮДЖЕТНИМИ ВИДАТКАМИ
ВИКОНАВЧА ВЛАДА; ВІДПОВІДНІСТЬ КОНСТИТУЦІЇ

Такого типу відповіді можуть слугувати інформаційною основою для побудови графових структур – семантичних мап, які одночасно є джерелом посилань, тому що кожний вузол і кожний зв'язок цієї мережі містить гіперпосилання на відповідні запити до пошукової системи порталу Верховної Ради України (https://zakon.rada.gov.ua/laws). Кожне екстраговане поняття може розглядатись як вузол мережі. Крім того, з подібним промптом можна звернутися до декількох систем ШІ, серед яких ChatGPT, Bard

(https://bard.google.com/chat), GPT Free (https://gptfree.co) тощо. Після отримання відповідей від різних систем їх можна поєднати, при цьому реалізується концепція "віртуальних експертів", якими виступають такі системи.

Аналіз і візуалізація семантичної мапи.

Аналіз мереж є важливим методом для розуміння взаємозв'язків між об'єктами та виявлення зв'язків між ними, що може значно полегшити дослідження конкретної сфери. Для проведення аналізу та візуалізації мереж, спільно з системами, подібними до ChatGPT, можна використовувати сучасні графові інструменти, такі як Neo4j та Gephi [7]. Однак при використанні таких програмних продуктів аналітики стикаються з двома труднощами: потребою встановлення програм, що не завжди можливо, особливо при обмеженнях на встановлення стороннього програмного забезпечення, та потребою досконально вивчити особливості функціонування цих систем, розібратися в численних параметрах, режимах розміщення графів, кластеризації тощо.

Для вирішення проблеми на основі бібліотеки системи GrahViz розроблено програму LegalGraph, доступного наразі в Інтернет за адресою https://bigsearch.space/legal.html. Ця програма забезпечує первинний аналіз і відображення графів, інформація про які відповідає формату CSV (від англ. Comma-Separated Values – значення, розділені комою), кожен запис в якому відповідає парі сутностей. При цьому кожному вузлу і ребру графа у відповідність ставиться гіперпосилання на законодавчу базу даних, розміщену в Інтернеті.

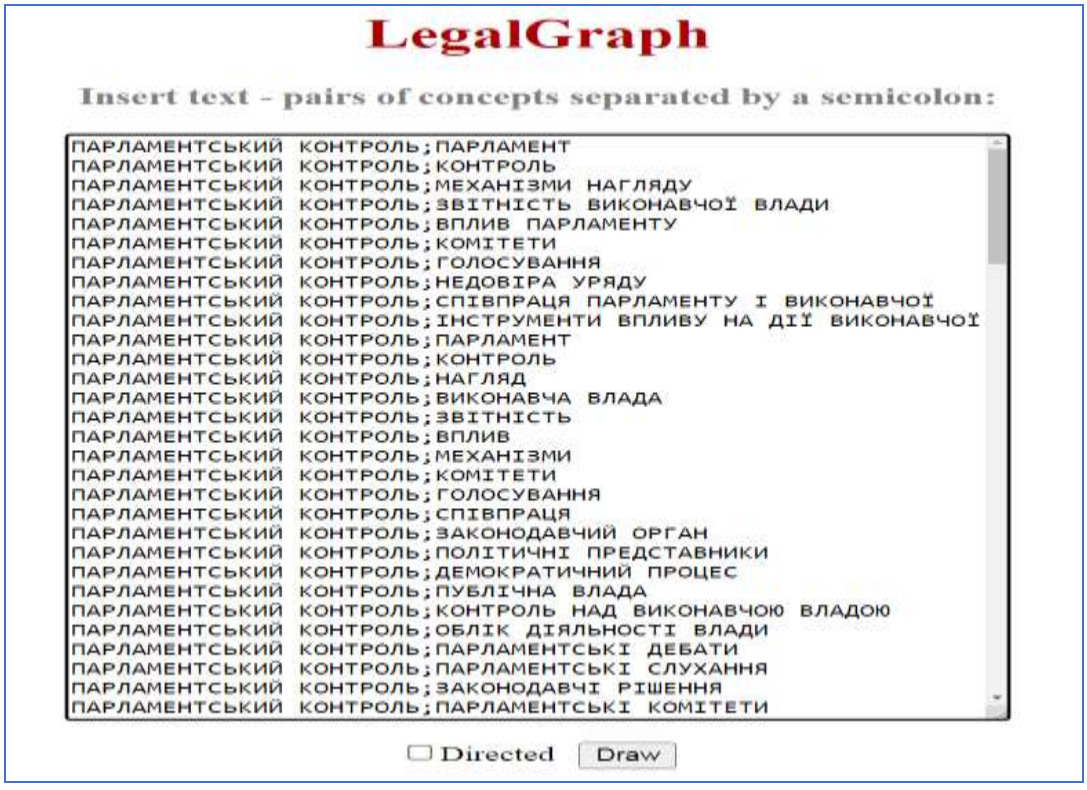

Рис. 1. Інтерфейс введення інформації в системі LegalGraph.

На Рис. 2 показано результат – фрагмент семантичної мапи предметної області "Парламентський контроль", який було сформовано на ресурсі сервісу ChatGPT. Як бачимо, ця мережа квазіієрархічна, до вузлів, що поєднують різні часткові поняття, тобто є транзитними, відіграють особливу роль в процесі парламентського контролю, віднесено такі:

КОНТРОЛЬ ЗА ВИКОНАВЧОЮ ВЛАДОЮ;
ЗВІТНІСТЬ ВІИКОНАВЧОЇ ВЛАДИ;
ПАРЛАМЕНТСЬКІ СЛУХАННЯ;
АУДИТ БЮДЖЕТНИХ ВИТРАТ;
ЗВІТУВАННЯ ПЕРЕД ПАРЛАМЕНТОМ;
ІНСПЕКЦІЇ ТА РЕВІЗІЇ;
ЗАКОНОДАВЧИЙ ОРГАН.

У наведеному графі – семантичній мапі предметної області кожний вузол і кожне ребро виступають гіперпосиланнями на пошукову систему. При активізації такого гіперпосилання здійснюється перехід на сторінку цього веб-ресурсу з результатами пошуку (Рис. 3).

Програмою формується відображення орієнтованих графів, вузли ранжуються за ступенем і розфарбовуються, визначається товщина і напрямок ребер. Покладання графа на площину виконується методами, вбудованими в GraphViz. При цьому формується зображення графа у форматі SVG, що дає можливість формувати гіперпосилання, що ведуть до пошукових форм системи Верховної Ради України. з вузлів і ребер графа. Масштабована векторна графіка (SVG) – це формат для визначення двовимірної графіки за допомогою XML. Він підтримує інтерактивність. Специфікація SVG, відкритий стандарт, розроблений World Wide Web Consortium з 1999 року, дозволяє масштабувати зображення без втрати якості. Ці зображення зберігаються в текстових XML-файлах, що робить їх доступними для пошуку, індексування, сценаріїв і стискання. Усі основні настільні браузери почали підтримувати SVG. Дані у файлі SVG є текстом, а не зображенням, тому можна вбудовувати інтерактивні функції, такі як гіперпосилання на веб-ресурси, які використовуються в програмі LegalGraph. Реалізація гіперпосилань надає можливість перегляду нормативних документів, що з одного боку надає інформаційне розкриття поняття або зв’язку, а з іншого – підтверджує коректність побудови семантичної мапи.

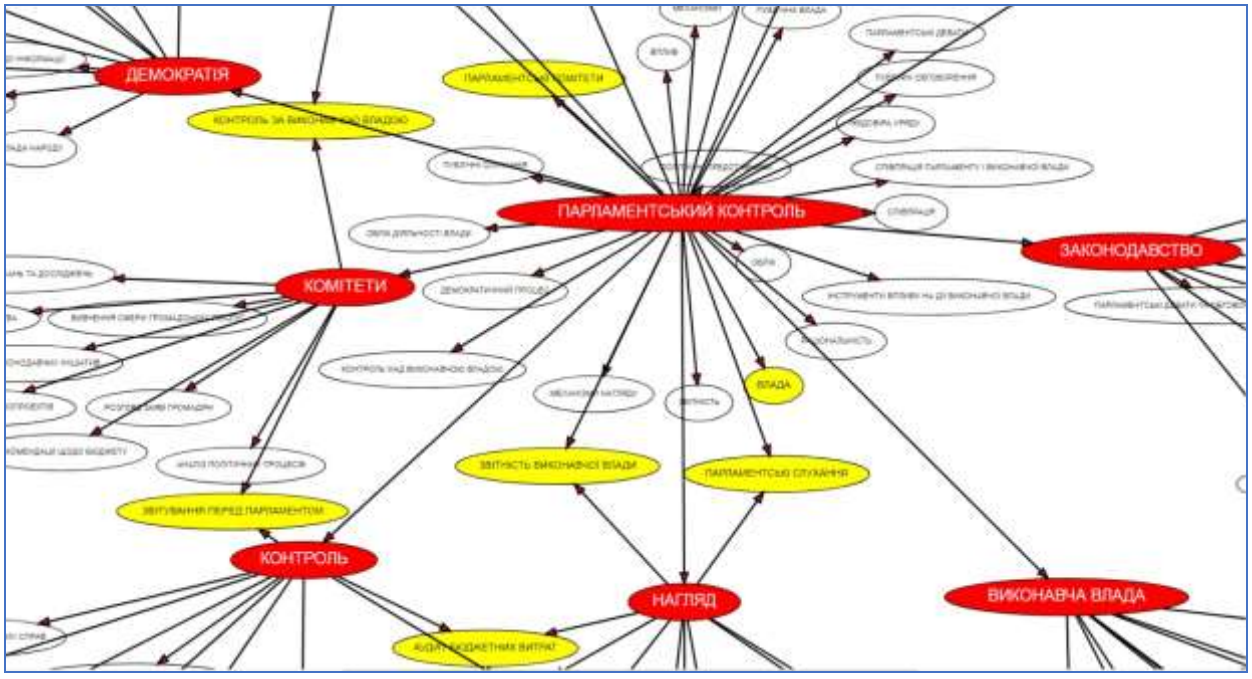

Рис. 2. Фрагмент мережі понять, що відповідають тематиці
“Парламентський контроль”.

Висновки.

Створення семантичної мапи на основі технології ГШІ і системи LegalGraph може допомогти юристам при використанні правових знань при здійсненні парламентського контролю завдяки:

– зручному доступу до інформації – мапа посилань робить навігацію по поняттях щодо парламентського контролю більш інтуїтивною, що дозволяє користувачам швидше і ефективніше знаходити потрібну інформацію;

– семантична мапа може допомогти в структуруванні та візуалізації знань, роблячи їх більш зрозумілими;

– семантична мапа дозволяє встановлювати зв'язки між різними сутностями і документами, допомагаючи користувачам легше розуміти, як різні інформаційні елементи взаємодіють між собою;

– семантична мапа може бути важливим методичним інструментом, дозволяючи здобувачам освіти швидше знаходити відповіді на свої питання, виходити на документи-першоджерела;

– семантична мапа може стати важливим інструментом для поширення знань серед широкої аудиторії, надаючи зручний доступ до правової інформації та сприяючи її поширенню.

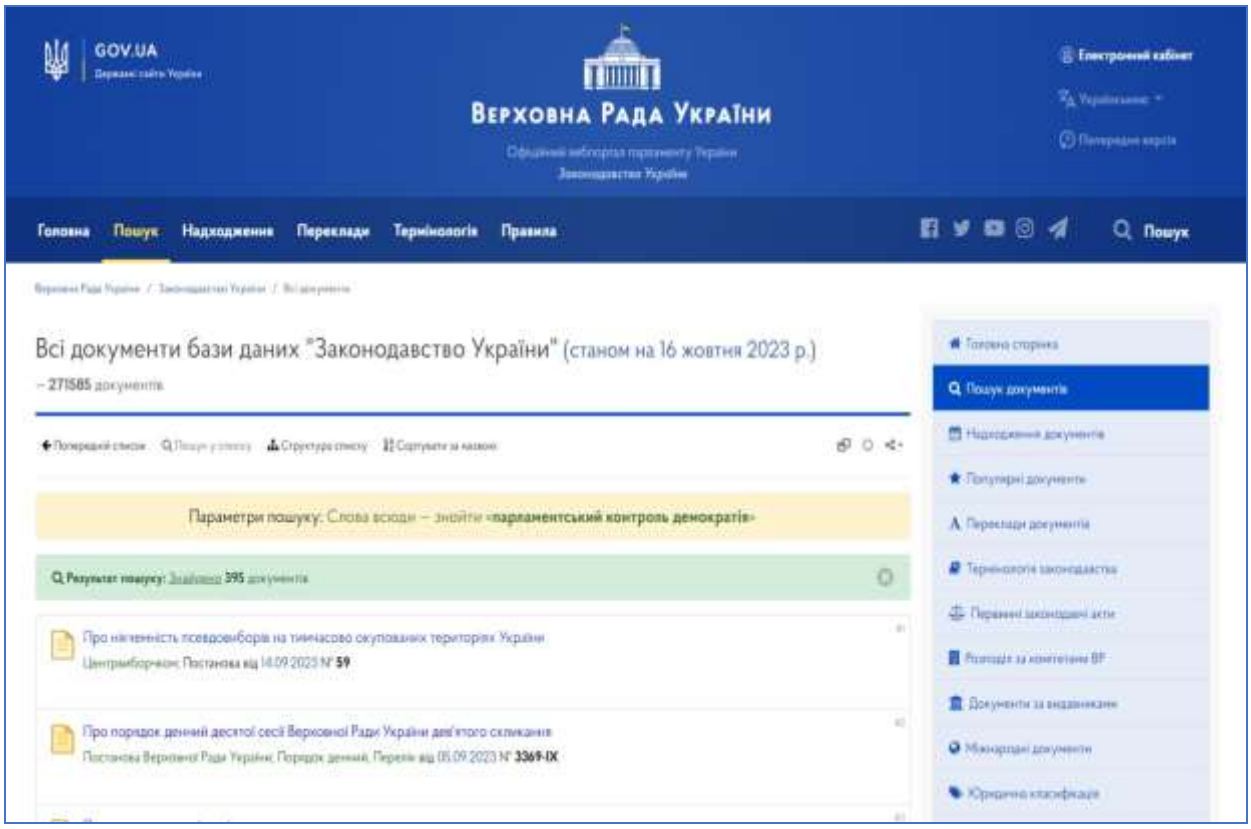

Рис. 3. Результат переходу за гіперпосиланням на ребрі між вузлами "Парламентський контроль" і "Демократія".

Отже, використання методики формування семантичних мап може сприяти покращенню рівня парламентського контролю завдяки зручному охопленню всієї понятійної бази і швидкому доступу до відповідної нормативно-правової інформації.

Загалом продемонстровано практичне застосування передової технології ШІ в галузі аналізу тексту та візуалізації мережі.

Показано, як використання алгоритмів машинного навчання може допомогти розблокувати раніше приховані ідеї та закономірності в великих обсягах текстових даних, а також отримати глибше розуміння складних явищ у різних областях, зокрема, в правовій науці.

Використана література

1. Lande, Dmitry and Strashnoy, Leonard, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. URL: http://dx.doi.org/10.2139/ssrn.4420452

2. Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community. URL: https://open datascience.com/ graph-viz-exploring-analyzing-and-visualizing-graphs-and-networks-with-gephi-and-chatgpt

3. Solat J. Sheikh, Sajjad Haider, Alexander H. Levis, On semi-automated extraction of causal networks from raw text, Engineering Applications of Artificial Intelligence, Volume 123, Part A, 2023, 106189, ISSN 0952-1976. URL: https://doi.org/10.1016/j.engappai.2023.106189

4. Д.В. Ланде, В.М. Фурашев, С.М. Брайчевський. Інформатика парламентського контролю: посібник. Київ, 2022. 256 с. ISBN 978-966-2344-80-6.

5. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web – The Time is Now. Kyiv: Engineering, 2023. 168 p. ISBN 978-966-2344-94-3.

6. Ken Cherven. Mastering Gephi Network Visualization. Packt Publishing, 2015. ISBN 78-1-78398-734-4.

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

УДК 343.98:004.77

НІЗОВЦЕВ Ю.Ю., *кандидат юридичних наук*, головний судовий експерт Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-7641-6403.
ПАРФИЛО О.А., *кандидат юридичних наук, старший науковий співробітник*, начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8787-7478.

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ WI-FI МАРШРУТИЗАТОРІВ ДЛЯ ВСТАНОВЛЕННЯ МОБІЛЬНОГО ТЕРМІНАЛУ ТА ЙОГО МЕРЕЖЕВОЇ АКТИВНОСТІ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Анотація. *Досліджено можливості Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності під час розслідування кіберзлочинів. Зокрема розкрито такі проблемні питання: яка доказова інформація може бути виявлена у Wi-Fi маршрутизаторі, як її зафіксувати і вилучити, а також обставини, що можуть перешкоджати пошуку зловмисника та доведенню його провини. Висвітлено роль та значення проведення експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи для аналізу лог-файлів на предмет відображення в них ознак кібератаки. Деталізовано особливості пошуку, фіксації та вилучення інформації про MAC-адресу мережевого інтерфейсу Wi-Fi-передавача.*

Ключові слова: *маршрутизатори, мобільні термінали, цифрові сліди, кіберзлочини, розслідування, спеціальні знання, дослідження, судова експертиза, методичні рекомендації.*

Summary: *The possibilities of Wi-Fi routers for establishing a mobile terminal and its network activity during the investigation of cybercrimes were investigated. In particular, the following problematic issues are revealed: what evidentiary information can be found in a Wi-Fi router, how to record and remove it, as well as circumstances that can hinder the search for an intruder and proving his guilt. The role and importance of electronic communications expertise or forensic comprehensive electronic communications expertise and computer-technical expertise to analyze log files for signs of a cyber attack are highlighted. The peculiarities of searching, fixing and extracting information about the MAC address of the network interface of the Wi-Fi transmitter are detailed.*

Keywords: *routers, mobile terminals, digital traces, cybercrimes, investigations, special knowledge, research, forensic examination, methodological recommendations.*

Постановка проблеми. Стрімкий розвиток сучасних цифрових технологій породжує пропорційно і кількість уразливостей в інформаційно-комунікаційних системах та відповідно зростає статистика вчинених кіберзлочинів із застосуванням комп'ютерних і телекомунікаційних пристроїв, особливо з використанням активного мережевого обладнання та можливостей Інтернет.

Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але й підприємства, установи, організації, державні органи і суспільство в цілому. Кіберзлочинність найчастіше ставить під загрозу критично важливі об'єкти

інфраструктури, які в багатьох країнах не контролюються публічним сектором, і такі посягання можуть вчиняти дестабілізуючий вплив як на окремих громадян, так і на національну безпеку держави.

Ефективність протидії злочинам, вчиненим у кіберпросторі, значною мірою визначається розумінням криміналістичної сутності способів їх вчинення та специфіки слідової картини. Крім того, потребує подальшого дослідження криміналістична характеристика правопорушень, що вчиняються з використанням комп'ютерних та мережевих технологій.

Слід зазначити, що використання інформації з Wi-Fi маршрутизаторів є актуальним під час розслідування різних злочинів. Наприклад, це може бути використання кіберзлочинцем публічної Wi-Fi мережі задля приховування слідів кібератаки. Або торговець речами, що мають обмеження обігу (зброя, наркотичні засоби тощо), може намагатись анонімізувати своє місцезнаходження під час переписки з покупцями, підключаючись до різних Wi-Fi мереж. Або це може бути просте користування мережею Wi-Fi на місці події, і встановлення факту такого користування буде доказом, що особа знаходилась на цьому місці.

Враховуючи актуальність описаної тематики, в Українському науково-дослідному інституті спеціальної техніки та судових експертиз СБ України було розроблено для спеціалістів та судових експертів методичні рекомендації "Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності" (далі – Методичні рекомендації) [1]. Основні положення вказаної науково-методичної праці буде представлено далі.

Результати аналізу наукових публікацій. Дослідженням проблемних аспектів використання спеціальних знань при фіксації, вилученні та збереженні цифрових (віртуальних) слідів, які утворюються під час вчинення правопорушення у кіберпросторі, присвячували свої праці такі науковці, як: Г.К. Авдєєва [2], Н.М. Ахтирська [3], В.Д. Басай [4], І.О. Крицька [5], Я. Найдьон [6], О.С. Омельян [7], О. А. Самойленко [8], А.В. Скрипник [9], Є.С. Хижняк [10] та інші.

Однак можна констатувати, що тема огляду та дослідження комп'ютерних і телекомунікаційних засобів (активного мережевого обладнання) під час розслідування злочинів, вчинених у кіберпросторі, досі залишає багато питань. Це й не дивно, враховуючи її об'єм та технічну складність. При цьому якісь аспекти залишаються невисвітленими повністю, якісь розкриті лише частково, а певну частину показано не зовсім коректно.

Зокрема, М.В. Кобець та Р.М. Кобець, описують використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень [11]. Автори стверджують, що "...для автентифікації входу до інтерфейсу роутера необхідно в пошуковій колонці ввести пароль: http://192.168.0.1 або http://192.168.1.1. Проте, у даному випадку мова йде не про пароль, а про IP-адресу, і вона може бути різною у різних роутерів навіть за базовими налаштуваннями від виробника. Так само їх твердження "...далі вводиться ім'я користувача: admin і пароль: admin" може бути вірним лише за умови, якщо такі дані були надані виробником роутера і вони не змінювались користувачем. Втім найбільш не обґрунтованим нам здається твердження, що "слідчий (оперативний працівник) на підставі ухвали слідчого судді суду першої інстанції направляє запит до мережевих операторів стільникового радіозв'язку з метою перевірки MAC-адрес, встановлених під час огляду місця події, і встановлення даних користувача (IMEI, номера телефону та інші дані), які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку". Але

оператори стільникового зв'язку не мають інформації про MAC-адреси абонентських терміналів. Ця інформація їм не потрібна, вона ніяк не впливає на надання послуг стільникового зв'язку і не передбачена специфікацією. Для стільникового зв'язку використовується інший радіоінтерфейс, який має інший ідентифікатор – IMEI, а не MAC-адресу. Щоб це з'ясувати, достатньо подивитись офіційну специфікацію протоколів стільникового зв'язку.

Метою статті є визначення можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності під час розслідування кіберзлочинів, зокрема отримання відповідей на такі питання: яка доказова інформація може бути виявлена у Wi-Fi маршрутизаторі, як її зафіксувати і вилучити, а також обставини, які можуть перешкоджати пошуку зловмисника та доведенню його провини.

Виклад основного матеріалу. Нерідко для приховування слідів кіберзлочинів зловмисники використовують публічний доступ до мережі Wi-Fi. Це може бути, наприклад, кафе чи готель. Разом з тим, можливі й інші варіанти підключення, які не мають принципових технічних відмінностей – Wi-Fi мережа офісу, власної квартири чи квартири сусідів або знайомих.

Для розуміння особливостей функціонування Wi-Fi маршрутизатора, до якого під'єднався мобільний термінал підозрюваної особи, для встановлення вказаного пристрою та його подальшого розшуку, розглянемо основні теоретичні положення, викладені в Методичних рекомендаціях [1].

Використання зафіксованої Wi-Fi маршрутизатором інформації про підключені мобільні термінали можливе у випадку, якщо маршрутизатор підтримує логіювання мережевих з'єднань і якщо таке логіювання активоване. Логіювання або журналювання – це функція автоматичної фіксації службової та статистичної інформації про дії програмного забезпечення або користувачів у хронологічному порядку. Така інформація зберігається у лог-файлах (лог-файл або просто лог, англ. Log file) походить від грец. logos – слово, смисл, думка, мова), які можуть бути різних форматів – від звичайних текстових з простою структурою до бінарних файлів та баз даних. У лог-файлах може фіксуватись різна інформація, все залежить від програмного забезпечення, якого стосується логіювання, та налаштувань цього логіювання.

У розглянутому випадку інтерес для розслідування будуть становити два види інформації:

1. Інформація, що характеризує безпосередньо під'єднані до Wi-Fi-мережі мобільні термінали. Фактично, ці дані є цифровими (електронними) слідами, за якими можна (не завжди, про це далі) ідентифікувати мобільний термінал підозрюваної особи.

2. Інформація, яка характеризує мережеву активність під'єднаних до Wi-Fi-мережі мобільних терміналів. Ця інформація може містити цифрові сліди конкретних протиправних дій зловмисника.

Конкретний перелік даних, що накопичуються у логах, залежить від моделі маршрутизатора, версії його програмного забезпечення та налаштувань (у маршрутизаторів побутового рівня, як правило, відсутні налаштування логіювання подій, є лише можливість активації/деактивації логіювання).

У випадку виявлення в логах необхідних даних, їх потрібно належним чином документувати та процесуально оформити задля набуття ними статусу доказів.

Аби успішно оперувати описаною вище інформацією у процесі доказування, варто розуміти доказове значення кожних даних. Розглянемо їх детальніше.

Інформація, що характеризує безпосередньо під'єднані до Wi-Fi-мережі мобільні термінали, зазвичай може містити дані про мережеву назву такого терміналу, його MAC-адресу, IP-адресу, час підключення до мережі та тривалість сеансу.

Мережева назва мобільного терміналу зазвичай збігається з його моделлю – це встановлюється заводом-виробником. Але цю назву може змінити користувач у налаштуваннях мобільного терміналу. Нерідко нова назва також тим чи іншим чином може ідентифікувати користувача, наприклад, містити його ім'я. Але може бути і цілком нейтральною, наприклад, просто "smartphone".

MAC-адреса (від англ. Media Access Control – управління доступом до середовища) – це унікальний ідентифікатор мережевого інтерфейсу. У мережевій моделі OSI (від англ. The Open Systems Interconnection model) MAC-адреса використовується на другому (канальному) рівні. Іноді цю адресу ще називають апаратною чи фізичною (англ. Hardware Address). MAC-адреса надається мережевому інтерфейсу заводом-виробником, при цьому адресний простір розподілений між виробниками. Використовуючи довідкові дані, за MAC-адресою зазвичай можна визначити виробника мобільного терміналу, а в окремих випадках – конкретну модель. Можливість визначення конкретної моделі залежить від того, чи відкрив виробник загальний доступ до такої інформації, інакше доведеться направляти офіційний запит до виробника. Проте слід враховувати певні особливості MAC-адреси. По-перше, цю адресу можна змінити у налаштуваннях мобільного терміналу або використовуючи спеціальне програмне забезпечення. Наприклад, сучасні смартфони мають функцію генерації випадкової MAC-адреси при кожному підключенні до мережі (див. Рис. 1). По-друге, MAC-адреса не передається разом з мережевим трафіком глобально. В рамках Wi-Fi-мережі MAC-адреса передається від терміналу лише до маршрутизатора, не далі. А отже, відслідкувати у глобальній мережі мобільний термінал за його MAC-адресою зазвичай неможливо.

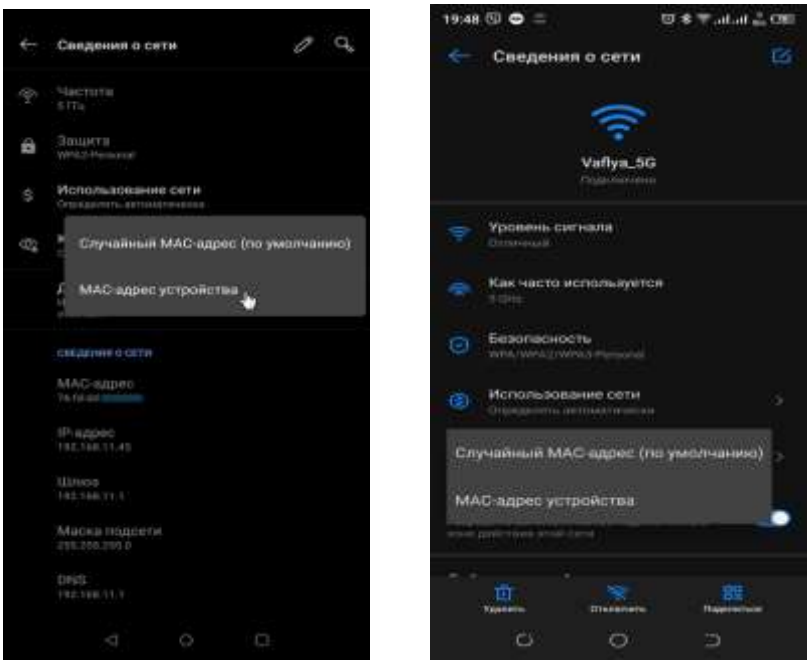

Рис. 1. Приклади налаштувань Wi-Fi-мережі у смартфоні, що функціонує під керуванням ОС Android.

IP-адреса (від англ. Internet Protocol address) – це також унікальний ідентифікатор мережевого інтерфейсу, який використовується для адресації комп'ютерів чи інших

пристроїв у мережах, які побудовані з використанням стеку протоколів TCP/IP, у тому числі – Інтернет. У мережі Інтернет потрібна глобальна унікальність адрес, а у разі роботи в локальній мережі – унікальність у межах цієї мережі (існують заздалегідь визначені адресні простори для локальних мереж). На відміну від MAC-адреси, IP-адреса використовується на третьому (мережевому) рівні моделі OSI. Ця адреса використовується для адресації пакетів інформації, а отже, може передаватись глобально. При цьому слід враховувати, що адреса вузла локальної мережі не передається назовні. Для взаємодії з глобальною мережею використовується технологія NAT (від англ. Network Address Translation – перетворення мережевих адрес), яка дозволяє змінювати IP-адресу у заголовку пакету інформації під час його проходу через пристрій маршрутизації трафіку (маршрутизатор). IP-адреса надається мережевому інтерфейсу вручну адміністратором чи користувачем, або автоматично з використанням протоколу DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла). У мережах Wi-Fi у переважній більшості випадків використовується саме динамічне розподілення IP-адрес, при цьому це адреси локальної мережі, які не передаються назовні.

Час підключення до мережі та тривалість сеансу дозволяють локалізувати в часі знаходження мобільного терміналу в межах покриття Wi-Fi-мережі. Також слід враховувати, що термінал міг знаходитись на цій же території і в інший час, але не будучи підключеним до Wi-Fi.

Інформація, яка характеризує мережеву активність під’єднаних до Wi-Fi-мережі мобільних терміналів, може містити дані про доменне ім’я та/або IP-адресу ресурсу, до якого звертався термінал, порт, тип протоколу, тип пакету, дату та час звернення тощо. Таким чином якщо, наприклад, зловмисник через публічну мережу Wi-Fi намагався підключитись до віддаленого сервера за протоколом SSH (від англ. Secure SHell – “безпечна оболонка” – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп’ютером і тунелювання TCP-з’єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються) і використовуючи його IP-адресу, у логах може відобразитись встановлення з’єднання з 22 TCP-портом мережевого вузла з відповідною IP-адресою.

Разом з тим, якщо зловмисник використовує сервіс VPN (від англ. Virtual Private Network – віртуальна приватна мережа), весь мережевий трафік у зашифрованому вигляді буде йти на адресу VPN-сервера. У логах, скоріше за все, відображатиметься лише IP-адреса та/або доменне ім’я цього сервера. А всю іншу інформацію доведеться запитувати у власника сервісу VPN.

Пошук, фіксація та вилучення інформації про MAC-адресу.

Якщо є підозра, що зловмисник у певному місці користувався Wi-Fi-мережею (зокрема, публічною) для вчинення протиправних дій, перш за все, слід з’ясувати, чи дійсно на місці події функціонує якась Wi-Fi-мережа. Для цього можна використати як спеціалізоване обладнання (наприклад, аналізатор частот), так і спеціальні утиліти (Wi-Fi аналізатори), які можна встановити на звичайний смартфон. Такі додатки дозволяють не лише виявити Wi-Fi-мережу, але й встановити ще багато даних: MAC-адреса мережевого інтерфейсу Wi-Fi-передавача, канал, потужність сигналу, наявність та вид шифрування каналу тощо (див. Рис. 2, 3). При застосуванні додатку потрібно враховувати апаратні можливості смартфона, адже якщо смартфон підтримує мережу Wi-Fi лише на частоті 2,4 ГГц, то мережа 5 ГГц у додатку не відобразиться.

Рис. 2. Вікно додатку Wifi Analyzer (розробник – farproc), доступного для завантаження з Google Play, працює під керуванням ОС Android.

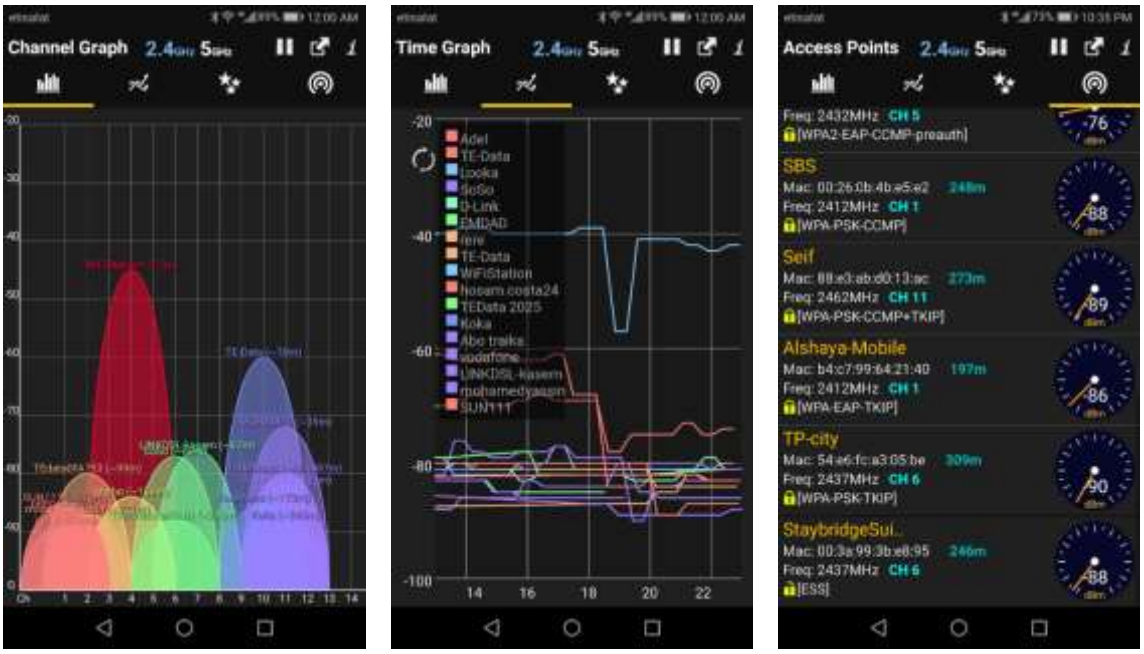

Рис. 3. Вікно додатку WiFi Analyzer (розробник – olgor.com), доступного для завантаження з Google Play, працює під керуванням ОС Android.

Якщо на місці події виявлено функціонуючу Wi-Fi-мережу, наступним етапом слід з'ясувати місце знаходження мережевого обладнання Wi-Fi та схему побудови мережі в цілому. Це може бути один пристрій – Wi-Fi маршрутизатор (характерно для домашніх помешкань), Wi-Fi маршрутизатор та декілька додаткових передавачів (точок доступу, ретрансляторів/повторювачів (або репітерів, від англ. repeater)) для розширення зони покриття (вони можуть поєднуватись у мережу як дротовим, так і бездротовим з'єднанням), декілька Wi-Fi маршрутизаторів або Wi-Fi маршрутизатор, який не має відповідного радіоінтерфейсу, а функціонує через окремі Wi-Fi-передавачі, що виступають як точки доступу (такий варіант більш характерний для професійного застосування, наприклад, забезпечення мережею Wi-Fi громадського місця – зали

ресторану, великого офісу тощо). В цілому варіантів побудови мережі безліч. Наприклад, останнім часом набувають поширення так звані Wi-Fi Mesh мережі. Найбільш складними є, зазвичай, корпоративні мережі. Крім того, логіювання може здійснюватися не лише на локальний носій інформації маршрутизатора, але й на сторонній носій (наприклад, окремий комп'ютер чи хмарне сховище).

Наступним кроком слід вжити заходів задля збереження логів Wi-Fi маршрутизатора. Якщо мережа корпоративна, слід звернутись до адміністратора цієї мережі, повідомивши йому про необхідність забезпечення збереження журналу подій для його подальшого вилучення у процесуальному порядку. У випадку огляду домашнього помешкання слід виявити місцезнаходження Wi-Fi маршрутизатора. Зазвичай у квартирах Wi-Fi маршрутизатор встановлюють біля входу до квартири, щоб не тягнути кабель всередину квартири, або приблизно посередині квартири, щоб забезпечити найкраще покриття. У всіх випадках бажано обмежити доступ будь-яких осіб до мережевого устаткування, аби уникнути будь-яких маніпуляцій (навмисних, ненавмисних чи випадкових) з ним: від'єднання (роз'єднання), вимкнення, перезавантаження, знеструмлення, переналаштування тощо. Для проведення будь-яких дій з маршрутизатором варто залучити спеціаліста (відповідно до ст. 71 КПК України "особу, яка володіє спеціальними знаннями та навичками…") [12], який допоможе професійно розібратися в особливостях комп'ютерного та телекомунікаційного обладнання, виявити носії інформації та запобігти умисному або випадковому знищенню інформації на них, проконсультує слідчого щодо інформації, яка підлягає копіюванню тощо. Профіль і кваліфікація спеціаліста, якого необхідно залучити до огляду, визначається, перш за все, об'єктом огляду (у розглянутому випадку це Wi-Fi маршрутизатор), а також залежно від мети і завдань слідчої (розшукової) дії, зважаючи на первинні дані про характер кримінального правопорушення.

На початковій стадії проведення слідчих (розшукових) дій, таких як огляд, обшук, а також виїмка, слідчому або оперативному працівнику на місці події, якщо виявлено Wi-Fi мережу, необхідно:

1. Прибувши на місце проведення слідчої (розшукової) дії заборонити всім особам, що перебувають у приміщенні, торкатися до комп'ютерної та/чи телекомунікаційної техніки, носіїв інформації, телекомунікаційних та електродротів, вмикати і вимикати пристрої й енергоживлення.

2. Провести фото-, відеозйомку приміщення, у якому здійснюється огляд або тимчасовий доступ до комп'ютерного та/чи телекомунікаційного обладнання.

3. У процесі огляду або тимчасового доступу до телекомунікаційного обладнання спеціаліст у присутності понятих має:

3.1. Встановити схему мережі, з'ясувати, які пристрої забезпечують функціонування мережі (мережеве обладнання) та які до неї під'єднані постійно та тимчасово (стаціонарні та мобільні термінали – стаціонарні комп'ютери, ноутбуки, смартфони тощо).

3.2. Зафіксувати дані, які зазвичай містяться у маркувальних позначеннях на корпусі пристроїв: марку, модель, серійний номер, MAC-адресу, стандартні дані автентифікації (ім'я користувача та пароль). Як правило, маркування містять й інші дані, але вони зазвичай не є суттєвими.

3.3. Підключитись до мережі. Для цього під'єднати до Wi-Fi-мережі службовий ноутбук (бажаний варіант) або використати вже під'єднаний до мережі "місцевий" комп'ютер. Використання "місцевого" комп'ютера має свої переваги і недоліки. Перевагою є те, що він вже підключений до мережі, а також можлива наявність у ньому

автентифікаційних даних (якщо з нього здійснювалось адміністрування маршрутизатора). Недоліком може бути внесення змін до інформаційного вмісту носіїв інформації комп'ютера, оскільки в окремих випадках це небажано. У випадку підключення службового ноутбуку чи іншого мобільного терміналу до Wi-Fi-мережі потрібно знати її назву (SSID, від англ. Service Set Identifier) та, якщо мережа захищена, пароль. При цьому слід враховувати, що SSID може бути скритим та/або підключення до мережі дозволене лише за білим списком MAC-адрес. Значна частина Wi-Fi маршрутизаторів підтримує підключення до Wi-Fi-мережі за допомогою WPS (від англ. Wi-Fi Protected Setup), що значно спрощує під'єднання до мережі і реалізується одним з таких способів: за допомогою PIN (зазвичай вказаний на етикетці маршрутизатора), з натисканням push-кнопки, з використанням NFC або з використанням флеш-накопичувача для перенесення налаштувань з маршрутизатора на ноутбук. Також не слід відкидати можливість підключення до мережі за допомогою дротового з'єднання, адже більшість Wi-Fi-маршрутизаторів мають також і дротові інтерфейси для локальної мережі. В останньому випадку SSID та пароль не знадобляться.

3.4. Здійснити вхід до інтерфейсу головного мережевого пристрою (Wi-Fi маршрутизатора). Слід враховувати, що вхід до адміністративного меню Wi-Fi маршрутизатора може бути заблокований з бездротової мережі (дозволено лише з дротової локальної мережі), може бути дозволений вхід лише за білим списком MAC-адрес тощо. Для входу до веб-інтерфейсу маршрутизатора за допомогою Інтернет-браузера необхідно в адресний рядок ввести адресу маршрутизатора. Для побутових маршрутизаторів це зазвичай "http://192.168.0.1" або "http://192.168.1.1", але не для всіх. Наприклад, для маршрутизаторів ASUS це може бути "http://192.168.50.1", а для маршрутизаторів MikroTik – це "http://192.168.88.1". Також слід враховувати, що ця адреса може бути змінена у налаштуваннях. У випадку професійного мережевого обладнання доцільно з'ясувати параметри входу у системного адміністратора. У низці випадків може бути неможливо увійти до меню маршрутизатора через веб-інтерфейс. У такому випадку, якщо маршрутизатор підтримує доступ через термінал, можна використати доступ за протоколами Telnet чи SSH (останній краще, бо використовує зашифрований канал зв'язку) (див. Рис. 4). Крім того, слід враховувати, що частина маршрутизаторів підтримують адміністрування за допомогою спеціального програмного забезпечення (фірмової утиліти).

3.5. Здійснити візуальний огляд відображеної інформації на екрані комп'ютера з подальшою її фіксацією;

3.6. Ввести автентифікаційні дані адміністратора. У багатьох Wi-Fi маршрутизаторів виробниками задаються стандартні параметри входу: ім'я admin і пароль admin. Разом з тим, стандартною є рекомендація змінити ці параметри відразу після першого входу. Нерідко система може навіть не пропустити користувача до меню, доки він не змінить стандартні автентифікаційні дані. Крім того, для автентифікації може знадобитись ключ HASP (від англ. Hardware Against Software Piracy). Отже, бажано дізнатися параметри входу у власника Wi-Fi маршрутизатора або системного адміністратора. Вказані параметри слід зафіксувати у протоколі.

3.7. У разі успішного входу до адміністративного меню варто спочатку переглянути налаштування логіювання, а потім – наявність логів за потрібний проміжок часу.

3.8. Виявлені дані слід вивести на екран та переглянути учасникам слідчої (розшукової) дії, зокрема, понятим.

3.9. Вказані дані слід зафіксувати у протоколі слідчої (розшукової) дії, до якого доцільно долучити роздруківки відповідних знімків екрану (скріншотів).

3.10. Після цього виявлені логи слід вилучити. В залежності від моделі Wi-Fi маршрутизатора та наявного криміналістичного обладнання це можна зробити шляхом копіювання лог-файлу, експорту логів у текстовий чи табличний файл, виділенням та копіюванням необхідної інформації у текстовий файл або скріншотами (останній варіант є найгіршим з точки зору подальшого використання вказаної інформації, зокрема, для проведення судової експертизи).

3.11. Отриманий файл або декілька файлів слід підписати з використанням кваліфікованого електронного підпису слідчого або обрахувати хеши цих файлів, які вписати до протоколу. У випадку, якщо файлів значна кількість, їх можна помістити до архіву та підписати (обрахувати хеш) лише цього одного архівного файлу. Файл записати на носій інформації (оптичний диск, флеш-носій, карта пам'яті тощо), який додати до протоколу слідчої (розшукової) дії.

Всі дії на екрані комп'ютера рекомендується фіксувати не лише у протоколі, але й шляхом створення знімків екрану (скріншотів), які потім можна роздрукувати та записати на цифровий носій інформації.

Враховуючи, що до Wi-Fi маршрутизатора у цей самий час могли бути підключені інші мобільні термінали (інших присутніх осіб), варто провести огляд цих терміналів та зафіксувати їх MAC-адреси. Виокремивши ці MAC-адреси зі списків адрес у логах можна встановити MAC-адресу мобільного терміналу підозрюваної особи (або декілька адрес, серед яких – адреса терміналу зловмисника).

```
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
merionetSw1>en
% No password set.
merionetSw1>
% Connection timed out; remote host not responding
C:\>
C:\>
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
merionetSw1>en
Password:
merionetSw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
merionetSw1(config)#hostname merionSwitch1
merionSwitch1(config)#
```

Рис. 4. Вікно терміналу з відображенням входу до адміністративних налаштувань маршрутизатора Cisco за допомогою протоколу Telnet.

4. На завершальній стадії необхідно оформити протокол огляду або тимчасового доступу, у якому поетапно описати усі дії спеціаліста (рекомендується під його диктовку та у присутності понятих, супроводжуючи роздруківками скріншотів усіх дій на екрані комп'ютера, які разом з схемами та матеріалами фото-, відеозйомки додаються до протоколу).

Можливості встановлення мобільного терміналу за MAC-адресою.

Після оформлення протоколу на місці події провадять подальші слідчі (розшукові) дії зі встановлення місцезнаходження мобільних терміналів, MAC-адреси яких виявлено на місці події. Оператори стільникового зв'язку не мають інформації щодо MAC-адрес мобільних терміналів, а отже, і не зможуть таку інформацію надати на відповідний запит слідчого, навіть оформлений з дотриманням усіх процесуальних вимог. Оператори мобільного зв'язку отримують лише ідентифікатор стільникового радіоінтерфейсу мобільного терміналу (IMEI, від англ. International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання), а також ідентифікатор абонента (IMSI, від англ. International Mobile Subscriber Identity – міжнародний ідентифікатор користувача мобільного зв'язку), який міститься у SIM/USIM/R-UIM картці. Якщо телефон має декілька слотів для SIM/USIM/R-UIM карток, то і IMEI та IMSI буде декілька, по одній парі IMEI+IMSI на кожен слот. Віртуальна (цифрова) SIM/USIM/R-UIM картка також має власний IMSI.

IMEI та IMSI є унікальними номерами. IMEI надається мобільному терміналу його виробником, IMSI – виробником SIM/USIM/R-UIM картки, зазвичай, оператором стільникового зв'язку (заводом на його замовлення). Отже, виробник мобільного терміналу має інформацію і про IMEI (який відстежується операторами стільникового зв'язку), і про MAC-адресу терміналу. Цим можна скористатись під час пошуку мобільного терміналу. Перш за все, слід встановити через довідникові джерела у мережі Інтернет-виробника терміналу, що має виявлену MAC-адресу. Зазначимо, що якщо за IMEI у довідникових Інтернет-джерелах можна, зазвичай, встановити точну модель терміналу, то за MAC-адресою – лише виробника. Маючи інформацію щодо виробника мобільного терміналу у певних випадках попередньо можна припустити, що то був за пристрій – смартфон, планшетний комп'ютер, ноутбук, окремий мережевий інтерфейс (плата) тощо. Але таке можливо в обмеженій кількості випадків, бо, наприклад, Xiaomi Communications Co Ltd виготовляє значну кількість різних типів пристроїв: смартфони, планшетні комп'ютери, ноутбуки, мережеве обладнання тощо, і все це має мережеві інтерфейси з MAC-адресами. Отже, за точною інформацією доведеться звернутись до виробника. Якщо запитуваний мобільний термінал має стільниковий мережевий інтерфейс (тобто, окрім Wi-Fi також може підключитись до стільникової мережі, наприклад, ноутбук чи планшетний комп'ютер – через вбудований 3G/4G модем), від виробника можна отримати інформацію про IMEI вказаного терміналу.

Отримавши цю інформацію, стає можливим отримати від операторів телекомунікацій інформації про зв'язок (абонента, надання електронних комунікаційних послуг, їх тривалість, зміст, маршрути передавання трафіку тощо). Для цього на підставі ухвали слідчого судді суду першої інстанції направляється запит до операторів стільникового радіозв'язку з метою перевірки отриманого від виробника IMEI і встановлення даних користувача, які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку.

Наступним кроком може бути проведення такої негласної слідчої (розшукової) дії, як установлення місцезнаходження радіоелектронного засобу, що може дати можливість установити місцезнаходження мобільного терміналу, який був підключений до мережі (маршрутизатора) у момент вчинення кримінального правопорушення.

Можливості дослідження цифрових слідів кібератак у лог-файлах.

Паралельно з встановленням терміналу, інформації про його володільця та місця знаходження терміналу може здійснюватися аналіз лог-файлів на предмет відображення в них ознак кібератаки.

При цьому послідовно здійснюються наступні операції:

- встановлення наявності у лог-файлах інформації про мережеву активність в цілому і конкретного терміналу зокрема;
- визначення наявності чи відсутності ознак використання сервісу VPN чи інших механізмів маскування трафіку;
- виявлення ознак кібератаки;
- встановлення механізму кібератаки, її класифікація.

Зазвичай дослідження лог-файлів на предмет виявлення ознак кібератаки, встановлення її механізму і віднесення до певного типу (класифікація) доцільно здійснювати шляхом експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи. При цьому для встановлення механізму кібератаки можуть знадобитись додаткові матеріали, наприклад, лог-файли атакованої електронної комунікаційної системи.

Висновки.

Використання зафіксованої Wi-Fi маршрутизатором інформації про підключені мобільні термінали можливе у випадку, якщо маршрутизатор підтримує логіювання мережевих з'єднань і якщо таке логіювання активоване. Інтерес для розслідування буде становити інформація щодо під'єднаних до Wi-Fi-мережі мобільних терміналів, що зазвичай може містити дані про мережеву назву пристрою, його MAC-адресу, IP-адресу, час підключення до мережі та тривалість сеансу, а також щодо мережевої активності, що може містити дані про доменне ім'я та/або IP-адресу ресурсу, до якого звертався термінал, порт, тип протоколу, тип пакету, дату та час звернення тощо.

Під час огляду здійснюється виявлення Wi-Fi-мережі, з'ясовується місце знаходження мережевого обладнання Wi-Fi та схема побудови мережі в цілому. Наступним кроком вживаються заходи задля збереження логів Wi-Fi маршрутизатора та їх вилучення у процесуальному порядку. Отримавши з логів MAC-адресу мобільного терміналу, слід встановити IMEI цього пристрою, що можливо зробити через довідкові дані або звернувшись до виробника терміналу. З цією інформацією (IMEI) можна звернутись до операторів стільникового зв'язку для отримання даних користувача, які є в системі баз даних постачальника електронних комунікаційних послуг стільникового радіозв'язку. Також можна, відповідно до положень ст. 268 КПК України [12], провести негласну слідчу (розшукову) дію – установлення місцезнаходження радіообладнання (радіоелектронного засобу).

Одночасно зі встановленням терміналу, інформації про його володільця та місця знаходження терміналу може здійснюватися аналіз лог-файлів на предмет відображення в них ознак кібератаки, що доцільно здійснювати шляхом проведення експертизи електронних комунікацій або судової комплексної експертизи електронних комунікацій та комп'ютерно-технічної експертизи. При цьому для встановлення механізму кібератаки можуть знадобитися додаткові матеріали, наприклад, лог-файли атакованої електронної комунікаційної системи.

Використана література

1. Нізовцев Ю. Ю. Використання можливостей Wi-Fi маршрутизаторів для встановлення мобільного терміналу та його мережевої активності: методичний посібник. Київ: Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, 2022. 18 с.

2. Авдєєва Г.К. Сутність цифрових слідів в криміналістиці: зб. матеріалів міжнар. наук.-практ. конфер. *Актуальні питання судової експертизи та криміналістики,* м. Харків, 10 – 11

жовт. 2018 р. Харків, 2018. С. 90-93. URL: http://dspace.nlu.edu.ua/bitstream/123456789/15677/1/Avdeeva_90-93.pdf (дата звернення: 17.09.2023).

3. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ "Київський університет", 2018. 229 с.

4. Басай В.Д., Томин С.В. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 220-223. URL: http://nbuv.gov.ua/UJRN/apdp_2008_44_44

5. Крицька І.О. Доріжка цифрових слідів: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні: зб. наук. пр. НДІ ПЗІР НАПрН України № 1 за матеріалами круглого столу *Цифрові трансформації України 2020: виклики та реалії,* м. Харків, 18 верес. 2020 р. С. 92-97. URL: http://openarchive.nure.ua/handle/document/13917 (дата звернення: 17.09.2023).

6. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304-307.

7. Омельян О.С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 457-466. DOI:10.33994/kndise.2020.65.45.

8. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

9. Скрипник А.В. Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія. Харків: Право, 2022. 408 с. DOI:https://doi.org/10.31359/9789669982940.

10. Хижняк Є.С. Поняття віртуальних слідів та їх значення у процесі розслідування злочинів: зб. наукових праць *"Актуальні проблеми держави і права".* 2017. № 79. С. 159-166.

11. Кобець М.В., Кобець Р.М. Використання можливостей Wi-Fi роутерів під час виявлення та розслідування кримінальних правопорушень. *Криміналістичний вісник*. Київ: ДНДЕКЦ МВС України, НАВС, 2022. № 2(38). С. 36-47.

12. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 17.09.2023).

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

УДК [004.62:004.855.5]+342.723

ДУБНЯК М.В., *кандидат юридичних наук,* в.о. завідувача наукової лабораторії правового забезпечення цифрової трансформації Наукового центру цифрової трансформації і права ДНУ "ІІБП" НАПрН України. Старший викладач кафедри інформаційного, господарського та адміністративного права КПІ ім. Ігоря Сікорського. ORCID: https://orcid.org/0000-0001-7281-6568.

ПРАВО НА РЕЗУЛЬТАТИ ОБРОБКИ ДАНИХ У ФОРМІ ПРОГНОЗНИХ ВИСНОВКІВ ОТРИМАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ

Анотація. *У статті досліджується правовий режим "прогнозних висновків" сформульованих за результатом обробки комбінованих наборів Великих Даних. Аналізуються право доступу та право на виправлення, як потенційні правові механізми протидії ефектам впливу прогнозних висновків. Доводиться, що прогнозні висновки, які отримуються штучним інтелектом у результаті обробки Великих Даних, впливають на суб'єкта даних в умовах економіки даних. Разом з цим встановлюється, що ні право доступу, ні право на виправлення не захищають суб'єкта даних від результатів використання прогнозних висновків. Обґрунтовується необхідність запровадження нового права, яке має доповнити систему правових гарантій захисту персональних даних – "право на результати обробки даних".*

Ключові слова: *персональні дані, штучний інтелект, прогнозні висновки, права суб'єкта даних, право на результат обробки даних, Великі Дані, набори не персональних даних.*

Summary*. The article investigated the legal regime of "predictive conclusions" formulated as a result of processing Big Data combined sets. The right of access and the right to rectification are analyzed as potential legal mechanisms for counteracting the effects of predictive conclusions. It is proven that predictive conclusions obtained by artificial intelligence as a result of processing Big Data affect the data subject in the conditions of the data economy. At the same time, it is established that neither the right of access nor the right of rectification protect the data subject from the results of the use of predictive conclusions. The necessity of introducing a new right, which should supplement the system of legal guarantees of personal data protection – "the right to the results of data processing" is substantiated.*

Keywords*: personal data, artificial intelligence, predictive conclusions, data subject rights, the right to the result of data processing. Big Data, sets of non-personal data.*

Постановка проблеми. В епоху збору та обробки Великих Даних, розвитку економіки даних, важливе місце займає захищеність приватного життя особи та існування реальних правових інструментів управління власними персональними даними (далі – ПД).

Поширення аналітики Великих Даних збільшило можливості збору та доповнення даних про особу. Великі Дані можуть включати в себе комбінований набір персональних і не персональних даних. Результат обробки такої категорії даних технологіями штучного інтелекту (далі – ШІ) дозволяє отримати прогнозні висновки. Такі висновки забезпечують конкурентні переваги для компанії, оскільки дозволяють змоделювати поведінку, а інколи, і безпосередньо вплинути на рішення особи. Суб'єкт ПД не може відстежити, що його ПД були включені до набору Великих Даних, особливо якщо їх було анонімізовано, отже важко навіть оцінити безпрецедентні масштаби втручання в право на приватність у процесі аналізу наборів Великих Даних.

З урахуванням особливостей розвитку технологій суб'єкти даних мають отримувати додаткові права для забезпечення приватності. Норми Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. (Загальний Регламент щодо захисту персональних даних, далі – GDPR) встановлюють ряд прав для суб'єкта даних, зокрема: право бути поінформованим про збирання даних (ст. 13-14), право доступу до даних (ст. 15), право на виправлення (ст. 16), право на стирання (право бути забутим) (ст. 17), обмеження опрацювання (ст. 18), право на мобільність (перенесення) даних (ст. 20), право на заперечення (ст. 21), захист від профайлінгу (ст. 22) [1].

Виникає сумнів, чи може суб'єкт ПД реалізувати право на доступ чи виправлення даних, та інші права передбачені GDPR, щодо даних, які були отримані у результаті обробки наборів даних технологіями ШІ. Попередньо назвемо таку категорію даних "прогнозними висновками". Особливістю такого виду даних є те, що ШІ обробляє дані з використанням різних алгоритмів, і інколи навіть розробники технологій не можуть пояснити, на підставі яких комбінацій, доступних наборів та методів обробки даних, ШІ сформував прогнозний висновок (ефект "чорної скриньки"). Ускладнює таку ситуацію динамічна властивість даних, оскільки одна і та сама інформація може одночасно перебувати у різних правових режимах захисту. Тому можуть виникати спори щодо правових підстав обробки даних, визначення власника отриманих результатів обробки [2, с. 72], а також те, що до набору даних могли не входити ПД, а тому суб'єкт даних не може вимагати доступу до них чи їх виправлення.

Практика тлумачення норм щодо захисту персональних даних в ЄС схиляється до розширеного тлумачення, коли до ПД можуть прирівняти інші дані, якщо вони "стосуються" фізичної особи чи здатні вплинути на неї [3]. Тобто норми GDPR надають суб'єктам даних права контролювати межі збору та обробки даних, але не надають механізмів для управління новими даними, які були отримані у результаті їх аналізу, та описують поведінку та можливі інтереси суб'єкта даних. Фактично це дані аналітичних прогнозів, на яких базуються комерційні інтереси суб'єктів економіки даних. Отже маємо проблему правової невизначеності даних, отриманих в результаті аналізу Великих Даних та отриманих прогнозних висновків. Крім того, у суб'єкта даних немає спеціальних прав (виправлення, стирання, мобільності, обмеження опрацювання), на результати обробки даних у формі прогнозних висновків, оскільки ці дані є згенерованими та не персональними і не охоплюються первісною згодою на обробку ПД. З іншого боку, при розробці законодавчого регулювання права на результати обробки даних це право має врівноважуватись із нормами про захист інтелектуальної власності, комерційної таємниці, свободи підприємництва [4].

Певні прогнозні висновки формуються у процесі надання адміністративних послуг на підготовчому етапі (до прийняття остаточного рішення). У такому випадку, у суб'єкта даних має бути чітко встановлено права на доступ до проміжних результатів обробки його даних (запиту), оскільки такі результати попередньої обробки можуть вплинути на остаточне рішення і остаточний результат надання адміністративної послуги.

Досліджуючи проблеми обробки ПД з урахуванням методів аналізу Великих Даних, машинного навчання, інших технологій ШІ необхідно відзначити, що не всі Великі Дані містять ПД. Але враховуючи прецедентну практику Суду ЄС, який використовує широкий підхід до тлумачення категорії "персональні дані", зокрема через критерій "стосується" фізичної особи, яку може бути ідентифіковано [3], виникає необхідність відмежування різних категорій даних, правових режимів їх захисту, та встановлення меж дії законодавства про захист персональних даних, у тому числі і GDPR.

Метою статті є обґрунтування права суб'єкта даних на результати обробки даних (прогнозних висновків), отриманих у зв'язку із використанням технологій штучного інтелекту і визначення місця такого права в системі інформаційного права.

Результати аналізу наукових публікацій. Особливості обігу даних в соціальних мережах, формування комбінованих наборів даних досліджували Graef I, Gellert R., Husovec, M. [3], Scism L. [4], Altenburger K., Ugander J. [7], особливості збирання даних в умовах розвитку Інтернету речей досліджували Cook J. [8], особливості застосування деяких прав згідно GDPR аналізуються в роботі Korff D. [9]. У роботі Wachter S., Mittelstadt B.D. [19] комплексно проаналізовано проблему, що фокус правового регулювання зміщено в бік процедур збору ПД, а не їх аналізу. Правовий режим ПД та окремі проблеми правового регулювання в умовах застосування технологій Інтернету речей досліджували Баранов О.А., Брижко В.М. [21], Пилипчук В.Г., Фурашев В.М. Деякий теоретичний аналіз необхідності впровадження "права на висновки" є в роботі Wachter S., Mittelstadt B.D. [19], однак, у цій праці аналізується як результати обробки даних формують враження третіх осіб про нас, як суб'єкта даних. З урахуванням деяких положень з роботи Wachter S., Mittelstadt B.D. [19] невирішеним залишилось питання місця права на результат обробки даних в системі інформаційного права, що є метою цього дослідження.

Виклад основного матеріалу. Методи аналізу Великих Даних можна розрізняти відповідно до ціннісного критерію. Існує дві сфери застосування Великих Даних для здійснення аналітики:

1) аналітика вихідних даних для прийняття рішень;

2) автоматизовані аналітичні процеси, які надають описову, діагностичну, прогнозну та практичну аналітику [5].

Описова аналітика надає відповіді на питання: "Що сталося?" і "Що відбувається зараз", описуючи світ таким, яким він є, і надаючи історію та сучасне уявлення про світ у минулому та теперішньому часі.

Діагностична аналітика руйнує закономірності та усталені тенденції, та відповідає на питання: "Чому це сталося?". При цьому аналізуються статистичні моделі з ключовими змінними параметрами та зв'язками між даними (наприклад, ринкова аналітика, цінова пластичність, моделі шахрайства, інтелектуальний аналіз і кореляція даних, виявлення взаємозв'язків у даних тощо). Діагностична модель необхідна для визначення дійсності даних, отриманих в Інтернеті речей.

Прогнозна аналітика зосереджена на отриманні даних, необхідних для розуміння майбутнього. Така аналітика представляє прогнози щодо невідомих майбутніх подій на основі діагностичної аналітики та генерує нові рішення на основі цих даних [6]. Тобто Великі Дані, які були оброблені методами прогнозної аналітики, необхідні для побудови нових соціальних моделей .

Використання даних для розвитку технологій машинного навчання створюють нові можливості для прийняття дискримінаційних та упереджених рішень, що порушують конфіденційність. Наприклад, через аналіз весільних фотографій, опублікованих у соціальній мережі, можна зробити висновок про релігійну приналежність особи, а з аналізу даних про "спільних друзів" та фотографій з місця відпочинку страхові компанії можуть використати для встановлення розміру страхових внесків [7]. Голосовий помічник Alexa від Amazon може оцінювати стан здоров'я з урахуванням особливостей мовлення [8]. Таким чином, більше занепокоєння викликають не стільки дані, які про себе поширюють користувачі соціальних мереж, а ті висновки, які впливають на конфіденційність особи після обробки та аналізу таких даних.

Процедури збору та аналізу Великих Даних для розробки технологій ШІ не регламентовані у правовому полі. Хоча у Кодексах етики розробки технологій ШІ містяться вимоги до прозорості і чесності обробки даних [9 – 13]. Звернемо увагу, що дотримання принципу прозорості компаніями-розробниками технологій ШІ, які його реалізують через опис процедур розробки ШІ, створення внутрішніх комітетів етики, для аналізу корпоративних правил компанії та "прозорість" у розумінні норм GDPR, це не одне і те саме. Наприклад, "прозорість", відповідно до ст. 12 GDPR встановлює, що *"контролер повинен вжити необхідних заходів для надання будь-якої інформації ...щодо опрацювання, суб'єкту даних у стислій, прозорій, доступній для розуміння формі";* п. 78 Преамбули GDPR *"прозорість щодо функцій та опрацювання персональних даних* (включає – *від Авт.*) *можливості суб'єкта даних відстежувати опрацювання даних*" [1].

Дотримання принципу прозорості часто виконується так, що компанія-розробник технологій ШІ, описує як працює алгоритм, але це не означає конкретного обґрунтування процесу отримання прогнозних висновків (результатів обробки даних). Адже повний і "прозорий" опис такого процесу позбавить компанію конкурентних переваг. Принцип прозорості для суб'єкта даних, означає можливість управляти тим, які дані збираються, з якою метою, і бути поінформованим про використання отриманих результатів обробки.

Отже, у суб'єкта даних має бути право управляти результатами обробки у формі прогнозних висновків, до того, як буде сформовано дані, які можуть порушити його конфіденційність.

У контексті дослідження проблем аналітики Великих Даних та впливу отриманих результатів на права суб'єкта даних поставимо питання – чи може суб'єкт даних отримати результати обробки даних, які його стосуються та чи має компанія право застосовувати отримані дані для формування прогнозних висновків щодо такого суб'єкта? Наприклад, прийняття рішення страховою компанією про розмір страхових внесків для конкретного клієнта, або рішення роботодавця щодо потенційного кандидата за результатом аналізу його профілю у соціальній мережі.

Для відповіді на ці питання звернемось до норм GDPR.

Положення статей 13, 14 GDPR, описують обов'язки контролера щодо змісту та порядку отримання згоди суб'єкта ПД, і окремі положення не застосовуються (до змісту згоди – *від Авт.*), якщо п. (b) ч.5 "надання такої інформації (строк опрацювання, цілі, категорії ПД, період зберігання, законні інтереси для опрацювання, джерело отримання даних та інші підстави визначенні вказаними статтями – прим. *Авт.*), стає неможливим, чи викликало б несумісні наслідки, зокрема, для опрацювання (даних) задля досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілях" [1].

Таким чином, компанії, які обробляють ПД, у разі посилання на "суспільний інтерес обробки", або "статистичні цілі", формально отримують звільнення від обов'язку інформування суб'єкта даних про факт обробки його даних.

Згідно з ст. 15 GDPR право доступу означає, що:

"1. Суб'єкт даних повинен мати право на отримання від контролера підтвердження факту опрацювання її або його персональних даних і, якщо це так – доступ до персональних даних та інформації.

3. Контролер повинен надати копію персональних даних, які знаходяться у процесі опрацювання...

4. ...отримання такої копії не повинно негативно впливати на права та свободи інших осіб" [1].

Згідно ст. 16 GDPR право на виправлення надає *"суб'єкту даних ...право на виправлення його або її неточних персональних даних, яке повинен здійснити контролер без будь-якої необґрунтованої затримки"* [1].

Для розуміння особливостей реалізації цих норм звернемось до практики Суду ЄС. Досліджуючи особливості реалізації права доступу до даних у справах "YS, M і S" [15] Суд ЄС розглянув питання про те, чи можна вважати правовий аналіз, сформований спеціалістом під час надання адміністративної послуги, персональними даними. Ця справа є актуальною для дослідження правового статусу результатів обробки даних.

У процесі прийняття рішення щодо розгляду запиту громадян "YS, M і S", посадова особа, яка не має повноважень підписувати остаточне рішення по суті заяви, готує протокол щодо процесу прийняття остаточного рішення для внутрішнього обґрунтування дотримання усіх процедур. Протокол є частиною підготовчого процесу в цій службі, але не є частиною остаточного рішення, навіть незважаючи на те, що деякі пункти, згадані в ньому, можуть знову з'явитися в поясненні причин такого остаточного рішення.

У протоколі описуються як персональні дані заявника (ім'я, дата народження, національність) так і не персональні дані, які його стосуються: деталі процесуальної історії; відомості про заяви заявника та подані документи; правові положення, які застосовуються до ситуації заявника; оцінка вищевказаної інформації через призму застосовних правових положень. Ця оцінка називається "правовим аналізом".

Підкреслимо, що дані протоколу містять комбінований набір персональних і не персональних даних. Тому виникає питання: при реалізації прав суб'єкта даних, вони будуть стосуватись всього документу в цілому, чи тільки в частині, де є персональні дані, або і протоколу в цілому і отриманих оцінок (прогнозних висновків)?

Спірні питання, які розглядав Суд у цій справі, були такі:

- чи є правовий аналіз, включений до протоколу, персональними даними в розумінні Директиви 95/46/ЄС ?;
- чи має державний орган надати доступ до протоколу?;
- чи може державний орган відмовити в наданні доступу до протоколу на підставі "дотримання законних інтересів конфіденційності".

Якщо заявник просить доступ до протоколу, державний орган має надати копію цього документа чи достатньо надати опис (резюме, пояснення), які ПД заявника обробляються ? [15].

Це рішення є цікавими, ще і тому, що розгляд справи дозволяє встановити правовий статус даних, які можна перевірити (наприклад, фактів про особу), а не оцінок або даних, які не підлягають перевірці.

Розглядаючи викладені обставини справи Суд ЄС встановив, що дані внесені в протокол, є персональними даними. Правовий аналіз "стосується" конкретної фізичної особи, ґрунтується на ситуації індивідуальних характеристиках цієї особи, тому підпадає під дію поняття "персональні дані".

Але сама по собі сукупність правових норм юридичного аналізу не може тлумачитись як ПД, не може бути предметом судової перевірки і не є об'єктом реалізації права на виправлення (п. 39, 41, 42 рішення [15]).

У п. 40 рішення вказано, що *"правовий аналіз не є інформацією, що стосується заявника, оскільки він не обмежується суто абстрактним тлумаченням закону. Це інформація про оцінку та застосування компетентним органом цього закону до ситуації заявника, а сама ситуація встановлюється, серед іншого, за допомогою персональних даних, які доступні для державного органу"* [15].

Таким чином, похідні оцінки (прогнозні висновки), які зроблені з використанням ПД заявника, підпадають під норми законодавства про захист ПД, оскільки зроблені оцінки і висновки безпосередньо стосуються заявника і впливають на його життя.

Згідно п. 44 рішення принцип поваги до приватного життя, у контексті обробки ПД, означає, що: "*особа може бути впевнена, що персональні дані, які її стосуються, є правильними, і що вони обробляються в законний спосіб. Право доступу є необхідним для того, щоб дозволити суб'єкту даних отримати, залежно від обставин, виправлення, видалення або блокування своїх даних контролером"* і, у такий спосіб, реалізувати вказане право [15].

У п. 60 рішення суд вирішує питання меж реалізації права доступу та права отримувати копію документів. Зокрема, *"заявник має право доступу до всіх персональних даних, що стосуються його, які обробляються національними адміністративними органами. Для дотримання цього права достатньо, щоб заявнику було надано повне резюме цих даних у зрозумілій формі, тобто формі, яка дозволяє йому ознайомитися з цими даними та перевірити їх точність, і те, що вони оброблюється відповідно до цієї директиви, щоб заявник міг, у відповідних випадках, користуватися правами, наданими йому цією директивою"* [15].

У рішенні Суду ЄС чітко зазначено, що аналіз і складові висновки не вважаються персональними даними. Суд ЄС не розрізняє правовий аналіз і результати обробки даних у вигляді окремих коментарів чи висновків, створених у процесі обробки вихідного набору даних (п. 39 рішення [15]).

Аналіз не є еквівалентом прогнозних висновків, а скоріше міркуванням (логікою), яка веде до висновку. Таке міркування можна сприймати як когнітивний процес, тоді як "аналіз даних" – це записаний результат міркування. Важко уявити міркування чи логіку "правового аналізу", який не передбачає створення висновків щодо справи заявника. Необхідно розрізняти факти та процес їх аналізу. "Факти" можна описати "об'єктивними" показниками (наприклад, кілограми) або "суб'єктивними" критеріями (наприклад, важкий). Самі оцінки, оскільки їх можна вважати суб'єктивним вираженням факту, можуть вважатися персональними даним, оскільки вони "стосуються" фізичної особи [15].

Але це не означає, що через право доступу до процесу прийняття рішення, у поєднанні з правом на виправлення даних, суб'єкт може вказати на неточності в аналізі фактів, чи попередніх висновків у юридичному аналізі. Відтак, потенційна незгода, з висновками про результат обробки даних, є предметом судового розгляду, і оскарження дій чи бездіяльності державних органів, а не підміни функції суду і процесу доказування через право доступу та виправлення даних.

Тому, при визначенні, чи поширюється на певні дані правовий режим "персональних даних", необхідно визначити:

1. Чи можуть дані використовуватись для оцінки суб'єкта (наприклад, його поведінки).

2. Чи впливають такі дані на результат поведінки і дії суб'єкта даних.

При такому підході проблемним аспектом є невизначеність конкретних критеріїв, в якому випадку проаналізовані дані виражені суб'єктивними критеріями, а коли результати проведеного аналізу даних конкретно ґрунтуються на фактах.

Отже, при формулюванні правових підходів для реалізації права на результати обробки даних необхідно розрізняти факти або результати процесу оцінки (тобто "оцінка" або "думка"), а також сам процес (тобто "міркування") і конкретний метод обробки даних.

Важливо відзначити, що закон про захист даних, і зокрема право на доступ, не створено для надання доступу до результатів обробки або точності процесів прийняття рішень. У практиці Суду ЄС зустрічається аналіз сфери застосування двох інших Регламентів, які мають сприяти реалізації прав громадян у процесі адміністративної практики:

1. Регламент (ЄС) № 1049/2001 Європейського Парламенту та Ради від 30 травня 2001 року щодо доступу громадськості до документів Європейського Парламенту, Ради та Комісії [16]. Він покликаний забезпечити якомога більшу прозорість процесу прийняття рішень органами державної влади та інформації, на основі якої вони ґрунтують свої рішення. Таким чином, цей Регламент має сприяти, здійсненню права на доступ до документів і сприяти належній адміністративній практиці.

2. Регламент (ЄС) № 45/2001 Європейського Парламенту та Ради від 18 грудня 2000 року "Про захист осіб щодо обробки персональних даних установами та органами Співтовариства, та про вільний рух таких даних" [17], який призначений для забезпечення захисту свобод і основних прав осіб, зокрема їхнього приватного життя, під час обробки ПД. Але вони не призначені для забезпечення максимально можливої прозорості процесу прийняття рішень органами державної влади для належної адміністративної практики шляхом сприяння здійсненню права доступу до документів (п. 47 рішення [15]).

Таким чином, законодавство про захист даних загалом, і право на доступ зокрема, не розроблено для забезпечення повної прозорості у прийнятті рішень, що стосуються ПД, або для гарантування "належної адміністративної практики".

Такі підходи до практики застосування норм Регламентів і Директив, відображених в практиці Суду ЄС, викликають занепокоєння щодо правових та етичних стандартів прийняття рішень.

По-перше, правовий аналіз містить попередні висновки, припущення або думки, які лежать в основі остаточних висновків і рішення органу державної влади. Виключення права доступу та перегляду такого аналізу зі сфери дії законодавства про захист даних означає, що суб'єкти даних не можуть оцінити, наскільки потенційно впливові попередні висновки отримує державний орган до основного рішення щодо суб'єкта даних [18].

По-друге, практика надання суб'єкту даних лише короткого викладу (резюме в зрозумілій формі) ПД, які обробляються, суттєво обмежує сферу дії права на доступ та можливість суб'єкта даних оцінити законність обробки даних та достовірність своїх ПД, які використовуються для прийняття рішення.

По-третє, обмежена сфера дії закону про захист даних у сфері прийняття рішень в державному секторі, не сприятиме формуванню культури поводження і обробки даних в приватному секторі. Адже компанії можуть формулювати власні правила і політику конфіденційності, у яких ще більше будуть обмежувати право доступу та виправлення, або надмірно ускладнювати такі процедури.

Поширення аналітики Великих Даних і, як наслідок, збільшення можливостей контролерів даних отримувати інформацію про приватне життя людей, змінювати їх особистість через поведінкові шаблони, а також впливати на їх репутацію, свідчить про те, що потрібні додаткові категорії прав, які сприятимуть реалізації прав суб'єкта даних, з урахуванням особливостей розвитку технологій [15]. У сукупності з практикою правозастосування, можемо побачити, що спеціальних прав суб'єкта ПД, передбачених GDPR, не достатньо для захисту від прогнозних висновків за результатами аналізу Великих Даних технологіями ШІ.

Таким чином, згідно з рішеннями Суду ЄС, коли приватна компанія робить прогнозні висновки на основі зібраних даних, або приймає рішення на їх основі, навіть якщо остаточні висновки або рішення розглядаються як персональні дані, суб'єкти даних не можуть виправити їх відповідно до законодавства про захист даних. Суб'єкти даних також не мають доступу до аргументації, що лежить в основі рішень, яка не вважається персональними даними, а також засобів для виправлення аналізу відповідно до законодавства про захист даних [19, с. 531].

Цікаво проаналізувати і інше рішення, де Європейський Суд відступив від висновків по справах "YS, M і S".

У справі "Peter Nowak v. Data Protection Commissioner" [20] заявник попросив скористатися своїм правом доступу і "виправлення" його оціненого бланку відповідей на іспит. При визначенні питання, чи є персональними даними відповіді на питання іспиту, а також коментарі екзаменатора, Суд встановив:

- письмові відповіді, подані кандидатом на професійному іспиті, являють собою інформацію, яка "стосується" заявника як суб'єкта даних (п. 36) [20].
- зміст цих відповідей відображає ступінь знань і компетентності кандидата в певній галузі, а в деяких випадках і його інтелект, процеси мислення та здатність до міркування. У випадку рукописного тексту відповіді містять інформацію про його почерк (п. 37) [20].
- метою збору цих відповідей є оцінка професійних здібностей кандидата та його придатності до практики у відповідній професії (п. 38) [20].
- коментарі екзаменатора відображають думку або оцінку екзаменатора індивідуальних результатів іспиту кандидата, зокрема його знань і компетенцій у відповідній галузі. Крім того, мета цих коментарів полягає саме в тому, щоб зафіксувати оцінку екзаменатором роботи кандидата, і ці коментарі мають конкретні наслідки для кандидата (п. 43) [20].

Отже, якщо відповіді та зміст коментарів є персональними даними, це означає не тільки виникнення обов'язків контролера щодо обробки таких даних, а відповідно і виникнення у заявника прав на доступ, виправлення, чи заперечення.

Звичайно, право на виправлення не може дозволити кандидату "виправити" відповіді, які є "не правильними" (п. 52.) [20]. З іншого боку, виправлення можливе, у ситуації зміни титульного аркушу і помилкового приписування відповідей іншій особі (п. 54) [20].

Описані у рішеннях особливості реалізації права доступу та виправлення доводять, що законодавство про захист даних не поширюється на процеси забезпечення точності у процесі прийняття рішень. На перший погляд, у справі Nowak Суд розширив сферу дії норм про захист ПД, поширивши їх на думки та оцінки, іншого суб'єкта (екзаменатора), як такі, що "стосуються" заявника і мають на нього безпосередній вплив. Однак, висновки по справі описують обсяг даних, що обробляються, можливість поширення режиму ПД на результати обробки даних, формулювання оцінки щодо законності обробки. Оцінка точності результатів обробки та процесів прийняття рішень залишається поза сферою дії норм про захист ПД.

Ці два рішення відрізняються визначенням ПД. У справах "YS, M і S" Суд ЄС чітко тлумачить персональні дані обмежено. Ім'я, стать та подібні "факти" про особу, вважаються персональними даними, а думки, міркування та оцінки, які лежать в основі рішень, не є такими. У справі "Nowak", Суд ЄС навпаки встановив, що думки та оцінки (тобто коментарі екзаменатора) є персональними даними за критерієм "стосуються" фізичної особи.

Обидва судові рішення залишають відкритим питання про те, чи є результат оцінювання (наприклад, остаточний висновок, оцінка) і подальше рішення (наприклад, незадовільно оцінити когось на іспиті, відмовити в наданні адміністративної послуги) персональними даними. Незважаючи на розширення сфери визначення ПД у справі "Nowak", рішенню бракує повторюваності такого ж підходу в інших справах.

Вважається, що формування прогнозних висновків та похідних оцінок на основі аналізу ПД виходить за межі передбаченої мети законодавства про захист даних. Однак, якщо права в GDPR (наприклад, статті 15 – 17) не застосовуються до похідних даних (прогнозних висновків) одночасно з охороною ПД, то прогнозні висновки, які "стосуються" суб'єкта даних, та можуть вплинути на його поведінку, і отримані за результатом аналізу ПД, залишаються за межами правового захисту GDPR.

Можна звісно припустити, що на результати обробки може розповсюджуватись широка класифікація ПД за критерієм "стосується", однак в контексті обробки Великих Даних ШІ, ефекту "чорної скриньки" видається проблематичним ідентифікувати, які саме дані суб'єкта були оброблені, яким може бути ступінь визначення суб'єктом даних щоб оцінити точність або обґрунтованість отриманих висновків.

З урахуванням проведеного аналізу сформулюємо два поняття:

Прогнозні висновки *– це дані, отримані у результаті аналізу Великих Даних технологіями штучного інтелекту*.

Право на результати обробки даних *– це право суб'єкта персональних даних отримувати прогнозні висновки, які були отримані у результаті обробки комбінованих наборів даних, у тому числі псевдонімізованих.*

Окремою проблемою є корпоративний інтерес в обробці даних. Якщо результат прогнозних висновків у процесі надання адміністративної послуги можна оскаржити, оскільки існує зв'язок: "суб'єкт даних – заява в адміністративний орган – незаконне рішення (бездіяльність) – скарга суб'єкта даних – суд". То суб'єкти приватного сектору захищені положеннями Хартії ЄС про свободу підприємництва та нормами про захист наборів даних в режимі комерційної таємниці. Таким чином, суб'єкти господарювання самостійно встановлюють, критерії, за якими вони будуть оцінювати отримані висновки, і довести факт незаконності цих критеріїв оцінки буде дуже проблематично.

Висновки.

1. Великі Дані можуть включати в себе комбінований набір персональних і не ПД. Результат обробки Великих Даних у формі прогнозних висновків створює конкурентні переваги для компанії, оскільки дозволяє змоделювати поведінку особи, а інколи і безпосередньо вплинути на її рішення.

2. У випадку, якщо набір Великих Даних містив персональні дані, навіть у псевдонімізованій формі, отримані прогнозні висновки можуть мати безпосередній вплив на суб'єкта даних. Прогнозні висновки впливають на сферу приватності особи, через особливі категорії даних, які були проаналізовані для отримання висновків.

3. Права передбачені GDPR (доступу до даних, право на виправлення, стирання, обмеження опрацювання) застосовуються до обробки даних отриманих на підставі згоди, однак суб'єкт персональних даних позбавлений правової можливості захистити свої дані, оскільки не має правових інструментів виявлення, що його дані включені до набору Великих Даних.

4. Прогнозні висновки є окремим результатом обробки даних, які знаходяться за межами правового регулювання законодавства про захист ПД.

5. Право доступу до ПД не призначене для забезпечення прозорості процесу обробки даних, процесу прийняття рішення та формування прогнозних висновків. Це

позбавляє суб'єкта даних можливості оцінити, наскільки впливовими можуть бути прогнозні висновки, отримані за результатом обробки даних.

6. Право на результат обробки даних повинно передбачати можливість суб'єкта даних отримати прогнозні висновки з метою оцінки ступеню їх впливу на поведінку суб'єкта даних.

7. Вбачається, що використання комбінованого набору даних у псевдонімізованій формі, для отримання прогнозних висновків, не допоможе суб'єкту даних встановити, чи були оброблені саме його персональні дані, чи це були дані іншої особи. Однак, це не має бути універсальною підставою для відмови в наданні таких висновків, оскільки, право на результат обробки даних має забезпечувати окреме право суб'єкту даних, а саме: можливість самостійно оцінити ступінь впливу на його поведінку (дії, бездіяльність) через використання компаніями прогнозних висновків, а не їх точність та обґрунтованість по відношенню до конкретного суб'єкта даних.

8. Право на результат обробки даних не має тлумачитись у вузькому сенсі – як окремий спосіб реалізації права на виправлення неточних даних у контексті обробки Великих Даних технологіями ШІ.

9. Право на результат обробки даних повинно мати самостійне значення. Якщо його розглядати у системі прав, передбачених законодавством про захист ПД, існує ризик відмови у наданні результатів обробки даних, оскільки до комбінованого набору Великих Даних можуть не включатись персональні дані. Отже, компанії не будуть зобов'язані надавати такі результати обробки.

10. З урахуванням поставленої юридичної проблеми у роботі [21, с. 90] про "необхідність створення багаторівневої і багатооб'єктної системи захисту ПД та формування нової системи правового забезпечення" зазначимо, що норми GDPR, які широко регламентують права суб'єкта даних, у контексті особливостей їх обробки технологіями ШІ не охоплюють прогнозні висновки, які впливають на майбутню поведінку і дії суб'єкта права, а право на результат обробки даних, може вважатись окремим елементом такого багаторівневого і багатооб'єктного правового забезпечення і повинно мати самостійне значення у системі інформаційних відносин.

Використана література

1. Regulation (EU) 2016/679 Of The European Parliament And Of The Council on General Data Protection Regulation. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A 32016 R0679&qid=1684155858687

2. Дубняк М.В. Економіка даних: правовий та етичний аспект. *Інформація і право.* № 3(46)/2023. С. 64-74.

3. Graef I., Gellert R., Husovec, M. (2018). Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation. Cybersecurity. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189

4. Charter of Fundamental Rights of the European Union (2016/C 202/02). URL: http://data. europa.eu/eli/treaty/char_2016/oj

5. Kennedy G. (2017) Asia Pacific News. *Computer Law and Security Review*, 33, 6, 896-904. URL: https://doi.org/10.1016/j.clsr.2017.09.006.

6. Scism L. (2019) New York Insurers Can Evaluate Your Social Media Use – If They Can Prove Why It's Needed, WALL ST. J. URL: https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social- media-useif-they-can-prove-why-its-needed-11548856802 (on file with the Columbia Business Law Review).

7. Altenburger K., Ugander J. (2018) Monophily in Social Networks Introduces Similarity among Friends-of-Friends. *Nature human behaviour*, at 284.

8. Cook J. (2018) Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine, *TELEGRAPH*. URL: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new- alexa-feature-knows-offers-medicine [https://perma.cc/V346-HFWE

9. Adobe AI Ethics Principles (2021) URL: https://www.adobe.com/about-adobe/aiethics.html

10. Ethical Norms for the New Generation Artificial Intelligence (2021) National Governance Committee for the New Generation Artificial Intelligence, China. URL: https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china

11. Samsung AI principles (2018). URL: https://www.samsung.com/us/about-us/digital-responsibility/ai-ethics

12. Baidu Four principles of AI ethics (2018). URL: https://www.fonow.com/view/208592.html

13. Google AI principles (2018). URL: https://ai.google/responsibilities/responsible-ai-practices/?category=general

14. Sage Ethics of Code: Developing AI for Business with Five Core Principles (2017). URL: https://www.sage.com/investors/investor-downloads/press-releases/2017/06/27/sage-shares-core-principles-for-designing-ai-for-business

15. YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S: Judgment of the Court (Third Chamber), 17 July 2014. ECLI identifier: ECLI:EU:C:2014:2081. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2014%3A2081

16. Regulation (EC) № 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049

17. Regulation (EC) № 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

18. Korff D. (2014) The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data, EU LAW ANALYSIS. URL: http://eulawanalysis.blogspot.com/2014/10/the- proposed-general-data-protection

19. Wachter S., Mittelstadt B.D. (2018). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 494-620. DOI: https://doi.org/10.7916/cblr.v2019i2.3424.

20. Peter Nowak v Data Protection Commissioner : Judgment of the Court (Second Chamber) of 20 December 2017, ECLI identifier: ECLI:EU:C:2017:994. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62016CJ0434

21. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. *Інформація і право.* № 2(17)/2016. С. 85-91.

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

УДК 342.56::004

МАНЬГОРА В.В., *кандидат педагогічних наук, доцент*, доцент кафедри права Вінницького національного аграрного університету.
ORCID: https://orcid.org/0000-0003-3812-3797.
МИХАЛЬЧУК Ю.О., студентка Вінницького національного аграрного університету.

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПРАВІ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Анотація. *Розглянуто вплив цифрових технологій на правову систему України та їхню роль у поліпшенні доступу до правосуддя та ефективності судової системи. Визначено, яку роль відіграють цифрові технології у сучасній правовій системі, а також їхній вплив на якість послуг правосуддя, забезпечення конфіденційності та кібербезпеки, а також доступність правосуддя для всіх громадян. Аргументовано важливість впровадження цифрових інструментів у правозастосуванні та надано огляд основних аспектів цієї проблеми. Цифрові технології нині впливають на всі аспекти сучасного життя, включаючи сферу права. Розглянуто використання цифрових технологій у правовій сфері та досліджено їх перспективи та виклики, питання конфіденційності даних, кібербезпеки та етичних аспектів використання цифрових технологій у правовій сфері. Висвітлено, як цифрові інструменти впливають на процеси розгляду судових справ, автоматизацію документообігу, підвищення доступності правових послуг для фізичних осіб та юридичних осіб. Акцентовано увагу на потенціалі та необхідності адаптації правової системи до викликів цифрової епохи і наголошено на важливості збалансованого підходу до використання цифрових технологій в інтересах справедливості та правопорядку.*

Ключові слова: *цифрові технології, право, автоматизація, доступність правових послуг, кібербезпека, справедливість, правопорядок, документація.*

Summary. *The impact of digital technologies on the legal system and their role in improving access to justice and the effectiveness of the judicial system are considered. It is determined what role digital technologies play in the modern legal system, as well as their impact on the quality of justice services, privacy and cyber security, as well as access to justice for all citizens. The importance of implementing digital tools in law enforcement is argued and an overview of the main aspects of this topic is provided. Digital technologies now affect all aspects of modern life, including the field of law. The use of digital technologies in the legal sphere is considered and their prospects and challenges, issues of data privacy, cyber security and ethical aspects of the use of digital technologies in the legal sphere are explored. It is highlighted how digital tools affect the processes of consideration of court cases, automation of document flow, increasing the availability of legal services for individuals and legal entities. Attention is focused on the potential and necessity of adapting the legal system to the challenges of the digital era, and the importance of a balanced approach to the use of digital technologies in the interests of justice and law and order is emphasized.*

Keywords: *digital technologies, law, automation, availability of legal services, cyber security, justice, law and order, documentation.*

Постановка проблеми. Використання цифрових технологій у сфері права є актуальною темою як в Україні, так і в усьому світі. Ці технології змінюють парадигму юридичного обслуговування, але водночас постають численні перспективи та виклики. Проблеми, пов’язані з використанням цифрових технологій у праві в Україні та світі, включають: з одного боку, цифрові технології роблять юридичні послуги більш доступними для громадян і підприємств через онлайн-консультації та автоматизовані

процедури. Проте це може залишити без роботи юридичних фахівців та зменшити їхні доходи. Перехід до цифрового середовища призводить до загроз кібербезпеці та можливого витоку конфіденційної інформації. Це особливо важливо у сфері права, де документи та дані клієнтів мають особливий характер. Правова система повинна адаптуватися до новітніх технологій, щоб відповідати сучасним вимогам та забезпечувати ефективність судових процесів. Використання цифрових технологій у праві може створити ризик виникнення нерівності в доступі до правосуддя та може порушувати принцип справедливості.

Вирішення цих проблем вимагає ретельного аналізу, розробки ефективних регулюючих механізмів, забезпечення кібербезпеки та створення етичних стандартів для використання цифрових технологій у праві в Україні та на міжнародному рівні.

Сучасний світ переживає період надзвичайних трансформацій, де цифрові технології стають необхідною частиною всіх сфер життя. З появою Інтернету, штучного інтелекту, блокчейн-технологій та інших інновацій, вплив цифрового віку відчутно впливає і на сферу права.

На фоні стрімкого розвитку технологій та зростаючої залежності суспільства від інформаційних систем, правові системи всіх країн стикаються з рядом нових викликів та можливостей. З одного боку, цифрові технології можуть покращити ефективність судових процедур, забезпечити швидкий та зручний доступ до правосуддя. З іншого боку, вони створюють загрози щодо приватності та безпеки особистих даних, а також підвищують ризик кіберзлочинності.

Результати аналізу наукових публікацій. Зазначена галузь досліджень стає дедалі більш актуальною, оскільки технологічний прогрес впливає на правову систему та її функціонування. Дослідники вивчають, як цифрові технології впливають на розвиток юридичної науки і практики, методи і засоби захисту правових інформаційних систем і даних. Дослідники, такі як О. Андрєєва, П. Біда, О. Вінник, Н. Левицька, О. Петрова, Т. Попович, О. Шаповалова, та інші приділяли увагу різним аспектам функціонування права і цифровізації. Д. Приймаченко, М. Віхляєва досліджували отримання інформації про діяльність суду та доступ до судових рішень як гарантія ефективності громадського контролю за діяльністю суддів.

Хоча деякі вчені, розглядали цю тематику у межах своїх наукових інтересів, вона все ще потребує більш комплексного дослідження. Зокрема, у зв’язку зі зростаючим суспільним попитом на ефективний контроль за забезпеченням якісного та справедливого правосуддя.

Метою статті є визначення впливу цифрових технологій на правову систему, переваг та ризиків їхнього використання у судовому процесі та з’ясувати, як ці технології можуть сприяти поліпшенню доступності та ефективності правосуддя, зокрема у аспектах захисту даних та кібербезпеки.

Виклад основного матеріалу. Перше, що хочеться розглянути говорячи про тему цифрових технологій у праві – це електронне ведення документації в судах, тобто заміна паперової документації електронними системами, переваги електронного ведення документації та приклади реалізації.

Міністерство цифрової трансформації України було створено в 2019 році. Основна мета Міністерства цифрової трансформації полягала в сприянні розвитку цифрових послуг в Україні, а також у впровадженні цифрових технологій в різні сфери життя країни.

Застосунок також можна використати для того, щоб повідомити про Після запровадження цифровізації в Україні, головним державним мобільним застосунком є “Дія”. У воєнний час запровадили єДокумент, який зараз є посвідченням особи. Його

можна показувати на блокпостах, а також в інших випадках. Він приймається як альтернатива паспорту та містить офіційні дані. Його також можна сканувати. Через програму також реалізували виплати для тих, хто залишився без роботи через війну. Такі люди також можуть перевірити можливість отримання 6500 гривень через "Дію". Фізичні особи-підприємці також можуть оплатити податки чи зареєструватись.

Застосунок також можна використати для того, щоб повідомити про пошкоджене майно. Якщо будинок чи квартира постраждали під час війни – це можна зафіксувати у "Послугах" та в подальшому отримати компенсацію. Ще через "Дію" можна зробити фінансовий внесок у фонд "Повернись живим", на допомогу Збройним Силам України. А також тут можна повідомити ЗСУ про ворожу техніку чи скупчення окупантів через систему "єВорог". Ці дані можуть бути дуже корисні.

Щоб бути в курсі подій, у застосунку можна увімкнути прямий ефір українського інформаційного марафону чи радіо. Особливо це корисна функція для тих регіонів, де є перебої зі звичайним телебаченням чи радіомовленням.

В одному з оновлень, в "Дію" додали повноцінну мобільну гру, в яку можна швидко зайти просто через основну програму, в розділі "Послуги".

У користувачів є можливість уявити себе в ролі оператора безпілотнику "Байрактар", утримуючи блокпост та знищуючи російську техніку. Кілька людей вже встановили доволі солідні рекорди. Кожен може спробувати покращити ці показники. Додаток "Дія" є досить важливим під час військового стану, адже він полегшує отримання різних документів [1].

Щодо діяльності Мінцифри, воно працює над створенням "держави у смартфоні", що поєднує в собі мобільний застосунок та портал державних послуг. Одним з важливих завдань міністерства є розвиток цифрової грамотності громадян, саме тому 21 січня 2020 року в Мінцифрі запустили курси з цифрової освіти.

Цілі міністерства до 2024 року:

- перевести 100 % усіх публічних послуг для громадян та бізнесу онлайн;
- забезпечити 95 % транспортної інфраструктури, населених пунктів та їхні соціальні об'єкти доступом до високошвидкісного Інтернету;
- навчити 6 млн. українців цифрових навичок;
- підвищити частку ІТ у ВВП країни до 10 %.

Відкриті дані мають потужний антикорупційний ефект, сприяють прозорості влади, позитивно впливають на розвиток економіки. 2017 року відкриті дані принесли в економіку України понад $700 млн., або 0,67 % ВВП. І при збереженні нинішніх темпів, за прогнозами, до 2025 року ця цифра зросте вдвічі – до понад $1,4 млрд., або 0,92 % ВВП.

Міністерство цифрової трансформації України спільно з іншими органами державної влади, органами місцевого самоврядування та міжнародними партнерами проводить роботу по забезпеченню інтероперабельності – принципу, коли різні інформаційні ресурси можуть взаємодіяти між собою на базі уніфікованих інтерфейсів та протоколів. Зокрема, впроваджується "Трембіта" – система взаємодії державних електронних інформаційних ресурсів, а також формується Національний реєстр електронних інформаційних ресурсів. В цьому напряму Україна використовує досвід Естонії – країни, яка має найбільш досконалу в світі систему електронного урядування [2].

Щодо судової системи в сучасних судах, електронне ведення документації стає стандартом. Суди все частіше відмовляються від паперових документів і переходять до електронних систем, де всі судові документи, включаючи позови, подання сторін,

рішення суду та апеляційні скарги, зберігаються в електронному форматі. Наприклад, у Сполучених Штатах, Портал судової інформації PACER (Public Access to Court Electronic Records) дозволяє адвокатам, сторонам у справі та громадськості отримувати доступ до судової інформації та документів в електронному вигляді [3].

Щодо переваг електронного ведення документації:

- ефективність: електронне ведення документації зазвичай пришвидшує судовий процес, оскільки документи можуть бути швидко оброблені та передані між сторонами, адвокатами та судами без необхідності фізичного переміщення паперових копій;

- зручність: сторони та адвокати можуть отримати доступ до судової документації з будь-якого місця, яке має Інтернет-з'єднання. Це полегшує участь у судових процедурах і зменшує необхідність фізичної присутності;

- зберігання: електронні системи забезпечують зберігання документів в безпечному та організованому вигляді, запобігаючи втратам або пошкодженню паперових документів.

Наведемо приклади реалізації.

Європейський суд з прав людини (ЄСПЛ) – Суд використовує систему ECHR CASE LAW, яка дозволяє зручно та ефективно шукати та отримувати доступ до рішень та матеріалів судових справ. ЄСПЛ приймає скарги електронним шляхом через систему e-Curia. Це дозволяє сторонам подавати скарги та документи безпосередньо в електронному вигляді.

Суд Співдружності ЄС використовує систему ECJ e-Curia для електронного подання скарг та інших документів, забезпечуючи ефективну обробку справ [4] .

Ці приклади ілюструють успішне впровадження електронних систем у судову практику, які полегшують роботу судів та забезпечують легкий доступ до судової документації для всіх зацікавлених сторін.

Друге, що розглянемо це віддалені судові засідання, а точніше переваги віддалених судових засідань, виклики та обмеження, приклади успішної реалізації віддалених судових засідань, детально ознайомимось з використанням відеоконференцій та інших засобів зв'язку для їх проведення.

Перевагами віддалених судових засідань є:

- зручність для учасників: віддалені засідання дозволяють сторонам, адвокатам, свідкам та суддям брати участь у судових процедурах, не виходячи з дому або офісу;

- економія часу та коштів: віддалені засідання можуть зменшити витрати на подорожі та витрати на оренду судових приміщень;

- доступність для важкодоступних віддалених регіонів: віддалені засідання роблять судову систему більш доступною для громадян.

Проблемами проведення віддалених судових засідань є:

- технічні проблеми: нестабільне Інтернет-з'єднання або недостатня технічна підтримка можуть створювати труднощі під час проведення віддалених засідань;

- конфіденційність та безпека: забезпечення конфіденційності та безпеки відеоконференцій може бути складною задачею, особливо в справах, де важливо зберігати конфіденційність інформації;

- необхідність регулювання: віддалені засідання вимагають розробки відповідних правил і нормативів для забезпечення справедливості та чесності процесу.

Приклади успішної реалізації віддалених судових засідань.

У Сінгапурі віддалені судові засідання стали загальноприйнятим практичним рішенням під час пандемії COVID-19. Суди використовували відеоконференції для проведення судових засідань та слухань, забезпечуючи безпеку і доступність.

В судах Каліфорнії США була запроваджена ініціатива для зменшення переповненості судових будівель та зменшення витрат. Вона передбачала проведення віддалених судових засідань для деяких типів справ, що дозволило ефективніше використовувати ресурси.

Європейський Суд з питань прав людини відкрив можливість проводити судові слухання в онлайн-режимі, забезпечуючи дотримання термінів та безпеки [5].

Ці приклади ілюструють успішну реалізацію віддалених судових засідань, яка дозволяє підтримувати судову діяльність у важкі часи та забезпечує доступність та ефективність правосуддя для громадян та учасників судових процесів.

Під час віддалених судових засідань, забезпечення конфіденційності та захист особистих даних стають критичними питаннями. Важливо забезпечити учасників судового процесу, щоб вони могли бути впевнені в тому, що їхні дані та інформація залишаються приватними та захищеними. Нижче розглянемо ці питання більш детально та наведемо приклади.

1. Конфіденційність і шифрування засобів зв'язку. Проблемою є те, що під час віддалених судових засідань, інформація, що передається через відеоконференції або інші засоби зв'язку, може стати предметом атак та перехоплення, що загрожує конфіденційності судового процесу та особистих даних учасників.

Рішенням може стати використання сучасних технологій шифрування, які забезпечують захист передачі даних від несанкціонованого доступу. Засоби зв'язку повинні бути налаштовані таким чином, щоб забезпечити ефективне шифрування під час віддалених судових засідань.

До прикладу, в інтересах захисту конфіденційності одна з популярних платформ для відеоконференцій Zoom удосконалила свої заходи безпеки, включаючи шифрування засобів зв'язку з початку до кінця для забезпечення конфіденційності розмов [6].

2. Аутентифікація та доступ до засідань. Проблемою є забезпечення правильної ідентифікації учасників судових засідань та обмеження доступу лише для авторизованих осіб є критично важливим для конфіденційності та безпеки.

Вирішити цю проблему можна легко, віддалені судові засідання повинні включати процедури аутентифікації, такі як введення паролів або використання біометричних методів ідентифікації, щоб підтвердити особу учасника. Крім того, контролювати доступ до засідань і обмежувати присутність лише до осіб, які мають легітимний інтерес у справі.

Як приклад суди можуть використовувати спеціальні платформи для віддалених судових засідань, які надають інструменти для аутентифікації учасників і керування доступом до конференцій, такі як Cisco Webex або Microsoft Teams.

3. Зберігання інформації та персональних даних. Оскільки судові засідання можуть бути записані або збережені для подальшого використання, важливо гарантувати безпеку та конфіденційність збережених даних та записів, але це є проблемою.

Інформація та записи судових засідань повинні зберігатися в захищеному та шифрованому середовищі. Важливо регулярно оновлювати системи зберігання даних та використовувати заходи безпеки для запобігання несанкціонованому доступу.

Суди можуть співпрацювати з провайдерами хмарних послуг, такими як Amazon Web Services або Microsoft Azure для зберігання даних та записів судових засідань у захищеному хмарному середовищі.

Ці приклади ілюструють важливість заходів забезпечення конфіденційності та захисту особистих даних під час проведення віддалених судових засідань, а також методи та інструменти, які можна використовувати для забезпечення цієї

конфіденційності та захисту. Важливо, щоб судові органи спільно з інформаційними та технологічними партнерами розробляли та дотримувалися найвищих стандартів безпеки та конфіденційності під час переходу до віддалених форматів судових засідань.

Загальний принцип полягає в тому, щоб вирішувати технічні та організаційні питання забезпечення конфіденційності на кожному етапі проведення віддаленого судового засідання, включаючи комунікацію, аутентифікацію, зберігання та контроль доступу. Такий підхід допомагає зберегти важливі аспекти судової процедури, такі як конфіденційність та справедливість.

Будучи відповідальними за використання цифрових технологій у судовій системі, суди мають ретельно розробляти політики та процедури, які забезпечують високий рівень конфіденційності та захисту особистих даних. Це важливо як для дотримання законів про захист даних, так і для забезпечення довіри громадськості до судової системи.

Захист від кіберзлочинності є надзвичайно важливим аспектом використання цифрових технологій у судовій системі. Кіберзлочинці можуть намагатися перешкодити роботі суду, отримати незаконний доступ до конфіденційної інформації, використовувати атаки для обману систем безпеки. Нижче розглянемо детальніші аспекти захисту від кіберзлочинності в судовій системі та наведемо приклади заходів захисту.

1. Захист мереж та інфраструктури. Судові системи зазвичай використовують складні мережі та інфраструктуру, що робить їх цільовими для кіберзлочинців. Атаки можуть спрямовуватися на відмову в обслуговуванні, витік чутливої інформації та інші загрози.

Рішенням даної проблеми є те, що суди повинні встановити сильні системи захисту, включаючи брандмауери, антивірусне програмне забезпечення та регулярно оновлювати їх. Важливо також проводити аудит безпеки та вразливостей [7].

Прикладом є Суд в Делавері (США), який зазнав DDoS-атакі в 2020 році, яка спричинила тимчасову недоступність судового веб-сайту. Після цього інциденту суд вдосконалив свої заходи захисту мережі [8].

2. Захист особистих (персональних) даних. Судова система містить велику кількість особистих даних, таких як імена, адреси, номери соціального страхування та інші конфіденційні дані. Злочинці можуть намагатися викрасти або незаконно отримати доступ до цих даних.

Суди повинні дотримуватися суворих стандартів захисту даних, включаючи шифрування збереження даних, контроль доступу до систем та процедур видалення даних. Також важливо навчати персонал з питань кібербезпеки проводити аудити для виявлення вразливостей.

Наприклад Великий судовий реєстр в Великобританії був атакований в 2017 році, і під час цієї атаки були скомпрометовані персональні дані близько 160000 осіб. Цей інцидент призвів до посилення заходів захисту даних в судовій системі.

3. Соціальний інжиніринг та освіта користувачів. Кіберзлочинці можуть намагатися обдурити користувачів, отримати доступ до їхніх облікових записів або використовувати фішингові атаки для отримання конфіденційної інформації.

Судова система повинна проводити навчання персоналу та користувачів щодо методів захисту від соціального інжинірингу та фішингу. Важливо надавати інструкції щодо виявлення підозрілих повідомлень та поведінки.

Уряд Онтаріо в Канаді запустив кампанію з навчання персоналу щодо ідентифікації та уникнення фішингових атак, щоб підвищити рівень свідомості та захисту від цього типу загроз і цим вирішив дану проблему [9].

Захист від кіберзлочинності в судовій системі вимагає комплексного підходу, який включає технічні засоби, механізм реалізації, а також навчання персоналу та користувачів. Незалежно від регіону або судової системи, суди повинні постійно моніторити загрози кібербезпеки та адаптувати свої заходи захисту для відповіді на сучасні та нові загрози.

4. Планування відновлення після інциденту. Навіть з усіма заходами захисту, інциденти кібербезпеки можуть відбуватися. Важливо мати план відновлення після інциденту для швидкого відновлення роботи суду після атаки.

Суди повинні розробляти та впроваджувати плани відновлення після інциденту, які включають резервне копіювання даних, відновлення систем та забезпечення безпеки під час відновлення. Це допоможе мінімізувати час простою та втрати даних.

Суд Флориди розробив та впровадив план відновлення після інциденту після того, як був підданий рейдерській атаці в 2020 році. План дозволив швидко відновити роботу суду та запобіг втраті важливих даних.

Загалом, захист від кіберзлочинності у судовій системі вимагає постійного вдосконалення та адаптації до нових загроз. Це питання стає все більш актуальним, оскільки суди використовують цифрові технології для покращення доступності та ефективності. Забезпечення надійного захисту є важливим для збереження довіри до судової системи та забезпечення конфіденційності та справедливості судових процедур.

Застосування цифрових технологій у судовій системі може призвести до значної економічної вигоди, включаючи зниження витрат. Розглянемо як це може бути досягнуто та наведемо приклади застосування цифрових технологій у судовій системі з різних країнах світу.

1. Оптимізація робочих процесів. Традиційні судові процеси можуть бути витратними та забирати багато часу через необхідність багаторазового друку документів, фізичне перебування та інші рутинні завдання.

Використання електронного документообігу та автоматизації процесів може значно зменшити витрати на паперову документацію, логістику та адміністративні операції.

Суд у штаті Огайо, США, впровадив систему електронного документообігу, що дозволило зменшити витрати на друк та обробку паперових документів на мільйони доларів щорічно.

2. Віддалені судові засідання. Участь у судових засіданнях, які вимагають фізичної присутності, може стати витратною для всіх учасників.

Віддалені судові засідання через відеоконференції або інші засоби зв′язку можуть зменшити витрати на подорожі, оренду приміщень та забезпечити зручність для всіх сторін.

Суди у Великобританії використовували віддалені засідання під час пандемії COVID-19 для зниження витрат на оренду судових будівель та подорожі [10].

3. Електронний доступ до документів. Доступ до судових документів може бути ускладнений та витратним через потребу у фізичному візиті до суду.

Впровадження системи електронного доступу до документів, таких як судові записи, рішення суду, дозволяє громадськості та сторонам легко отримувати інформацію в електронному форматі, що робить процес більш доступним та ефективним.

Суд у Сінгапурі надає громадськості доступ до судових рішень та документів через онлайн-портал, що дозволяє значно зменшити витрати на запити на інформацію та фізичні візити до суду [11].

4. Ефективне управління справами. Управління великим обсягом справ та документів може бути витратним та вимагати багато ресурсів.

Використання цифрових систем управління справами дозволяє автоматизувати процеси, відстежувати хід розгляду справ та ефективно розподіляти завдання між працівниками.

Суд у Швейцарії впровадив цифрову систему управління справами, що дозволило покращити ефективність та знизити витрати на адміністративні процеси [12].

Загальною ідеєю є те, що використання цифрових технологій може покращити ефективність та знизити витрати в судовій системі через оптимізацію процесів, забезпечення доступу до інформації та підвищення продуктивності. Це стає особливо актуальним у сучасному цифровому світі.

Використання цифрових технологій у судовій системі може суттєво покращити доступність правосуддя для громадян та зробити судову систему більш доступною та ефективною.

5. Електронний доступ до інформації та документів. Громадяни часто мають обмежений доступ до інформації про судові рішення, документи та розклад судових засідань. Створення онлайн-порталів і систем для громадського доступу до судової інформації дозволяє громадянам отримувати доступ до рішень, справ та іншої інформації в будь-який зручний для них час.

В Україні, проект “е-суд” надає громадянам доступ до судової інформації та документів через онлайн-портал, де можна перевіряти стан справ, дізнаватися розклад засідань та багато іншого.

6. Віддалені судові засідання. Деякі громадяни можуть мати обмежений фізичний доступ до суду через відстань, обмежену мобільність або інші обставини.

Віддалені судові засідання через відеоконференції та інші засоби зв’язку роблять участь у судових процесах більш доступною для всіх сторін.

В Індії, Верховний Суд розробив систему “Віртуальний суд” для проведення судових засідань віддалено під час пандемії, що дозволило сторонам брати участь в судових процесах без фізичної присутності [13].

7. Електронні подачі та комунікація. Фізичне подання судових документів та комунікація з судом може бути не зручним та займати багато часу.

Використання електронних систем подачі документів та комунікації з судом дозволяє сторонам здійснювати ці процедури в онлайн-режимі.

У Норвегії, система “Altinn” дозволяє громадянам та компаніям подавати судові документи та спілкуватися з судом онлайн.

8. Покращення доступності для осіб з обмеженою мобільністю. Особи з обмеженою мобільністю можуть мати складнощі з фізичним доступом до судових будівель. Забезпечення доступності судових будівель та віддалених судових засідань для осіб з обмеженою мобільністю, включаючи можливість віддаленої участі в судових засіданнях через спеціальні інтерфейси та підтримку від асистентів.

У Великобританії, “Суд для всіх” (Court for All) розробив умови для забезпечення доступності судових послуг для осіб з різними видами обмеженої мобільності.

Україна активно працює над цифровізацією системи права та юстиції з метою поліпшення доступу до правосуддя, забезпечення прозорості та швидкості роботи судів та інших правових органів.

Єдиний реєстр досудових розслідувань – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних про кримінальні правопорушення та хід досудового розслідування у кримінальних провадженнях.

Державна реєстрація прав на нерухоме майно – електронна система "Дія" надає послуги з реєстрації права власності на нерухоме майно. Це полегшує процес купівлі-продажу майна та забезпечує прозорість у галузі нерухомості.

Впровадження системи електронного документообігу вимагає створення оптимальних умов для зберігання електронних документів та інформаційних ресурсів на державному рівні. У зв'язку з цим виникла потреба у створенні Центрального державного електронного архіву України, який був створений 12 травня 2007 року, як єдиний пункт зберігання електронних документів Національного архівного фонду України. Центральний державний електронний архів України зберігає електронні записи та інформаційні ресурси Національного архівного фонду, веде їх облік , забезпечує цілісність та створює умови для їх використання [14].

Єдиний портал державних послуг "Дія" в Україні надає доступ до різних громадянських, адміністративних та інших правових послуг для громадян та бізнесу. Найбільш популярні з них:

1. Реєстрація місця проживання – громадяни можуть змінювати своє місце проживання, зареєструвати нове місце проживання чи отримати витяг з реєстру.

2. Отримання державних соціальних послуг – громадяни можуть подавати заяви на отримання допомоги та субсидій, включаючи субсидії на оплату комунальних послуг.

3. Реєстрація транспортних засобів – власники автотранспортних засобів можуть реєструвати та отримувати технічний паспорт для авто.

4. Подача декларацій – громадяни та підприємці можуть подавати податкові декларації та інші документи, пов'язані з оподаткуванням та фінансовою звітністю.

5. Реєстрація бізнесу – підприємці можуть реєструвати свої бізнеси та отримувати необхідні документи для ведення діяльності.

6. Оформлення паспорта громадянина України – громадяни можуть подавати заяви на оформлення паспорта та інших документів.

7. Подача заяв та скарг –громадяни можуть подавати заяви, скарги та звернення до різних органів державної влади.

8. Реєстрація актів цивільного стану – відомості про народження, шлюби та смерть можна реєструвати через портал.

9. Отримання інформації про нерухомість – громадяни можуть отримати витяги з реєстру нерухомості та іншу інформацію про власність.

Це лише частина послуг, які можна отримати через портал "Дія". Важливо зауважити, що перелік послуг та їх умови можуть змінюватися з часом і користувачам слід перевіряти актуальну інформацію на самому порталі або на веб-сайтах відповідних державних органів.

Протягом травня 2023 р. в умовах повномасштабного воєнного вторгнення на українську територію в країні тривала діяльність щодо цифрової трансформації економіки на основі впровадження інновацій, оптимізації та переведення інструментів державного регулювання бізнесу в електронну форму, а також інтеграції української інноваційної екосистеми в європейську мережу.

У межах підготовки до саміту країн "Великої сімки" Україна взяла участь у засіданні міністрів цифровізації – G7 Digital and Tech Ministers'Meeting 2023, на якому основну увагу приділено принципам управління новими технологіями. З-поміж пріоритетних

напрямів обговорення – цифровізація суспільства, забезпечення стійкої цифрової інфраструктури, транскордонне передавання даних, використання штучного інтелекту й виклики у сфері кібербезпеки. Окрему сесію засідання присвячено: впливу російської війни проти України на світову економіку; інноваційним рішенням у протидії атакам агресора. У комюніке, підписаному лідерами G7 у Хіросімі 20 травня 2023 р., у частині цифровізації визнано, що цифрові інновації, прискорені новими технологіями та інноваційними моделями управління, здатні розблокувати інклюзивне економічне зростання та сталий розвиток суспільства на засадах прозорості, відкритості, справедливості, неупередженості, конфіденційності та інклюзивності [15].

Про партнерство України в роботі GovTech-інкубатора ЄС (Govtech4all) та реалізацію трьох пілотних проектів на суму €6 млн. протягом 2023-2025 рр. для створення нових моделей транскордонного надання цифрових державних послуг оголошено під час Digital Transformation Summit у Брюсселі 11 травня 2023 року [16].

Європейська інноваційна рада надасть €20 млн. за програмою Seeds of Bravery для розвитку інновацій в Україні. Грантовий фонд для українських стартапів та інноваційних компаній становитиме €12 млн. Окрім грантового фінансування, передбачено залучити додаткові інвестиції українським стартапам для впровадження інноваційних рішень, що спрямовані на відбудову України та реалізацію проєктів комерціалізації наукових досліджень. Програма Seeds of Bravery дає змогу залучати грантове фінансування компаніям сумою до €60 тис. [17].

У межах відбору учасників до глобальної програми Start Path Ukraine п’ять українських фінтех-стартапів доєдналися до програми Mastercard Start Path Ukraine і продемонстрували інструменти для активізації фінтех-сектору та масштабування позитивного впливу на вітчизняну економіку. Серед цифрових рішень фінтех-стартапів: автоматизація процесу залучення клієнтів (Electronic KYC); автоматизація процесів фінмоніторингу (AML Point); комплексне рішення для запуску споживчого кредитування (Neofin); створення універсальної платформи для автоматизації бізнес-процесів для малого й середнього бізнесу (RemOnline); інноваційне платіжне рішення для підприємців (Zhabka). Програму Start Path Ukraine реалізують з ініціативи Mastercard за підтримки Міністерства цифрової трансформації України та Національного банку України для розвитку цифрової економіки, фінансової інклюзії та інноваційного клієнтського досвіду [18].

На основі аналітичних матеріалів Офісу ефективного регулювання (BRDO) у травні п. р. триває робота Міжвідомчої робочої групи з питань прискореного перегляду інструментів державного регулювання господарської діяльності (МРГ). Розглянуто 12 ініціатив з оптимізації та переведення інструментів державного регулювання бізнесу в електронну форму. Цьому сприятиме ухвалена Кабінетом Міністрів України постанова, яка визначає порядок пошуку та виявлення потенційних вразливостей в електронних системах, що дасть змогу тестувати електронні сервіси, вчасно виявляти ризики та підвищувати стійкість систем [19].

На основі розглянутого матеріалу, можна зробити рекомендації для України:

- Україні потрібно надалі розвивати електронну систему судочинства, включаючи електронні судові сесії, онлайн-засідання та електронний обмін документами;

- у зв’язку з використанням цифрових технологій важливо забезпечити надійну кібербезпеку для захисту конфіденційної інформації та документів, що обробляються в електронній судовій системі;

- використання цифрових технологій може спростити процедури реєстрації, подання документів та інші процеси для громадян і бізнесу;

- створення мобільних додатків для громадян може полегшити доступ до правової інформації, послуг та ресурсів;

- навчання суддів, адвокатів, працівників судової системи та інших учасників процесу щодо використання цифрових інструментів є важливим елементом успішної цифрової трансформації правової системи;

- важливо враховувати інтереси людей з обмеженими можливостями, забезпечуючи доступність цифрових послуг та ресурсів.

Ці рекомендації спрямовані на те, щоб Україна могла ефективно використовувати цифрові технології для поліпшення правової системи, забезпечення доступу до правосуддя та підвищення прозорості та ефективності у сфері права.

Висновки.

Використання цифрових технологій у судовій системі є важливим напрямком сучасних реформ, які спрямовані на покращення якості надання правосуддя, забезпечення доступності судових послуг та зниження витрат. У цій статті ми розглянули різні аспекти використання цифрових технологій у праві, включаючи:

Електронне ведення документації та судових процесів – впровадження електронного документообігу, автоматизація процесів та електронний доступ до судової інформації сприяє покращенню продуктивності та зменшенню витрат.

Віддалені судові засідання за допомогою використання відеоконференцій та інших засобів зв'язку дозволяє здійснювати судові засідання віддалено, що покращує доступність та зменшує необхідність у фізичній присутності.

Захист конфіденційності та особистих даних є важливим аспектом їх забезпечення під час використання цифрових технологій у судових процесах.

Суди повинні приділяти особливу увагу кібербезпеці та вживати заходів для захисту від кібератак та інших загроз.

Оптимізація робочих процесів, ефективне управління справами та використання електронних систем дозволяють знижувати витрати в судовій системі.

Використання цифрових технологій робить судову систему більш доступною для громадян, забезпечуючи доступ до інформації, віддалене участь та ефективну комунікацію.

Цифровізація права в Україні має потенціал поліпшити доступність та якість правових послуг, забезпечити більшу прозорість і ефективність судової системи, тому вона залишається важливим напрямком реформ для подальшого розвитку правового середовища в країні.

Упровадження нових інструментів цифрової трансформації економіки, окреслених у травні 2023 року, продемонструвало важливість застосування цифрових технологій для подолання вразливостей, спричинених війною та участі бізнес-середовища у відбудові країни.

Загалом, використання цифрових технологій у праві сприяє покращенню судових та юридичних послуг, забезпеченню справедливості та зменшенню адміністративних витрат. Проте важливо приділяти увагу заходам безпеки та захисту даних, а також забезпечувати рівний доступ до судових послуг для всіх громадян. Розвиток цифрових технологій у праві вимагає спільних зусиль судових органів, правозахисних організацій та технологічних партнерів для досягнення кращої судової системи в майбутньому.

Використана література

1. Додаток "Дія": чим корисна програма під час війни. – (Kashtan Media). URL: https://kashtan.media/diia (дата звернення: 18.10.2023).

2. Система Трембіта. URL: https://trembita.gov.ua (дата звернення: 02.10.2023).

3. Приймаченко Д.В., Віхляєв М.Ю. Отримання інформації про діяльність суду та доступ до судових рішень як гарантія ефективності громадського контролю за діяльністю суддів. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 6. URL: http://apnl.dnu. in.ua/6_2022/ 27.pdf (дата звернення: 17.09.2023).

4. e-Curia. CURIA. URL: https://curia.europa.eu/jcms/jcms/P_78957/en (дата звернення: 17.10.2023).

5. Шуневич К., Кіт Х., Змисла М., Нарок Т., Литвинюк К. Звіт за результатами дослідження. Jurfem. URL: https://jurfem.com.ua/wp-content/uploads/2021/11/доступ-до-правосуддя -підчас-ковіду-юрфем.pdf (дата звернення: 17.10.2023).

6. Що потрібно знати про розгляд справи у ZOOM / Сьомий апеляційний адміністративний суд. URL: https://7aac.gov.ua/shho-potribno-znati-pro-rozglyad-spravi-u-zoom (дата звернення: 17.10.2023).

7. Брандмауер – що таке брандмауер (файрвол), як працює ця функція? Переваги – ESET. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer (дата звернення: 17.10.2023).

8. Кіберпростір як новий вимір геополітичного суперництва. URL: https://shron1.chtyvo. org.ua/Dubov_Dmytro/Kiberprostir_iak_novyi_vymir_heopolitychnoho_supernytstva.pdf (дата звернення: 20.10.2023).

9. Центр інноваційних технологій "Програма". CIT PROGRAM. URL: https://cit-program. com/social-engineering (дата звернення: 20.10.2023).

10. COVID-19 and the Courts Contents. URL: https://publications.parliament.uk/pa/ld5801/ ldselect/ldconst/257/25705.htm (дата звернення: 20.10.2023).

11. Apply for court records – civil and family cases. URL: https://www.judiciary.gov.sg/ services/civil-family-court-records (дата звернення: 20.10.2023).

12. Remote Courts: Switzerland. Remote Courts Worldwide. URL: https://remotecourts.org/ country/switzerland.htm (дата звернення: 20.10.2023).

13. Adoption of Virtual Courts in India / SCC Blog. URL: https://www.scconline.com/ blog/ post/2022/01/24/virtual-courts-in-india (дата звернення: 20.10.2023).

14. Central State Electronic Archives of Ukraine. – (Центральний державний електронний архів України). URL: https://tsdea.archives.gov.ua/en (дата звернення: 02.10.2023).

15. Мінцифра взяла участь у засіданні міністрів цифровізації G7. – (Міністерство цифрової трансформації України). URL: https://thedigital.gov.ua/news/mintsifra-vzyala-uchast-u-zasidanni-ministriv-tsifrovizatsii-g7 (дата звернення: 04.10.2023).

16. Україна – одна із 14 країн, які ввійшли до govtech-інкубатору Європейського Союзу Govtech4all. – (Міністерство цифрової трансформації України). URL: https://thedigital.gov.ua/ news/ukraina-odna-iz-14-krain-yaki-vviyshli-do-govtech-inkubatoru-evropeyskogo-soyuzu-govtech4a ll (дата звернення: 04.10.2023).

17. Seeds of Bravery: Європейська інноваційна рада надасть 20 млн. Євро на розвиток інновацій в Україні. – (Міністерство цифрової трансформації України). URL: https://thedigital. gov.ua/news/seeds-of-bravery-evropeyska-innovatsiyna-rada-nadast-20-mln-evro-na-rozvitok-innovat siy-v-ukraini (дата звернення: 04.10.2023).

18. П'ять українських фінтех-стартапів отримають гранти в $10000 у межах програми Start Path Ukraine. – (Міністерство цифрової трансформації України). URL: https://thedigital.gov. ua/news/pyat-ukrainskikh-fintekh-startapiv-otrimayut-granti-v-10-000-u-mezhakh-programi-start-path-ukraine (дата звернення: 04.10.2023).

19. Посилюємо кіберзахист: Уряд ухвалив механізм проведення Bug Bounty. – (Міністерство цифрової трансформації України). URL: https://thedigital.gov.ua/news/posilyuemo-kiberzakhist-uryad-ukhvaliv-mekhanizm-provedennya-bug-bounty (дата звернення: 04.10.2023).

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

Інформаційна і національна безпека

УДК 341.232

КОВАЛЬОВ К.Є., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1243-3973.

ІНФОРМАЦІЙНА БЕЗПЕКА: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Анотація. *У статті висвітлені міжнародно-правові аспекти інформаційної безпеки. Представлені результати аналізу міжнародно-правових норм у сфері інформаційної безпеки, а також зарубіжного досвіду у цій сфері. Підкреслено значущість досвіду окремих зарубіжних країн у сфері забезпечення інформаційної безпеки для України. З огляду на глобальний характер мереж зв'язку зроблено висновок, що інформаційна безпека має бути забезпечена лише за умови ефективної міжнародної взаємодії держав. В ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у країнах Східної Європи. Виділені пріоритетні напрями правового забезпечення інформаційної безпеки України.*

Ключові слова*: інформаційна безпека, кібербезпека, національна безпека, правовий аспект, міжнародна співпраця.*

Summary. *The article highlights the international legal aspects of information security. The results of the analysis of international legal norms in the field of information security, as well as foreign experience in this field, are presented. The importance of the experience of certain foreign countries in the field of information security for Ukraine is emphasized. Given the global nature of communication networks, it is concluded that information security should be ensured only through effective international cooperation between states. During the research, priorities and issues related to information security in Eastern European countries are determined. Prioritized directions for legal support of information security in Ukraine have been identified.*

Keywords: *information security, cyber security, national security, legal aspect, international cooperation.*

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій, тотальна комп'ютеризація, створення глобального інформаційного простору зумовлює послаблення інформаційного суверенітету держави. Глобалізація інформаційного простору не може не впливати на стан інформаційної безпеки будь-якої держави.

Створення інформаційного суспільства зумовило виникнення багатьох новітніх загроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому інформаційну безпеку цілком виправдано розглядають як самостійний елемент національної безпеки [1, с. 284].

Захищаючи свої інформаційні інтереси, кожна держава має дбати про інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України повинна формуватися як складова її національної безпеки та частина соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством [2, с. 68].

В умовах сучасного розвитку інформаційних комунікацій кожна держава виробляє власну стратегію поведінки та політики у сфері інформаційної безпеки.

Так, в країнах, які постійно знаходяться у фокусі інформаційного впливу (Китай, США, Ізраїль, Британія, ФРН та ін.), функціонують найбільш розвинуті системи інформаційної безпеки.

Проблема забезпечення інформаційної безпеки не обійшла й Україну. У зв'язку з подіями, що відбулися 24.02.2022 р., введенням в Україні воєнного стану, з боку російської федерації відбувається інформаційна експансія, упереджене та систематичне висвітлення спотворених фактів та явищ, спрямованих на пропаганду національної ворожнечі, насильства та сепаратизму.

Інформаційно-психологічні операції росії спрямовані на руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави тощо. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіа-заходи відбувається вплив не лише на свідомість громадян України, а й на світову спільноту. Мета цих заходів – забезпечити домінування (утримання медійної переваги) як в українському, так і міжнародному інформаційному просторі.

Результати аналізу наукових публікацій. Дослідженням сучасних загроз інформаційної безпеки займалися багато вітчизняних дослідників, серед яких можна виділити роботи Н.М. П.Д. Біленчука [3], О.Р. Вайцеховської [4], М.М. Присяжнюка [5], В.А. Ліпкана [3], М.О. Сенченка [6], О.Л. Гурковського, О.М. Яхно, О.В. Левченко, В.М. Бебика, Г.Г. Почепцова, І.С. Чижа, В.М. Скалацького, О.В. Сосніна, В.М. Абакумова, Є.О. Кирильчука та ін.

Проблематика наукових досліджень не втрачає своєї актуальності, оскільки загрози інформаційній безпеці держави в сучасних умовах розвитку інформаційного суспільства є динамічними та постійно змінюються.

Метою статті є визначення міжнародно-правових аспектів забезпечення інформаційної безпеки держави в контексті удосконалення законодавства у цій сфері.

Виклад основного матеріалу. Переважна більшість дослідників вважає, що під інформаційною безпекою слід розуміти стан захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства та держави, від внутрішніх та зовнішніх загроз.

З точки зору П.Д. Біленчука, безпека в інформаційній сфері передбачає забезпечення інформаційного суверенітету; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження сучасних технологій у цій сфері, наповнення інформаційного простору достовірною інформацією; забезпечення конституційного права громадян на свободу слова, доступу до інформації, недопущення протиправного втручання органів державної влади у діяльність засобів масової інформації; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери держави [3, с. 54-55].

Про інформаційний суверенітет також пише і О.Р. Вайцеховська [4, с. 243]. Осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки має велике значення як для окремого суспільства, так і міжнародного співтовариства в цілому.

Інформаційна безпека є не лише складовою національної безпеки, а й невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки,

адже всі типи взаємовідносин між суб'єктами інформаційного суспільства ґрунтуються на споживанні й обміні інформацією. З цього приводу В.А. Ліпкан зазначає, що національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу [6].

Український учений М. Сенченко справедливо відзначає, що Україні для ефективного протистояння інформаційній війні з боку росії потрібно мати хоча б: 1) ефективну систему ведення інформаційної війни; 2) ефективну правову концепцію інформаційної війни; 3) стратегію ведення інформаційної війни [7]. Лише та держава може розраховувати на лідерство в економічній, військово-політичній чи інших сферах, мати стратегічну й тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби [5].

Інформаційна безпека України передбачає головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені. Реалізація такого завдання зумовлює потребу створення системи протидії будь-якій інформаційній загрозі та захисту власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Застосування росією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України росія використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [8].

Механізми захисту інформаційної безпеки України можна розділити на два рівні – законодавчий та адміністративний. Найважливіше на законодавчому рівні – створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, що може спричинити послаблення інформаційної безпеки.

Адміністративний механізм забезпечення інформаційної безпеки охоплює установи, діяльність яких спрямована на формування та реалізацію інформаційної безпеки. Головне на адміністративному рівні – сформувати програму заходів в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи поточний стан справ.

Сьогодні запорукою створення надійної системи забезпечення охорони інформаційної безпеки може бути тільки зміцнення самої української держави та державних органів, відповідальних за її забезпечення. Реалізація цього завдання зумовлює масштабні завдання, пов'язані з виробленням системи забезпечення інформаційної безпеки, пошуком принципово нових, нестандартних форм організації, взаємодії, координації діяльності, удосконалення всіх засобів, спрямованих на забезпечення процесу управління ризиками та загрозами [9].

Серед основних напрямів забезпечення інформаційної безпеки виділяють: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом

впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки [10].

Інформаційна безпека як поняття розглядається у декількох ракурсах.

У найзагальнішому вигляді – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави [11, с. 64].

Оскільки суспільні відносини, що виникають у зв'язку із забезпеченням інформаційної безпеки регулюються нормами права, є необхідним проаналізувати основні принципи і норми, спрямовані на забезпечення інформаційної безпеки.

Український законодавець за роки незалежності сформував потужну правову базу у сфері національної безпеки, основою для якої є чинна Конституція України. Так, у ч. 1 ст. 3 Конституції України сформульовано концептуальні засади забезпечення безпеки людини: "людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визначаються в Україні найвищою цінністю". У ч. 1 ст. 17 Конституції України передбачено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [12].

Загалом, у Конституції України містяться правові норми, пов'язані із забезпеченням інформаційної безпеки, які становлять основу законодавства у цій сфері і мають вищу юридичну силу. У цих нормах закріплено право на інформацію, передбачена охорона відомостей, що становлять державну таємницю.

Конституційні норми, пов'язані із забезпеченням інформаційної безпеки, вказують на те, що це питання є настільки багатоаспектним та багатогранним, що кожна з зазначених правових норм може стати окремими темами наукових досліджень.

Правові засади національної безпеки України також регламентуються Законом України "Про національну безпеку України" від 21 червня 2018 р. [13].

У різних державах розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного простору. Застосовуючи різні засоби, країни-лідери достатньо ефективно здійснюють національну політику інформаційної безпеки.

Відповідно до національної специфіки й унікальної ролі нашої держави в сучасній геополітиці, необхідно постійно аналізувати та застосовувати закордонний досвід.

Наразі йдуть активні процеси формування міжнародного досвіду у сфері забезпечення інформаційної безпеки в рамках діяльності таких міжнародних організацій, як ООН, Ради Європи, Європейського Союзу та інших.

Основні принципи законодавчого регулювання суспільних відносин у сфері міжнародної інформаційної безпеки сформульовані в основних міжнародних документах, їх потрібно постійно вивчати та аналізувати, а головне робити висновки та постійно удосконалювати законодавство України.

Враховуючи масштаби глобального інформаційного виклику, неможливість вирішення зазначених проблем зусиллями однієї або навіть декількох держав, слід усвідомити необхідність розвитку міждержавного співробітництва в сфері забезпечення міжнародної інформаційної безпеки в межах Організації Об'єднаних Націй, здатної комплексно вирішувати будь-які політичні проблеми, при найширшому представництві і

максимально враховуючи інтереси всієї світової спільноти. Ідея забезпечення міжнародної інформаційної безпеки вперше отримала практичну реалізацію в Резолюції Генеральної Асамблеї ООН A/RES/53/70 "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки" від 4 грудня 1998 р. Цей документ започаткував спільне обговорення питань створення абсолютно нового міжнародно-правового режиму, структурним елементом якого в перспективі стали інформація, інформаційна технологія і методи її використання [14].

Отже важливу участь у безпекових заходах традиційно бере ООН. Її діяльність у сфері інформаційної безпеки спрямована на розробку міжнародно-правової бази та вироблення документів для протидії протиправному використанню науково-технологічного прогресу терористичними угрупованнями та організованою злочинністю. Проблема інформаційної безпеки в контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема, ЮНЕСКО та МСЕ, враховуючи гуманітарні та технічні програми та проекти організацій [15].

Невизначеність на глобальному рівні та відсутність єдиних підходів змушує керівництво держав формувати політику кібербезпеки на національному рівні.

Серед міжнародних організацій, основною метою яких є саме безпека, НАТО найбільш ефективно модернізувала політику щодо інформаційної безпеки. Організація заснувала центри у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту представників країн-членів і країн-партнерів. Наразі Центр кібербезпеки НАТО функціонує в Естонії, він не є підрозділом військового командування або структури збройних сил НАТО, а персонал та фінансування забезпечуються державами-спонсорами та державами-учасниками [16].

Активну політику щодо забезпечення інформаційної безпеки проводить і Європейський Союз. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки стало одним із пріоритетних напрямів діяльності ЄС.

У 2001 р. Європейською Комісією було представлено перший документ під назвою "Мережева та інформаційна безпека: європейський політичний підхід", в якому була представлена концепція вирішення проблеми інформаційної безпеки. У документі використовується термін "мережева та інформаційна безпека", який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [17].

Усвідомлюючи той факт, що ефективність забезпечення інформаційної безпеки в європейському кіберпросторі також залежить від розвитку співпраці держав у рамках міжнародних органів у 2013 р. в структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю.

До пріоритетних напрямів діяльності Центру відноситься розслідування шахрайства через Інтернет-мережі, а також розслідування злочинів, що посягають на безпеку критично важливої інфраструктури та інформаційних систем ЄС [18].

З метою протидії інформаційним загрозам, таким як кібертероризм та кіберзлочинність, Україна враховує стандарти ЄС та НАТО, постійно співпрацює та переймає досвід багатьох країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних стандартів.

Розуміючи актуальність проблеми забезпечення інформаційної безпеки як складової системи національної безпеки, більшість держав світу почали здійснювати внутрішньодержавні комплексні заходи з забезпечення безпеки в кіберпросторі.

Європейські країни активно модернізують власні сектори безпеки у кіберпросторі у відповідності до викликів сучасності.

Цей процес відбувається шляхом:

- впорядкування нормативної бази, що має забезпечити цілісність державної політики в даній сфері;
- вироблення європейських керівних принципів щодо забезпечення інформаційної безпеки;
- збільшення чисельності підрозділів, що забезпечують інформаційну безпеку;
- посилення контролю за національним інформаційним простором;
- зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС тощо.

Ці заходи пов’язані, перш за все, з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі.

На сьогодні кібербезпека є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті такими державами як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Великобританія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія тощо. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі.

Україна схвалила Стратегію кібербезпеки України [21]. Цей документ визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики інформаційної безпеки, яка відповідатиме світовому рівню.

На основі вивчення міжнародних правових актів, що стосуються протидії новим викликам та загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, очевидним є висновок про необхідність подальшої імплементації положень міжнародних правових актів та гармонізації з законодавствами іноземних держав.

Заходи щодо забезпечення інформаційної безпеки України повинні здійснюватися шляхом: забезпечення інформаційного суверенітету України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України тощо [21].

Отже, в умовах сучасного розвитку інформаційного суспільства, захист національного інформаційного простору та забезпечення інформаційної безпеки вже стали пріоритетними стратегічними завданнями багатьох держав світу.

Інформаційна безпека визнається невід'ємним елементом системи національної безпеки. При цьому, інформаційна безпека як складова національної безпеки держави може розглядатися як її самостійна частина. Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у зазначеній сфері. Питання забезпечення інформаційної безпеки є вкрай важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України. Зважаючи на те, що стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, то завданням для української влади повинен стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки [1].

На нашу думку, використання взаємодоповнюючих та скоординованих заходів на регіональному та міжнародному рівнях дозволить успішно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері, що можуть порушити доступність, цілісність і конфіденційність інформації, що зберігається або передається за допомогою мережі або інформаційної системи.

Інтенсивний розвиток інформаційних технологій призводить до появи нових загроз національній безпеці, а тому використання скоординованих та взаємодоповнюючих заходів на двосторонньому, регіональному та міжнародному рівнях дозволить адекватно протистояти сучасним викликам та загрозам безпеці в інформаційній сфері.

Інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії. У зв'язку з цим необхідно посилити взаємодію України із закордонними країнами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки. Аналіз зарубіжного законодавства, що регулює інформаційну сферу, дозволяє стверджувати, що в сфері правового регулювання права на інформацію, доступу до інформації, ЗМІ, а також обмеження свободи інформації відбулися істотні зміни. Аналіз міжнародних і зарубіжних правових актів в інформаційній сфері свідчить про те, що є значний і різноманітний досвід правового регулювання як на міжнародному, так і на національному рівнях. Зарубіжні державні органи відіграють вирішальну роль в координації дій суб'єктів у сфері забезпечення інформаційної безпеки. Пріоритетним напрямком стає вдосконалення законодавства, що встановлює відповідальність за правопорушення, розробка та законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки [10].

Висновки.

Міжнародний характер загроз інформаційної безпеки зумовлює необхідність вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва в рамках міжнародних організацій у цій сфері. У зв'язку з цим необхідно посилити взаємодію України із зарубіжними партнерами, міжурядовими організаціями з питань правового забезпечення інформаційної безпеки.

Провідні держави в сучасних міжнародних відносинах використовують інформацію як стратегічний ресурс для реалізації своїх геополітичних завдань. Тому інформаційна безпека сьогодні є одним із пріоритетних напрямів національної безпеки України. Могутність країни на зовнішньополітичній арені визначається її можливостями впливати на міжнародне інформаційне поле, а отже, і на інформаційне середовище інших держав.

З метою протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність,

сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання [9].

Сучасні інформаційні протистояння засвідчили, що інформаційний простір України потребує додаткового захисту від зовнішніх негативних інформаційно-психологічних впливів. Таким чином, національні інтереси України у сфері інформаційної безпеки повинні полягати у розвитку сучасних телекомунікаційних технологій, у захисті державних інформаційних ресурсів від несанкціонованого доступу.

Саме тому дослідження багатоаспектної проблематики інформаційної безпеки держави, соціуму і людини є сьогодні надзвичайно актуальним і важливим завданням, що постає перед науковою спільнотою нашої країни.

З урахуванням викладеного, можна виділити такі пріоритетні напрями правового забезпечення інформаційної безпеки України:

- удосконалення законодавства України у сфері забезпечення інформаційної безпеки з метою створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі;
- ухвалення нормативно-правових актів, що забезпечують реалізацію концепції електронного уряду, у тому числі надання державних послуг із використанням інформаційно-комунікаційних технологій, розвиток довіреного електронного документообігу на основі використання загальнодоступних інформаційно-телекомунікаційних мереж;
- законодавче закріплення переліку правопорушень та видів відповідальності в сфері інформаційної безпеки;
- вироблення спільної стратегії інформаційної безпеки і розвиток міждержавного співробітництва у зазначеній сфері.

Використана література

1. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н.Каразіна*. *Серія "ПРАВО"*. 2020. № 29. С. 281-288.

2. Бондар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. № 1. С. 68-75.

3. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

4. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації: дис. …докт. юрид. наук. Харків, 2020. 472 с.

5. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. *Вісник національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 32-46.

6. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ: КНТ, 2006. 280 с.

7. Сенченко М.О. Запорука національної безпеки в умовах інформаційної війни. *Вісник книжкової палати*. 2014. № 6. С. 3-9.

8. Доктрина інформаційної безпеки України: Указ Президента України: від 25.02.17 р. № 47/2017. URL: //www.president.gov.ua

9. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. URL: http://journals.maup.com.ua/index.php/political/article/view/2295/2778.

10. Грабар Н.С. Зарубіжний досвід правового регулювання забезпечення інформаційної безпеки. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12388/1/stGrabar.pdf

11. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

12. Конституція України: Закон України. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр

13. Про національну безпеку України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.

14. United Nations. A/RES/53/70 "Developments in the fi eld of information and telecommunications in the context of international security" Resolution Adopted By The General Assembly. 4 January 1999 URL: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_53_70.pdf

15. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки. URL: http://journals.iir.kiev.ua/index. php/pol_n/article/viewFile/3468/3140

16. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurity intelligence.com/natocooperative-cyber-defence-centre-ccdcoe-395.html

17. Network and information security: proposal for a european policy approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN

18. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу. URL: http://p.dw.com/p/17HRW

21. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon5.rada.gov.ua/laws/show/96/2016

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

УДК 342.951

АЛЕКСЕЄВА О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6629-3606.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *У статті висвітлено питання правового забезпечення кібербезпеки об'єктів критичної інфраструктури. Розглядається понятійний апарат у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури. Міститься аналіз чинного законодавства України у сфері забезпечення кібербезпеки, а також зарубіжного досвіду у цій сфері. Аналізується проект Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" в контексті оптимізації законодавства України у сфері забезпечення кібербезпеки. Визначено доцільність застосування комплексного підходу до забезпечення кібербезпеки об'єктів інформаційної критичної інфраструктури. Внесені пропозиції щодо удосконалення системи забезпечення кібербезпеки об'єктів критичної інфраструктури.*

Ключові слова: *правове забезпечення, об'єкти критичної інфраструктури, об'єкти інформаційної критичної інфраструктури, кібербезпека.*

Summary. *The article highlights the issue of legal support of cyber security of critical infrastructure objects. The conceptual apparatus in this area is considered. It contains an analysis of the current legislation of Ukraine in the field of cyber security. The project of the Law of Ukraine "On Amendments to Some Laws of Ukraine Regarding Urgent Measures to Strengthen Cybersecurity Capacities of State Information Resources and Critical Information Infrastructure Objects" is analyzed in the context of optimizing Ukrainian legislation in the field of cyber security. The expediency of applying a comprehensive approach to ensuring cyber security of critical information infrastructure objects has been determined. A proposal has been introduced to improve the legislation of Ukraine in the field of cybersecurity.*

Keywords: *legal support, critical infrastructure, critical infrastructure objects, critical information infrastructure objects, cyber security.*

Постановка проблеми. З 14 січня 2022 року, коли відбулася кібератака росії на низку об'єктів критичної інфраструктури, Україна перебуває в стані першої в історії кібервійни з рф [1, с. 9]. Повномасштабне вторгнення військ рф на територію України, що триває із 24 лютого 2022 року, супроводжується численними актами агресії у кіберпросторі, який визнано одним з можливих театрів воєнних дій. Відповідно до оприлюднених Державною службою спеціального зв'язку та захисту інформації України даних, від 15 лютого Україна зазнала понад 3000 DDoS-атак; постійно розповсюджується шкідливе програмне забезпечення, здійснюються фішингові розсилки та інші прояви війни у кіберпросторі [2]. У зв'язку зі збільшенням кількості та масштабу кібернападів як одного із проявів агресії рф проти України, що спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України, а також на об'єкти критичної інформаційної інфраструктури, набуває необхідність вдосконалення нормативного

забезпечення у сфері захисту об'єктів критичної інформаційної інфраструктури. Проблемою є фактична відсутність дієвої узгодженої політики у сфері захисту таких об'єктів, що зумовлюється як відсутністю системного підходу на національному рівні, так і законодавчою невизначеністю форм взаємодії державних органів між собою. Незважаючи на низку законів та інших нормативно-правових актів, що визначають повноваження й компетенцію державних органів у цій сфері, в Україні досі бракує системного підходу до управління комплексом таких систем та об'єктів [3, с. 58]. Відсутні й будь-які узгоджені прояви здійснення державно-приватного партнерства у сфері взаємодії із забезпечення кібербезпеки, що є одним з пріоритетних напрямів з огляду на світовий досвід [3, с.58].

Результати аналізу наукових публікацій. Ще до великомасштабних атак в Україні наукові дослідження у сфері захисту критичних інфраструктур від кібератак проводились такими вченими, як П.Д. Рогов [4], І.П. Сініцин, П.П. Ігнатенко, О.О. Слабоспицька, О.В. Артеменко [5], Н.О. Ткачук [6], І. Субач [7] та ін.

Закордонний досвід забезпечення захисту об'єктів критичних інфраструктур був предметом поглиблених досліджень таких науковців, як Батюк О.В. [8], Єрменчук О.П. [9], Гора І.В. [8], Кондратов С.І., Суходоля О.М. [3], Пядишев В.Г. [10] та ін.

Однак, не зважаючи на наявність значної кількості наукових праць щодо цієї теми, варто зазначити, що вони не вичерпують усіх аспектів проблеми правового забезпечення кіберзахисту об'єктів критичної інфраструктури. Крім того, залишаються не достатньо дослідженими результати зарубіжних наукових досліджень забезпечення кібербезпеки критичної інфраструктури. Водночас, євроатлантичні прагнення України однозначно передбачають надалі зближення нормативно-правової бази, програмних та інших технічних засобів та методів протидії кібератакам на критичні інфраструктури, а також забезпечення стійкості останніх [10, с. 230]. Проблематика забезпечення кібербезпеки критичної інфраструктури загострюються в умовах воєнного стану, що зумовлює актуальність цієї статті.

Метою статті є визначення шляхів та удосконалення правового забезпечення кібербезпеки об'єктів критичної інфраструктури на основі аналізу законодавства окремих зарубіжних країн а також нормативно-правової бази з питань захисту об'єктів критичної інфраструктури.

Виклад основного матеріалу. Сьогодні тематика кіберзахисту об'єктів інформаційної критичної інфраструктури дедалі частіше обговорюється під час наукових конференцій, семінарів, міжнародних форумів, присвячених питанням розвитку та захисту критичної інфраструктури. Термін "забезпечення кібербезпеки об'єктів критичної інфраструктури" дедалі частіше вживають журналісти в засобах масової інформації. Помітним кроком у забезпеченні кібербезпеки стало створення в Україні Національного координаційного центру кібербезпеки у 2016 році.

Проблематика критичної інфраструктури пов'язана із бурхливим розвитком нових підходів до забезпечення національної безпеки в розвинених країнах світу, що спричинено швидкими змінами, які відбуваються у безпековому середовищі у глобальному, регіональному та національному вимірах. Зрозуміло, що це знаходить відповідне відображення у розвитку національних законодавств, у т.ч. в термінологічному забезпеченні діяльності державних органів тієї чи тієї країни [3, с. 32].

Значне місце цьому безпековому напрямку відведене в нормах чинного законодавства України, де він визнаний пріоритетним у контексті політики національної безпеки. Нормативно-правову базу в цій сфері утворюють: Закон України "Про основи забезпечення кібербезпеки України"; Указ Президента України "Про затвердження

Стратегії кібербезпеки України" від 26.08.21 р. № 447; Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.19 р. № 518; Постанова Кабінету Міністрів України "Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимогу щодо захисту якої встановлено законом" від 11.11.20 р. № 11; Постанова Кабінету Міністрів України "Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури від 9.10.20 р. № 1109; Вимоги до функціонування системи кіберзахисту у банківській системі України (постанова Правління Національного банку України від 12.08.22 р. № 178). Також можна стверджувати, що сьогодні у процесі протидії кібератакам в умовах воєнного стану напрацьовується безцінний новий досвід.

В Україні під критичною інфраструктурою розуміється сукупність об'єктів такої інфраструктури до кола яких віднесено: об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [11]. Відповідно до Закону України "Про критичну інфраструктуру" об'єкти критичної інфраструктури – це підприємства, установи й організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике 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, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. До критичної інфраструктури належать й особливо небезпечні виробництва, аварії на яких викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями), також можуть обернутися катастрофічними для певних територій і їх населення наслідками [12].

Термін "критична інфраструктура" з'явився порівняно недавно і ввійшов до обігу ділового, наукового та дипломатичного спілкування із середини 1990-х рр. і спершу був пов'язаний з інформаційною інфраструктурою [13, с. 151]. Критично важливі об'єкти інфраструктури діють як система життєзабезпечення повсякденного існування людей, співтовариство яких підтримується доволі комплексною і складною мережею інфраструктурних систем. Виведення з ладу, серйозні і дрібні збої, постійні недоліки в роботі та функціонуванні певної інфраструктури чи її елементів можуть створювати загрозливі, а іноді й критичні для нормальної життєдіяльності ситуації [8, с. 134].

Цілісна концепція критичної інфраструктури вперше була сформована та розроблена у США і саме цю країну вважають піонером у розробленні й запровадженні концепції критичної інфраструктури та її захисту, оскільки саме у 1996 р. уперше дано визначення терміну "критична інфраструктура", до якого вносилися зміни й він набув сучасного розуміння [13, с. 4; 14]. Натомість посилений розвиток відповідного безпекового напряму розпочався як наслідок уроків, винесених із терактів 11 вересня 2001 р., коли було усвідомлено рівень загроз міжнародного тероризму [3, с. 31].

Під критичною інфраструктурою законодавство США розуміє "системи та засоби, фізичні чи віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів підривало би національну безпеку, національну економіку, загрожувало би здоров'ю чи безпеці населення, чи мало би результатом будь-яку комбінацію із переліченого" [15].

Директива Президента США (PPD-21) визначає безпеку “як зменшення ризиків для критичної інфраструктури шляхом вжиття фізичних заходів чи захисних кіберзаходів стосовно вторгнень, нападів або дії природних лих чи техногенних аварій” [16].

Відповідно до директиви Президента США № 63 “Стратегія спільних зусиль адміністрації США і приватного сектору у сфері захисту критичної інфраструктури” головне завдання досліджень у цій сфері полягає у виявленні ключових об’єктів (або їх сукупності), вплив на які може спричинити найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці прогнозованих наслідків подібного впливу й розробці механізмів зниження таких ризиків [17]. США сьогодні є лідером у запровадженні інноваційних підходів, мають розвинуту, добре розгалужену національну державну систему забезпечення безпеки об’єктів критичної інфраструктури, яка спрямована на посилення безпеки та стійкості критичної інфраструктури стосовно фізичних і кіберзагроз. З цією метою Федеральний уряд цієї країни співпрацює із власниками та операторами відповідних об’єктів і систем, державними органами всіх рівнів, місцевими органами влади з тим, щоб вживати активних заходів з управління ризиками, враховуючи при цьому всі види загроз, реалізація яких може призвести до тяжких наслідків для національної безпеки, стабільності економіки, здоров’я та безпеки населення чи будь-якої комбінації з переліченого. При цьому зусилля спрямовуються на зменшення уразливостей, мінімізацію наслідків, ідентифікацію та ліквідацію загроз, прискорення реагування та застосування відновлювальних заходів, пов’язаних з такою інфраструктурою. Уряд ураховує міжнародний контекст проблем, пов’язаних із безпекою та стійкістю такої інфраструктури, та взаємодіє з міжнародними партнерами у цій сфері [3, с. 34]. Крім цього, плідною і ефективною визнається діяльність кібервійськ США, які проводять операції в кіберпросторі.

У США серед актів, що становлять нормативно-правову основу у цій сфері, слід виокремити: Національну стратегію внутрішньої безпеки (жовтень 2007 р.); Національну стратегію фізичного захисту критичної інфраструктури та ключових активів (лютий 2003 р.); Національну стратегію захисту кіберпростору (лютий 2003 р.); Закон про внутрішню безпеку (листопад 2002 р.).

Заслуговує на увагу прийнятий у 2002 р. в США Акт щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act (“CIIA”) [5], в якому регулювалися положення стосовно обміну інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов’язаних із терористичними загрозами [18]. Цей Акт запровадив термін “інформація щодо критичної інфраструктури” і розуміння інформації, яка зазвичай не перебуває в полі зору суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем [8, с. 134].

Нині в більшості розвинених країн широко використовують досвід і напрацювання з питань кіберзахисту критичної інфраструктури, які отримали й продовжують отримувати фахівці з США.

Водночас розуміння критичної інфраструктури та її об’єктів у окремих європейських країнах за спільних до їх визначення підходів може дещо різнитись, що зумовлене національними традиціями, розуміннями національних цінностей, безпеки країни, добробуту населення тощо [8, с. 135].

Ще у 2004 р. на рівні ЄС та Європейської Комісії розпочали створення проекту захисту критичної інфраструктури “European Programme for Critical Infrastructure Protection” (“EPCIP”), в рамках якого важливу увагу приділено захисту від терористичних загроз. Тоді під критичною інфраструктурою розуміли “обладнання,

служби й інформаційні системи, життєво важливі для держави, знищення чи відмова від яких призведе до послаблення суспільства, національного господарства, системи охорони здоров'я, безпеки ефективного функціонування державного устрою" [8, с. 135].

У законодавстві Євросоюзу з питань захисту від кібератак на себе звертає увагу Директива (ЄС) 2016/1148 Європейського Парламенту та Ради "Про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем на території Союзу" від 6 липня 2016 р. [19], яка приймалася з урахуванням 75-ти визначальних факторів. Ця Директива встановлює заходи, спрямовані на досягнення високого рівня безпеки мережевих та інформаційних систем у Євросоюзі [10, с. 232]. З цією метою Директива: (a) встановлює зобов'язання для всіх держав-членів прийняти національну стратегію безпеки мереж та інформаційних систем; (b) створює групу співробітництва для підтримки та сприяння стратегічній співпраці та обміну інформацією між державами-членами, а також для розвитку довіри між ними; (c) створює мережу груп реагування на інциденти комп'ютерної безпеки ("мережа CSIRT"), щоб сприяти розвитку довіри між державами-членами та сприяти швидкому та ефективному оперативному співробітництву; (d) встановлює вимоги безпеки та сповіщення для операторів основних послуг та постачальників цифрових послуг; (e) встановлює зобов'язання для держав-членів щодо призначення національних компетентних органів, єдиних контактних осіб та CSIRT із завданнями, пов'язаними з безпекою мереж та інформаційних систем [19; 10, с. 232]. Для посилення протидії проявам кіберзлочинності у 2013 році в структурі Європолу був створений Європейський центр боротьби з кіберзлочинністю [8; 10].

У червні 2023 року депутати Європарламенту ухвалили нові правила обміну електронними доказами між правоохоронними органами з метою підвищення ефективності транскордонних розслідувань.

За висновками зарубіжних експертів [20; 21], 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 [22]. Вбачається, що складовою цієї системи є й чітко визначені правові засади захисту об'єктів критичної інфраструктури від кіберзагроз.

Попри наявність загальновизнаних принципів та підходів щодо забезпечення безпеки об'єктів інформаційної інфраструктури кожна національна система є по суті унікальною і неминуче несе на собі відбиток національної специфіки, тому слід уникати механічного копіювання зарубіжного досвіду на українських теренах [3, с. 54]. Україна перебуває на початковому етапі створення державної системи забезпечення безпеки таких об'єктів, тому при розгляді зарубіжного досвіду в цій слід пам'ятати, що механічне перенесення навіть передового досвіду без належного урахування специфіки та реалій українського сьогодення може лише підірвати зусилля на цьому напрямі, скомпрометувати його та в такий спосіб суттєво затримати його розвиток у нашій країні [3, с. 32].

В Україні ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, в основу якої покладено методологічний підхід аналізу ризиків, які обумовлювалися надійністю функціонування елементів, складових, об'єктів тощо. Іншими словами, ризик виникнення надзвичайної ситуації визначався вірогідністю відмов природнього характеру, аварій, інших

надзвичайних подій (ймовірність виникнення та розвитку подій внаслідок умисного пошкодження елементів не враховувався та не розглядався взагалі) [23, с. 92].

Проте, комплексне забезпечення об'єктів критичної інфраструктури, у т.ч. об'єктів інформаційної інфраструктури, передбачає інший підхід, в основу якого має бути покладено: удосконалення механізмів та процедури взаємодії та обміну інформацією на всіх рівнях управління, функціонування на основі ризик-орієнтованих підходів, чіткого розподілу повноважень і відповідальності щодо критичної інфраструктури (для цього зазвичай визначають відповідальний державний орган або органи); розвиток взаємодії з іншими суб'єктами системи з метою ефективного залучення населення, суспільства, бізнесу та державних установ і організацій до розв'язання проблем забезпечення безпеки та стійкості критичної інфраструктури; налагодження ефективного обміну інформацією між усіма суб'єктами процесу забезпечення безпеки та стійкості критичної інфраструктури; забезпечення виконання функцій інтегрування та аналізу даних для підтримки процесів планування та прийняття рішень стосовно критичної інфраструктури; проведення підготовки кадрів і населення для забезпечення безпеки та стійкості критичної інфраструктури; постійна перевірка готовності сил і засобів, планів і процедур взаємодії та обміну інформацією під час регулярних навчань на всіх рівнях управління [3, с. 54-55].

Відповідно до положень Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.21 р. № 447, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Серед передумов та чинників, що формують загрози кібербезпеці України, Стратегія кібербезпеки України називає: недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації; відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом; відсутність механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави; невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі; незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; недостатню захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом [24].

Беручи до уваги вищеназвані чинники, усунення яких є необхідним для зменшення загроз кібербезпеці України, а також нагальну потребу у посиленні спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, було розроблено проект Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" (реєстр. №8087 від 29.09.22 р.), впровадження якого, на думку розробників, створить належну правову основу для стримування збройної агресії рф у кіберпросторі та надання відсічі агресору. Цим проектом, зокрема, передбачено: створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-

комунікаційних систем; визначення завдань, функцій та повноважень суб'єктів національної системи реагування: Національного координаційного центру з кібербезпеки, галузевих та регіональних команд реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, уповноважених представників Національної поліції України і Служби безпеки України, Об'єднаної групи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, приватних команд реагування; створення та забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки: закріплення обов'язку власників та розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, повідомляти про всі інциденти кібербезпеки, кібератаки; закріплення обов'язку операторів критичної інфраструктури повідомляти про всі значні інциденти кібербезпеки, кібератаки щодо об'єктів критичної інформаційної інфраструктури; впровадження системи державного контролю за станом технічного захисту інформації та кіберзахисту. За результатами громадських слухань щодо цього законопроекту підприємці, юристи, експерти дійшли згоди, що він потребує суттєвого серйозного доопрацювання через невідповідність сучасним європейським стандартам у сфері кібербезпеки та створення загроз для бізнесу [26].

Узгодженню різних підходів сприятиме обговорення цього проекту з громадськістю та широким колом науковців та практичних фахівців, а його реалізація допоможе якісному удосконаленню законодавства України у сфері кібербезпеки та захисту інформації.

Висновки.

У багатьох розвинутих країнах світу забезпечення кібербезпеки об'єктів критичної інфраструктури визнано пріоритетним напрямом політики національної безпеки, в рамках якого активно розбудовуються національні системи із забезпечення кіберзахисту (безпеки) таких об'єктів, ухвалюються законодавчі акти для регламентації діяльності учасників системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення тощо [3, с. 7].

На підставі аналізу законодавства окремих зарубіжних країн, а також нормативно-правової бази з питань захисту об'єктів критичної інфраструктури, можна вважати, що система забезпечення кібербезпеки об'єктів критичної інфраструктури нашої держави потребує:

створення та забезпечення функціонування єдиної національної системи реагування на інциденти кібербезпеки, кібератаки, кібертероризм;

створення та забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кібертероризм;

удосконалення державно-приватної взаємодії у сфері кібербезпеки;

законодавчого визначення повноважень уповноваженого органу з питань захисту критичної інфраструктури України з науково-технічного забезпечення процедур захисту об'єктів інформаційної критичної інфраструктури (у т.ч. реалізації функцій з координації, здійснення контролю та нагляду, експертної оцінки, організації заходів компенсаційного та превентивного характеру тощо);

створення науково-дослідних установ, які будуть забезпечувати наукове супроводження функціонування єдиної національної системи реагування на кіберінциденти;

розробки та впровадження необхідного методичного та нормативного забезпечення аналізу та прогнозування наслідків кібердиверсії або кібертероризму на об'єктах інформаційної критичної інфраструктури [23, с. 92].

Використана література

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа "Інститут інформації, безпеки і права НАПрН України"; Національна бібліотека України ім. В.І.Вернадського. Київ, 2023. № 6. 153 с. URL: https://ippi.org.ua/sites/default/files/2023-6.pdf (дата звернення: 14.10.2023).

2. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: пояснювальна записка до проєкту закону України. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490885 (дата звернення: 14.10.2023 р.).

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Бобро Д.Г., Іванюта С. П., Кондратов С.І., Суходоля О.М. / за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 224 с. URL:https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

4. Рогов П.Д. Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http:// nbuv.gov.ua/UJRN/Znpcvsd_2017 _1_13 (дата звернення: 06.01.2023).

5. Сініцин І.П., Ігнатенко П.П., Слабоспицька О.О., Артеменко О. В. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. *Проблеми програмування*. 2017. № 3. С. 128-148. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1 (дата звернення: 06.01.2023).

6. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *Інформація і право.* № 1(24)/2018. С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf (дата звернення: 06.01.2023).

7. Субач І., Микитюк А., Кубрак В. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об'єктів критичної інфраструктури. *Information Technology and Security*. 2019. Vol. 7, Iss. 2 (13). Pp. 208-215.

8. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. Вип. 1 (11). С. 132-139. URL: https://dspace. lvduvs.edu.ua/bitstream/1234567890/3709/1/18-.pdf (дата звернення: 14.10.2023).

9. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: ДДУ ВС, 2018. 180 с.

10. Пядишев В.Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Південноукраїнський правничий часопис.* 2022. № 4. Ч. 3. С. 229-234. URL: http://www.sulj. oduvs.od.ua/archive/2022/4/part_3/38.pdf (дата звернення: 14.10.2023).

11. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon. rada.gov.ua/laws/show/1882-20#n80 (дата звернення: 14.10.2023 р.).

12. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act) ACT OF 2001. URL: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW107publ56.htm (дата звернення: 14.10.2023).

13. Курбанов Я.Л. Забезпечення природно-техногенної безпеки в Україні і проблема визначення поняття "критична інфраструктура". *Південноукраїнський правничий часопис.* 2016. № 2. С. 150-154.

14. On July 15, 1996, President Clinton signed Executive Order 13010 establishing President's Commission on Critical Infrastructure Protection (PCCIP). Critical Infrastructure Protection. Federal Register. July 17, 1996. Vol. 61. No. 138.

15. USA PATRIOT ACT (2001) defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". URL: https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

16. Presidential Policy Directive 21 (PPD-21). Critical Infrastructure Security and Resilience. (2013, February 12). URL: https://obamawhitehouse.archives.gov/the-press-office/2013/ 02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата звернення: 14.10.2023).

17. Executive Order. 13010. Critical Infrastructure Protection. Federal Register. Vol. 61, № 138. July 17. 1996. P. 3747-3750.

18. Critical Infrastructure Information Act of 2002 ("CIIA"). URL: https:// www.fas.org/sgp/crs/RL31762.pdf

19. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O J.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 06.01.2023).

20. Keating C, Rogers, R., Dryer D., Sousa-Poza A., Safford R., Peterson W., Rabadi G. System of Systems Engineering. *Engineering Management Journal*. 2003. Vol. 15. № 3.

21. Jackson, M. Systems Methodology for the Management Sciences. New York. Plenum, 1991. 298 p.

22. Congressional Research Service Report for Congress. Critical Infrastructures: Background, Policy and Implementation. 2002. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата звернення: 19.06.2023).

23. 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. URL: https://ippi.org.ua/sites/default/files/12_18.pdf (дата звернення: 19.09.2023).

24. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 19.09.2023).

25. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт закону України (реєстр. № 8087 від 29.09.22 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 (дата звернення: 19.09.2023).

26. Депутати готуються проголосувати за законопроект про кібербезбеку, проти поточної редакції якого виступив бізнес, юристи, Міноборони та експерти. URL: https://racurs.ua/ua/n184973-vlada-proignoruvala-golos-biznesu-schododoopracuvannya-zakonoproektu-pro-kiberbezpeku.html (дата звернення: 10.07.2023).

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

УДК 343.341:342.9 (477)

ЛЕОНОВ Б.Д., *доктор юридичних наук, професор,*
головний науковий співробітник МНДЦ при РНБО України.
ORCID: https://orcid.org/0000-0002-2488-7377.

КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ ФІНАНСУВАННЮ ТЕРОРИЗМУ В КОНТЕКСТІ РАТИФІКАЦІЇ ДОДАТКОВОГО ПРОТОКОЛУ ДО КОНВЕНЦІЇ РЄ ПРО ЗАПОБІГАННЯ ТЕРОРИЗМУ

Анотація. *Стаття присвячена актуальним питанням удосконалення кримінально-правової протидії фінансуванню тероризму. Проаналізовано положення нещодавно прийнятого Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом", виділено його недоліки, у зв'язку з чим визначено потребу його подальшого удосконалення. Запропоновано комплекс заходів з удосконалення кримінально-правової протидії фінансуванню тероризму, насамперед шляхом удосконалення законодавства про кримінальну відповідальність за фінансування тероризму, що, на думку автора, дозволить виконати Україні її міжнародно-правові зобов'язання у цій сфері.*

Ключові слова: *тероризм, фінансування тероризму, кримінально-правова протидія, запобігання тероризму, кримінальна відповідальність.*

Summary*. The article is devoted to the topical issues of improving the criminal and legal counteraction to the financing of terrorism. The provisions of the recently adopted Law of Ukraine "On Amendments to the Criminal and Criminal Procedural Codes of Ukraine in connection with the ratification of the Additional Protocol to the Convention of the Council of Europe on the Prevention of Terrorism, as well as to some legislative acts of Ukraine on improving the fight against terrorism" are analyzed, its shortcomings are highlighted, in connection with which the need for its further improvement was determined. A set of measures is proposed to improve the criminal and legal countermeasures against the financing of terrorism, primarily by improving the legislation on criminal liability for the financing of terrorism, which, according to the author, will allow Ukraine to fulfill its international legal obligations in this area.*

Keywords: *terrorism, financing of terrorism, criminal and legal counteraction, prevention of terrorism, criminal liability.*

Постановка проблеми. Фахівцями Комітету MANEYVAL у п. 48 Рекомендації 5 "Злочини фінансування тероризму" Звіту за результатами 5-го раунду взаємної оцінки України (у ході його 55-го планерного засідання у м. Страсбург 5-7 грудня 2017 року) одним з недоліків законодавства України про кримінальну відповідальність за терористичні злочини визнавалася неповна криміналізація перетинання державного кордону в терористичних цілях відповідно до резолюції Ради Безпеки ООН № 2178. З урахуванням цієї резолюції держави члени Ради Європи уклали Додатковий протокол до Конвенції Ради Європи про запобігання тероризму (далі – Протокол).

22 жовтня 2015 року Україна підписала цей Протокол, положення якого, серед іншого, передбачають зобов'язання для держав встановити кримінальну відповідальність за фінансування виїзду за кордон з метою терористичної діяльності (ст. 5 Протоколу), організацію чи сприяння іншим способом виїзду за кордон з метою

терористичної діяльності (ст. 6 Протоколу). Підписання Протоколу зумовлює потребу імплементації його норм у національне законодавство України, у т.ч. у сфері протидії фінансуванню тероризму.

У рамках аналізу основних тенденцій поширення тероризму у частині виявлення джерел фінансування терористичної діяльності фіксується зростання популярності використання криптовалют та веб-ресурсів, які надають можливість проведення фінансових операцій з використанням заборонених на території України платіжних систем (QIWI, WebMoney) у протиправних фінансових операціях, у т.ч. пов'язаних з фінансуванням тероризму. Загострює проблему протидії фінансуванню тероризму агресивна політика російської федерації, спрямована на дестабілізацію ситуації в державі, яка переросла у повномасштабну збройну агресію проти нашої країни.

Результати аналізу наукових публікацій. Питання протидії фінансуванню тероризму досліджували такі вчені, як В. Антипенко [2], Л. Багрій-Шахматов [3], В. Ємельянов [4], К. Жаринов [5], В. Ліпкан, Д. Мельник [6], Д. Никифорчук [7], І. Рижов [4], М. Руденко [7] та ін. Окремі кримінально-правові аспекти протидії діяльності терористичних груп та організацій висвітлено у працях В. Глушкова, Ю. Данильченка, В. Крутова, В. Мокляка, М. Рибачука, О. Семенюка, І. Серкевич, О. Шамари та ін.

Звертаючи увагу на період проведених досліджень зазначених авторів, потрібно вказати, що у них не враховано останні зміни до ст.ст. 258-4 – 258-5 КК України, пов'язані з ратифікацією Протоколу. Суспільно небезпечні діяння з використанням криптовалют для фінансування терористичних груп та організацій залишаються поза увагою поглибленого дослідження науковців. Наведене свідчить про недостатність розробки питань кримінальної відповідальності за фінансування тероризму.

Метою статті є удосконалення норм, що встановлюють кримінальну відповідальність за фінансування тероризму, в контексті ратифікації Протоколу.

Виклад основного матеріалу. Серед основних напрямів державної політики Стратегія національної безпеки України (затверджена Указом Президента України від 14 вересня 2020 року № 392) визначає активну участь держави у протидії тероризму (п. 33) [8].

Відповідно до цієї Стратегії протидія тероризму має бути спрямована на виявлення і припинення терористичної діяльності, передбачати вирішення завдань щодо пошуку та аналітичної обробки інформації про загрозу вчинення терористичних актів, джерел фінансування терористичної діяльності.

Підпунктом 2 пункту 4 Плану заходів з реалізації Концепції боротьби з тероризмом (затверджений розпорядженням Кабінету Міністрів України від 05.01.21 р. № 7-р) на СБУ спільно з іншими заінтересованими державними органами покладено завдання з розробки пропозицій щодо приведення у відповідність з вимогами 5-ї Рекомендації FATF статей Кримінального кодексу України в частині включення злочинів, зазначених у Міжнародній Конвенції про боротьбу з фінансуванням тероризму та Протоколах до неї в частині фінансування тероризму, та щодо застосування кримінальної відповідальності за фінансування поїздок у терористичних цілях відповідно до Резолюції Ради Безпеки ООН 2178 [9].

З метою імплементації міжнародних норм у національне законодавство Законом України від 20.11.22 р. № 2589-IX [10] ратифіковано Протокол, положення якого передбачають, зокрема, удосконалення норм про кримінальну відповідальність за фінансування тероризму. Імплементація міжнародних норм у національне законодавство є фактичною реалізацією міжнародних зобов'язань, а також способом включення норм міжнародного права до національної правової системи [11].

Відповідно до ст. 2 згаданого Закону цей акт набирає чинності з дня набрання чинності законом України про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з Протоколу[10].

23.03.2023 року за результатами розгляду в другому читанні проект Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом" (реєстр. № 8146) прийнято Верховною Радою України в цілому як Закон України №2997–IX [12] (далі – Закон), текст якого підписано Головою Верховною Радою України (23.03.2023) та Президентом України (21.04.2023).

Як зазначають розробники цього Закону, його метою є імплементація в національне законодавство положень Протоколу, а також всебічне посилення спроможностей загальнодержавної системи боротьби з тероризмом з урахуванням європейських та загальносвітових практики у сфері протидії терористичній діяльності [13].

Для досягнення поставленої мети Законом передбачені зміни до: 1) Кримінального кодексу України та Кримінального процесуального кодексу України, відповідно до яких: а) встановлюється кримінальна відповідальність за "проходження навчання тероризму", "перетинання державного кордону України з терористичною метою", а також за фінансування цих діянь; б) визначається підслідність зазначених злочинів — досудове розслідування таких злочинів здійснюватимуть слідчі Служби безпеки України; в) розширюються підстави для застосування до юридичної особи заходів кримінально-правового характеру в разі вчинення її уповноваженою особою названих злочинів; 2) до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" у частині удосконалення визначення фінансування тероризму; 3) Закону України "Про санкції" в частині розширення видів санкцій, що можуть застосовуватись, зокрема до терористичних організацій та груп [13].

Згідно з положеннями цього Закону до КК України було введено нову статтю 258-6, а ст. 258-4, а також абзац перший частини першої ст. 258-5 КК України викладено у новій редакції. Досконале ознайомлення з цими законодавчими новелами свідчить про те, що вони не повною мірою відповідають Протоколу, більш того, вони містять неузгодженості та протиріччя з іншими нормами законодавства у сфері боротьби з тероризмом, що зумовлює потребу їх вдосконалення.

За Законом статтю 258-4 КК України доповнено положеннями про відповідальність за сприяння вчиненню терористичного акту шляхом проходження навчання тероризму.

У примітці до ст. 258-4 КК України під проходженням навчання тероризму в цій статті слід розуміти отримання особою інструкцій, включаючи набуття знань чи практичних навичок, від іншої особи щодо виготовлення або використання вибухових речовин, вогнепальної чи іншої зброї або шкідливих чи небезпечних речовин, або щодо інших специфічних методів чи засобів з метою здійснення діяльності, яка відповідно до закону є терористичною.

Виходячи зі змісту примітки до ст. 258-4 КК України, суб'єктивна сторона проходження навчання тероризму характеризується прямим умислом та наявністю спеціальної мети – здійснення діяльності, яка відповідно до закону є терористичною. За таких умов, притягнення винної особи до відповідальності за проходження навчання тероризму суб'єктами правозастосування буде можливим при доведенні того, до якої саме діяльності готується така особа. Враховуючи те, що сам суб'єкт проходження

навчання тероризму може й не знати достеменно під час набуття знань стосовно використання вибухових речовин, чи буде він вчиняти у подальшому диверсію (ст. 113 КК України), терористичний акт (ст. 258 КК України) чи захоплення заручників (ст. 147 КК України), можливість доказування кримінально-процесуальними засобами факту вчинення вищезазначеного злочину може бути зведена нанівець. На це звертали увагу фахівці Головного науково-експертного управління Верховної Ради України під час експертизи законопроекту № 7699, який містив схожі приписи [13].

Зауважимо, що для цілей Протоколу "проходження навчання тероризму" означає "отримання інструкцій, включаючи набуття знань чи практичних навичок, від іншої особи стосовно виготовлення або використання вибухових речовин, вогнепальної чи іншої зброї або шкідливих чи небезпечних речовин або стосовно інших специфічних методів чи засобів з метою вчинення або сприяння вчиненню терористичного злочину" (п. 1 ст. 3 Протоколу), а не терористичної діяльності як це передбачено Законом. Звідси випливає, що на законодавчому рівні потребує уточнення коло суспільно небезпечних проявів тероризму, навчання яким є кримінально караним.

Відповідно до Закону абзац перший частини 1 ст. 258-5 КК України викладено у новій редакції:

"1. Надання чи збір будь-яких активів прямо чи опосередковано з метою їх використання або усвідомленням можливості того, що їх буде використано повністю або частково для будь-яких цілей окремим терористом чи терористичною групою (організацією), або для організації, підготовки або вчинення терористичного акту, втягнення у вчинення терористичного акту, публічних закликів до вчинення терористичного акту, створення терористичної групи (організації), сприяння вчиненню терористичного акту, навчання тероризму, перетинання державного кордону України з терористичною метою, провадження будь-якої іншої терористичної діяльності, а також спроби вчинення таких дій".

Новелою цієї норми є посилання на мету такого фінансування – надання чи збір будь-яких активів прямо чи опосередковано з метою їх використання для проходження навчання тероризму або перетинання державного кордону України з терористичною метою. На нашу думку, диспозиція цієї статті містить недоліки, які роблять її застосування проблематичним.

З цього приводу слід погодитись з позицією В.П. Ємельянова: "…незрозуміло, для чого захаращувати диспозицію статті зайвим переліком діянь, передбачених статтями 258 – 258-4 КК України, якщо попередньою фразою "тобто дії, вчинені з метою фінансового або матеріального забезпечення окремого терориста чи терористичної групи (організації)" цей перелік цілком охоплюється [15, с. 80-81]. Схожої думки додержується Л.В. Новікова, яка вважає, що при встановленні в диспозиції статті ознак фінансування тероризму не слід робити спробу дати визначення тероризму за допомогою переліку деяких конкретних статей КК України України, а необхідно використовувати вироблене у кримінально-правовій науці загальне визначення злочинів терористичної спрямованості. На думку Л.В. Новікової, під фінансуванням тероризму слід розуміти надання коштів чи їх збирання особою для вчинення будь-якого з діянь, спрямованих на залякування населення з метою спонукання органу державної влади, органу місцевого самоврядування, міжнародної організації, фізичної чи юридичної особи до вчинення якоїсь дії або утримання від її вчинення [16]. До речі, такий підхід випливає **Ошибка! Ошибка связи.**, де передбачено, що "будь-яка особа чинить злочин за змістом цієї Конвенції, якщо вона будь-якими методами, прямо чи опосередковано, незаконно та умисно надає кошти або здійснює їх збір з наміром, щоб вони

використовувались, або при усвідомленні того, що вони будуть використані, повністю чи частково, для вчинення будь-якого діяння, яке являє собою злочин відповідно до сфери застосування одного з договорів, перелічених у додатку, та до визначення, що міститься в ньому" [17]. Ми підтримуємо підхід, згідно з яким не слід переобтяжувати КК України зайвими приписами, які не несуть ніякого особливого правового навантаження, вирішують конкретні кримінально-правові ситуації, які вже вирішені шляхом застосування вже передбачених в КК України норм [18, с. 24].

Неабиякий інтерес викликає введення в КК України нової статті 258-6, якою встановлено відповідальність за перетинання державного кордону України для здійснення діяльності, яка відповідно до закону є терористичною. Водночас, Закон України "Про боротьбу з тероризмом" перетинання державного кордону з терористичною метою визначає складовою терористичної діяльності, що свідчить про тавтологічність наявного у цій нормі словосполучення "яка відповідно до закону є терористичною". Зауваження щодо формулювання мети виїзду з України та в'їзду в Україну (ст. 258-6 КК України у редакції проекту) висловлювали експерти Апарату Верховної Ради України, адже для цілей Протоколу "виїзд за кордон з терористичною метою" означає виїзд особи до держави, громадянином якої вона не є і яка не є місцем постійного проживання такої особи, з метою вчинення, сприяння або участі у терористичному злочині або здійснення чи проходження навчання тероризму [14]. Натомість законодавець криміналізував будь-яке перетинання державного кордону з такою метою.

Крім цього, відповідно до статті 6 Протоколу "організація чи сприяння іншим способом виїзду за кордон з терористичною метою" означає будь-яку дію, спрямовану на організацію або сприяння, що допомагає будь-якій особі у виїзді за кордон з терористичною метою, як визначено в пункті 1 статті 4 цього Протоколу, з усвідомленням, що така допомога слугує терористичним цілям [1]. За Протоколом кожна сторона вживає таких заходів, які можуть бути необхідними для визнання відповідно до національного законодавства вчиненої незаконно та умисно "організації чи сприяння іншим способом виїзду за кордон з терористичною метою" (визначено в пункті 1) злочином.

Аналіз запропонованих змін дозволив експертам Головного юридичного управління Апарату Голови Верховної Ради України дійти висновку, що задекларована в пояснювальній записці мета акта не повною мірою буде досягнута у частині імплементації в національне законодавство положень статті 6 Протоколу ("організація чи сприяння іншим способом виїзду за кордон з терористичною метою") [19]. До речі, за змістом ст. 7.2.10 проекту КК України підготовка терористичної діяльності охоплює широкий перелік дії винної особи, яка: 1) проходила навчання; 2) проводила навчання, 3) прибула до України чи держави-члена Європейського Союзу або переміщувалась транзитом через територію України; 4) залишила територію України чи держави-члена Європейського Союзу, 5) заволоділа матеріальними засобами, коштами чи інформацією або 6) склала чи використала підроблений офіційний документ [20]. Наведене зумовлює потребу криміналізації організації чи іншого сприяння перетинання державного кордону з такою метою, як це передбачено ст. 6 Протоколу.

Законом передбачені й зміни до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" у частині доповнення визначення фінансування тероризму посиланням на мету – перетинання державного кордону України з терористичною метою. Як зазначалося раніше, така мета

цілком охоплюється законодавчим формулюванням “дії, вчинені з метою фінансового або матеріального забезпечення окремого терориста чи терористичної групи (організації)” у визначенні фінансування тероризму. Тому, на нашу думку, така деталізація є зайвою й такою, що не несе особливого правового навантаження.

Новелою Закону є доповнення Закону України “Про боротьбу з тероризмом” ст. 24-1 “Відповідальність терористичної організації (групи)”, зміст якої передбачає, що до терористичної організації (групи) можуть застосовуватися санкції в порядку, визначеному Законом України “Про санкції”, коло яких розширено новими спеціальними економічними та іншими обмежувальними заходами (санкціями): а) заборона діяльності на території України; б) відмова в наданні або скасування дозволу на імміграцію, дії посвідок на постійне чи тимчасове проживання в Україні; в) примусове повернення або примусове видворення за межі України; г) заборона демонстрації та використання символіки терористичних організацій і груп, пропагування ідей та програмних цілей таких організацій (груп), блокування доступу до інформаційних ресурсів, які використовуються для зазначених цілей.

Зауважуємо, що механізм застосування санкцій визначено Законом України "Про санкції", який передбачає: розгляд пропозицій щодо застосування, скасування та внесення змін до санкцій, які вносяться Верховною Радою України, Президентом України, Кабінетом Міністрів України, Національним банком України, Службою безпеки України, на засіданні Ради національної безпеки та оборони України, прийняття за результатами такого розгляду рішення Радою національної безпеки та оборони України та введення в дію указом Президента України; відповідне рішення набирає чинності з моменту видання указу Президента України і є обов’язковим до виконання (частини перша та третя статті 5 Закону України “Про санкції”).

На думку Головного юридичного управління Апарату Верховної Ради України, застосування таких санкцій Радою національної безпеки та оборони України як координаційним органом з питань національної безпеки і оборони при Президентові України, який координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони, не узгоджується з вимогами статті 107 Конституції України та Закону України Про Раду національної безпеки і оборони України (ст. 1, 3, 4 цього Закону), що суперечитиме конституційному статусу цього органу [19].

На переконання переважної більшості фахівців, передбачені вказаним законом спеціальні обмежувальні заходи (санкції), внаслідок свого тимчасового характеру можуть лише доповнювати наявні заходи кримінальної репресії щодо терористів та терористичних організацій (груп) разом із передбаченими Законом України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення” фінансово-контрольними заходами щодо блокування, заморожування, арешту і конфіскації активів, які збираються, акумулюються та спрямовуються на фінансування тероризму, та підлягають застосуванню у рамках загальнодержавного комплексу заходів з протидії тероризму [21]. Прорахунки застосування та недоліки норм Закону України “Про санкції” вже мали наслідком оскарження в судах рішень РНБО України, оголошених указами Президента України щодо застосування санкцій до контрабандистів та пособників терористичної діяльності НЗФ т.зв. “ДНР”/“ЛНР”.

Застосування відносно вітчизняних терористичних організацій та окремих терористів (насамперед учасників “ДНР”/“ЛНР”, та інших, які перебувають у межах правового поля держави) механізму політико-правового впливу, передбаченого Законом України “Про санкції” наразі видається нераціональним та неефективним – як через

недоліки самого Закону (загальний характер правових норм, недосконаліть визначених процедур тощо), так і у зв'язку з необхідністю вжиття адекватних заходів правового реагування до таких суб'єктів, дії яких вже криміналізовані законодавцем (ст. 109, 110, 112, 147, 194, 258 – 258-5, 260, 265 – 266, 278, 279, 292, 349, 349-1, 439, 440, 443, 444 КК України) відповідно до законодавства України про кримінальну відповідальність[21].

Крім того, санкційний підхід не повною мірою узгоджується з положеннями ст. 24 "Відповідальність організації за терористичну діяльність" Закону України "Про боротьбу з тероризмом", згідним з якими організація, відповідальна за вчинення терористичного акту, визнається терористичною за рішенням суду. Давно назрілою є потреба належного унормування порядку визнання організацій терористичними та формування відповідного реєстру, що забезпечуватиме належні умови для протидії їх діяльності в Україні.

Відсутність в законодавстві повноцінного порядку визнання організації терористичною унеможливлює застосування й інших положень ст. 24 Закону України "Про боротьбу з тероризмом", які передбачають правові наслідки для організації, визнаної за рішенням суду відповідальною за вчинення терористичного акту (підлягає ліквідації, а належне їй майно конфіскується).

Неврегульованість цього питання не дає змоги реалізовувати окремі положення законодавства з протидії фінансуванню тероризму, виявлення, арешту та вилучення активів організацій та осіб, пов'язаних із провадженням терористичної діяльності [22, с. 87].

Крім цього, відсутність такого порядку значно ускладнює процедуру притягнення осіб до відповідальності за вчинення злочину, передбаченого ст. 258-3 КК України, негативно позначається на практиці застосування санкцій до осіб, які сприяють злочинній діяльності терористичних груп та організацій [22, с. 51].

Таким чином, до вад Закону можна віднести й те, що він не конкретизує механізм (процедуру) визнання організації терористичною в судовому порядку.

Слід зауважити, що викладені зауваження і пропозиції до Закону не вичерпують проблематику фінансування тероризму.

Враховуючи суспільну небезпечність заздалегідь не обіцяного сприяння терористичному акту вважається за доцільне встановити відповідальність за таке діяння (за аналогією ст. 256 КК України), досудове розслідування за яким здійснюватимуть органи СБУ.

Заходом, який сприятиме підвищенню ефективності застосування заходів кримінально-правового впливу за терористичну діяльність, можуть стати запропоновані зміни до статті 67 КК України, які визначатимуть вчинення злочину з терористичною метою обставиною, що обтяжує покарання.

Отже, на підставі здійсненого аналізу, існує потреба удосконалення законодавчих актів України щодо боротьби з тероризмом з урахуванням висновків експертів, рішень РНБО України, Концепції боротьби з тероризмом, Плану її реалізації та вимог міжнародно-правових актів у цій сфері.

Висновки.

Аналіз Протоколу свідчить про недостатню імплементацію в національне законодавство його положень. З урахуванням змісту Конвенції РЄ про запобігання тероризму (ст. 5 – 7, 9), Протоколу (ст. 2 – 6), а також беручи до уваги згадані вади КК України в частині регламентації відповідальності за різні прояви терористичної діяльності, можна виділити кілька концептуальних підходів до внесення змін та доповнень до КК України у зв'язку з ратифікацією згаданого міжнародного акта. Один з

них полягає у внесенні змін та доповнень до КК України, які забезпечать мінімальний рівень узгодження його змісту з окремими положеннями Конвенції РЄ про запобігання тероризму (ст. 5 – 7, 9), Протоколу (ст. 2 – 6) Міжнародної конвенції про боротьбу з фінансуванням тероризму (ст. 2). Ці зміни мають забезпечити "спеціальну криміналізацію" тих різновидів суспільно небезпечної поведінки, які виражаються в Протоколі термінами "виїзд за кордон з терористичною метою", "фінансування виїзду за кордон з терористичною метою", "організація чи сприяння іншим способом виїзду за кордон з метою терористичної діяльності". Реалізація іншого концептуального підходу передбачає внесення системних змін та доповнень до КК України, які повинні забезпечити близький до оптимального рівень узгодження його змісту з більшістю положень Конвенції РЄ про запобігання тероризму, Протоколу, що мають кримінально-правовий характер, а також усунути найбільш очевидні вади КК України в частині регламентації відповідальності за різні прояви тероризму. Основними орієнтирами для таких змін та доповнень є: а) необхідність забезпечення "спеціальної криміналізації" окремих різновидів суспільно небезпечної поведінки, передбаченої статтями 5 – 7, 9 Конвенції, ст. 2 – 6 Протоколу (реалізація першого концептуального підходу); б) хоча б часткове вирішення у КК України проблем, пов'язаних з термінами "терористичний злочин" (ч. 1 ст.1 Конвенції ЄС про запобігання тероризму, ст. 2 Міжнародної конвенції про боротьбу з фінансуванням тероризму) та "терористична діяльність"; в) вдосконалення змісту диспозицій та санкцій тих статей Особливої частини КК України, які передбачають відповідальність за різні прояви тероризму. Реалізація такого підходу є перспективою подальших наукових розвідок у напрямку кримінально-правової протидії тероризму.

З метою повної імплементації в національне законодавство положень Протоколу у межах першого з названих підходів необхідно: передбачити організаційне чи інше сприяння терористичним правопорушенням серед ознак сприяння вчиненню терористичного правопорушення (ч. 1 ст. 258-4 КК України); встановити кримінальну відповідальність за заздалегідь не обіцяне сприяння терористичному акту (за аналогією ст. 256 КК України); визнати вчинення злочину з терористичною метою обставиною, що обтяжує покарання (зміни до статті 67 КК України України). Бажано ч. 1 ст. 258-5 КК України викласти у новій редакції, обмежившись формулюванням, що фінансування тероризму (тобто надання чи збір будь-яких активів) може бути використано повністю або частково для підготовки та вчинення терористичного злочину.

У зв'язку з цим доцільно внести зміни до КК України України, а саме:

доповнити частину 1 статті 67 новим пунктом 14 такого змісту:

"14) вчинення кримінального правопорушення з терористичною метою";

у частині 1 статті 258-4:

після слів "навчання тероризму" доповнити словами "чи інше сприяння вчиненню терористичного правопорушення";

у примітці слова "здійснення діяльності, яка відповідно до закону є терористичною" замінити словами "вчинення терористичного правопорушення";

частину 1 статті 258-5 викласти у такій редакції: "Фінансування тероризму, тобто надання чи збір активів особою, яка усвідомлювала, що це може бути використано повністю або частково для підготовки та вчинення терористичного правопорушення".

у частині 1 статті 258-6 слова "діяльності, яка відповідно до закону є терористичною" замінити словами "терористичної діяльності".

доповнити статтею 258-7 такого змісту:

“Стаття 258-7 Заздалегідь не обіцяне сприяння учасникам терористичних організацій

1. Заздалегідь не обіцяне сприяння учасникам терористичних організацій чи терористичних груп та укриття їх терористичної діяльності шляхом надання приміщень, сховищ, зброї, бойових припасів, вибухових речовин, військової техніки, транспортних засобів, інформації, документів, технічних пристроїв, грошей, цінних паперів, переміщення терористів через державний кордон України, а також заздалегідь не обіцяне здійснення інших дій зі створення умов, які сприяють їх терористичній діяльності, – караються позбавленням волі на строк від трьох до п’яти років.

2. Ті самі дії, вчинені повторно або службовою особою з використанням службового становища, – караються позбавленням волі на строк від п’яти до десяти років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років”.

З метою визнання організації терористичною на законодавчому рівні потребує визначення: 1) перелік підстав для ініціювання питання про визнання організації терористичною та заборони її діяльності на території нашої країни; 2) юрисдикція суду, до компетенції якого буде віднесено розгляд справ про визнання організації терористичною та заборони її діяльності на території України; 3) суб’єкт (чи коло суб’єктів), уповноважених ініціювати питання про визнання в судовому порядку організації терористичною та заборони її діяльності на території України; 4) особливий порядок кримінального провадження щодо таких організацій. Зокрема, потребують унормування особливості розгляду судами матеріалів кримінальних проваджень щодо терористичних правопорушень, в ході яких уповноваженими суб’єктами може бути ініційований розгляд питання про визнання організацій терористичними та прийняття відповідного судового рішення [23, с. 162-163].

Врегулювання порядку визнання організації терористичною сприятиме протидії фінансуванню тероризму, виявленню, арешту та вилученню активів організацій та осіб, пов’язаних із провадженням терористичної діяльності.

Використана література

1. Додатковий протокол до Конвенції Ради Європи про запобігання тероризму. URL: https://zakon.rada.gov.ua/laws/show/994_001-15#Text

2. Антипенко В.Ф. Тероризм: кримінологічна та кримінально-правова характеристика. Київ, 1999. 61 с.

3. Багрій-Шахматов Л.В. Методи боротьби з тероризмом. Погляд світового товариства. Тероризм і боротьба з ним: аналітичні розробки, пропозиції наукових та практичних працівників. 2000. Т. 19. С. 338-343.

4. Емельянов В.П., Иманлы М.Н., Рыжов И.Н. Уголовно-правовое противодействие терроризму. Харьков: Право, 2014. 88 с.

5. Жаринов К.В. Терроризм и террористы. Исторический справочник; минск: Харвест, 1999. 606 с.

6. Мельник Д., Леонов Б. Поняття та зміст кримінологічної характеристики фінансування тероризму. *Інформація і пр*аво. № 2(41)/2022. С. 84-94.

8. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 14.04.2022).

9. План заходів з реалізації Концепції боротьби з тероризмом: розпорядження Кабінету Міністрів України від 05.01.21 р. № 7-р. URL: https://zakon.rada.gov.ua/laws/show/7-2021-%D1%80#Text

10. Про ратифікацію Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму: Закон України від 20.09.22 р. № 2589-IX. URL: https://zakon.rada.gov.ua/laws/show/2589-20#n2

11. Лиховая С.Я. Уголовная ответственность юридических лиц по законодательству Украины. *Criminology Journal of Baikal National University of Economics and Law*. 2014. № 2. С.155-161.

12. Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом: Закон України від 21.03.23 р. № 2997-IX. URL: https://zakon.rada.gov.ua/laws/show/2997-20#Text

13. Пояснювальна записка до проекту Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом" (реєстр. № 8146). URL:https://itd.rada.gov.ua/billInfo/Bills/pubFile/1697843

14. Висновок Головного науково-експертного управління Апарату Верховної Ради України на проект Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму" від 07.09.22 р. №16/03-2022/149985. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1465386

15. Ємельянов В.П. Питання вдосконалення кримінально-правових засад протидії терористичним злочинам кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку: матеріали міжн.-наук. практ. конф., м. Харків, 2019 р. С. 79-81. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/35.pdf

16. Новікова Л. В. Кримінальна відповідальність за фінансування тероризму: автореф. дис. …канд. юр. наук. спец. 12.00.08. Інститут держави і права імені В.М. Корецького НАН України, Київ, 2007. 20 с.

17. Міжнародна Конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999 р. URL: https://zakon.rada.gov.ua/laws/show/995_518#Text

18. Лихова С.Я. Злочини проти громадянських, політичних та соціальних прав і свобод людини і громадянина за Кримінальним кодексом України (теоретико-правове дослідження): автореф. дис. …докт.-ра юр. наук. спец. 12.00.08. КНУ імені Тараса Шевченка, Київ, 2006. 39 с.

19. Зауваження Головного юридичного управління Апарату Верховної Ради України на проект Закону України "Про внесення змін до Кримінального та Кримінального процесуального кодексів України у зв'язку з ратифікацією Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму, а також до деяких законодавчих актів України щодо вдосконалення боротьби з тероризмом" (друге читання) від 30.11.22 р. № 07/2-2022/205090. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1563730

20. Проект Кримінального кодексу України за станом на 22 травня 2023 року. URL: ewcriminalcode.org.ua/upload/media/2023/05/22/kontrolnyj-tekst-proektu-kk-22-05-2023.pdf

21. Маркєєва О.Д., Розвадовський Б.Л. Загальнодержавна система боротьби з тероризмом: проблеми та перспективи: аналіт. доповідь. Київ: НІСД, 2022. 88 с.

22. Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доповідь / за заг. ред. О.О. Резнікової. Київ: НІСД, 2017. 102 с.

23. Мельник Д., Леонов Б. Актуальні питання удосконалення порядку визнання організацій терористичними та формування їх реєстру. *Вісник кримінального судочинства*. 2023. № 1-2. С. 151-163.

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

УДК 343.2/.7:004.056(477)

КОВАЛЬЧУК А. Ю., *доктор юридичних наук, професор,* професор кафедри міжнародного права та інших галузевих правових дисциплін Київського університету права НАН України.
ORCID: https://orcid.org/0000-0003-4807-2436.
ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, с.н.с.,* головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0001-7496-9904.

КІБЕРЗЛОЧИНИ, ЯК ЗАГРОЗА ДЕРЖАВНІЙ БЕЗПЕЦІ: КРИМІНОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНІ ОСОБЛИВОСТІ ОБЛІКУ

Анотація. *У статті підіймається проблема законодавчої невизначеності кіберзлочину. Серед науковців та практиків також немає єдиного підходу до окреслення підстав та ознак протиправного діяння, яке визначається як кіберзлочин. Разом з тим, така невизначеність негативно відображається на ефективності протидії кіберзлочинності в Україні. Разом з тим, у світі поширеність вчинення кіберзлочинів та кібератак, особливо на фінансові системи, державні органи, критичну інфраструктуру лише зростає.*

Ключові слова: *кіберзлочини, протидія злочинності, державна (національна) безпека, правоохоронні органи, кримінологічні засади протидії злочинності, статистична звітність.*

Summary. *The article analyzes the types, forms and content of statistical reporting reflecting the state and structure of cybercrime in Ukraine. It is noted that there is no universally recognized concept of cybercrime in international legislation. There is currently no clear definition of the concept of cybercrime in domestic legislation. Among scientists and practitioners, there is also no single approach to delineating the grounds for classifying illegal acts as such crimes. The reports were developed without further analysis of cybercrime. On the basis of official state reporting prepared by the Office of the Prosecutor General of Ukraine and the State Judicial Administration of Ukraine, it is possible to analyze a small group of criminal offenses, namely, those provided for by the articles of Chapter XVI of the Criminal Code of Ukraine. Some of the "traditional crimes" that fall under the concept of cybercrime are reflected in the departmental statistical reporting of the National Police of Ukraine, but it does not cover all cybercrimes and, of course, takes into account only those assigned to the jurisdiction of the National Police of Ukraine. Therefore, in Ukraine, there is no official state statistical reporting on cybercrime. Considering the high latency of this type of criminal offense, it can be stated that it is impossible to conduct an analysis that would fully and reliably reflect the state of cybercrime in Ukraine.*

Keywords: *cybercrime, crime prevention, state (national) security, latent cybercrime, criminological principles of crime prevention, statistical reporting.*

Постановка проблеми. Сьогоднішня ситуація в світі приносить з собою нові виклики безпеки, що пов'язані з війнами, техногенними катастрофами, які можуть бути спричинені загрозами здійснення кібератак. Враховуючи залежність сучасного життя від інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, унаслідок щоденного функціонування майже всіх аспектів суспільного життя у кіберпросторі набуває актуальності розробка організаційних та правових заходів його захисту. Лише з початку 2023 року Служба безпеки України нейтралізувала майже чотири тисячі кібератак на електронні системи центральних органів влади та критичної

інфраструктури України. Більшість ворожих кібератак спрямована на пошук несанкціонованого доступу до електронного документообігу держустанов і технологічних систем інфраструктури [1]. У аналітичному звіті ГО "Платформа прав людини" (2023) висвітлені значні показники здійснених кібератак:

1) 16 539 759 кібератак, які було здійснено на державний сектор;

2) 179 814 фішинг атак;

3) 159 дезінформаційних повідомлень [2].

Така значна кількість кібератак вимагає перегляду правових та організаційних заходів захисту кіберпростору України, у тому числі притягнення винних до відповідальності за їх вчинення. Разом з тим, практична діяльність правоохоронних органів визначається чинною кримінальною обстановкою, яка впливає як на прийняття конкретних управлінських рішень, так і на координацію наявних сил та засобів. У зв'язку з цим для правоохоронних органів завжди є актуальним аналіз поточного стану злочинності та динаміки її змін. Це звичайно стосується і протидії злочинності у кіберпросторі, яка на сьогодні розвивається досить динамічно. У вітчизняному законодавстві нині не існує чіткого визначення поняття кіберзлочин. Серед науковців та практиків також немає єдиного підходу до окреслення підстав віднесення протиправних діянь до таких злочинів, відсутній перелік "традиційних" злочинів, які можуть відноситися до категорії кіберзлочинів, а отже і відсутня офіційна статистична звітність щодо облікованих кіберзлочинів. Це негативно позначається на можливості запобігання цим злочинам, зумовлюючи труднощі у боротьбі з кіберзлочинністю. Аналіз такої статистичної звітності надав би можливість аналізувати 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 [1; 2].

Результати аналізу наукових публікацій. Окремі аспекти аналізу кіберзлочинності 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, О.В. Таран, В.І. Трапезніков, В.О. Туляков та ін. Водночас, проблемам аналізу кіберзлочинності, зокрема і у частині офіційної статистики, приділяється недостатньо уваги. Крім того, зважаючи на те, що значна частина кіберзлочинів знаходяться поза межами статистики, актуалізується проблема латентної кіберзлочинності в Україні.

Метою статті є системний аналіз та оцінка наявних державних статистичних даних, що стосуються кіберзлочинності, осіб, які вчинили кіберзлочини та інших даних, що відображені у різних джерелах; оцінка структури і змісту таких даних та можливостей їх використання для запобігання і та протидії кіберзлочинності; висвітлення проблемних питань стосовно формування офіційної статистичної звітності щодо облікованих кіберзлочинів.

На основі офіційної державної статистичної звітності, що готується Офісом Генерального прокурора України та Державною судовою адміністрацією України, можна проаналізувати незначну групу кримінальних правопорушень, а саме, передбачених статтями Розділу XVI КК України. Частина "традиційних злочинів", які підпадають під поняття кіберзлочини, відображені у відомчій статистичній звітності Національної поліції України, але вона охоплює не всі кіберзлочини і, звичайно ж, враховує лише віднесені до підслідності Національної поліції України. Зроблено висновок про те, що в Україні, відсутня офіційна державна статистична звітність щодо кіберзлочинності. Враховуючи високу латентність цього виду кримінальних правопорушень, можна констатувати, що на сьогодні провести аналіз, який повно і достовірно відобразив б стан кіберзлочинності в Україні неможливо.

Виклад основного матеріалу. Як свідчать дослідження фахівців, на сьогодні у світі не існує ні релевантної статистики, яка відображає реальний стан кіберзлочинності, ні надійних методів збору таких даних, та й збитки від кіберзлочинів є досить приблизними. Справа не тільки у відсутності ідентичності національного кримінального законодавства країн у сфері боротьби з кіберзлочинністю і різної практики його застосування, а й у відмінності у формуванні кримінальної статистики та особливості правоохоронної системи [3].

Проведений аналіз офіційної державної статистичної звітності щодо боротьби зі злочинністю в Україні, яка готується Офісом Генерального прокурора України та Державною судовою адміністрацією України, свідчить, що і в Україні про статистику, яка повно й достовірно відбиває стан кіберзлочинності, сьогодні не йдеться [4].

В Україні лише через 12 років після ратифікації Конвенції про кіберзлочинність [5] на законодавчому рівні було визначено терміни "кіберзлочин" та "кіберзлочинність". У Законі України "Про основні засади забезпечення кібербезпеки України" ці терміни визначено наступним чином: "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", "Кіберзлочинність – сукупність кіберзлочинів [5]. Проте на сьогодні рекомендації, інструкції щодо віднесення кримінальних правопорушень, які вчиняються у кіберпросторі до кіберзлочинів відсутні. Серед науковців та практиків немає єдиної думки з цього приводу, а тому й єдиного підходу до окреслення підстав віднесення протиправних діянь до таких злочинів. А якщо немає чіткого розуміння чи переліку цих злочинів, то звісно неможливо отримати об'єктивні статистичні дані про кіберзлочини.

Варто вказати, що більшість дослідників, які вивчають проблему кіберзлочинності, 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, тобто які вчиняються у кіберпросторі. І якщо основу першої групи кіберзлочинів складають кримінальні правопорушення, передбачені статтями Розділу XVI КК України (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку) та ст. 376-1 КК України (Незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя), то злочини, які мають бути віднесені до другої частини повністю не визначені. І офіційна державна статистична звітність про ці злочини відсутня.

Окремі показники по таких кримінальних правопорушеннях відображені у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України (у Розділі "Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій[1], у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції", де крім злочинів, окреслених статтями Розд.

[1] Злочини у сфері високих інформаційних технологій можна визначити як вчинені умисно або з необережності суспільно небезпечні діяння (дії або бездіяльність), що посягають на відносини у сфері обробки інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах, надання та отримання телекомунікаційних послуг, проведення електронних розрахунків.

XVI КК України, зазначалася ще низка, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 “Порушення авторського права і суміжних прав” і ст. 185 “Крадіжка”, чч. 3 і 4 ст. 190 “Шахрайство”, ст. 200 “Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення”, ст. 229 “Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару” і ст. 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю”, чч. 3 – 5 ст. 301 “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів”.

Нещодавно цей перелік злочинів був доповнений такими статтями: ст. 120 “Доведення до самогубства”, ст. 149 “Торгівля людьми”, ст. 156 “Розбещення неповнолітніх”, ст. 156-1 “Домагання дитини для сексуальних цілей”, ч. 1, 2 ст. 190 “Шахрайство”, ст. 191 “Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем”, ст. 203-2 “Незаконна діяльність з організації або проведення азартних ігор, лотерей”, ст. 301-1 “Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження”, ст. 301-2 “Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи”, ст. 307 “Незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів”, ст. 321 “Незаконне виробництво, виготовлення, придбання, перевезення, пересилання, зберігання з метою збуту або збут отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів”, ст. 321-1 “Фальсифікація лікарських засобів або обіг фальсифікованих лікарських засобів”, ст. 357 “Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження”, ст. 358 “Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів”.

Але це не всі “традиційні” злочини, що вчиняються у кіберпросторі, відображено у звіті як кіберзлочин, зокрема, 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.

Водночас деякі науковці, зокрема доктор юридичних наук, професор Савченко А.В., вважають, що крім кримінальних правопорушень, зазначених у вищевказаному звіті, під категорію кіберзлочинів можуть підпадати й інші злочини, передбачені Кримінальним кодексом України (частина з них віднесені до підслідності інших органів досудового розслідування), за умови, що *знаряддям* їх вчинення будуть інформаційні мережеві технології та (або) їх наслідки позначатимуться у кіберпросторі [6].

До таких злочинів належать: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України); посягання на територіальну цілісність і недоторканність України (ст. 110); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114); розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини

чи іншої невиліковної інфекційної хвороби (ст. 132); незаконне розголошення лікарської таємниці (ст. 145); надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158); порушення таємниці голосування (ст. 159); порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (ст. 161); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення таємниці усиновлення (удочеріння) (ст. 168); порушення недоторканності приватного життя (ст. 182); розголошення комерційної або банківської таємниці (ст. 232); завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259); незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (*в частині збуту через Інтернет*) (ст. 263); заклики до вчинення дій, що загрожують громадському порядку (ст. 295); ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300); сутенерство або втягнення особи в заняття проституцією (ст. 303); незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307); викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (*в частині збуту через Інтернет*) (ст. 312); викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (*в частині збуту через Інтернет*) (ст. 313); розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330); погроза або насильство щодо працівника правоохоронного органу (ст. 345); погроза або насильство щодо журналіста (ст. 345-1); погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346); погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350); незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376-1); розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381); розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398); розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422); пропаганда війни (ст. 436); виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436-1).

Отже, на сьогодні ще значна частина злочинів, що вчиняються у кіберпросторі не враховується як кіберзлочини, тобто такі показники відсутні як у офіційній державній статистичній звітності, так і у відомчій, зокрема.

Аналіз статистичних даних показує, що кількість кримінальних правопорушень, передбачених статтями Розд. XVI КК України, протягом 2013-2022 років зросла у 5,7 рази (595 у 2013 році проти 3415 у 2022 році). (див. табл.1).

Таблиця 1

Кількість облікованих кримінальних правопорушень, передбачених статтями Розділу XVI КК України
(протягом 2013-2022 рр. та 10 міс. 2023 р.)

Рік	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	10 міс. 2023
Всього	595	443	598	865	2573	2301	2204	2498	3310	3415	3495

При цьому за 10 місяців 2023 року вже було обліковано 3495 кримінальних правопорушень, що на 2,3 % більше порівняно з 12 місяцями 2022 року. Але їхня частка у загальному рівні злочинності в Україні сьогодні незначна і становить близько одного відсотка, зокрема, у 2022 році – 0,9 %, у 2021 цей показник складав 1,0 %.

У рік повномасштабного вторгнення рф в Україну обліковано 3415 кримінальних правопорушень. Питома вага особливо тяжких складає 3,2% (108), тяжких – 63,0 % (2151), нетяжких – 26,5 % (905), кримінальних проступків – 7,2% (247).

Із облікованих 3415 кримінальних правопорушень у 3279 (96,0 %) провадженнях досудове розслідування здійснювалося органами Національної поліції України, 102 (3,0 %) – Державним бюро розслідувань України.

У 2022році на 16,4 % зменшилася кількість кримінальних правопорушень, передбачених ст. 361 КК України (1679 у 2021 р. проти 1403 у 2022 р.). Значно зменшилася кількість кримінальних правопорушень, передбачених ст. 361-2 КК України – на 57,4 % (141 у 2021 р. проти 60 у 2022 р.), а також передбачених ст. 363 КК України – на 75,0 % (12 у 2021 р. проти 3 у 2022 р.).

При цьому в 8 раз збільшилася кількість кримінальних правопорушень, передбачених ст. 361-1 КК України (35 у 2021 р. проти 280 у 2022 р.), на 15,6 % – передбачених ст. 362 КК України (1440 у 2021 р. проти 1664 у 2022 р.).

Збільшилася на 24,7 % кількість кримінальних правопорушень, за якими провадження направлені до суду з обвинувальним актом (1953 у 2021 р. проти 2435 у 2022 р.).

Збільшилася на 61,6 % кількість виявлених кримінальних правопорушень вчинених особами, які раніше вчиняли кримінальні правопорушення – 229 у 2021 р. проти 141 у 2022 р.

П’ять кримінальних правопорушення вчинено неповнолітніми або за їх участю (13 у 2021 р.).

Дещо збільшилася (+5,4 %) кількість кримінальних правопорушень, у яких провадження закрито – 333 у 2021 р. проти 351 у 2022 р.

Найбільшу частку складають кримінальні правопорушення, передбачені ст. 362 КК України (48,7 %) та ст. 361 КК України КК України (41,1 %).

Кількість виявлених осіб, які вчиняли кримінальні правопорушення, передбачені статтями Розд. XVI КК України, протягом 2016-2022 років зросла у 3,6 рази (52 у 2016 році проти 187 у 2022 році) (див. табл. 2).

При цьому за 10 місяців 2023 року вже було виявлено 331 особу, що на 77,0 % більше порівняно з 12 місяцями 2022 року.

Загалом у 2022 р. виявлено 187 осіб, які вчинили кримінальні правопорушення, що на 15,4 % менше порівняно з аналогічним періодом 2021 р. (221 у 2021 р.). У 2022 році виявлено менше на 47,4 % осіб, які вчинили кримінальні правопорушення, передбачені

ст. 361-2 (19 у 2021 р. проти 10 у 2022 р.), на 32,0 % – передбачених ст. 362 (75 у 2021 р. проти 51 у 2022 р.), на 27,3 % – ст. 361-1 (11 у 2021 р. проти 8 у 2022 р.) та на 3,2 % – ст. 361 (124 у 2021 р. проти 120 у 2022 р.). Найбільше виявлено осіб, які вчинили кримінальні правопорушення, передбачені ст. 361 КК України КК України (64,2 %) та ст. 362 КК України (27,3 %).

Таблиця 2

Кількість виявлених осіб, які вчинили кримінальні правопорушення, передбачені статтями Розділу XVI КК України, у поточному році та минулих роках
(2016-2022 рр. та 10 міс. 2023 р.)

Рік	2016	2017	2018	2019	2020	2021	2022	10 міс. 2023
Виявлено осіб, які вчинили кримінальні правопорушення у звітному періоді	52	103	136	103	152	221	187	331
Виявлено осіб, які вчинили кримінальні правопорушення у минулих роках (до звітного періоду)	38	65	118	117	168	189	197	254

У 2022 році 23 особи вчинили кримінальні правопорушення у групі, в т.ч. 8 – у складі організованої групи або злочинної організації 1 – за участю неповнолітніх (змішаної групи). Виявлено 31 особу, які раніше вчиняли кримінальні правопорушення, у тому числі у 12 осіб, судимість не знята і не погашена.

Варто звернути увагу на статистичні дані про виявлених осіб, які вчинили кримінальні правопорушення у минулих роках – таких осіб виявлено 197, що на 5,3 % більше порівняно з тими, що вчинили кримінальні правопорушення у 2022 році. При цьому за 10 місяців 2023 року вже було виявлено 254 особи, що на 28,9 % більше порівняно з 12 місяцями 2022 року.

Відповідно статистичним даним Державної судової адміністрації України кількість осіб, які вчинили кримінальні правопорушення, передбачені статтями Розділу XVI КК України, провадження щодо яких перебували у судах першої інстанції протягом 2013-2022 р.р. зросла в 5,8 рази (76 у 2013 році проти 437 у 2022 році) (див. табл. 3).

Таблиця 3

Кількість осіб, провадження щодо яких перебували в суді
(протягом 2013-2022 рр.)

Рік	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Всього	76	77	89	94	142	224	242	308	459	437
Із них засуджено осіб, судові рішення щодо яких набрали законної сили	49	37	31	24	42	49	50	56	76	74

Згідно Звіту про склад засуджених у 2022 році з 74 засуджених осіб, судові рішення щодо яких набрали законної сили, з позбавленням волі засуджено 10, з них 7 – понад 2 роки до 3 років включно, 2 – понад 3 роки до 5 років включно, 1 – понад 1 рік до 2 років. До 23 засуджених застосовано штрафи, 38 засуджених осіб звільнено від

покарання з випробуванням. Варто відмітити, що осіб, які вчинили злочини у складі організованої групи або злочинної організації засуджено у 2022 році не було.

Протягом же 10 років засуджено 6 осіб, які вчинили злочини у складі організованої групи або злочинної організації і судові рішення щодо яких набрали законної сили у звітному періоді.

Однією з найважливіших соціально-демографічних ознак, які характеризують особистість злочинця, є вік засуджених. У 2022 році найбільше засуджено осіб, які вчинили злочини у віці від 30 до 50 років – 27 (36,5 %) осіб; у віці від 25 до 30 років – 20 (27,0 %) осіб; від 18 до 25 років – 19 (25,7 %) осіб; 5 осіб вчинили злочин у віці від 50 до 65 років та 2 особи у віці від 16 до 18 років.

Також суттєве значення для характеристики особистості злочинця мають відомості про його соціальний стан і рід занять. Так 56,8 % (42 особи) були працездатні, які не працювали і не навчалися; далі йдуть лікарі, фармацевти – 8 (10,8 %); робітники – 4 (5,4 %) особи; службовці – 3 (4,1 %) особи; військовослужбовці та пенсіонери, у т.ч. інваліди – по 2 (2,7 %) особи; по одній особі – приватні підприємці, учні шкіл, ліцеїв, коледжів, гімназій, студенти навчальних закладів, безробітні, утримувалися в установі виконання покарань, під вартою, інші заняття – 8 (10,8 %).

Важливою характеристикою особистості злочинця є освіта. Найбільше засуджено осіб з повною вищою освітою – 28 (37,8 %) осіб. Далі йдуть особи у яких базова загальна середня освіта – 20 (27,0 %); повна загальна середня – 10 (13,5 %); по 7 (9,5 %) осіб мали базову вищу та професійно-технічну – 7 особи; 2 особи мали початкову загальну освіту.

Варто звернути увагу на те, що кожна четверта засуджена особа є жінка. У 2022 році засуджено 19 (25,7 %) жінок.

Аналіз питомої ваги окремих видів покарань засуджених відносно кількості осіб, судові рішення щодо яких набрали законної сили у звітному періоді вказує, що найбільший відсоток покарань засуджених – це засуджені особи, яких звільнено від покарання з випробуванням. У період з 2013 року по 2022 рік лише у 2018 та 2019 роках кількість покарань у виді штрафу була більше порівняно з кількістю засуджених осіб, яких звільнено від покарання з випробуванням.

Кількість засуджених осіб, яким призначено покарання у виді позбавлення волі, за кримінальні правопорушення, передбачені статтями Розділу XVI КК України, судові рішення щодо яких набрали законної сили у звітному періоді незначна. За період з 2013 по 2022 роки найбільше таких засуджених було у 2022 році – 10 осіб, що складає 10 % від кількості осіб, судові рішення щодо яких набрали законної сили у звітному періоді. Цей показник близький до загального показника, який складає 14,4 % – загальна кількість осіб, судові рішення щодо яких набрали законної сили у звітному періоді в Україні у 2022 році складала 65 795, з яких 9 462 особам було призначено покарання у виді позбавлення волі.

Відповідно до статистичної звітності Національної поліції України у 2022 році кількість кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій зросла на 49,2 % порівняно з 2021 роком (10020 у 2021 році проти 14948 у 2022 році). Найбільше (у 7,5 рази) зросла кількість кримінальних правопорушень, передбачених ст. 361-1 КК України (38 у 2021 році проти 285 у 2022 році), у 4,4 рази – ст. 358 КК України (47 у 2021 році проти 205 у 2022 році), у 3,6 рази – ст. 301-1 КК України (43 у 2021 році проти 154 у 2022 році), у 3,4 рази – ч.3,4 ст. 190 КК України (1928 у 2021 році проти 6591 у 2022 році). При цьому у 6,3 рази зменшилася кількість кримінальних правопорушень передбачених ст. 176 КК України (19 у 2021

році проти 2 у 2022 році), у 2,3 рази – ст. 361-2 КК України (113 у 2021 році проти 49 у 2022 році), у 1,9 рази – ст. 200 КК України (1010 у 2021 році проти 531 у 2022 році).

Варто вказати на значні розбіжності окремих ідентичних показників у статистичних звітах, що готуються Офісом Генерального прокурора України та Національною поліцією України. Так, у 2022 році Офісом Генерального прокурора України обліковано 1371 кримінальних правопорушень, передбачених ст. 361 КК України (Єдиний звіт про кримінальні правопорушення Розділ 2. Кримінальні правопорушення у провадженнях, досудове розслідування у яких здійснюється органами Національної поліції), а у Звіті про результати роботи підрозділів Національної поліції України, цей показник – 1636. Різниця складає 265 кримінальних правопорушень.

Висновки.

У вітчизняному законодавстві на сьогодні не існує чіткого визначення поняття кіберзлочин, кібератака тощо. Серед науковців та практиків також немає єдиного підходу до окреслення підстав віднесення протиправних діянь до таких кримінальних правопорушень. Однозначно до кіберзлочинів відносяться кримінальні правопорушення, передбачені статтями Розділу XVI КК України, статистичні дані про які є в офіційних державних звітах, що готуються Офісом Генерального прокурора України та Державної судової адміністрації України. Аналіз статистичних даних цих звітів дає можливість розкрити рівень, інтенсивність, динаміку, структуру цієї групи кіберзлочинів (кримінальні правопорушення у сфері використання комп'ютерних систем і мереж). Щодо "традиційних" кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів, офіційна державна звітність відсутня. Є лише відомча статистична звітність Національної поліції України, але вона охоплює не всі кіберзлочини, звичайно ж враховує лише віднесені до підслідності Національної поліції України, а також окремі показники значно різняться з аналогічними показниками в державній звітності. Це негативно позначається на можливості запобігання та боротьбі з кіберзлочинністю. Аналіз такої статистичної звітності надав би можливість розробляти на їхній основі організаційно-правові заходи для більш ефективної протидії кіберзлочинності на національному рівні.

Використана література

1. З початку року нейтралізовано майже 4000 кібератак на органи влади та критичну інфраструктуру – (СБУ, 2023). – Радіо Свобода. URL: https://www.radiosvoboda.org/a/news-ataky-sbu-khakery/32621583.html#:~:text=%D0%9D%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8%20%7C%20%D0%9F%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0

2. Війна у цифровому вимірі і права людини. Аналітичний звіт за лютий 2023. URL: https://www.ppl.org.ua/wp-content/uploads/2023/04/%D0%9B%D1%8E%D1%82%D0% B8%D0% B9-2023_%.pdf

3. Хахановський В.Г., Гавловський В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. № 2(33)/2020. С. 99-110.

4. Гавловський В.Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право.* № 2(30)/2019. С. 105-110.

5. Таран О.В., Гавловський В.Д. Організована кіберзлочинність в Україні: проблеми формування офіційної статистики та її аналізу. *Інформація і право*. № 4(39)/2021. С. 193-201.

6. Про ратифікацію Конвенції про кіберзлочинність: Закон України. *Відомості Верховної Ради України (ВВР)*. 2006, № 5-6. Ст. 71. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text

7. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/term/39984 (дата звернення: 26.05.2023).

8. 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.

9. Статистика Офісу Генерального прокурора України. URL: https://old.gp.gov.ua

10. Бутузов В.М. Співвідношення понять “комп’ютерна злочинність” і “злочинність у сфері високих інформаційних технологій” використання. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2010. № 23. С. 302-307.

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

УДК 51.86:659.3

МАЛАХОВ Г.Б., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5333-0666.

ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджено зміст та форми державно-приватного партнерства у сфері кібербезпеки в Україні, актуальність даного напряму у контексті забезпечення кібербезпеки України. Проаналізовано досвід США та ЄС у сфері розвитку державно-приватного партнерства. Запропоновано актуальні напрями вдосконалення державно-приватного партнерства. Сформульовано пропозиції щодо вдосконалення чинного законодавства України щодо такого партнерства у сфері кібербезпеки.*

Ключові слова: *державно-приватне партнерство, шляхи удосконалення, кібербезпека, приватний сектор, інвестиції.*

Summary. *The article examines the content and forms of public-private partnership in the field of cyber security in Ukraine, the relevance of this direction in the context of cyber security of Ukraine. The experience of the USA and the EU in the field of public-private partnership development is analyzed. Actual areas of improvement of public-private partnership are proposed. Proposals for improving the current legislation of Ukraine regarding such a partnership in the field of cyber security have been formulated.*

Keywords: *public-private partnership, ways to improve, cyber security, private sector, investments.*

Постановка проблеми. Сьогодні державно-приватне партнерство (далі – ДПП) визнається як державами, так і недержавними суб'єктами ключовим елементом побудови дійсно ефективної системи кібербезпеки держави. Інтегрованість мереж державного та приватного секторів стає дедалі більш важливою для національної безпеки [1]. Україна максимально сприяє залученню до цього процесу представників приватного сектору, наукових та освітніх кіл, інститутів громадянського суспільства. У рамках ДПП залучаються інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки. Стратегія кібербезпеки України містить згадки про розвиток ДПП.

У той же час, у цій Стратегії серед невирішених питань відзначається відсутність "дієвої моделі державно-приватного партнерства" у сфері кібербезпеки [2]. Також зазначається, що невирішеними залишаються питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів, що вказано як недолік попередньої Стратегії кібербезпеки 2016 року[2].

Результати аналізу наукових публікацій. Серед авторів наукових праць з питань розвитку ДПП слід зазначити таких українських науковців: В. Григоренко [3], Ю. Заскока [4], А. Марушак [5], А. Сороченко, В. Панченко [5], Р. Прав, Н. Ткачук [6], Б. Шулюк, В. Воротін, Я. Ізмайлов, І. Єгорова, Н. Малиновська, О. Крутій, О. Радченко, В. Козлов, Ю. Шимов, О. Федорчак, О. Кравченко та інші.

Спроба розпочати в Україні більш широку дискусію з цього питання, висвітлюючи, з одного боку, вже наявний досвід окремих західних держав у сфері побудови ДПП,

а з іншого – ключові українські проблеми в контексті створення КДПП, міститься в аналітичній доповіді “Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України” [1].

Значний внесок у розв’язання проблеми ДПП зробили зарубіжні вчені, серед яких слід виділити праці С. Ліндера [7], В. Коувенховена [8] та А. Ягасія [9].

Аналіз різних аспектів механізму державно-приватного партнерства, особливостей його становлення і розвитку в розвинутих країнах світу, також проводиться міжнародними організаціями і аналітичними центрами, серед яких слід виділити діяльність: Європейської економічної комісії ООН, Європейського інвестиційного банку, Міжнародної фінансової корпорації, Українського центру сприяння розвитку публічно-приватного партнерства, а також Національного інституту стратегічних досліджень, тощо. Проведений аналіз свідчить, що більшість досліджень механізму ДПП присвячені його економічній складовій і проводяться дослідниками у сферах культури, надання послуг, інфраструктурній галузі та інших [4].

Водночас, не достатньо дослідженими залишаються проблеми законодавчого, методичного та експертного забезпечення державно-приватного партнерства в сфері кібербезпеки України. Дискусійним залишається і питання того, в яких конкретно формах може реалізовуватись “справжнє” ДПП – тут так само відчувається брак методологічних напрацювань [1, с. 7]. Недостатніми є й організація і проведення наукових досліджень у сфері кібербезпеки. Ці обставини зумовлюють актуальність цієї статті.

Метою статті є удосконалення державно-приватного партнерства на базі аналізу нормативно-правової бази із забезпечення кібербезпеки, а також зарубіжного досвіду у цій сфері в контексті створення дієвої моделі такого партнерства.

Виклад основного матеріалу. Історичний тренд щодо участі приватного сектору в житті держави виник ще у кінці 70-х років XX ст. у країнах Заходу, що було пов’язано із глобальною економічною кризою того часу. І якщо перші проекти ДПП стосувалися передусім розвитку інфраструктури міст, екологічних проектів, охорони здоров’я та освіти, то в подальшому кількість сфер, до яких застосовується поняття ДПП, розширилось за рахунок нових або невідомих раніше форм співробітництва між державою та приватним сектором [7; 10].

Найбільш неоднозначним стало проникнення ДПП до сфери забезпечення державної безпеки, тобто туди, де держава традиційно зберігала свою монополію. Щоправда така монополія завжди була досить умовною: майже в усі періоди історії людства існували приклади специфічних державно-приватних відносин у сфері національної безпеки, однією з яких є відносини із забезпечення кібербезпеки [1, с. 6].

Ключове розуміння ДПП концентрується навколо мети та характеру такого партнерства.

Стівен Ліндер (Stephen Linder) характеризує цілі такого партнерства таким чином: “Метою ДПП є використання синергії у спільному інноваційному використанні ресурсів та застосуванні управлінських знань задля оптимального досягнення цілей усіх залучених сторін, якщо ці цілі не могли бути досягнуті без залучення цих сторін” [11]. Крім того, він слушно зазначає, що в межах ДПП обидві сторони, для забезпечення успішності партнерства, мають змінювати характер свого мислення – суб’єкти ДПП змушені думати та діяти як їх партнери, тобто державні учасники мають думати та діяти як підприємці, в т.ч. як бізнес має враховувати суспільний інтерес, і очікувати, що їм доведеться бути більш підзвітними громадськості [12].

Інший дослідник Вінсент Коувенховен (Vincent Kouwenhoven) конкретизує, що ДПП є неможливим без: взаємної довіри та встановлення обмежень, спрямованих на

недопущення зловживань; наявності чітких, недвозначних цілей та стратегії, яка зафіксована у документальному вигляді; чіткого розподілу ризиків; відповідальності, повноважень, а також функцій забезпечення партнерських бізнес-інтересів [8].

Доповнює цей підхід Арнав Ягасія (Arnav Jagasia), який вважає, що партнери мають ідентифікувати та визначити (detect) поведінку, яка викликає занепокоєння; учасники партнерства мають переконатися, що учасники – як від державного, так і приватного сектору – повністю погоджуються із засадами (standards) партнерства; ДПП має запропонувати механізм відповіді на ситуації після кіберзагроз (це включає аналіз атаки та виявлення рішень для обов'язкового вирішення уразливостей в атакованих системах) [9].

Водночас кібербезпекова сфера має свої унікальні аспекти, які ще не достатньо досліджені та не мають універсальних "рецептів" рішень (більше того, можливо, вони взагалі їх не мають) [1, с. 8]. Американська дослідниця М. Карр (Madeline Carr) звертає увагу, що навіть у США, де майже 15 років ДПП визначалось як ядро (cornerstone) національної системи кібербезпеки, сторонам так і не вдалося визначити параметри, характер та масштаби такого співробітництва [13].

Дискусійним залишається питання й про форми такої взаємодії, характер спільних дій, їх методологічне та організаційне забезпечення. Не менш дискусійним є питання, в яких саме сферах кібербезпеки може взагалі застосовуватись ДПП. Американські вчені виділяють чотири ключові сфери: 1) крадіжка даних у мережі (online identity theft); 2) індустріальне кібершпигунство; 3) захист критичної інфраструктури; 4) ботнети [14].

На думку українських дослідників, говорячи про таке партнерство, частіше за все мають на увазі дві макросфери: економіку в цілому (від якої залежить процвітання держави та її громадян) та критичну інфраструктуру (від роботи якої часто залежить безпека і держави, й її громадян). І перша, і друга сфери абсолютно переважно перебувають у руках приватних власників, але якщо кібератака на економічну міць держави матиме переважно фінансові наслідки, то кібератака на критичну інфраструктуру може призвести до людських жертв [1, с. 8].

При цьому є низка факторів, які є спільними для структур обох секторів, які можуть стати аргументом для формування ефективної моделі ДПП: організації мають негативний досвід бути атакованими і тепер хочуть усунути вразливості; організації розуміють, що вони дублюють зусилля; організації визнають, що існує недостатня координація чи/та обмін інформацією в певних секторах; організації визнають наявність провалів у забезпеченні всіх етапів життєвого циклу безпеки; організації визнають, що загрози розвиваються разом із подальшим злиттям комунікацій та інформаційних технологій, а отже, потребують спільної відповіді, а не розподіленої по окремих секторах; організації визнають злиття загроз від тероризму та кібератак; організації визнають, що загрози еволюціонують та зміщуються з національного/секторального рівня на міжнародний; спостерігається брак довіри між конкурентами в межах географічних, секторальних або тематичних сфер, а отже, існує потреба у створенні довіреної структури для вирішення цієї проблеми [1, с. 12].

Важливим компонентом посилення спроможностей держави у сфері забезпечення кібербезпеки є саме побудова конструктивного діалогу у форматі державно-приватного партнерства [3, с. 156]. Користь від спільної робити з кібербезпеки взаємна як для державного, так і приватного секторів.

Візьмемо як приклад досвід США, оскільки саме ця країна є піонером у галузі ДПП. Так як приватний сектор контролює більшу частину критичної інфраструктури США, що часто є привабливою для дій кіберзлочинців, багато приватних компаній уже

мають програми з кібербезпеки, володіють спеціальними знаннями та досвідом у вирішенні потенційних загроз. Державний сектор, зі свого боку, має ширші можливості для розслідування кіберзлочинів та переслідування кіберзлочинців [1, с. 15].

Уперше питання необхідності спільного з приватним сектором захисту кіберпростору було висвітлено у Директиві про рішення Президента США "Про захист критичної інфраструктури" № 63 (Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD) від 1998 р., де визначено захист критичної інфраструктури та ключових ресурсів (CIKR) як національну ціль, реалізація якої уможливила співпрацю між урядом та приватним сектором з метою захисту кіберсистем [15].

Відповідно до цієї Директиви, для кожного з основних секторів економіки, які є вразливими до інфраструктурної атаки, федеральний уряд призначає представника сектору для зв'язків з приватним сектором (Sector Liaison Offi cial), який після обговорення та узгодження з суб'єктами приватного сектору визначає Координатора сектору (Sector Coordinator) для представлення приватного сектору. Разом ці дві особи, а також відомства та корпорації, які вони представляють, сприяють розробленню галузевого плану національної інфраструктури шляхом: оцінки вразливості сектору до кібер- або фізичних атак; надання рекомендацій щодо усунення вразливості; пропозиції щодо системи виявлення та запобігання спробам потужних атак; розроблення плану для оповіщення про атаки, з подальшим швидким відновленням мінімально необхідного потенціалу після атаки [1, с. 15-16].

Цією ж Директивою в рамках національної системи попередження та обміну інформацією з питань кібербезпеки в межах ФБР був створений Центр захисту державної інфраструктури (National Infrastructure Protection Center, NIPC), функцією якого є оцінка загроз, попередження, виявлення вразливостей державної критичної інфраструктури та сприяння правоохоронним органам у розслідуванні та реагуванні кіберінцидентів [1, с. 22]. Крім того, цей Центр встановлює партнерські відносини безпосередньо з компаніями приватного сектору та зі структурами з обміну та аналізу інформації, які створені приватним сектором.

Більшість обмінів інформацією приватного сектору проводяться за допомогою центрів обміну та аналізу інформації, які створюються як неприбуткові організації, і являють собою ресурс для збору інформації про кіберзагрози для об'єктів критично важливої інфраструктури та забезпечення двостороннього обміну інформацією між приватним та державним сектором [1, с.19]. Ключовим напрямом діяльності є двосторонній обмін інформацією: партнери надають індикатори зафіксованих кіберзагроз та інформацію про кіберінциденти та виявлені вразливі місця Міністерству внутрішньої безпеки США [1, с. 20].

Позитивним прикладом сучасних моделей паритетної взаємодії державного та приватного секторів у сфері забезпечення кібербезпеки є створення на базі Департаменту внутрішньої безпеки США автоматизованої програми відстеження кіберзагроз, яка надає змогу забезпечити автоматизований обмін інформацією між державним і приватним секторами [3, с. 158].

Також у США з метою прогнозного супроводження діяльності державних інституцій та приватного сектору у сфері забезпечення кібербезпеки створено некомерційний дослідний центр "TechAmerica Foundation", який об'єднує фахівців та експертів 1200 компаній з метою визначення орієнтовно-планових обсягів щорічного фінансування кібероборони, при цьому акценти діяльності постійно передбачають значне збільшення витрат виходячи із потенційних та реальних кіберзагроз [3, с. 158].

Окремим документом, що фіксує процедури співпраці між приватними компаніями та урядовими установами у сфері інформаційної безпеки є "Акт про обмін інформацією у сфері кібербезпеки" (Cybersecurity Information Sharing Act, CISA), затверджений Конгресом наприкінці 2015 р. [16]. Відповідно до нього організації, які на добровільній основі обмінювалися інформацією про кіберзагрози між собою і Федеральним урядом, отримали право обмеженої відповідальності. Документ надає додатковий захист компаніям, що добровільно вирішили ділитися даними про кіберзагрози з урядовими установами [1, с. 19].

Цікавим видається досвід ЄС у цій площині. На рівні ЄС метою ДПП є створення платформи для кібербезпеки різних секторів (таких як енергетика, охорона здоров'я, транспорт та фінанси, а також включення у цей процес органів влади, науково-дослідних центрів та інших зацікавлених сторін), яка розвивала б дослідницький та інноваційний потенціал приватного сектору [1, с. 23].

Основою ініційованого Європейською Комісією загального плану дій слугують: Стратегія єдиного цифрового ринку 2015 р. (Digital Single Market Strategy for Europe) [17], Кіберстратегія Європейського Союзу 2013 р. (Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace) [18] та Директива ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems) [19]. Невипадково у стратегічних документах ЄС з кібербезпеки неодноразово наголошується на важливості розбудови державно-приватного партнерства в боротьбі з кібератаками і кіберзлочинністю [3, с. 159].

Ухвалена у 2013 р. Європейська стратегія кібербезпеки визначила головні напрями політики Європейського Союзу у сфері забезпечення безпеки кіберпростору [20].

Відповідно до цієї Стратегії Європейська Комісія запропонувала перший всеосяжний елемент законодавства ЄС щодо кібербезпеки [1, с. 24] – Директиву ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems), ухвалену Європейським Парламентом 6 липня 2016 р., яка набрала чинності в серпні 2016 р. [21].

Ця Директива передбачила створення координаційного механізму реагування держав-членів у співпраці з приватним сектором на погрози та власне самі кібератаки, тим самим сприяючи стратегічному співробітництву та обміну інформацією і підтримуючи рівень довіри між учасниками процесу. Комісія також запустила державно-приватну платформу на рівні ЄС – т.зв. платформу мережевої та інформаційної безпеки (Network and Information Security public private Platform) для визначення ефективної практики кібербезпеки з метою сприяння подальшому впровадженню Директиви [1, с. 24-25].

На основі узагальнення здобутків зарубіжного досвіду ДПП у сфері забезпечення кібербезпеки можна виділити такі його складові: основною його метою є побудова конструктивного діалогу та плідної співпраці, реальна довіра між приватним сектором та державними інституціями; заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу [3, с. 160].

Досвід США та ЄС у цій сфері є корисним для України, органи влади якої постійно працюють над кібербезпекою на національному та міжнародному рівні. Наша країна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини,

Забезпечення розвитку державно-приватного партнерства у сфері в кібербезпеки є одним з пріоритетних завдань національної політики України.

На національному рівні під пріоритетними завданнями державно-приватного партнерства в сфері кібербезпеки, як правило, розуміють розширення взаємодії держструктур з приватними науковими установами, громадськими об'єднаннями та волонтерським організаціями, в тому числі в підготовці кадрів, а також підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі [4]. З цього приводу СБУ зазначає, що "державно-приватна взаємодія є одним з головних принципів забезпечення кібербезпеки держави, який передбачає широку співпрацю з громадянським суспільством у сфері кібербезпеки і кіберзахисту. …Вказаний принцип ґрунтується на спільній відповідальності держави та приватного сектору за стан забезпечення кібербезпеки, що передбачає передачу приватному партнеру частини ризиків, а також внесення останнім відповідних інвестицій у сферу забезпечення кібербезпеки держави. Принцип державно-приватної взаємодії, в першу чергу, спрямований на підвищення ефективності діяльності як державних, так і недержавних суб'єктів у сфері забезпечення кібербезпеки за умов їх належної співпраці, а також посилення спроможностей національної системи кібербезпеки України" [22].

Нова Стратегія кібербезпеки України визначає пріоритети забезпечення кібербезпеки України та стратегічні цілі, що мають бути досягнуті протягом періоду реалізації цієї Стратегії. Зазначається, що для формування потенціалу стримування (С) необхідним є досягнення стратегічних цілей, серед яких виділяється ціль С.4. "Розвиток асиметричних інструментів стримування" – "Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору" [2].

Для досягнення цієї цілі Україна має запровадити асиметричні інструменти стримування шляхом: врегулювання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі; розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі; 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; проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів [2].

У Стратегії передбачається, що для досягнення стратегічних цілей Україна у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі, шляхом врегулювання на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері [2].

Основні шляхи державно-приватного партнерства у сфері в кібербезпеки визначені у ст. 10 Закону України "Про основні засади забезпечення кібербезпеки України", де згадується: 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; 2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства

щодо кіберзагроз та кіберзахисту; 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події; 5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 6) надання консультативної та практичної допомоги з питань реагування на кібератаки; 7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки; 9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; 10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі [23].

З приводу останнього слід зауважити, що в Україні на ринку кібербезпеки діє досить багато асоціацій, ІТ-компаній, структур громадянського суспільства, які мають значний досвід і техніко-технологічні напрацювання в зазначеній сфері, надають послуги з виявлення комп'ютерних атак, розслідування обставин виявлених інцидентів, формування доказів при виконанні обстеження комп'ютерних систем і проведенні комп'ютерних експертиз. Чимало вітчизняних ІТ-компаній, які посіли міцні позиції в зазначеній сфері, не тільки демонструють високу ефективність, напрацювали багаторічний досвід, мають значний штат компетентних фахівців та експертів необхідної кваліфікації, але й проявляють зацікавленість у розширенні своєї діяльності, опануванні нових сегментів ринку послуг кібербезпеки [3, с. 160].

Як у Законі України "Про основні засади забезпечення кібербезпеки України", так і в Стратегії кібербезпеки України держава декларує готовність до системної роботи щодо розвитку ДПП у сфері забезпечення кібербезпеки.

Іншим важливим законодавчим актом є Закон України "Про державно-приватне партнерство", за змістом якого проекти ДПП повинні відповідати таким основним критеріям: 1) мати довготривалий характер (понад п'ять років); 2) передбачати передання приватному партнеру частини ризиків у процесі реалізації проектів; 3) мати вищі техніко-економічні показники ефективності, ніж у разі реалізації без участі приватного партнера [24]. Але, на жаль, сфера забезпечення кібербезпеки у зазначеному законі не фігурує в переліку сфер застосування ДПП (стаття 4). Не достатньо визначеними залишаються й форми такої взаємодії.

Серед основних форм реалізації ДПП виділяються: контракти на виконання визначених робіт і надання послуг, взаємне консультування, інформаційний обмін, спільне ведення баз даних, незалежна експертиза проектів нормативно-правових актів, підготовка і внесення спільних пропозицій щодо реалізації державної політики в кіберпросторі, захисту внутрішнього ринку ІТ-послуг, державну підтримку підприємств ІТ-бізнесу, інформаційне забезпечення державних і комерційних підприємств, громадських об'єднань і громадян з питань забезпечення кібербезпеки тощо. Інструменти ДПП можуть бути ефективно задіяні для залучення приватних інвестицій у фінансування високобюджетних проектів [4]. До речі, зарубіжний досвід свідчить, що державно-приватні інвестиції активно спрямовуються на дослідницькі програми щодо

розробки інструментів та прототипів у сфері посилення кіберзахисту та його складових [3, с. 160].

Певні елементи удосконалення ДПП містяться в проєкті Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" (реєстр. № 8087 від 29.09.2022 р.). Зокрема, положення проекту передбачають створення національної системи реагування на інциденти кібербезпеки, зміст якої передбачає: порядок надання приватними командами реагування послуг з управління інцидентами кібербезпеки для операторів критичної інфраструктури, органів державної влади та місцевого самоврядування; взаємодію в установленому порядку з суб'єктами приватного сектору, в тому числі, з іноземними суб'єктами господарювання, з питань реагування; закріплення обов'язку операторів критичної інфраструктури повідомляти про всі значні інциденти кібербезпеки, кібератаки щодо об'єктів критичної інформаційної інфраструктури [25].

Серед ключових напрямів у сфері ДПП СБУ відповідно до своєї компетенції виділяє: надання власникам та операторам критичної інфраструктури інформації щодо виявлення кібератак та/або кіберінцидентів, вразливостей власних систем кіберзахисту; розроблення організаційно-правових засад та безпосереднє залучення фахівців приватного сектору (в т. ч. хактивістів) до проведення негласних перевірок готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів; організація на базі провідних ІТ-компаній тренінгів та навчальних програм з підвищення кваліфікації для фахівців СБ України; забезпечення виконання операторами та провайдерами телекомунікацій положень Конвенції РЄ про кіберзлочинність у частині термінового збереження та надання на вимогу компетентного правоохоронного органу даних, необхідних для протидії кіберзлочинності [22].

На сьогодні проблемним питанням залишається відсутність ефективного правового механізму щодо отримання в інтересах забезпечення національної безпеки від операторів та провайдерів телекомунікацій комп'ютерних даних, необхідних для своєчасного реагування на кіберзагрози, у т.ч. попередження і локалізації кіберінцидентів та кібератак на критичну інформаційну інфраструктуру [6, с. 106].

Висновки.

ДПП визнається як ключовий елемент кібербезпекової системи держави, який вимагає максимального ресурсного забезпечення. Хоча більшість розвинених країн мають тією чи іншою мірою працюючі форми ДПП, однак майже в кожному випадку вони формуються у режимі ad-hoc і під значним впливом історичного досвіду кожної конкретної країни. Зокрема, позитивним вбачається законодавчий досвід США у площині взаємного обміну інформацією про кіберзагрози між урядом та приватним сектором. У ЄС у межах пошуку ефективних форм ДПП проводяться програми консультацій з великим, малим та середнім бізнесом, асоціаціями, дослідницькими інституціями, громадським сектором, органами державної влади та органами регіонального рівня, що може стати основою відповідного процесу, якого потребує Україна [1, с. 71].

Питання створення загальнонаціональної системи ДПП все ще залишається надзвичайно складним. ДПП потребує удосконалення в контексті створення дієвої моделі державно-приватного партнерства у сфері кібербезпеки. Серед актуальних напрямів розвитку ДПП доцільно виділити:

- формування довіри приватного сектору до державних суб'єктів забезпечення кібербезпеки в контексті створення основи для "обміну інформацією", контролю за інформацією з обмеженим доступом;

- ініціювання проектів, які б могли розвивати ДПП в нашій країні, у т.ч. активізація залучення інвестицій у цивільний сектор кібербезпеки, покращення фахової підготовки спеціалістів у цій сфері, спільної діяльності щодо організації дієвого кіберзахисту [3, с. 161], залучення експертів до розслідування кіберінцидентів;
- створення стратегії ДПП у сфері забезпечення кібербезпеки, зміст якої передбачатиме: формування цілей ДПП (як для держави, так і приватного сектору); визначення критеріїв, за яких ДПП стане привабливим рішенням для обох сторін; здійснення системних заходів, спрямованих на посилення довіри учасників ДПП один до одного; допомога з боку неурядових структур та науково-експертного співтовариства обом сторонам у формуванні довгострокових стратегій такого партнерства; пошук ефективних підходів до визначення ризиків для кожної із сторін, а також відповідальності сторін;
- реалізація законодавчо визначених (ст. 10 Закону України "Про основні засади забезпечення кібербезпеки України") шляхів державно-приватного партнерства у сфері в кібербезпеки;
- визначення взаємовідношення державно-приватного партнерства та державно-приватної взаємодії у сфері кібербезпеки. Зокрема, чи є така взаємодія різновидом державно-приватного партнерства, та відповідно, чи підпадає під дію Закону України "Про державно-приватне партнерство" [6, с. 109]; у разі такого визнання внесення до переліку сфер застосування державно-приватного партнерства, визначених у статті 4 цього Закону сферу кібербезпеки та кіберзахисту [1, с. 76; 6, с.109];
- механізми та процедури галузевого регулювання захисту об'єктів кібербезпеки з врахуванням можливості ДПВ у цій сфері (зокрема, запровадження недержавних галузевих регуляторів, що довело свою ефективність у міжнародних практиках) [1, с. 76].

Реалізації зазначених напрямів сприятиме розвиток дискусій між обома сторонами партнерства із залученням фахівців та науковців у цій сфері.

Використана література

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberb ezpeka.pdf

2. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 19.09.2023).

3. Григоренко В.А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. *Інформація і право*. № 2(37)/2021. С.155-161.

4. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи*. 2021. № 9 (15). URL: http://perspectives.pp.ua/index.php/np/article/view/467/470

5. Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. *Інформаційна безпека людини, суспільства, держави*. 2014. № 3(16). С. 58-59.

6. Ткачук Н.А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки. *Інформація і право*. 4(27)/2018. С. 104-111. URL: https://ippi.org.ua/tkachuk-na-pravove-regulyuvannya-vza%D1%94modii-sluzhbi-bezpeki-ukraini-z-privatnim-sektorom-u-sferi-zabe

7. Linder S. Coming to terms with the Public-Private Partnership – A grammar of multiple meanings. Public-Private Policy Partnerships / P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge MA, 2000. P. 19-36.

8. Kouwenhoven V., Public-Private Partnership: A model for the management of Public-Private cooperation Modern Governance / J. Kooiman (Ed.). New Government-Society Interactions, Sage, London, 1993. P. 119-130.

9. A Look into Public Private Partnerships for Cybersecurity. URL: https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

10. Cavelty Myriam Dunn, Suter Manuel. Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. December, 2009. Vol. 2, Is. 4. P. 179-187.

11. Linder S., Vaillancourt P. Rosenau, Mapping the terrain of the Public-Private Policy Partnership. Public-Private Policy Partnerships. P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge, MA, 2000. P. 1-19.

12. Linder, S. H. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings. *American Behavioral Scientist*. 1999. № 43(1). P. 35-51. DOI: 10.1177/0002764992195 5146.

13. Madeline Carr. Public-Private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

14. Moore T. Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. URL: https://www.nap.edu/read/12997/chapter/3

15. Presidential Decision Directive/NSC-63. URL: https://fas.org/irp/off docs/pdd/pdd-63.htm

16. Cybersecurity Information Sharing Act of 2015. URL: https://www.congress.gov/bill/114 thcongress/senate-bill/754/text

17. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions. URL: http://eur-lex. europa.eu/legal-content/EN/ TXT/?uri=celex%3A52015DC0192

18. Повідомлення про стратегію кібербезпеки Європейського Союзу – відкритий та безпечний кіберпростір. URL: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-europeanunion-%E2 %80 %93-open-safe-and-secure-cyberspace

19. Директива про захист мережевих та інформаційних систем (Директива щодо ННД) URL: https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

20. Стратегія кібербезпеки Європейського Союзу: відкритий та безпечний кіберпростір. URL: http://eur-lex.europa.eu/procedure/EN/202369

21. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 року щодо заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

22. Лист Служби безпеки України № 30/5/2-3288 від 05.03.18 р. на запит НІСД № 293/54 від 31.01.18 р.

23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19

24. Про державно приватне партнерство: Закон України від 01.07.10 р. № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text

25. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт Закону України (реєстр. № 8087 від 29.09.2022 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 (дата звернення: 19.09.2023).

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

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.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПИТАННЯХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *Визначено роль та значення штучного інтелекту у сфері забезпечення кібербезпеки та деталізовано методи його використання. Визначено переваги та пріоритети використання штучного інтелекту у сфері кібербезпеки. Узагальнено недоліки та вади, пов'язані із застосуванням хакерами технологій штучного інтелекту у сфері кібербезпеки. Висвітлено інноваційні здобутки практичного впровадження технологій генеративного штучного інтелекту ChatGPT (Generative Pre-trained Transformer). Окреслено правові засади регулювання штучного інтелекту у сфері кібербезпеки в Україні. Визначено загрозливі тенденції використання технологій штучного інтелекту на підставі звіту Європолу 2023 року. Проведено огляд законодавчих ініціатив ЄС, спрямованих на врегулювання сфери штучного інтелекту, зокрема, й у питаннях забезпечення кібербезпеки. Узагальнено шляхи удосконалення правових засад щодо використання технологій штучного інтелекту у сфері кібербезпеки, особливо в умовах правового режиму воєнного стану в Україні.*

Ключові слова: *штучний інтелект, кібербезпека, кібератака, кіберзагроза, національна безпека, інформаційні технології, машинне навчання.*

Summary*. The role and importance of artificial intelligence in the field of cyber security is determined. The methods of using artificial intelligence in cyber security are detailed. The advantages and priorities of the use of artificial intelligence in the sphere of cyber security are defined. The shortcomings and problematic issues related to the use of artificial intelligence technologies by hackers in the field of cyber security are summarized. The innovative achievements of the practical implementation of generative artificial intelligence technologies ChatGPT (Generative Pre-trained Transformer) are highlighted. The legal principles of the regulation of artificial intelligence in the field of cyber security in Ukraine are outlined. Threatening trends in the use of artificial intelligence technologies have been identified based on the Europol report 2023. A review of the legislative initiatives of the EU aimed at regulating the field of artificial intelligence, in particular in the issue of cyber security, was conducted. The directions of improvement of the legal framework and regulatory requirements regarding the use of artificial intelligence technologies in the field of cyber security are summarized, especially in the conditions of the legal regime of martial law in Ukraine.*

Keywords: *artificial intelligence; cybersecurity; cyberattack; cyberthreat; national security; information technology, machine learning.*

Постановка проблеми. Динамічний розвиток сучасних передових технологій, зростаюча суцільна залежність від Інтернету провокують постійний ризик появи нових кіберзагроз. В сучасних умовах актуалізується проблематика поширення та впровадження у сфери життєдіяльності людства ноу-хау – інноваційних технологій штучного інтелекту(далі – ШІ). ШІ стає однією із важливих технологій, поява яких вже змінила чимало сфер людського життя. У сфері комп'ютерних наук ШІ означає здатність машин виконувати завдання, для яких, зазвичай, вимагається наявність людського інтелекту. Сюди відносяться такі завдання, як розпізнавання мови, вирішення технологічних проблем

та схвалення оперативних рішень. Аналізуючи великі обсяги інформації та даних, алгоритми ШІ можуть розпізнавати закономірності, з'ясування яких дасть їм змогу згодом покращувати свою роботу. Існують різні види ШІ, кожен з яких володіє унікальними властивостями та обмеженнями, які засвідчують його у якості інноваційної технології.

Штучний інтелект – це швидкозростаюча сфера публічного інтересу та інвестицій, яка все активніше використовується для покращення аналізу, прогнозування та захисту від кіберзагроз. Завдяки технологіям ШІ стає можливим відстежувати кіберзагрози, моніторити, прогнозувати й моделювати ситуацію у кіберпросторі, вчасно реагувати на кіберінциденти. На фоні динамічного розвитку інноваційних технологічних рішень, ШІ досить широко застосовується для посилення кібербезпеки, виявлення та ліквідації загроз, посиленого захисту від кібератак, сприяє прийняттю виважених та скоординованих управлінських рішень. У відповідь на зростаючу стурбованість світової спільноти у цій площині, останнім часом, саме технології ШІ відіграють дедалі більш важливішу роль у питаннях посилення захисту цифрового світу, зокрема, персональних даних, забезпечення кібербезпеки. Загальноприйнятою у світі є позиція про те, що ШІ у сфері кібербезпеки стає дедалі більш важливою складовою останньої у міру розвитку глобального цифрового ландшафту. Розширюючи інструментарій та можливості виявлення й запобігання кіберзагрозам, автоматизуючи рутинні завдання та значно скорочуючи час для реагування на кіберінциденти, технології ШІ допомагають захиститися від кібератак, нівелюючи загрозливі тенденції у цьому сегменті. В умовах правового режиму воєнного стану проблематика використання та застосування ШІ у сфері кібербезпеки набуває неабиякої актуальності та потребує окремого розгляду.

Результати аналізу наукових публікацій. Доцільно вказати, що деякі теоретичні та практичні питання використання ШІ у кібернетичній сфері в Україні та зарубіжних державах раніше вже розглядалися у науковій літературі. Так, наприклад, технічну компоненту та особливості використання систем ШІ в контексті забезпечення кібербезпеки розглядали у своїх наукових працях: О. Неретін та В. Харченко [1], В. Савченко та О. Шаповаленко [2], І. Стьопочкіна та О. Новіков [3]. Перспективні можливості ШІ як важливого механізму автоматизованої та негайної реакції на розвиток та модифікацію кіберзагроз вивчав С. Шаров [4]. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій ШІ у кібербезпеці здійснював С. Цяпа [5]. У зарубіжній науковій літературі роль та значення ШІ у сфері кібербезпеки та подальші шляхи його розвитку досліджували: Т. Сіпола [6], Р. Мостіну [7], Р. Дас та Р. Сандхейн [8].

Проте питання використання ШІ у сфері кібербезпеки недостатньо досліджено на науковому рівні. Особливо це відчувається в умовах появи у листопаді 2022 року феномену генеративного ШІ – ChatGPT та триваючого (протягом останніх 18 місяців) правового режиму воєнного стану, що актуалізує тематику цієї наукової статті.

Метою статті є визначення ролі та значення, переваг і недоліків штучного інтелекту у питаннях посилення стану кібербезпеки, особливостей використання штучного інтелекту у сфері кібербезпеки, регламентації подальших шляхів удосконалення законодавчого забезпечення кібербезпеки.

Виклад основного матеріалу. В сучасних умовах кібербезпека безпосередньо пов'язана із стрімким розвитком Інтернет технологій, сервісів та додатків. Кібербезпека напряму захищає цифрові системи та мережі від несанкціонованого доступу, а ШІ може значно підвищити кібербезпеку, автоматизуючи виявлення загроз та реагуючи на них. За оцінками міжнародних експертів, світовий ринок продуктів кібербезпеки на базі ШІ

сягатиме $133,8 млрд. до 2030 року. ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків, знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки. Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей та слабких місць в системах та мережах, що надає змогу упереджено та завчасно ліквідувати їх. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз.

Одним із основних способів використання ШІ у кібербезпеці є розробка передових алгоритмів, які допомагають виявляти та запобігати кібератакам. Ці алгоритми призначені для структурного аналізу великих обсягів даних та виявлення закономірностей, які можуть вказувати на реальну або потенційну загрозу. Обробляючи цю інформацію зі швидкістю та масштабами, які фізично не можливі для людини, системи ШІ можуть швидко виявляти потенційні та реальні кіберзагрози, вчасно реагувати на них, таким чином значно знижуючи ризики здійснення кібератак та її наслідки. Крім того, ШІ може використовуватися з метою автоматизації рутинних завдань кібербезпеки, чим значно спрощує роботу ІТ-спеціалістів на усіх рівнях. Системи на базі технологій ШІ можуть автоматично сканувати мережі на наявність уразливостей, виявляти загрози та навіть схвалювати заходи щодо зниження ризиків, наприклад, виправлення програмного забезпечення або блокування шкідливих IP-адрес. Цей рівень автоматизації не тільки підвищує ефективність, але й допомагає забезпечити послідовне його використання у питаннях забезпечення кібербезпеки.

Ще одна сфера, де ШІ значно впливає на кібербезпеку – структуризація інтелектуальної та оперативної інформації про кіберзагрози. Використовуючи методи машинного навчання, системи ШІ можуть оперативно аналізувати великі обсяги даних з різноманітних джерел, таких як: месенджери, соціальні мережі, е-публікації, телеграм-канали, дарк веб-форуми з метою виявлення загрозливих тенденцій та уразливостей. Цей аналіз у режимі реального часу надає змогу залишатися на крок попереду та розробляти й адаптувати стратегії кібербезпеки з метою прогнозування ситуацій та ризиків. Також з метою виявлення та запобігання кіберзагрозам, ШІ досить широко використовується для розширення можливостей реагування на кіберінциденти. За наслідками кібератак важливим є стримання та недопущення масштабування збитків і попередження подальших порушень штатного режиму роботи комп’ютерної техніки та систем. Саме завдяки технологіям ШІ можливо проаналізувати характер та властивості кібератаки, визначити ступінь уразливості системи та окреслити оптимальний перелік заходів оперативного реагування з метою локалізації та вирішення проблеми. Це надає сприятливі можливості, які дозволяють значно зменшити негативний вплив від кібератак та їх наслідків на штатний режим роботи інформаційно-комунікаційних систем, діяльність та репутацію державних органів, установ й організацій приватного сектору.

Однією із вагомих переваг використання ШІ є його здатність швидко та оперативно аналізувати великі обсяги даних. ШІ може швидко проаналізувати масиви даних, які би людина не змогла опрацювати за короткий проміжок часу. Це надає можливість завчасно виявляти загрози та оперативно схвалювати рішення з метою їхнього попередження та недопущення. Використання ШІ також допомагає автоматизувати процеси виявлення та реагування на кібератаки. ШІ може безперервно у режимі 24/7 моніторити мережу та виявляти аномальну поведінку, яка у свою чергу, може свідчити

про кібератаку. Крім того, ШІ може автоматично реагувати на загрози, блокуючи доступ хакерів до систем та запобігати витоку конфіденційних даних.

Ще одним важливим аспектом використання ШІ у кібербезпеці є його здатність до машинного навчання на підставі набутого досвіду. ШІ може використовувати дані про попередні кібератаки з метою покращення своїх алгоритмів та забезпечення більш точного виявлення ризиків та загроз у майбутньому. ШІ дозволяє гарантувати ефективний захист від автоматичних або скерованих кібератак. Цілком логічно розуміти той факт, що ШІ є важливим та ефективним інструментом для боротьби із кіберзагрозами, проте він, на наше переконання, повністю не може замінити людський фактор. Хоча деякі науковці помилково стверджують, що інтелектуальні системи позбавлені недоліків людського фактора: вони працюють швидше і помиляються значно рідше людей, що дозволяє практично повністю виключити людей з процесів забезпечення захисту і залишає їм допоміжні функції моніторингу та корекції [9, с. 66]. Дійсно, ШІ може допомогти автоматизувати процеси виявлення та реагування на кіберзагрози, проте вважаємо, що схвалення остаточного рішення про безпеку та гарантії її дотримання все ж належить виключно людині. Тобто ШІ у питаннях кібербезпеки значно допомагає, проте не здатний бути альтернативою та абсолютно замінити людський фактор. ШІ надає змогу розширювати масштаби та швидкість кібербезпеки, створюючи ефективний захист від кібератак та кіберзагроз.

Алгоритми ШІ можуть стати революційним підходом щодо виявлення нових кібератак, сприяти посиленню захисту систем, прогнозувати ситуації навколо поширення нових уразливостей, розробляти нові більш складні методи захисту від шкідливих програм тощо. Таким чином, за допомогою ШІ управляти мережевою безпекою стає значно простіше, упереджено мінімізуючи помилки та уразливості. Тобто, ШІ стає потужним інструментом під час захисту від кібератак. ШІ допомагає командам реагування на кіберінциденти (CERT) створювати потужні сервіси та спільні людсько-машинні проекти, які розширяють знання, навички та вміння, сприяючи посиленню кібербезпеки, запроваджуючи новий рівень кіберзахисту. Завдяки ШІ стає можливим упереджувати загрози та отримувати оперативну інформацію у режимі реального часу про кіберінциденти.

Важливим пріоритетом використання ШІ у сфері кібербезпеки є його здатність прогнозувати кібератаки ще навіть до їхнього повноцінного здійснення, що надає змогу своєчасно посилити засоби захисту. Іншою його перевагою є значне скорочення людського фактору – тобто ШІ не схильний до різних психологічних впливів або втоми. Реагування безпеки на кіберзагрози, автоматизоване за допомогою ШІ вимагає менше часу та знижує ризик людської помилки. Так, ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків та знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки.

Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей в системах та мережах, що надає змогу ліквідувати їх завчасно. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз. За таких умов ШІ зданий революціонізувати підхід до вирішення складних проблем у сфері кібербезпеки та стає її невід'ємною частиною. Системи ШІ навіть можуть навчити розпізнавати аномалії поведінки та попереджувати про небезпеку, виявляти нові штами шкідливого програмного забезпечення та захищати критично важливі дані.

Транформації та динамічний розвиток передових технологій змінюють цифровий світ, зокрема й інструменти та тактики забезпечення кібербезпеки. Важливою подією сучасності стало відкриття у листопаді 2022 року нового генеративного інструменту ШІ, такого як ChatGPT (Generative Pre-trained Transformer). Це чат-бот зі ШІ, розроблений компанією OpenAI – дослідницькою установою, яка вивчає та опановує ШІ та зробила революційний крок у питаннях його розвитку. Він може генерувати тексти на задані теми та відповідати на питання зрозумілою мовою. Запуск чат боту ChatGPT став революційним кроком у сфері технологій і дав поштовх до активної розробки продуктів зі ШІ. Водночас зростає ризик дезінформації, а особисті дані користувачів можуть опинитися в небезпеці. Сучасна технологія генеративного ШІ, яка може створювати прозу з текстових підказок, захопила громадськість після того, як чат бот ChatGPT був запущений трохи більше півроку потому, і став додатком, котрий глобально розвивається швидкими темпами. На цьому фоні ШІ став предметом занепокоєння через його здатність створювати підроблені зображення та іншу дезінформацію. У січні 2023-го ChatGPT досяг 100 млн. активних користувачів. Спочатку цей чат-бот був доступний безоплатно, згодом компанія заявила про запуск підписки на ChatGPT у США вартістю $20. Розробник чат-бота заборонив деяким окремим країнам користуватися своїми сервісами відповідно накладених санкцій, тож в рф він поки що недоступний. 18 лютого 2023 року міністр цифрової трансформації України М. Федоров повідомив, що ChatGPT став доступний в Україні, проте ця програма не працюватиме на тимчасово окупованих рф територіях України для того, щоб нею не скористалися військові держави-агресора [12].

Таким чином, ШІ може успішно допомагати захищатися від кібератак шляхом: автоматизованого пошуку загроз із використанням алгоритмів машинного навчання та за наслідками виявлення проблем у роботі систем, що може свідчити про порушення безпеки; того, що машинне навчання використовується з метою аналізу великих обсягів даних та прогнозування розвитку ситуації на підставі виявлених уразливостей та закономірностей, що надає змогу навчати системи ШІ розпізнаванню невідомих або непередбачуваних атак; предикативної аналітики, яка надає можливість прогнозувати майбутні загрози, наприклад, які облікові дані співробітників з найбільшою вірогідністю можуть бути зламані та які типи атак можуть відбутися у той чи інший день, у зв’язку з чим такий аналіз допомагає визначити, де знаходяться ймовірні проблеми в системі, щоб упереджено виявити та блокувати їх заздалегідь; виявлення аномалій у мережевому трафіку або у інших потоках даних, аналізуючи шаблони на предмет тотожності або відмінності між ними. Такий тип моніторингу допомагає виявити аномальну поведінку до того, як вона трансформується у майбутню шкідливу діяльність; автоматизації безпеки та впровадження нових політик й протоколів безпеки, що захищає від таких кібератак, як загрози спуфінгу або фішингу тощо. Автоматизація безпеки надає змогу запровадити економію часу та витрат; суттєвого зменшення помилок, пов`язаних із людським фактором, надання економічно ефективних рішень з 100 % точністю.

Застосування технологій ШІ у кібервійні є досить важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України. На фоні окресленого позитивного досвіду використання технологій ШІ у питаннях забезпечення кібербезпеки та наявності його беззаперечних переваг, ця технологія не позбавлена своїх проблем й недоліків.

Однією із основних проблем є можливість використання технології ШІ кіберзлочинцями та хакерами з метою розробки більш складних та цілеспрямованих атак. Тобто продумані кібератаки з використанням технологій ШІ – глобальна загроза сучасності. Тобто хакери та кіберзлочинці можуть також використовувати ці технології для скоєння потужних та інноваційних кібератак. Наприклад, шкідливе програмне забезпечення на базі ШІ може навчатися та адаптуватися, щоб уникнути виявлення за допомогою традиційних інструментів мережевої безпеки. Кіберзлочинці можуть використати ШІ для виявлення закономірностей у комп'ютерних мережах, які визначають слабкі місця у програмному забезпеченні, що надає змогу хакерам виявляти та використовувати ці уразливості на власний розсуд. Постійно змінюючись, сигнатури шкідливих програм можуть допомогти зловмисникам обійти статичні засоби захисту, такі як брандмауери та системи виявлення за периметром. Аналогічним способом, шкідливе програмне забезпечення зі ШІ може перебувати усередині системи, збираючи дані та спостерігаючи за поведінкою користувача, доки не буде готове розпочати нову фазу атаки. Враховуючи економіку кібератак, зазвичай, простіше та дешевше організувати атаки, аніж будувати ефективний захист, про що впевнено знають й зловмисники. Більш того, ШІ є інноваційною технологією, яка призводить до появи нових кіберзагроз.

Так, за допомогою ШІ, а саме нейтронних мереж став можливим синтез високоякісних зображень, відео, аудіо матеріалів, створених з метою введення в оману пересічних користувачів, вимушеного впливу на системи розпізнавання обличчя. Ця технологія підробки зображень, в основі якої перебуває ШІ, отримала назву "deepfake" та вона вже була успішно використана на практиці з метою реалізації шахрайських схем та інших протиправних дій. Завдяки цій зловмисній програмі кібершахраї можуть видавати себе за іншу людину: скопіювати зовнішність, міміку, голос. Так, наприклад, був зафіксований резонансний випадок, коли керівнику підрозділу компанії зателефонувала стороння людина та голосом генерального директора попросила про переказ коштів у розмірі 220 тис. Євро, у зв'язку з чим вказані грошові кошти були переведені шахраю. Спеціалісти з кібербезпеки компанії "Check Point Research" з'ясували, що хакери розробили спосіб використання чат бот ChatGPT з метою розробки шкідливих програми та фішингових електронних листів. Раніше кіберспеціалісти "Check Point Research" з'ясували, що за допомогою ChatGPT можливо розробити скрипт для створення даркнет-маркетплейсу, на якому можна було придбати скомпрометовані облікові дані, інформацію про платіжні картки, шкідливі програми, інші незаконні товари тощо.

Тобто хакери можуть використовувати ШІ з метою обходу систем захисту та створення більш складних та удосконалених кібератак. У зв'язку з цим доцільно забезпечити захист даних та алгоритмів безпеки ШІ від кібератак та взломів. Хакери вірогідно можуть використовувати шкідливі алгоритми з метою впровадження їх в систему ШІ щоб обійти системи захисту. Тому необхідно посилити заходи захисту систем, які працюють на базі ШІ, проводити регулярні перевірки на наявність уразливостей. Також необхідно навчати ШІ різним видам кібератак та кіберзагроз, використовувати при цьому актуальні дані про нові типи та види. За таких умов важливо, щоб індустрія кібербезпеки випередила ці події та постійно впроваджувала інновації для протидії новим загрозам. Тобто завдання щодо посилення кіберзахисту є актуальним на перманентій основі, виходячи із нового формату динамічно розроблених нових сучасних технологій, які продикують появу нових загроз. На сьогодні не існує жодних надійних та універсальних методів захисту від кібератак на системи ШІ. Тому будь-яке використання технологій ШІ може надавати користь та одночасно формувати нові потужні загрози та виклики.

Отже, світова спільнота активно переймається проблематикою поширення та впровадження технологій ШІ у сферу кібербезпеки та його унормування, у зв`язку з чим навколо світу набуває обертів та триває обговорення необхідності здійснення правового врегулювання ШІ, особливо у питаннях забезпечення кібербезпеки. Оскільки відсутні міжнародні правила та правові засади використання ШІ, то це питання залишається відкритим. Також доцільно враховувати організаційні та правові питання використання ШІ у кібербезпеці, оскільки схвалення рішень на основі ШІ може призвести до порушення прав людини на приватність. Оскільки провідні держави світу моделюють свої політики, включаючи ШІ у різні сфери та галузі, існує нагальна потреба розробки та затвердження етичних правил і правових стандартів, які мають врегулювати сферу використання ШІ у питаннях забезпечення кібербезпеки. Так, зокрема, перед країнами-членами "Великої сімки" на порядку денному стоїть питання щодо обговорення розробки та удосконалення законодавства, яке має регулювати використання та застосування технологій, пов'язаних зі ШІ. Очікується, що ШІ несе певні ризики для безпеки, оскільки він може продукувати фейкові новини та руйнівні рішення для суспільства, якщо дані, на яких він базується, є несправжніми. Тому доцільним є врегулювання сфери ШІ на законодавчому рівні, що водночас має зберегти відкрите та сприятливе середовище для розвитку його технологій, а також ґрунтуватися на демократичних цінностях та засадах.

Україна не відстає у питаннях регулювання ШІ від світових тенденцій сучасності. У 2020 році була схвалена Концепція розвитку сфери штучного інтелекту. Нормативно задекларовано, що основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі ШІ є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян. Задекларовано, що комплексне розв'язання проблем кібербезпеки вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик ШІ у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології ШІ для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок ШІ у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень тощо [10].

12 травня 2021 року Кабінет Міністрів України затвердив План заходів щодо реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки [11]. Цим стратегічним документом регламентовані питання впровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню. У рамках стратегічного планування наприкінці 2021 року за сприяння РНБО України на державному рівні мали бути затвердженими заходи протидії кіберзагрозам з використанням технологій ШІ. Проте, на

жаль, нормативно ці заходи ще й досі не визначені, що актуалізує діяльність державних органів за цим напрямком, особливо в умовах правового режиму військового стану.

Занепокоєння щодо негативних наслідків та загрозливих тенденцій використання ШІ знайшли своє відображення у звіті Європолу, який було оприлюднено у березні 2023 року [13]. Так, на підставі аналізу здобутих результатів роботи Європейського поліцейського офісу з'ясовано, що чат-бот ChatGPT та інші генеративні системи ШІ можуть бути використані для онлайн-шахрайства та скоєння інших видів злочинів. Попри позитивні приклади та користь, яку можуть принести звичайним людям генеративні моделі ШІ, серед яких чат-бот ChatGPT, поширення таких інструментів може вірогідно призвести до нових проблем, з якими стикнуться правоохоронні органи. Експерти Європолу підкреслюють, що правила модерації ChatGPT можна обійти за допомогою т.зв. "оперативного проектування", тобто практики надання вхідних даних у модель ШІ саме для отримання певного результату. Оскільки чат-бот ChatGPT є відносно новою сучасною технологією, незважаючи на його постійне оновлення, у цьому інструменті постійно виявляються прогалини. Наприклад, існують команди, завдяки яким ШІ може використовуватися у злочинній діяльності, хоча, якщо такі команди надати чат-боту ChatGPT у звичайному форматі, він обов'язково попередить, що його роботу не можна застосовувати у протиправній діяльності та злочинним умислом. Якщо ж змінити окремі слова запиту чи контекст, він може стати дієвим інструментом для реалізації своїх цілей кіберзлочинцями. Експерти підкреслюють, що обхідні шляхи, якими вдається позбавити модель від будь-яких обмежень, постійно розвиваються та стають все складнішими.

Розуміючи ризики та загрози, які несе суцільне використання ШІ, зокрема у питаннях кібербезпеки, 14 червня 2023 року Європарламент схвалив проект закону, який регулюватиме правила у сфері ШІ на території країн ЄС [14]. Цей законопроект висвітлюватиме питання поширення та використання ШІ відповідно до рівня ризику: чим він вищий для прав чи свобод людей, тим більше зобов'язань. Особливі нормативні вимоги висуватимуться до генеративних систем, таких як ChatGPT, що здатні створювати текст, зображення, аудіо та медіафайли. Законодавчо встановлюється вимога щодо інформування користувачів про те, що контент був створений машиною, а не людиною. Прийнятий нещодавно законопроект про регулювання ШІ в ЄС стане першим у світі документом, в якому закладені основи використання цієї технології та враховані обмеження й застереження щодо її негативного впливу. Хоча документ передбачає велику кількість різноманітних обмежень, його основною ідеєю є мінімізація впливу ШІ на базові права людини. Цей законопроект декларує доволі жорстку обрану тактику стосовно використання ШІ загалом та чатботів в бізнесі та інших галузях життєдіяльності європейського співтовариства зокрема. Перспективне схвалення цього законопроекту, яке планується у 2026 році, має стати важливим та актуальним кроком у питаннях правової регламентації розвитку ШІ на теренах ЄС.

Очікується, що цей закон допоможе забезпечити більшу безпеку та відповідальність при використанні ШІ та захистити права та свободи користувачів. Законопроект може бути застосовано відносно різних галузей, включаючи кібербезпеку, банківську, медичну та страхову. В ньому регламентовані вимоги щодо збору та зберігання даних, але найголовніше – правила використання алгоритмів, зокрема чат-ботів, у різноманітних взаємодіях з клієнтами. Головна вимога закону – інструменти ШІ можуть бути використані лише тоді, коли вони гарантуватимуть неупередженість й безпеку та здатність до відновлення у разі збою. Окремою вимогою є забезпечення прозорості використання ШІ. Досить жорстким рішенням є встановлення відповідальності за будь-

які помилки, що можуть виникнути при використанні чатботів в медичній галузі. Іншими сферами, які регулюватимуться цим законом, є судова система та правоохоронні органи. Одночасно європейський "AI Act" встановлює загальні принципи та вимоги до використання ШІ в будь-якій галузі, зокрема у кібербезпеці. Очікувано, цей модельний закон може стати прикладом для інших країн та підгрунтям для розробки міжнародних стандартів використання ШІ. Зокрема, його може бути покладено в основу ініціатив з боку ООН та інших світових організацій щодо створення міжнародного законодавства в цій сфері.

Висновки.

Роль та значення ШІ у питаннях забезпечення кібербезпеки без перебільшення не можна недооцінювати. ШІ стає невід`ємною частиною архітектури сучасної кібербезпеки. У зв'язку із динамічним та перспективним розвитком передових технологій, ШІ досить широко використовуєтсья для виявлення кіберзагроз, формування дієвих механізмів захисту від кібератак та схвалення оперативних управлінських рішень. Можливості ШІ сприяють удосконаленню процесів моніторингу змін ландшафту загроз на кіберфронті, виявленню кібератак, надають змогу покращити стан забезпечення кібербезпеки в цілому. Технології ШІ дають змогу, на постійній основі, автоматизувати процеси сканування мереж з метою виявлення та реагування на кібератаки. Однозначно не можна повністю виключати людський фактор під час використання ШІ у сфері кібербезпеки, оскільки остаточне рішення за наслідками використання ШІ належить саме людині. Тобто ШІ допомагає людині, проте не замінює її.

Беззаперечно, ШІ відіграє подвійну роль у питаннях забезпечення кібербезпеки. На фоні позитивного аспекту, з одного боку, можна констатувати, що за його допомогою, хакери та кіберзлочинці можуть планувати та здійснювати потужні й руйнівні кібератаки. Загрози, реалізовані за допомогою ШІ, є особливо небезпечними. Позитивним здобутком сучасності стала поява генеративної системи ШІ зокрема чат-боту ChatGPT. Проте, на підставі досвіду, який склався за останні півроку його активного використання, фахівці засвідчили та підтвердили можливість його реалізації хакерами у злочинних цілях: викрадати конфіденційні дані, створювати шкідливе програмне забезпечення тощо. Тобто вірогідно чат-бот ChatGPT може використовуватися для поширення комп'ютерних вірусів, надавати зловмисникам та хакерам неабияку підтримку під час використання ними цих технологій для проведення кібератак, поширення шкідливого програмного забезпечення.

Застосування технологій ШІ у кібервійні є важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати потенційні зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України. Навіть попри деякі негативні тенденції, пов'язані із можливостями використання ШІ, його застосування з метою проведення потужних кібератак може стати найнебезпечнішим атрибутом**.** Здатність зламувати кібермережі супротивника матиме вирішальне значення, оскільки військові продовжують проводити бойові операції, логістику, націлювання, розвідку і всі інші аспекти сучасної кібервійни, в основі яких перебуває мережа Інтернет.

Важливим та перспективним напрямком залишається розробка нормативних вимог та подальша їх уніфікація щодо використання технологій ШІ у сфері кібербезпеки, особливо в умовах правового режиму воєнного стану в Україні. Також необхідним є

унормування правової регламентації як на державному, так і міжнародному рівнях, використання технологій ШІ у сфері кібербезпеки з метою недопущення порушень прав людини на приватність.

Використанна література

1. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Information Systems And Networks.* 2022. № 12. С. 7-20.

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

3. Стьопочкіна І.В., Новіков О.М. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 "Кібербезпека". Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.

4. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання*:* зб. наук. пр. *Інноваційні обрії України*. 2023. № 6. С.136-144. – (Громадська організація Українські студії в європейському контексті).

5. Цяпа С.М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 51-59.

6. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition (December 8, 2022). 311 p. DOI 10.1007/978-3-031-15030-2

7. Narcisa Roxana Mosteanu. Artifical Inelligence and cyber security – face to face with cyber attack – a maltese case of risk management approach. *Ecoforum journal.* 2020. Vol 9. № 2. URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

8. Rammanohar Das, Raghav Sandhane. Artificial Intelligence in Cyber Security. ICACSE 2020. IOP Publishing. Journal of Physics: Conference Series 1964 (2021). P.1-10 doi:10.1088/1742-6596/1964/4/042072. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf

9. Гладка Ю.А., Назаренко Є.О. Аналіз застосування технологій штучного інтелекту в кібербезпеці: наукові праці третьої Міжнар. наук.-практ. конф. *Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій*, м. Київ, 25 – 26 січня 2021 р. Київ: НУХТ, 2021. С. 64-66.

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

11. Про затвердження Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки: Розпорядження Кабінету Міністрів України від 12.05.21 р. № 438 URL: https://zakon.rada.gov.ua/laws/show/438-2021-р#Text

12. Федоров: в Україні став доступний чат-бот зі штучним інтелектом ChatGPT. – (Українські національні новини від 18.02.23 р.). URL: https://www.unn.com.ua/uk/news/2016033-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

13. ChatGPT. The impact of Large Language Models on Law Enforcement. Europol Public Information. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20Enforcement.pdf

14. 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

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

УДК 004.8/007:159.955

АНДРОЩУК Г.О., *кандидат економічних наук, доцент,* головний науковий співробітник НДІ інтелектуальної власності НАПрН України.
ORCID: https://orcid.org/0000-0003-0781-9740.

РІВЕНЬ ДОВІРИ ДО ШТУЧНОГО ІНТЕЛЕКТУ: АНАЛІЗ РЕЗУЛЬТАТІВ ГЛОБАЛЬНИХ ДОСЛІДЖЕНЬ ТА СТАН В УКРАЇНІ [*]

Анотація. *У статті, на основі аналізу матеріалів глобальних досліджень, визначено та оцінено рівень довіри та ставлення до штучного інтелекту (ШІ) серед людей різних країн, національностей, статі, вікових груп, соціального статусу. Досліджено вплив таких факторів, як рівень освіти, місце проживання, ступінь ознайомлення з новими технологіями, зокрема генеративним ШІ, та чинники, що впливають на сприйняття ШІ. Розглянуто чотири різні "шляхи до довіри" – інституційний, мотиваційний, зменшення невизначеності та шлях знань, визначено їх важливість у прогнозуванні довіри. Оцінено рівень довіри до ШІ в Україні порівняно зі світовими тенденціями, розглянуто важливі аспекти довіри: прозорість, надійність, зрозумілість, обізнаність, конфіденційність, етика, точність, можливість контролю тощо. Показані ризики і загрози генеративного ШІ, виділено три сегменти, які необхідно контролювати з точки зору управління корпоративними ризиками: інтелектуальна власність, конфіденційність даних та кібербезпека, запропоновано способи та інструменти сприяння довірі до ШІ.*

Ключові слова: *штучний інтелект, генеративний штучний інтелект, рівень довіри, оцінка ризиків, загрози, безпека технології, регулювання, контроль.*

Summary*. The article, based on the analysis of global research materials, defines and evaluates the level of trust and attitude towards artificial intelligence (AI) among people of different countries, nationalities, gender, age groups, and social status. The influence of such factors as the level of education, place of residence, the degree of familiarity with new technologies, in particular generative AI, and factors affecting the perception of AI were studied. Four different "paths to trust" are considered - institutional, motivational, uncertainty reduction and knowledge path, and their importance in predicting trust is determined. The level of trust in AI in Ukraine compared to global trends was assessed, important aspects of trust were considered: transparency, reliability, comprehensibility, awareness, confidentiality, ethics, accuracy, controllability, etc. The risks and threats of generative AI are shown, three segments that need to be controlled from the point of view of corporate risk management are highlighted: intellectual property, data privacy and cyber security, methods and tools for promoting trust in AI are proposed.*

Keywords: *artificial intelligence (AI), generative AI, intellectual property, level of trust, threats, regulation, control.*

Постановка проблеми. Протягом останніх років штучний інтелект (далі – ШІ) активно застосовується практично у всіх сферах людського життя, зокрема медицині, транспортуванні, навчанні, електронній комерції, оборонній сфері тощо. ШІ здатен виконувати надскладні завдання, робити прогнози, планувати та аналізувати дані.

Високорозвинені країни, такі як США та Китай, щорічно вкладають величезні кошти у розробки пов'язані зі ШІ, для того щоб здобути конкурентні переваги та бути першими у світовій гонці за новими технологіями. Згідно з даними консалтингової компанії Preqin, інвестиції в ШІ у США перевищують показники КНР у шість разів, склавши

[*] Стаття підготовлена в рамках виконання теми НДР "Інтелектуальна власність в цифровій економіці" (РК № 0118U007601), яку виконує НДІ інтелектуальної власності НАПрН України.

цьогоріч 26,6 млрд. доларів проти 4 млрд. доларів Пекіна [1]. Особлива увага почала приділятися ШІ у сфері оборони, починаючи з передиктивного обслуговування техніки та завершуючи автономною зброєю. ШІ може також автоматично розпізнавати образи, що зменшує ризик для військовослужбовців та аналізувати дані, що допомагає швидко знаходити інформацію про ворожі дії та приймати точні рішення. Загалом нові розробки можуть бути корисними для проведення успішних військових операцій в Україні. Попри те, що ШІ приносить багато позитивних змін у повсякденне життя, питання довіри користувачів до ШІ та їх готовності на повну використовувати його потенціал є досить гострим та потребує детального аналізу.

Однією з проблем, пов'язаних із використанням ШІ в різних галузях, є досить низький рівень довіри та насторожене ставлення до нього населення. Такі настрої не дивні, адже існує багато історій пов'язаних з тим наскільки небезпечним може бути ШІ та які наслідки може спричинити. Саме тому виникає питання: чому люди не довіряють ШІ і які основні чинники на це впливають? По-перше, багато людей ставлять під сумнів надійність і точність ШІ, особливо коли потрібно врахувати фактори, які є суб'єктивними та неочевидними, що може призвести до неправильної інтерпретації даних. По-друге, дехто має страх втратити своє робоче місце та бути усуненим з посади через розробку технологій, які будуть виконувати роботу швидше і ефективніше. Ще однією значимою причиною є необізнаність людей. Вони не розуміють що таке ШІ, як з ним взаємодіяти та які основні принципи його роботи. Як наслідок споживачі або недооцінюють або ж переоцінюють можливості та потенціал ШІ.

Результати аналізу наукових публікацій. Протягом останнього десятиріччя була проведена досить велика кількість досліджень, пов'язаних з рівнем довіри до ШІ. Багато вчених-авангардистів (наприклад, Стівен Хокінг) та бізнес-лідери (наприклад, Ілон Маск, Білл Гейтс) вважають, що складні рішення ШІ несуть у собі серйозні загрози для суспільства. Так у статті "Довіра до штучного інтелекту: від базової системи довіри до нових можливостей для досліджень" (Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities) [2] автори досліджують проблему довіри до ШІ та пропонують фреймворк (англ. framework – "каркас") – програмне середовище, яке спрощує та прискорює створення програмного забезпечення) для того, щоб розібратися з цим поняттям. У статті виділяють основні елементи довіри, а саме прозорість, етику, технічну безпеку та інформаційну конфіденційність. На основі цього було розроблено фреймворк, що містить такі поняття як особистість, технічні аспекти та контекст. Завдяки цьому можна проаналізувати взаємодію між людиною та ШІ, виявити роль етики у прийнятті рішень, зрозуміти як різні рівні ШІ впливають на довіру, а також дослідити зв'язок між довірою та рівнем користування ШІ. Крім цього, у роботах [3 – 5] здійснено аналіз публікацій на тему довіри до ШІ, які відкривають нові можливості у проведенні майбутніх досліджень щодо розвитку ШІ, його впливу на громадськість та способів підвищення рівня довіри.

У 2023 році було опубліковано результати дослідження "Довіра до штучного інтелекту: глобальне дослідження" (Trust in artificial intelligence: A global study) [6]. У ньому аналізується рівень довіри та ставлення громадськості до використання ШІ, а також очікування щодо управління ШІ у 17 країнах. Звіт надає вичерпну глобальну інформацію про довіру та сприйняття систем ШІ, висвітлює передбачувані переваги та ризики використання ШІ, очікування спільноти, регулювання та управління ШІ. З дослідження видно як люди ставляться до використання ШІ на роботі, наскільки громадськість є обізнаною щодо ШІ та зміна ставлення до ШІ з часом. Загалом результати опитування пропонують методи надійного та відповідального використання

систем ШІ та його впровадження в економіку і суспільство. Ці висновки є актуальними для вироблення політики та побудови стратегії щодо ШІ в бізнесі, уряді та неурядових організаціях, а також для інформування про стандарти щодо ШІ на загальнодержавному та міжнародному рівнях. Питання правового регулювання сфери цифрових технологій та ШІ в Україні досліджують такі вчені як О. Баранов, В. Брижко, О. Вінник, О. Костенко, О. Радутний, В. Пилипчук, М. Стефанчук, О. Харитонова та інші. Проте динамічність змін у цій сфері, комплексний, міждисциплінарний характер проблематики потребує нових досліджень.

Нещодавно у видавництві Варшавського політехнічного університету вийшла монографія "Довіра до систем штучного інтелекту" ("Zaufanie do systemów sztucznej inteligencji"). Ця праця, за редакцією Марека Якуб'яка та Павла Стацевича, була створена в рамках роботи дослідницької групи "Гуманістичні аспекти штучного інтелекту", яка працює на кафедрі економічного права та економічної політики WAiNS PW, а її співавторами є вчені з різних академічних центрів. Метою авторів було привернути увагу до зростаючої міждисциплінарності сучасних досліджень ШІ. Попри те, що інформатика є основою ШІ, експерти зазначають, що рівень довіри людини до ШІ також залежить від виконання умов, визначених гуманістами, зокрема психологами, соціологами та філософами [7].

У своїх попередніх роботах [8; 9] автор дає аналіз рівня довіри до ШІ на основі національного, вікового та статевого складу людей в п'яти розвинених країнах світу. Виявлено, що такі драйвери як віра в правильне правове регулювання, позитивний вплив ШІ на робочі місця, доступність для розуміння принципів роботи та позитивний вплив ШІ на суспільство загалом є ключовими для підвищення рівня довіри. Підкреслюється важливість розуміння людьми того, що системи ШІ не є повністю автономними і що, як правило, є люди, які забезпечують контроль та управління ними. У підсумку надається цінний огляд досліджень з проблеми довіри до систем ШІ як в міжнародному контексті, так і в межах України. В них наголошується на важливості розуміння людьми того, як саме працюють ці системи та який контроль здійснюється за ними.

У 2022 році в 28 країнах було проведене глобальне опитування "Global opinions and expectations about artificial intelligence", в якому взяли участь 19504 чоловік [10] На основі аналізу даних зроблено такі висновки: більшість людей у всьому світі чули про ШІ, але лише невелика частина добре розуміє його можливості; люди загалом позитивно ставляться до ШІ, лише меншість висловлює стурбованість його негативними наслідками; населення найбільше зацікавлене в тому, щоб ШІ використовувався для покращення сфери охорони здоров'я, розширення можливостей для навчання та підвищення безпеки транспортування; довіра людей до ШІ є відносно низькою, і лише меншість висловлює високий рівень довіри; основні чинники, що впливають на довіру, включають прозорість, зрозумілість і підзвітність; люди вважають, що ШІ слід регулювати, щоб забезпечити його відповідальне використання.

Метою статті є визначення стану довіри людей щодо розробки, використання та управління, а також їх ставлення до рішень ШІ, та які зміни відбулися протягом 2022 – 2023 років у зазначеній сфері. Завдяки цьому можна виявити фактори, що впливають на рівень довіри, існуючі ризики та загрози, запропонувати способи покращення довіри.

Серед завдань роботи визначимо такі: виявити та оцінити рівень довіри до ШІ серед людей різних національностей, статі, вікових груп, соціального статусу та країн; дослідити вплив таких факторів, як рівень освіти, місце проживання, ступінь ознайомлення з новими технологіями, зокрема генеративним ШІ, та чинники, що

впливають на сприйняття ШІ; оцінити рівень довіри до ШІ в Україні та порівняти зі світовими тенденціями; розглянути важливі аспекти довіри: прозорість, надійність, зрозумілість, обізнаність, конфіденційність, етика, точність, можливість контролю тощо; запропонувати способи та інструменти сприяння довірі до ШІ.

Виклад основного матеріалу. Для того, щоб дослідити рівень довіри людей до ШІ, визначимо що таке ШІ. Згідно Вікіпедії, штучний інтелект (англ. Artificial Intelligence – AI) – розділ комп'ютерної лінгвістики та інформатики, що опікується формалізацією проблем та завдань, які подібні до дій, що виконує людина. Це поняття ввів у 1956 р. професор Дартмутського коледжу Джон МакКарті, який цікавився, чи можна навчити машину, як і дитину – оперувати абстрактними поняттями, використовувати мову і самостійно вдосконалюватись методом спроб і помилок. Відомий український дослідник інформаційного права д.ю.н. О.А. Баранов дає таке визначення: "***штучний інтелект*** – це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини" [11, с. 46]. ШІ – це здатність машин навчатися, міркувати, здійснювати планування, аналізувати, приймати рішення та робити відповідні висновки. ШІ може імітувати людські когнітивні здібності та навички, такі як розпізнавання мови, візуальне сприйняття, самовдосконалення, творчість та покращення власних алгоритмів. ШІ включає в себе різноманітні техніки, такі як нейронні мережі, машинне навчання, генетичні алгоритми та інше. За допомогою цього ШІ може адаптуватися до різних ситуацій, вирішуючи складні завдання. ***Поняття довіри до ШІ*** *можна визначити як впевненість та віра користувача в те, що дії ШІ та рішення які він буде пропонувати, відповідатимуть стандартам якості, безпеки, надійності та етики.* Саме тому довіра до ШІ залежить від кількох факторів та принципів, основними з яких є:

1. Надійність та точність. Для того, щоб люди довіряли ШІ, вони повинні переконатися в тому, що ШІ працює надійно та точно. Цього можна досягти шляхом високої якості результатів роботи ШІ, відстежуючи виконання завдань.

2. Прозорість та зрозумілість: Прозорість ШІ – це можливість пояснити, як ШІ прийняв своє рішення та які джерела він використовував для свого аналізу.

3. Безпека та конфіденційність даних: ШІ має бути захищено від несанкціонованого доступу та зловживань. Дані, які використовуються для ШІ, повинні зберігатися в безпеці, використовуватись лише для конкретної мети і не передаватися іншим програмам або третім особам без дозволу. Для забезпечення безпеки, ШІ має використовувати надійні методи шифрування та захисту даних.

4. Нагляд. Має існувати належний нагляд і контроль за системами ШІ та їхнім впливом людьми, які мають необхідні для цього знання та ресурси. Системи ШІ мають регулярно перевірятися щоб переконатися, що вони працюють надійно.

5. Підзвітність та оспорюваність. Повинна існувати чітка підзвітність і відповідальність у разі збою в системі ШІ. Будь-який користувач може оскаржити результати системи ШІ через справедливий і доступний процес перевірки людьми.

6. Етика: ШІ має дотримуватися етичних стандартів. Це означає, що він має бути побудований на принципах правосуддя, довіри та рівності.

7. Зменшення ризику та впливу. Усі ризики та потенціал шкоди від системи ШІ повинні адекватно оцінюватися та пом'якшуватися при проведенні нових розробок та вдосконаленні існуючих систем.

8. ШІ-грамотність. Людям надається підтримка в розумінні систем ШІ, зокрема, коли їх доречно використовувати, і етичних міркувань їх використання.

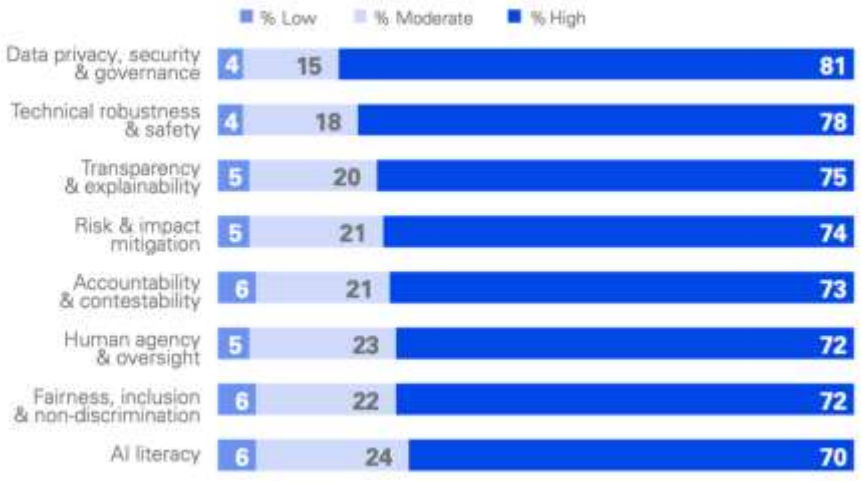

Рис. 1. Важливість при**н**ципів довіри до ШІ.
Джерело: "Trust in artificial intelligence: A global study" (2023). URL: https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf

Згідно з дослідженням Trust in artificial intelligence ("Довіра до штучного інтелекту: глобальне дослідження") попри те, що всі вісім принципів є важливими *конфіденційність даних, безпека та практики управління вважаються найважливішими для довіри до систем ШІ в усіх країнах*, крім Китаю, де він посів друге місце [12].

На противагу, практика грамотності ШІ вважається найменш важливою у більшості країн. Досить значимими факторами довіри до ШІ є також технічна стійкість і безпека та прозорість і зрозумілість, що займають відповідно друге та третє місце.

Окрім принципів та факторів довіри, варто звернути увагу на драйвери / шляхи до довіри, що впливають на прийняття ШІ. Саме вони є важливою ланкою побудови довіри до систем ШІ. Розглянемо, згідно дослідження (див. Рис. 2), чотири різні ***шляхи до довіри*** – *інституційний, мотиваційний, зменшення невизначеності та шлях знань*, а також визначимо їх важливість у прогнозуванні довіри.

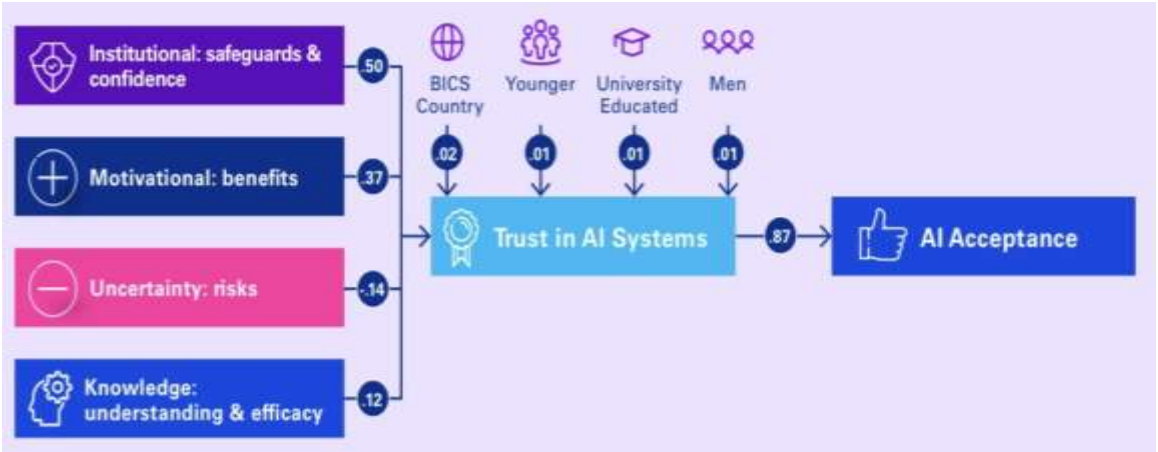

Рис. 2. Модель ключових факторів довіри та сприйняття систем ШІ.
Джерело: "Trust in artificial intelligence: A global study" (2023). URL: https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf

Інституційні драйвери включають запобіжні заходи – віра людей в те, що діючих законів та правил достатньо для забезпечення безпеки використання ШІ. Довіра до уряду і технологічних/комерційних організацій щодо розробки, використання та управління ШІ.

Мотиваційні чинники – це передбачувані переваги ШІ – ступінь, до якої користувачі очікують отримати переваги від використання системи ШІ.

Факторами невизначеності є передбачувані ризики ШІ – ступінь занепокоєності людей щодо низки ризиків, пов'язаних із використанням систем ШІ.

Драйвери знань включають суб'єктивні знання – ступінь, до якої люди відчувають, що вони розуміють ШІ, а також коли і де він використовується, за умов оцінки людьми своєї здатності використовувати цифрові технології та онлайн-сервіси.

Інституційні гарантії є найсильнішими рушіями довіри, адже люди часто покладаються на авторитетні джерела та очікують, що вони гарантуватимуть безпеку та надійність нових технологій. Як показано в моделі, *люди більше довіряють системам ШІ, коли вони вірять, що діючих норм і законів достатньо для безпечного використання ШІ.* Інституційний шлях є найсильнішим драйвером довіри (B = 0,50) і значно важливішим, ніж інші фактори.

Мотиваційний шлях є другим найсильнішим драйвером довіри (B = 0,37) і є більш значимим фактором, ніж передбачувані ризики ШІ. Це допомагає пояснити, чому люди готові використовувати ті технології, які забезпечують негайну вигоду, попри побоювання щодо потенційних ризиків.

Аналіз моделі показує, що чим більше люди стурбовані передбачуваними ризиками використання ШІ, тим менша ймовірність, що вони довірятимуть системам ШІ (B = 0,14). Це включає як технічні ризики, пов'язані з використанням ШІ (наприклад кібербезпека та конфіденційність), так і ширші суспільні ризики (наприклад, маніпуляції, декваліфікація). Це третій найсильніший фактор довіри, що підкреслює важливість постійних дій для пом'якшення ризиків, пов'язаних із ШІ [13]. Згідно з аналізованою моделлю, люди з більшою ймовірністю довірятимуть ШІ, якщо відчуватимуть, що розуміють, коли і як використовується ШІ, і мають достатньо навичок для використання цифрових технологій (B = 0,12).

Шлях знань є четвертим чинником довіри та підкреслює важливість підтримки технологічної та цифрової грамотності.

Якщо ж брати до уваги інші фактори (демографічні та вікові відмінності), то вони мали менший вплив на довіру: Люди в країнах BICS більше довіряють ШІ (B = 0,02). Молоде покоління більше довіряє ШІ (B = 0,01), Люди з вищою освітою більше довіряють ШІ (B = 0,01). Чоловіки більше довіряють ШІ (B = 0,01).

Глобальне опитування Global opinions and expectations about artificial intelligence ("Глобальні думки та очікування щодо штучного інтелекту"), що проводилося для Всесвітнього економічного форуму, дослідило обізнаність людей щодо ШІ та рівень довіри у відповідності до демографічних чинників, рівня освіти та доходу. Було встановлено, що у "середньому з усіх 28 опитаних країн майже дві третини (64 %) стверджують, що вони добре розуміють, що таке ШІ, але лише половина (50 %) знають, які типи продуктів і послуг використовують ШІ" [13].

Обізнаність зі ШІ найвища серед осіб, що приймають бізнес-рішення (74 %), які є власниками бізнесу (73 %), ті, хто має вищу освіту (71 %), і тих, хто має високий рівень доходу (71 %). Серед чоловіків він також помітно вищий, ніж серед жінок (на 9 %).

У звіті також здійснено аналіз кореляції (статистичного взаємозв'язку) (Рис.3) між рівнем довіри та сприйняттям (розумінням) ШІ.

Рис. 3. Аналіз кореляції між рівнем довіри та сприйняттям (розумінням) ШІ.
Джерело: IPSOS. Global opinions and expectations about artificial intelligence (January 2022). URL: https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Global-opinions-and-expectations-about-AI-2022.pdf

Як видно з діаграми на Рис. 3, лише половина опитаних довіряють компаніям, що використовують ШІ, так само, як і іншим компаніям. З іншого боку жителі країн, що розвиваються, значно частіше, ніж жителі країн з високим рівнем доходу, повідомляють про те, що вони обізнані з ШІ, довіряють компаніям, які використовують ШІ, і позитивно сприймають вплив ШІ на продукти та послуги. Майже у всіх країнах, що розвиваються населення однаково довіряє звичайним компаніям і тим, що використовують ШІ. Найбільше в Китаї (76 %), Саудівській Аравії (73 %) та Індії (68 %). На противагу, лише третина громадян з високим рівнем доходу так само довіряє компаніям, що використовують ШІ, включаючи Канаду (34 %), Францію (34 %), США (35 %), Велику Британію (35 %) та Австралію (36 %).[10].

В дослідженні Trust in artificial intelligence 2023 р. також був проведений аналіз довіри населення до ШІ за демографічними показниками. Отримані результати співвідносяться з показниками глобального опитування “Глобальні думки та очікування щодо штучного інтелекту”. Дослідження виявило також значні відмінності в рівні довіри та сприйнятті систем ШІ в різних країнах.

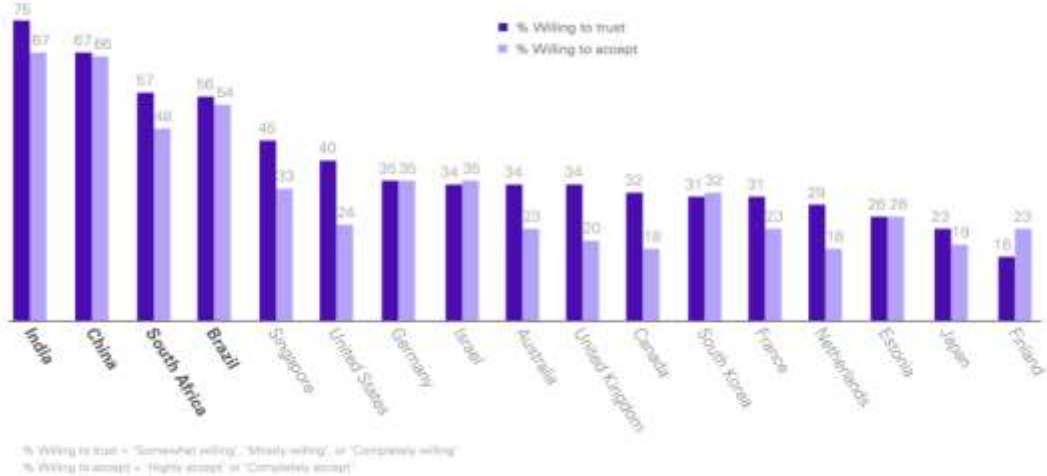

Рис. 4. Готовність довіряти та сприймати системи ШІ в різних країнах
Джерело: “Trust in artificial intelligence: A global study” (2023). URL: https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf

Як видно з Рис. 4 рівень довіри до ШІ найвищим є в Індії, Китаї, Бразилії та Південній Африці. Кожна з цих країн є частиною альянсу BICS (Brazil, India, China and South Africa) із великими економіками, що розвиваються. Альянс цих країн показав суттєво відмінні результати від інших країн світу. У країнах BICS більшість людей (56 – 75 %) довіряють системам ШІ, при цьому жителі Індії повідомляють про найбільше бажання довіряти. За Індією слідує Китай та Південна Америка. Найменше з досліджуваних країн довіряють ШІ громадяни Фінляндії (лише 16%). Подібна тенденція щодо довіри до ШІ прослідковується також у процесі сприйняття ШІ. Країни BICS значно краще сприймають ШІ : 48 – 67% людей у цих країнах повідомляють про високий рівень сприйняття. Серед лідерів знову Індія та Китай, де 66 – 67 % опитаних повідомили про високе сприйняття ШІ, порівняно з лише 18 % у Нідерландах та Канаді відповідно. Загалом *у всіх західних країнах спостерігається досить низький рівень сприйняття ШІ*, причому Німеччина повідомляє про найвищий рівень схвалення (35 %).

Більш висока довіра та визнання ШІ в країнах BICS, ймовірно, може бути пов'язана з прискореним впровадженням систем ШІ в цих країнах і дедалі важливішою економічною роллю розвитку нових цифрових технологій. Люди в країнах BICS позитивно ставляться до ШІ, бачать у ньому найбільшу користь і потенціал, повідомляючи про найвищий рівень впровадження та використання ШІ на роботі.

Якщо розглядати рівень довіри до ШІ в межах України, то досить детальний аналіз був здійснений автором у роботі "Ступінь довіри до штучного інтелекту: аналіз результатів досліджень" [8]. Результати були отримані на основі аналізу соціологічного дослідження: "Штучний інтелект: український вимір"(дата проведення 2 – 20 вересня 2018 р.), в якому взяло участь 1000 респондентів віком від 16 до 65 років [14]. Загалом населення України є обізнаним із терміном "штучний інтелект". Так, 84,7 % опитаних відповіли, що чули цей термін. В частини (34,8 %) він викликає асоціації, пов'язані з роботами та робототехнікою. Велика частина (18,2 %) асоціюють ШІ з комп'ютерами та комп'ютерними програмами. Дослідження показало також, яке відчуття виникає у них думка про існування ШІ, який може сам мислити і навчатися.

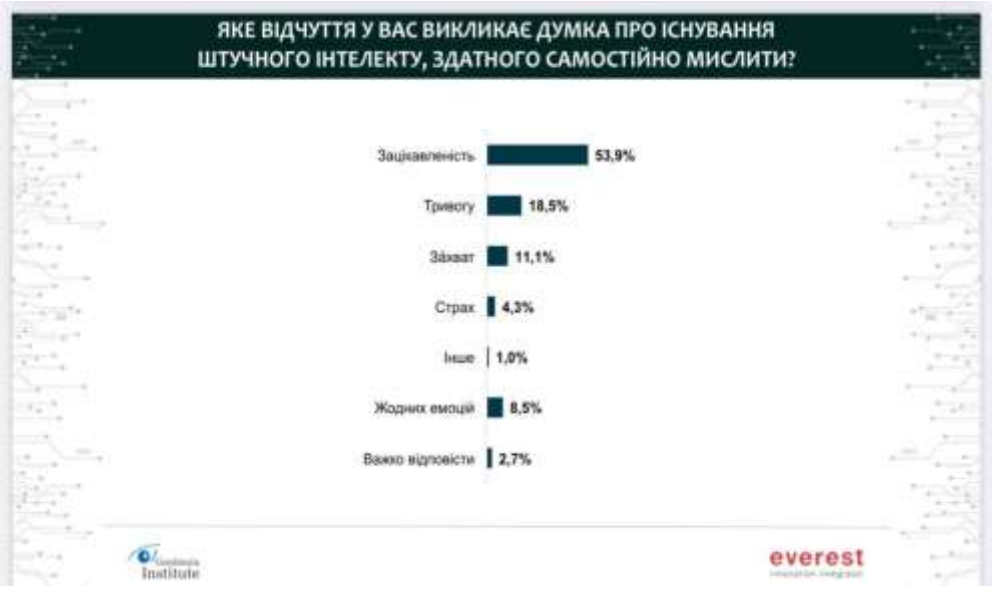

Рис. 5. Відчуття, що викликає думка про існування ШІ, здатного мислити самостійно.
Джерело: Everest. "Штучний інтелект: український вимір". URL: https://gorshenin.ua/wp-content/uploads/2018/12/Iskusstvennyj-intellekt.pdf

Відповідно до показників на Рис. 5 більшість населення (53,9 %) ставиться до ШІ із зацікавленістю, хоча 18,5 % громадян відчують тривогу. Ще однією досить поширеною емоцією є захват (11,1 %). Окремі опитані (8,5 %). не відчують нічого. Це свідчить про недостатню обізнаність щодо роботи та можливостей ШІ і відповідно ризиків та загроз. Досить невелика кількість людей в Україні (4,3 %) стикаються з відчуттям страху при думці про ШІ. Це свідчить, що українці цікавляться цифровими технологіями та розвитком ШІ і вбачають в ньому значний потенціал та можливість застосування в певних сферах економіки. [8; 14].

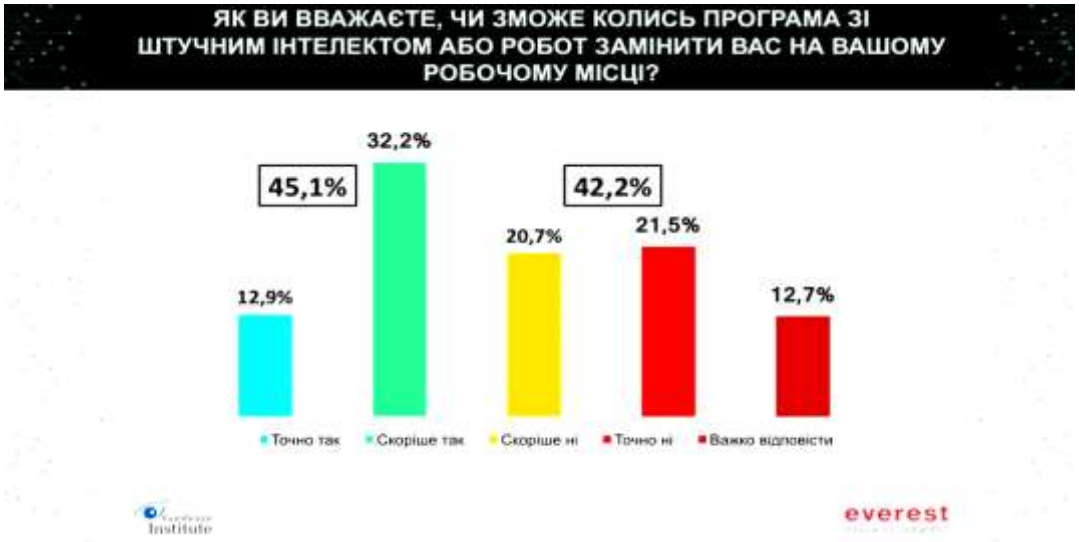

Рис. 6. Чи зможе програма зі ШІ або робот замінити Вас на робочому місці?
Джерело: Everest. “Штучний інтелект: український вимір”. URL: https://gorshenin.ua/wp-content/uploads/2018/12/Iskusstvennyj-intellekt.pdf

Попри велику зацікавленість ШІ, досить велика кількість респондентів (45,1 %) (Рис. 6), вважають, що роботи зможуть замінити їх на робочому місці. Однак, 21,5 % опитаних впевнені у тому, що програма зі ШІ не замінить їх на робочому місці [8; 9; 14]. З того часу пройшло п’ять років, з’явились нові технології. Які зміни у рівні довіри і ставленні до ШІ відбулися за цей час?

Наведемо результати нового дослідження щодо ставлення українців до ШІ.

Соціологічна служба Центру Разумкова на замовлення українського суспільно-політичного тижневика Дзеркало тижня (ZN.UA) з 23 до 28 червня 2023 р. провела дослідження серед 2018 українців віком від 18 років про те, чи використовують вони ШІ та як ставляться до нього. Теоретична похибка вибірки не перевищує 2,3 % [15]. Ось головні показники дослідження.

Обізнаність про ШІ. Майже 34 % опитаних відповіли негативно на питання “Чи знаєте ви, що таке штучний інтелект?”. Це переважно люди старше 50 років. Серед респондентів віком 30 – 39 років: 20 % не знають, що це таке; 24 % впевнені, що добре знають, про що йдеться; 42 % мають приблизне уявлення про цю технологію.

Використання ШІ. Водночас 64 % респондентів відповіли, що не використовують чат-ботів, а 8,7 % не знають, що це таке. Решта ж дійсно грається із технологією (переважно це люди від 18 до 39 років): 10,2 % опитаних використовують їх для ознайомлення; 12 % – у приватних цілях; 5,6 % – у навчанні; 8,6 % – у роботі.

Ставлення до ШІ. Серед тих, хто розуміє, що таке ШІ, на запитання, чи має держава обмежувати використання чат-ботів та інших подібних технологій ШІ, понад 27 % респондентів обрали варіант “не знаю”; 32,4 % вважають, що жодних обмежень технологія не потребує; 34 % кажуть, про потребу контролювати та обмежувати технологію; 3 % переконані, що технології треба заблокувати повністю.

Для порівняння, у США людей, переконаних, що технологія ШІ завдасть більше шкоди, ніж принесе користі, за даними AI Index Report’2023, складеного у Стенфордському університеті, наразі близько 65 % [16].

Загалом у світі складається досить схожа ситуація. Відповідно до глобального дослідження “Довіра до штучного інтелекту: глобальне дослідження” більшість людей (55 %) сприймають використання ШІ на роботі як доповнення та автоматизацію завдань і інформування про прийняття управлінських рішень, якщо ШІ не буде використовуватися для цілей управління чи контролю персоналу. Люди хочуть, щоб ШІ знаходився під повним контролем. Лише велика частина населення Китаю та Індії вважає, що ШІ забере більше робочих місць, ніж створить.

Важливе значення у ставленні людей до ШІ та довіри до його систем відіграє регулювання та контроль.

Якщо розглядати це у межах України, то більшість громадян (61,7 %) під час першого опитування вважала, що Україні потрібна власна стратегія, подібна до Національної стратегії розвитку технологій штучного інтелекту до 2030 року, яку було прийнято в Китаї. (Зазначимо, що нині у нас діє лише Концепція розвитку штучного інтелекту в Україні, а повноцінна стратегія відсутня). З них 41,3 % вибрали відповідь “радше так”, а 20,4 % – “точно так” Схожа ситуація спостерігається в міжнародному контексті. 97% людей у всьому світі вважають, що принципи та практики, на яких ґрунтуються системи ШІ, є важливими для довіри. Ці принципи повинні надавати організаціям план того, що вони мають впровадити для забезпечення довіри до використання ШІ.

Більшість людей (71 %) вважають, що регулювання ШІ є необхідним. Люди очікують певної форми зовнішнього незалежного нагляду, але лише 39 % вважають, що поточне управління, правила та закони достатні, щоб захистити людей і зробити використання ШІ безпечним.

Досить важливою складовою дослідження “Довіра до штучного інтелекту: глобальне дослідження” було виявити, які зміни відбулися у ставленні до ШІ протягом 2022 – 2023 років. Основою праці було порівняти тенденції щодо довіри до ШІ в Австралії, Великобританії, США, Канаді та Німеччині. Бажання довіряти системам ШІ суттєво зросло з 2020 по 2022 рік. Найбільше зростання відбулося щодо оцінки надійності систем ШІ в цілому, яка зросла з 35 % тих, хто погоджується, що системи ШІ є надійними у 2020 році, до 56 % у 2022 році. Підвищення відбулося в усіх країнах, з найбільшим зростанням у Німеччині. Довіра до ШІ в цілому зросла з 28 % до 36 %. Це зростання довіри, швидше за все, пов’язане із збільшенням використання, розуміння та ознайомлення з ШІ.

Можна спостерігати, що обізнаність і об’єктивне розуміння ШІ з часом зросли. Більше людей повідомляють, що користуються звичайними програмами на основі ШІ, такими як соціальні мережі чи навігаційні додатки (зросло з 56 % до 67 %), і більше людей знають, що ці програми використовують ШІ (46 % проти 56 % знають). Частка людей, які читали або чули про ШІ, також зросла (62 % до 78 %). Зокрема, люди більше обізнані про використання ШІ щодо розпізнавання тексту, облич, віртуальних помічників і додатків для навігації на дорогах. Хоча обізнаність і використання зросли в усіх країнах, найбільше зрушення відбулося у Німеччині. Попри підвищення обізнаності про ШІ, суб’єктивне розуміння людьми того, як і коли використовується ШІ, з часом не

покращилося. Не відбулося жодних змін ні в сприйнятті адекватності нормативних актів, законів і заходів безпеки для захисту людей від ризиків та загроз ШІ, ні в довірі людей до організацій щодо розробки, використання та управління ШІ.

Дослідити зміни у ставленні людей до ШІ в межах України досить складно через війну (за кордон виїхали понад 6,2 млн. українців), нестачу інформації та статистичних даних. Насторожує те, що майже 34 % опитаних українців не знають що таке ШІ. Водночас, більшість дослідників вважають, що наразі спостерігається позитивний тренд щодо використання ШІ та довіри до нього. В Україні ШІ активно використовують у різних напрямах. Зокрема на основі ШІ Мінцифри України розробляє віртуального помічника в мобільному застосунку "Дія". ШІ допомагатиме Держстату України обробляти та аналізувати дані.

Окремий тренд – використання ШІ у сфері військових технологій. Мінцифри спільно з Міноборони представили національну військову платформу Delta, яка відповідає стандартам НАТО, надаючи об'ємне розуміння поля бою в режимі реального часу: збирає дані від противника і представляє їх на цифровій мапі. ШІ допомагає фіксувати переміщення техніки та особового складу окупантів, збивати ворожі ракети, ефективніше наводити на цілі БПЛА тощо. ШІ використовують в розмінування деокупованих територій [17]. Уряд ухвалив рішення про запуск так званої "регуляторної пісочниці" (sandbox) для розробників ШІ. Сформувався і відповідний ринок кадрів: майже 10 тис. ІТ-інженерів спеціалізуються на системах ШІ. В Україні створюють умови, щоб топові міжнародні компанії, які займаються ШІ, приходили на український ринок.

Ризики і загрози генеративного ШІ. Генеративний штучний інтелект (далі – ГШІ) – це новий різновид ШІ. Він не лише інтерпретує інформацію, а й створює оригінальний контент, поєднує в собі можливості машинного навчання, глибокого навчання та ШІ для створення тексту, відео, аудіо, коду та зображень. Популярний чат ChatGPT – один із прикладів ГШІ. Найчастіше ним користуються представники покоління бебі-бумерів – 53,5 % із них. (Бебі-бумери є демографічною когортою, яка прийшла після мовчазного покоління і передує поколінню X. Покоління бебі-бумерів визначають як осіб народжених між 1946 та 1964 роками). Більше того, до 70 % з них готові звернутися за порадою до ГШІ щодо особистих стосунків або життєвих та професійних планів. ГШІ використовується для створення аудіоконтенту, зображень, текстів та відео. Він має потенціал виконувати завдання, які досі були доступні тільки людям. Популярність його інструментів – ChatGPT, Midjurney чи DALL-e 2 – постійно зростає. ChatGPT зараз має понад 100 млн. користувачів. DALL-e 2, який використовується для створення зображень, знадобилося близько 2,5 місяців, щоб охопити 1 млн. людей. Згідно з звітом Capgemini, "Чому споживачі люблять генеративний ШІ?" 51 % споживачів знають останні тенденції в галузі ГШІ та використовували його інструменти. 35 % знають про існування ШІ, але не використовували його на практиці. Цікаво, що люди із покоління бебі-бумерів демонструють найвищий рівень використання цих інструментів (53,5 %). Це більше, ніж у молодших представників поколінь X (51,7 %), Z (50,8 %) та міленіалів (50,2 %). Користувачі найчастіше використовують ГШІ для створення контенту (52 %) та мозкового штурму (28 %). З погляду статі результати дуже схожі. Жінки (49,7 %) та чоловіки (51,9 %) знають останні тенденції у ГШІ та використовують такі інструменти, як ChatGPT або DALL-E. Найвищий відсоток користувачів (56,5 %), які використовували інструменти ГШІ, знаходиться у Японії. Сінгапур посідає друге місце (54,4 %), а Швеція – третє (54,3 %).

Чи довіряють користувачі інструментам ГШІ? Рівень довіри до ГШІ надзвичайно високий: 73 % респондентів довіряють контенту з генеративних платформ, навіть за такими складними темами, як фінанси, медицина чи міжособистісні стосунки. Найбільшу ступінь

довіри мають норвежці (79 %) та іспанці (75 %). Звіт показує, що 53 % опитаних довіряють фінансовому плануванню на основі ГШІ. 67 % могли б отримати користь від медичних консультацій, що ґрунтуються на ГШІ. Однак не всі (66 %) користувачів, були б готові отримати пораду від ГШІ щодо особистих взаємодій або відносин (робота, дружба, романтичні відносини), а також кар'єри. Так бебі-бумери частіше (70 %) звертаються за порадою щодо особистих стосунків чи планів життя та кар'єри, ніж респонденти молодого покоління. Однак, це небезпечно – надто висока довіра. На думку авторів звіту, високий рівень довіри може наразити людей, які використовують ГШІ, на небезпеку, що походить від фейкових новин, дипфейків, кібератак та плагіату. ГШІ вже масово використовується для створення фейкових новин. Нещодавно у Китаї арештували чоловіка за використання ChatGPT для створення фейкової статті про катастрофу поїзда, якого ніколи не було. Напередодні майбутніх президентських виборів у США у 2024 р. експерти попереджають про можливість ГШІ поширювати дезінформацію, яка може маніпулювати громадською думкою. Попри дедалі частіші заклики до обмеження довіри до ГШІ, майже половину (49 %) респондентів проблема фейкових новин не турбує. Автори доповіді "Чому споживачі люблять генеративний ШІ?" підсумовують: експериментуючи з ГШІ, важливо пам'ятати, що це технологія, що зароджується, яка ще не готова діяти автономно в будь-якій ситуації. Організації, які розробляють або використовують ГШІ, повинні гарантувати, що результати їх діяльності є неупередженими, надійними, безпечними та поважають конфіденційність. Людський нагляд є ключем до спільного вирішення проблем, що виникають після появи генеративного ШІ [18].

7 вересня 2023 р. ЮНЕСКО оприлюднило перше керівництво щодо застосування генеративного штучного інтелекту (GenAI) у сфері освіти (Guidance for generative AI in education and research), в якому закликало уряди контролювати технологію, зокрема захищати приватність даних та встановлювати вікові обмеження для користувачів [19].

Опитування: 66 % ризик-менеджерів назвали ГШІ загрозою для організацій. ГШІ став одним із головних ризиків для організацій, що випливає з опитування Gartner. Його згадали 66 % респондентів. Опитування провели серед 249 керівників служб управління корпоративними ризиками у другому кварталі 2023 року. ГШІ вперше потрапив до цього рейтингу. До топ-5 основних ризиків для організацій за частотою згадок увійшли: життєздатність контрагентів (67 %); масова доступність ГШІ (66 %); невизначеність фінансового планування (62 %); концентрація операцій у хмарі (62 %); напруженість у торгівлі з Китаєм (56 %). У зв'язку з розвитком ГШІ можна виділити три сегменти, які необхідно контролювати з точки зору управління корпоративними ризиками: *інтелектуальна власність, конфіденційність даних та кібербезпека*.

Економічний потенціал ГШІ. Опублікований нещодавно звіт компанії McKinsey про економічний потенціал ГШІ [20] свідчить про його значний вплив на підвищення продуктивності. У звіті вивчено 16 бізнес-функцій та розглянуто 63 сценарії використання, в яких технологія може вирішувати конкретні бізнес-завдання, приносячи один або кілька вимірюваних результатів. Серед головних прогнозів варто відзначити такі: На думку аналітиків, ГШІ може щорічно додавати до світового ВВП від 2,6 до 4,4 трлн. дол., що, для прикладу, перевищує ВВП Італії. Загалом це збільшить віддачу всього ШІ на 15 – 40 %. ГШІ вплине на всі галузі. Банківська справа, високі технології та медико-біологічні науки входять до числа індустрій, які можуть отримати від застосування таких технологій найбільший ефект у відсотковому відношенні до своїх доходів. Близько 75 % цінності, яку можуть принести рішення на основі ГШІ, припадає на чотири області: клієнтські операції, маркетинг та продаж, розробка ПЗ та науково-дослідні роботи. ГШІ здатний змінити анатомію праці, розширивши можливості окремих працівників за рахунок автоматизації

деяких видів їхньої діяльності. Нині ця та інші технології здатні автоматизувати трудову діяльність, що займає 60 – 70 % робочого часу працівників. Прискорення темпів автоматизації багато в чому пов'язане з розширенням можливостей ГШІ з розуміння природної мови, що необхідно для виконання робіт, на які припадає 25 % загального робочого дня. Темпи трансформації робочої сили, ймовірно, прискорюватимуться з огляду на зростання потенціалу автоматизації. Згідно з оновленими сценаріями McKinsey, що включають розвиток технології, економічну доцільність та терміни поширення, половина сучасних видів трудової діяльності може бути автоматизована в період з 2030 по 2060 рр., з медіаною у 2045-му, що приблизно на десятиліття раніше, ніж у попередніх оцінках. Загалом експерти впевнені, що ГШІ здатний суттєво підвищити продуктивність праці в усій економіці, однак для цього будуть потрібні інвестиції на підтримку працівників при зміні видів діяльності або місця роботи. У період до 2040 року ГШІ може забезпечити зростання продуктивності праці на 0,1 – 0,6 % на рік, залежно від темпів впровадження технології та перерозподілу робочого часу на користь інших видів діяльності.

AI Index Report'2023. У річному звіті AI Index за 2023 рік Стенфордського інституту ШІ відстежуються, зіставляються та візуалізуються дані, що стосуються ШІ. Їх аналіз дозволяє особам, які приймають рішення, робити відповідні висновки та вживати дії для відповідального та етичного розвитку ШІ з урахуванням інтересів людини. Цього року звіт включав новий аналіз базових моделей, їхню геополітику та витрати на навчання, вплив систем ШІ на навколишнє середовище, освіту в галузі ШІ та тенденції громадської думки в галузі ШІ. Індекс ШІ також розширив відстеження глобального законодавства в галузі ШІ з 25 країн у 2022 році до 127 у 2023 році. Зростає інтерес політиків до ШІ. Аналіз законодавчих актів 127 країн показує, що кількість законопроектів, що містять термін "штучний інтелект", які були прийняті як закон, зросла з 1 у 2016 році до 37 у 2022 році. Аналіз парламентських протоколів щодо ШІ також у 81 країні показує, що з 2016 року кількість згадок про ШІ у світових законодавчих процедурах зросла майже в 6,5 разів [16].

Висновки.

Сфера ШІ продовжує стрімко розвиватися, попри те, що сам ШІ існує вже кілька десятиліть. Враховуючи нещодавнє стрімке зростання ГШІ та автоматизації на основі ШІ, ця еволюція, схоже, рухається вже з подвійною швидкістю – або навіть швидше. Водночас, попри підвищення обізнаності про ШІ, суб'єктивне розуміння людьми того, як і коли використовується ШІ, з часом не покращилося. Не відбулося змін ні в сприйнятті адекватності нормативних актів, законів і заходів безпеки для захисту людей від ризиків та загроз ШІ, ні в довірі людей щодо розробки, використання та управління ШІ. Довіра та ставлення до ШІ відрізняються в залежності від країни, рівня освіти, статі та рівня доходу. Західні країни, а також Японія, Південна Корея та Ізраїль, як правило, мають нижчу довіру та менш позитивне ставлення до ШІ, ніж люди в країнах з економікою, що розвивається. Різні рівні довіри та сприйняття ШІ в країнах в основному спричинені трьома ключовими факторами:

– Відмінності у сприйнятті переваг ШІ та ступеня, до якого вони переважають потенційні ризики: люди в західних країнах, Японії, Південній Кореї та Ізраїлі менш схильні вірити, що переваги ШІ перекривають ризики в порівнянні з людьми в країнах BISC і Сінгапурі.

– Уявлення про інституційні гарантії: дослідження показують, що між країнами існують відмінності в сприйнятті адекватності гарантій і правил для безпечного використання ШІ, а також у довірі до установ, які повинні бути відповідальними до дотримання всіх правил. Лише невелика кількість людей у західних країнах, Японії,

Південній Кореї та Ізраїлі вважають чинні закони та правила щодо захисту ШІ достатніми. Також вони повідомляють про набагато меншу довіру до компаній щодо розробки, використання та управління ШІ порівняно з жителями Бразилії, Індії, Китаю та Сінгапуру.

– Ознайомлення зі ШІ та розуміння принципів роботи: люди в західних країнах зазвичай повідомляють про те, що вони менше використовують ШІ на своїх робочих місцях, а також менше користуються ШІ в звичайних програмах порівняно з людьми в країнах BICS і Сінгапурі.

Встановлено, що інституційні гарантії та довіра до суб'єктів використання та управління ШІ є найсильнішим рушієм довіри. На жаль, інституційні процеси підтримки ШІ відстають і не встигають за очікуваннями суспільства. Враховуючи, що громадськість найбільше довіряє університетам і дослідницьким організаціям у розробці, використанні та управлінні системами ШІ, потенційним рішенням для бізнесу та уряду є співробітництво з цими організаціями щодо ініціатив ШІ. Ще однією практикою підвищення довіри є збереження участі людей щодо нагляду за рішеннями, які впливають на користувача ШІ. Важливим елементом впливу на довіру є також демонстрація відчутного позитивного впливу ШІ на людей і суспільство. Це підкреслює важливість наявності чіткої корисної мети на початку створення проектів ШІ.

Загалом Європейський Союз і Канада вважаються лідерами в області ШІ, управління даними та етики. У Європейському Парламенті зробили важливий крок до регулювання ШІ, визначивши потенційно шкідливі наслідки цієї технології. ЄС до 2025 р. збирається ухвалити закон Artificial Intelligence Act. Одна з головних цілей документа полягає у захисті прав і свобод осіб, які підлягають впливу ШІ. Закон визначає принципи та правила для оброблення персональних даних, використання систем автоматизованого прийняття рішень та інших аспектів ШІ, забезпечуючи прозорість, справедливість і законність оброблення даних. Прийняття акта безпосередньо вплине і на регулювання ШІ в Україні, адже країни-кандидати до ЄС повинні будуть імплементувати його норми у своє законодавство. Хоча рівень довіри до ШІ в Україні протягом останніх років дещо зростає, питання правового регулювання ШІ залишається відкритим. Попри це Україна має великі перспективи виростання ШІ в різних сферах економіки і в т. ч. в оборонній сфері, що зможе прискорити перемогу. Україні варто здійснити такі необхідні кроки: розробити Стратегію розвитку ШІ, дослідити особливості та основні вимоги законопроекту ЄС (AI Act) для підготовки до його імплементації; розпочати роботу із розробки державних стандартів України у галузі ШІ, Кодексу етики ШІ, запровадження законодавчого закріплення роботи "регуляторних пісочниць" (sandbox) з ШІ; організувати роботу експертних груп спеціалістів у сфері ГШІ та законотворення, які визначать основні сфери правового регулювання ШІ та підготують відповідні законопроекти; визначити регуляторний орган у сфері ГШІ з основною функцією контролю за дотриманням законодавства.

Використана література

1. Китай вступив у перегони зі США у сфері штучного інтелекту. – (Bloomberg). Цьогорічні інвестиції в штучний інтелект у Сполучених Штатах перевищують показники КНР у шість разів. URL: https://lb.ua/tech/2023/06/28/562639_kitay_vstupiv_peregoni_zi_ssha_sferi.html

2. Roman Lukyanenko, Wolfgang Maass, Veda C. Storey. Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities. URL: https://libraopen.lib.virginia.edu/downloads/pz50gw351

3. Wolfgang Maass, Veda C. Storey. Trust in artifcial intelligence: From a Roman Lukyanenko Foundational Trust Framework to emerging research opportunities. 28 November 2022. URL: https://link.springer.com/content/pdf/10.1007/s12525-022-00605-4.pdf?pdf=button

4. Ella Glikson, Anita Williams Woolley. Human trust in artificial intelligence: review of empirical research. 2020. URL: https://leeds-faculty.colorado.edu/dahe7472/OB2022/glickson2021.pdf

5.René Riedl. Is trust in artifcial intelligence systems related to user personality? Review of empirical evidence and future research directions. 11 February 2022. URL:https://link.springer.com/content/pdf/10.1007/s12525-022-00594-4.pdf?pdf=button

6. Professor Nicole Gillespie, Dr Steve Lockey, Dr Caitlin Curtis and Dr Javad Pool. Trust in artificial intelligence: A global study (2023). URL: https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf

7. Monografia Zaufanie do systemów sztucznej inteligencji. URL: https://www.ans.pw.edu.pl/Aktualnosci/Monografia-Zaufanie-do-systemow-sztucznej-inteligencji

8. Андрощук Г.О. Ступінь довіри до штучного інтелекту: аналіз результатів дослідження. URL: https://ndipzir.org.ua/wp-content/uploads/2021/Conf_20.09.21/3.pdf

9. Андрощук Г.О. Рівень довіри і ставлення до штучного інтелекту*:* аналіз результатів досліджень. *Часопис Київського університету права*. 2021. № 3. С.195-201.

10. IPSOS. Global opinions and expectations about artificial intelligence. January 2022. URL : https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Global-opinions-and-expectations-about-AI-2022.pdf

11. Баранов О.А. Визначення терміну "штучний інтелект". *Інформація і право*. № 1(44)/2023. С. 32-49.

12. Trust in artificial intelligence: A global study (2023). URL: https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/trust-in-ai-global-insights-2023.pdf

13. GLOBAL OPINIONS AND EXPECTATIONS ABOUT ARTIFICIAL INTELLIGENCE A Global Advisor survey. URL: https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Global-opinions-and-expectations-about-AI-2022.pdf

14. Everest. "Штучний інтелект: український вимір". Київ, 2018. URL: https://gorshenin.ua/wp-content/uploads/2018/12/Iskusstvennyj-intellekt.pdf

15. Як українці ставляться до ШІ. – (Опитування ZN.UA та Центру Разумкова). URL: https://media maker.me/news/yak-ukrayinczi-stavlyatsya-do-shi-opytuvannya-zn-ua-ta-czentru-razumkova

16. THE AI INDEX REPORT Measuring trends in Artificial Intelligence. URL AI Index Report 2023 – Artificial Intelligence Index (stanford.edu)

17. Кацімон О. Україна почала роботу над правовим регулюванням штучного інтелекту. URL: https://suspilne.media/543113-ukraina-pocala-robotu-nad-pravovim-reguluvannam-stucnogo-intelektu-fedorov

18. Gartner Survey Shows Generative AI Has Become an Emerging Risk for Enterprises. URL: https://www.gartner. com/ en/newsroom/press-releases/2023-08-08-gartner-survey-shows-generative-ai-has-become-an-emerging-risk-for-ent erprises

19. Supantha Mukherjee UNESCO seeks regulation in first guidance on GenAI use in education. URL: UNESCO seeks regulation in first guidance on GenAI use in education | Reuters

20. Дослідження: генеративний ШІ прискорить темпи трансформації робочої сили. URL: https://www. pcweek.ua/themes/detail.php?ID=167311&THEME_ID=13880

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

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

УДК 327:342.76

ОМЕЛЬЧЕНКО І.К., *кандидат юридичних наук,* старший науковий співробітник НДІ інформатики, безпеки та права НАПрН України.
ЯЩЕНКО В.А., *доктор юридичних наук, професор,* головний науковий співробітник НДІ інформатики, безпеки та права НАПрН України.
ORCID: https://orcid.org/0000-0002-2257-318X.

ЄВРАЗІЙСТВО ЯК ПРЕТЕНЗІЙНІСТЬ НА ІДЕОЛОГІЧНУ ПАРАДИГМУ РОСІЇ

Анотація. *У статті простежується зародження, еволюція й трансформація євразійських ідей, поглядів та постулатів протягом значного, майже столітнього часу, констатується теоретична неспроможність означеного феномену набути статусу державної ідеології рф. Зважаючи на перетворення російської православної церкви у сателіт злочинного кремлівського путінського режиму, спростовується запропонована євразійцями ідея провідної ролі руського православ'я у формуванні духовної особистості росіян і піддається критиці постулат формування церквою "симфонічної особистості". Розглядаються складові ідеологічної парадигми євразійства як визначальної компоненти поглядів і орієнтацій його авторів, з позицій цивілізаційних досягнень людства, критично оцінюються окремі постулати євразійства щодо зведення функцій народу лише до задоволення господарських потреб, збереження ієрархічного поділу громадян, ідеократичний, елітарний спосіб формування влади, агресивно месіанські погляди стосовно інших народів. Робиться висновок, що ці погляди об'єктивно можуть сприяти зростанню геополітичних амбіцій росії і намаганнями їх реалізувати найбільш небезпечним, військовим способом.*

Ключові слова*. Євразійство, руське православ'я, соборність, симфонізм, демотія, ідеократія, серединна євразійська ідеологія.*

Summary*. The article traces the emergence, evolution and transformation of Eurasian ideas, views and postulates over a considerable (almost a century) period of time, and states the theoretical inability of this phenomenon to acquire the status of the state ideology of the rf. In view of the transformation of the russian orthodox Church into a satellite of the criminal kremlin putin regime, the author refutes the idea of the leading role of russian orthodoxy in shaping the spiritual personality of russians proposed by Eurasians and criticises the postulate of the church's formation of a "symphonic personality". The author analyses in detail the substantive components of the ideological paradigm of Eurasianism as a defining component of the views and orientations of its authors from the standpoint of the civilisational achievements of mankind, critically assesses certain postulates of Eurasianism regarding the reduction of the functions of the people to the satisfaction of economic needs, the preservation of the hierarchical division of citizens, the ideological, elitist way of forming power, and aggressively messianic views towards other peoples. It is concluded that these views can objectively contribute to the growth of russia's geopolitical ambitions and attempts to realise them in the most dangerous, military way.*

Keywords*. Eurasianism, russian orthodoxy, conliliarity, symphonism demotia, ideocracy, middle Eurasian ideology.*

Постановка проблеми. Останнім часом в інформаційному, політичному просторі рф дедалі більше здійснюється апеляція до євразійського вчення як однієї з можливих ідеологічних основ побудови російської держави і її майбутнього. Оскільки окремі ідеї

євразійства взято на озброєння путінським режимом як знаряддя інформаційної війни, зокрема виправдання відкритої широкомасштабної агресії проти України, використовуючи аргументи "єдності росії та Євразії, приналежності історичних територій" тощо, виникла потреба критично проаналізувати ідеологію євразійства і реальний стан проблеми.

Результати аналізу наукових публікацій. Підвищення інтересу до євразійського вчення зумовило перевидання у 2000 роках теоретичних праць засновників євразійства: Н. Алексєєва [2], М. Трубецького [3] та ін., звернення науковців до документів програмного, доктринального змісту, в першу чергу маніфесту: "Євразійство. Досвід узагальненого бачення. Видання 1926 р." [1].

Цей інтерес спонукав також до аналізу різних аспектів євразійства. Це, зокрема, праці Замараєвої Є.І. про питання нації і націоналізму у філософії євразійства [4], Абаєва Н.В., Фельдмана В.Р. щодо євразійства і майбутнього росії [5], Лебедева С.Н. про проблеми держави у вченні євразійців [6] та багато інших. Основний зміст цих праць зводиться до того, щоб пов'язати традиційні євразійські постулати з сучасними російськими реаліями, апеляцією до потреби врахування євразійських ідей в російському державотворенні, представити євразійський союз як політичну та економічну інтеграцію країн, що входять до сфери впливу росії. Ще на початку 2000-х років тодішнє керівництво кремля здійснило спробу актуалізувати питання створення економічного та політичного євразійського союзу, використовуючи ідеї та принципи євразійців. Крім цього, критично-конструктивний аналіз євразійства був здійснений українською вченою В.І. Тимошенко, яка ґрунтовно розглянула головне в євразійському вченні – його державне "ідеократичне" ядро [8].

Метою статті є оцінка євразійського вчення через призму його основних постулатів: побудови "ідеократичної" держави, ідеї "соборності" та "симфонічності" особистості і здійснення висновків про його фактичну роль у формуванні світобачення у громадян росії.

Виклад основного матеріалу. У сучасній енциклопедичній літературі феномен євразійства визначається як "ідеократичне геополітичне і соціально-філософське вчення, морфологічний комплекс ідей і інтелектуальний рух, який конституювався в 1921 році в середовищі російської еміграції" [9, с. 351]. Це фактично була їх реакція на події, що відбулися в росії на початку XX століття і призвели до повалення царської влади та встановлення більшовицького режиму, як ностальгія по втраченому. Цей об'єктивний за змістом, але суб'єктивний за формою соціально-психологічний чинник і лежить, на нашу думку, в основі означеного вище "конституювання" євразійства.

Показово, що соціально-психологічний феномен ностальгії за втраченим був не лише приводом до зародження євразійства. Він згодом ввійшов органічним атрибутом в його зміст (уявлення про майбутнє росії як держави імперського типу (подібної до монголо-татарської імперії) з транскордонним впливом на всю Євразію, нерівноправність громадян держави, месіанство стосовно інших народів тощо) став притаманним будь-якому представнику цієї течії. При цьому Західна Європа не включається до євразійства, вона йому протиставляється і, більш того, навіть виступає "ворожою" росії.

Так, туга за старим об'єднує, наприклад, одного з засновників євразійства – Н. Алексєєва, який ще в 30-і роки залишався на імперських позиціях щодо статусу росії, і "модерного" ліворадикального євразійця С. Кара-Мурзу, що ідеалізує радянський режим [10]. Означене є свідченням того, що євразійці, як засновники цього вчення, так і

сучасні його послідовники, незалежно від їх політичної орієнтації, перебувають у полоні ретроградства й обскурантизму, оскільки, не дивлячись на апеляцію до модернізму, з ідеологічної точки зору стоять на позиціях вчорашнього, утопічного. Гадаємо, що ця, відкрита нами закономірність здійснила вплив і на всі інші теоретичні побудови євразійців.

Перш за все – на їх гносеологію, зокрема, діалектику сутності та явища. Якщо у кожного предмета чи явища при багатстві його проявів сутність завжди лише одна, євразійство, на думку його представників, є двосутнісним феноменом. З одного боку, воно конституюється як територіальна даність, а саме, "територія між лінією Балтика – Адріатика і Кавказьким хребтом, що включає Середню Азію, обмежена Курилами й кордоном з Китаєм на сході й південному Сході" [9, с. 351]. З іншого – як унікальна ідеологічна парадигма, що поєднує у своєрідний конгломерат російське православ'я і державний устрій росії, що нібито є зразком для інших народів. У зв'язку з цим Н. Алексєєв називає росію "центральним сонцем Євразії" [2].

Те, що термін "євразійство" запозичений з географічного лексикону, цілком природно, але у євразійців цей термін, як і більшість інших географічних понять, що ними запозичені, соціально заангажовані.

Як наслідок, росія, як державний інститут, територіально (географічно) ототожнюється з євразійством. Як пишуть євразійці: "Євразія це росія, тож під євразійством розуміється все російське і слід вживати термін не "російська нація", а "євразійська нація". Звідси вибудовується концепція росії як "серединної" імперії, що зумовлює особливі геополітичні амбіції: росія розповсюджує свої інтереси на всю сферу навколишнього світу, в якому у тій чи іншій мірі існує російська мова та культура. Тому ця культура, наполягають євразійці, і особливо рашисти, не євразійська, а російська.

Уже цей контекст дає можливість зробити висновок про те, що в центрі цього вчення була здійснена спроба саме ідеологічного обґрунтування євразійства. Але при цьому в ідеологічний арсенал вони включають фактично будь – яке знання, а не лише теоретичне: неоформлене, несуттєве, повсякденне. Хоча насправді ідеологічний чинник слід розглядати лише в межах співвідношення двох парадигм людської свідомості – теоретичної і психологічної.

Водночас ідеологічний рівень свідомості проявляється в певних формах. Ці форми відомі: політична ідеологія, правова, наукова, релігійна ідеологія тощо. Особливість ідеології євразійства в тому, що в їх вченні здійснюється апеляція не стільки до політичної ідеології, скільки до релігійної, зокрема православ'я.

Водночас цю релігійну форму вони наповнюють політичним змістом, вказуючи на панівну роль у світі саме російського православ'я. Цим самим мимоволі надаючи цій релігійній складовій політичного статусу і формування свідомості "зверхності" над іншими релігійними течіями. Вже навіть у цьому проявляється імперська амбіційність євразійства.

На нашу думку, релігійно-ідеологічний чинник насправді є інститутом другого порядку. Він лише освячував те, що реально здійснювалось іншими повсякденними факторами. В основі ідеологічної концепції євразійців – вороже ставлення Заходу до росії, яка змушена від нього захищатися. Не останню роль при цьому відіграли ті обставини, що десятками років офіційна політика як більшовицької росії так і путінського режиму була спрямована на те, щоб довести, що Захід нібито намагається силою захопити необмежені природні багатства росії і тому оточує її військовими блоками.

Фактично ця обставина у сучасній політиці росії була зведена до абсолюту і стала ключовою у протистоянні росії Заходу і сформувала у росії відповідний ідеологічний стереотип, який залишається, на жаль, незмінним і до сьогоднішнього дня, лише загострюючись.

Поряд з цим, вважаємо, що заграваннz з релігійним чинником не є просто даниною минулому, воно викликано тим, що на думку євразійців, цей чинник є природним для світобачення росіян. Тобто, він і спосіб буття, і формування свідомості, і включення у так звану релігійну віртуальність, яка створює свою реальність, що не відповідає об'єктивному ходу подій.

Цим вимогам, на думку євразійців, відповідає саме російське православ'я, якому ними надається статус особливого релігійно – політичного вчення, що домінує над усіма іншими і є водночас таким, що відповідає потребам усього руського. Фактично цим самим в ранг ідеології зводиться не лише політична, правова, релігійна форми свідомості, а вона розглядається значно ширше, як уся конструкція моральних принципів та норм поведінки росіян.

Тому практичним інструментом ідеології у авторів євразійства, регулятором суспільного життя, виступає "соборність" особистості, яку повинне забезпечити руське православ'я. Цей архетип дійсно виступає одним із постулатів православної церкви, а також досить детально розроблявся ще слов'янофілами. Так, у публікації ""Православна релігійна думка XIX-XX ст." вказується на наступне: "Розв'язання проблеми співвідношення свободи і необхідності, індивідуального та соборного начала служить у слов'янофілів важливим методологічним принципом для розробки ключового поняття їх релігійно-філософських поглядів – поняття соборності". Визначальною ознакою соборності визнається принцип "єдності у множинності". Поняття "соборний" розкриває не тільки зовнішнє, видиме єднання людей у будь-якому місці, але й постійну можливість такого з'єднання на основі духовної спільності. Соборність проявляється у всіх сферах життєдіяльності людини: в церкві, в сім'ї, в суспільстві, у відношеннях між державами тощо. Вона є наслідком, результатом взаємодії вільного людського начала ("свободи волі людини") та божественного начала ("благодаті") [11, с. 1]. Водночас яким чином досягти цієї соборності євразійці не розкривають. Тому навряд чи цей принцип можна віднести до здобутків євразійської ідеології. Тим більше, що внаслідок об'єднання православ'я з самодержавною владою, з нинішнім фашистським режимом у росії "соборність" фактично стала теократичною утопією.

Це пояснює те, чому євразійці підмінюють ідеологічний чинник буденним, повсякденним, пов'язаним безпосередньо не лише зі свідомістю чи виробництвом, а й з тим, що так би мовити, знаходиться між ними. Наприклад, мова, звичаї, традиції тощо.

На нашу думку, такий підхід дає можливість сформувати ще на психологічному, буденному рівні ті ідеологеми, які кон'юнктурне вигідні будь – якому політичному режиму росії і сприймаються її громадянами як об'єктивна необхідність. Немає сумніву в тому, що саме такий підхід використаний сучасним політичним керівництвом росії для виправдання широкомасштабної війни проти України.

Важливим фактором ідеології євразійства є надання цій парадигмі "системно-утворюючого" зв'язку. Така ідеологія, на думку М. Трубецького, "може впливати з деякої абсолютної стрижневої ідеї і, заземлюючись", конкретизуючись, стає "правительницею", а вся система влади оформляється в "ідеократію" [3, с. 314]. Термін "ідеократія" був введений в євразійський лексикон М. Алексєєвим як поняття про такий соціально-державний устрій, в основі якого лежить державна ідея, ідея "правительниця", а вся система влади оформляється в ідеократію. Євразійська держава,

– пише він, – є політичним утворенням, як ми говоримо, демотичної природи. Ми хочемо цим сказати, що держава наша побудована на глибоких народних основах і відповідає "народній волі" …ми будуємо нашу державу на суверенітеті народу, але не на тому дезорганізованому, анархічному суверенітеті, на якому будуються західні демократії), а на суверенітеті організованому і тактичному Ми вважаємо "народом" чи "нацією" не будь-який набір громадян, що задовольняють умовам загального виборчого права, а сукупність історичних поколінь, минулих, нинішніх і майбутніх, що створюють оформлену державою єдність культури. Ми усвідомлюємо, що нація в такому розумінні неспроможна до будь-якої політичної дії, що вона недієздатна, що вона повинна діяти через якихось заступників, що воля її повинна отримати вираження через визначеного реального носія" [2, с. 315]. Тим самим, писав Н.С. Трубецкой: "Згідно євразійського вчення про правлячий відбір, у всякій державі обов'язково повинні існувати правлячі верстви, але основні ознаки, за якими ці верстви відбираються, не у всіх державах однакові. Існують різні типи відбору, наприклад, аристократичний, плутократичний, демократичний і т.п. і відповідно з цим різні типи держав. Той тип відбору, який, згідно євразійськоого вчення, нині має установитися у світі, і, зокрема, в росії – Євразії, називається ідеократичним і відрізняється тим, що основною ознакою, якою при цьому типі відбору об'єднуються члени правлячих верств, є спільність світогляду" [2, с. 1].

Один з засновників євразійства В.Н. Ільїн вважав ідеологію не лише основоположним, а й процедурно-технологічним феноменом, тому, за Ільїним: "Ідеократія – не лише фундамент держави й суспільства, а й стиль управління країною, саме шляхом ідеологічної інформації мас, або, якщо завгодно, шляхом ідеологічного їх інструктування, що повинно обов'язково супроводжуватися їх заінтересованістю і пробудженням в них ідеологічних симпатій" [10, с. 352].

Ключовим тут виступав спосіб побудови держави як рушійної сили здійснюваних перетворень. Водночас за основу побудови росії – Євразії пропонувалась ідеократична модель влади, яка функціонує за елітарним принципом, де народ (демотія) виконує лише господарчі функції, не втручаючись у владні повноваження.

Аналіз цих висловлювань свідчить про те, що фактично мова йде про запровадження тоталітарного режиму, який зберігався в росії незалежно від типу та форми державного устрою і пропонується під назвою "євразійство". Для Європи XX століття така форма держави не сприймалася як європейська демократія, скоріше як напів теократична, з елементами феодалізму, яку Європа пройшла ще в середньовіччі. Тобто, претендувати на європейськість через побудову держави ідеократичного типу неправомірно. Наступний історичний досвід свідчить про відсутність перепон переростання ідеократії у фашизм, як це було, зокрема в Італії, "який у первісному варіанті італійської ідеократії тяжів до забезпечення національної єдності під владою сильної держави, передбачав синтез концепції нації як цінності та догматизованого принципу справедливості…, як синтезований тип ідеократії, який передбачає втілення ідей расизму, шовінізму, зовнішньополітичної експансії" [13, с. 85].

Важливим елементом механізму реалізації ідеократичної держави у євразійців виступає поняття "автаркії", через яке проводиться ідея співпадіння євразійської території і євразійської держави – росії. "Природня автаркія євразійської території зумовлює політичну автаркію держави й особливості його ідеократичного устрою, його закритої всередині себе ідеології: територія справжньої ідеократичної держави неодмінно повинна співпадати з будь-яким автарктичним особливим світом" [10, с. 316].

Дослідники євразійства констатують існування двох концепцій держави у теоретиків євразійства: концепції "держави правди" і концепції "ідеократичної,

демотичної й гарантійної" держави [9,с.566). Між цими концепціями існують суттєві розбіжності. У концепції "держави правди" гарантом існування і реалізації внутрішньодержавних заходів виступає народ, а в концепції "ідеократичної" держави сама держава виступає таким гарантом.

Як стверджує В.І. Тимошенко: "Держава правди" євразійців поєднує в собі правові закони й гарантійні норми з началами моралі ті совісті… Головна місія "держави правди", справедливої держави – підпорядкування державності цінностям, які мають неперехідне значення. З цього випливає, що "держава правди" – не кінцевий ідеал, досягнутий в результаті соціальних перетворень, а лише етап на шляху до істини" [9, с. 566].

Для прибічників євразійської концепції "ідеократичної, демотичної держави" всі означені цінності – релятивні, плинні. "Ідеократичність, – вважає В. Тимошенко, – вимагає жертовності. Ця жертовність здійснюється не в ім'я поняття "народ" або "людина", вона в ім'я серединного поняття – "особливого світу", під яким розуміється "росія – Євразія" [9, с. 568].

Утопічність такого ідеалу очевидна. Її не можуть заперечувати навіть самі євразійці. Н.С. Трубецкой навіть охрестив його "кошмаром": "Ми цілком вірно зрозуміли, що державний устрій сучасності й найближчого майбутнього є устрій ідеократичний. Але, якщо вглядишся пильніше в конкретні втілення цього устрою, то приходиш до висновку, що це не ідеал, а найповніший кошмар, при чому дуже сумнівно, щоб такий устрій і надалі міг стати чим небудь іншим" [10, с. 306].

Щоб не бути звинуваченими в дистанціюванні від народу, євразійці ввели термін "демотія", що наближене до грецького – народ. Тому прибічники цієї течії й оголосили євразійство не лише "ідеократичним", а й "демотичним вченням". Однак що стосується способу реалізації демотичного аспекту, то в даній концепції цей постулат є формальним.

З одного боку, євразійці визнають народ суб'єктом державного життя. Ось як про це пише М. Алексєєв: "Демотичність" означає органічний зв'язок між індивідами, котрий перетворює їх в певне органічне ціле. Симфонічну особистість. Демотична держава будується на глибоких народних засадах і відповідає народній волі. "Демотія" – це органічна демократія, принцип співучасті народу у своїй власній долі. Народ… – не випадковий набір громадян, а сукупність історичних поколінь: минулих, нинішніх і майбутніх, котрі створюють оформлену державну єдність культур" [2, с. 185].

Однак що стосується змістовно-функціональної діяльності народу, то євразійці вбачають в ньому лише суб'єкта господарської діяльності. Один з ідеологів євразійства П. Савицький навіть ввів термін "господарство держав'я", наділивши народ терміном "хазяїн суспільства". "Господарство держав'я", – пише він, – передбачає можливість діяльності "хазяїна-суспільства" там, де потрібне збереження, а не розвиток. Там же, де є необхідність розвитку й творчості, виступає "хазяїн-особа", на відміну від "хазяїна-суспільства" [14, с. 103]. Тобто, це представник привілейованого провідного прошарку. Більшість громадян – нижчий прошарок – залежний від вищого, підпорядкований йому. Явище володарювання, за Алексєєвим, чисто психологічна, зумовлена усвідомленням залежності підвладних. Тому "ніяка держава неможлива без провідного прошарку. Цей провідний прошарок виконує свою місію саме тому, що є виразником "вищого", символом "переваги", носієм "ідеалів" тощо [2, с. 431].

Нижчий прошарок не виступає суб'єктом політичного життя. Як справедливо зазначає В. Тимошенко, "демотичність" євразійської державної моделі зумовлена тим, що в центрі її уваги "практичне життя", а не політика, котра відволікає від реальних

господарських потреб" [9, с. 574]. Отже, політика – це сфера дій провідного прошарку, який є панівним, правлячим в державі. Головне його завдання – боротьба з деструктивністю, притаманною нижчому прошарку.

Звідки ж береться цей провідний прошарок? За М. Трубецьким він формується шляхом особливого типу відбору через об'єднання на засадах загального сприйняття світу: "Тип відбору визначає собою не лише тип державного устрою, а й тип соціальної будови суспільства, тип народного господарства й культури. Такий тип відбору, котрий, згідно євразійському вченню повинен встановитися у світі, зокрема, в росії – Євразії, називається ідеократичним і відзначається тим, що основною ознакою, котрою при цьому типі відбору об'єднуються члени правлячого прошарку, є спільність світогляду" [4, с. 35]. Цим самим в основу всієї життєдіяльності суспільства ставиться ідеологія елітарних концепцій.

При цьому євразійці претендують на статус ідеологічного вчення всесвітньо планетарного масштабу. Ці претензії червоною ниткою проходять в програмному документі євразійства "Євразійство. Досвід систематичного викладу. Париж, 1926 р." [1], який самі євразійці вважають своєю "книгою – маніфестом".

Сам документ за змістом містить виклад ідеології євразійства, починаючи з критики всіх інших ідеологічних течій. Вони відзначають їх неістинність і навіть шкідливість. Мова йде про ідеології "смєновєховства", гегельянства, а також про ті сучасні течії, які в 20-і роки вже існували, або лише зароджувались: марксизм, позитивізм, екзистенціалізм, прагматизм тощо. Їх неістинність і шкідливість ніби – то полягає в тому, що вони є "абстракцією", тобто, відірвані від життя, від конкретності і тому є недієвими. "Вона не ідеологія, а абстракція, і ми робимо їй честь, називаючи її "абстрактною ідеологією", краще назвати її доктринерством. Подібна абстрактна ідеологія може залишатися порівняно безневинною, згубною лише для тих, хто її дотримується й тим самим перетворюється на безідейного опортуніста. Тоді вважайте, що її нема" [1, с. 1-2].

Навряд чи з такою трактовкою абстрактного навряд чи можна погодитися. Нове руйнує старе життя через його ідеологічну абстрактність? Звичайно ні. В даному випадку євразійці здійснюють гносеологічну помилку, відриваючи дві форми знання одне від одного – абстрактне і конкретне, і протиставляють їх, вважаючи антиподами. Насправді будь-яка абстракція можлива лише тому, що її природа принципово конкретна. Бо є нічим іншим як втіленням конкретного знання, але втіленням не будь-якого знання, а лише того, яке є суттєвим, необхідним, закономірним. Будь-яка абстракція, у тому числі й ідеологічна, є концентровано стислим синтезом саме такої конкретики.

Таким чином євразійці, перебуваючи в полоні гносеологічної буденщини, абсолютизують в ідеологічному абстрагуванні не сутнісно-атрибутивне, тобто, те, що абстракція є стисло консервована сутнісно-змістовна конкретика, а так би мовити, інститут другого порядку, а саме – процес відволікання, що породжує повсякденне уявлення про абстрагування як принципову анти конкретику, відірвану від усього дійсного, реального, життєво важливого.

Однак в такому разі більшості ідеологій, які критикують євразійці, притаманна не стільки абстрактність, а скоріше за все легковір'я і утопізм як головний атрибут такого світогляду. Звідси євразійці упереджено ставляться і до прогностичної функції будь-якої ідеології, вони орієнтуються не на конкретне минуле чи конкретне майбутнє, а мається на увазі конкретне як те, що є тут і зараз в даний момент. "Для того, щоб знешкодити абстрактні і неістинні ідеології, пишуть вони у маніфесті, – й разом з тим не відняти у

конкретної діяльності надихаючого її пафосу, необхідно протиставити їм ідеологію істинну – не абстрактну, а з конкретним життям органічно пов'язану, не випадково примарну, а безсумнівно істинну… Рівною мірою не може істинна ідеологія відкидати конкретну дійсність і суперечити їй, адже вона здійснюється в повноті життя індивіда" [1, с. 4-5].

Звернення до поняття "індивід" не є випадковим, євразійці викладають своє розуміння особистості як необхідну передумову істинної ідеології. "Основному поняттю старого світобачення, поняттю окремого й замкнутого в собі соціального атома протиставляємо поняття особистості як живої й органічної єдності або – вірніш і точніш – єдності особистісного. Особистість – така єдність великої кількості (чисельності) й велика кількість (чисельність) єдності. Вона – всеєдність, всередині якої немає місця зовнішнім механічним і причинним зв'язкам… Разом з тим, ми визнаємо реальністю лише індивідуальну особистість (котра за сутністю своєю не лише "індивідуальна"), а й соціальну групу й при тому не лише стани й класи, як це роблять марксисти, а й народ і суб'єкта культури руське-євразійської, об'єднуючий багато народів культури європейської і людства в цілому" [1, с. 7-8].

І далі висувають досить сумнівну ідею можливості взаємодії особистості з іншими людьми: "Ставлення індивідів до своєї спільноти, їх міжособистісні відносини не повинні бути антагоністичними. Але вони не можуть існувати і як співпадаючі, гармонійні. Вони повинні бути узгоджено партнерськими, "соборно-симфонічними". Тому ми й користуємося терміном "соборна" або "симфонічна" (тобто узгоджена, хорова) особистість" [1, с. 8].

На нашу думку, навряд чи таке трактування особистості євразійцями було на той час новацією. Воно лише модифікує Марксове вчення про особистість як сукупність соціальних відносин і не враховує існуюче на кінець 20-х років XX століття дійсно гуманістичне вчення про особистість – екзистенціалізм – філософський клімат сучасної епохи. Гуманістичність екзистенціалізму в першу чергу полягає у тому, що він зробив значний крок уперед у конкретизації, поглибленні розуміння особистості, розглядаючи її як комунікаційний діалог індивідуального "Я" з "Я-іншим".

Аналіз євразійства, особливо в частині його ідей щодо побудови держави засвідчує про те, що його автори практично ігнорують правовий регулятор суспільного життя, залишаючи його в полоні містичних ілюзій релігійно-політичного змісту. Як результат – суспільна дезорієнтація громадськості, можливість її маніпулятивного використання.

Висновки.

Євразійство, як єдине цільне вчення не набуло відповідної завершеної логіки, є суперечливим за своїм змістом і у вченні про державу і у ставленні до народу, і у визначенні окремих владних функцій, орієнтоване фактично на вчорашній день і тому не могло мати історичної перспективи в росії, яка продовжує претендувати нині на статус цивілізаційного орієнтиру в Євразії. Використання ідеї євразійців щодо потреби формування росії як автократичної держави, тобто, такої владної структури, в якій фактично відсутні політичні, правові, моральні перепони переростання її в абсолютизм, могло певною мірою сприяти тому, що росія, як держава, стала сповідувати тоталітарну, фашистську ідеологію, яка завуальовується євразійською ідеологічною парадигмою.

Ідеологія євразійства, не дивлячись на намагання його авторів, не набула характеру дійсної ідеологеми, націленої на формування нової світоглядної парадигми, яка втілювала б європейські та азійські світобачення. Вона фактично звелась до релігійного православно-політичного тлумачення постулатів, які не мають реального змісту і тому не могли бути використані в державотворенні. Посил євразійців до особливого типу

ідеологеми “серединної ідеології” залишився без її змістовного визначення, і сучасні дослідники теж цю проблему залишають поза увагою, а між тим у сучасну інформаційну епоху поміркована геополітична позиція могла б стати спроможною об’єднати різні народи, країни, континенти.

Особливістю євразійства є те, що їх концепції не позбавлені месіанських невиправданих ідей, наділення росіян виключними напівбожественними властивостями відносно інших народів, що створює умови для зверхнього ставлення до них і формування на цій основі нацистських поглядів, що потребує подальшого розвінчання ідеологічної парадигми цього псевдовчення.

Головне полягає у тому, що парадигми ідеології кремля та розрекламоване в рф так зване “євразійське вчення”, як одне з можливих основ побудови російської держави, не відповідають визначеними сторіччями світової цивілізації загальним ідеям та принципам формування гуманістичних орієнтирів світобачення у громадян росії.

Використана література

1. Евразийство: Опыт систематического изложения. Париж: Евраз. кн. изд-во, 1926. 80 с.

2. Алексеев Н.Н. Русский народ и государство; москва: Аграф, 2003. 790 с.

3. Трубецкой Н.С. Идеократия и армия. URL: http://gumilevica.kulichki.net/TNS/tns15.htm

4. Трубецкой Н.С. Об идее правительнице идеократического государства. *Евразийская хроника*. Берлин, 1935. Вып. 2. С. 35.

5. Замараєва Є.І. Нация и национализм в философии евразийства. *Соловьевские исследования.* Вып. (52). 2016. С. 150-162.

6. Абаєв Н.В., Фельдман В.Р. Евразийский проект и будущее россии. *Вестник Тувинского государственного университета. № 1. Социальные и гуманитарные науки*. 2015. № 1 (24). С. 155-159.

7. Лебедев С.Н., Замараева Е.И. Проблемы государства в учении евразийцев. *Вестник РУДН. Серия: Социология*. 2016. № 2. С . 426-437.

8. Мир Евразии: от древности к современности: сборник материалов Всероссийской научной конференции, г. уфа, 15 март. 2019 г. Т. 1 / отв. ред. Р.Р. Тухватуллин; уфа: БашГУ, 2019. 304 с.

9. Тимошенко В.І. Теория государства в политико-правовой мысли Украины и россии (конец Х1Х начало ХХ века). Чернигов, 2014. С. 566.

10. Новейший философский словарь / сост. и гл. науч. ред. А.А. Грицанов; минск: Интерпрессервис, 2001. 1279 с.

11. Кара-Мурза С.Г. Советская цивилизация. От начала Великой Победы. Харьков: Книжный клуб “КСД”, 2007. 640 с.

12. Православна релігійна думка XIX-XX ст. / упорядник доц. Охріменко О.Г. URL: http://www.philsci.univ.kiev.ua/biblio/Pravos.html

13. Маргарита Чабанна. Політичний менеджмент. № 2. 2003. С. 83-92.

14. Савицкий П.Н. Подданство идеи. Мир россии – Евразия: Антология / сост. Л.И. Новикова, И.Н. Сиземская. С. 72.

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

До відома читачів

Перелік статей,
опублікованих у журналі **ІНФОРМАЦІЯ І ПРАВО** у 2023 р.

№ з/п	Назва статті	Автор(и)	№ журналу, стор.
Інформаційне право			
1	Політико-правова аберація: нігілізм та зброя	Корж І.Ф., Кірієнко В.М.	1(44)/2023, с. 9-24
2	Інтелектуальні агенти в сфері парламентського контролю	Брайчевський С.М.	1(44)/2023, с. 25-31
3	Визначення терміну “штучний інтелект”	Баранов О.О.	1(44)/2023, с. 32-49
4	Еволюція інформаційних прав людини	Тихомиров О.О.	1(44)/2023, с. 50-57
5	Медіа безбар’єрність: поняття та удосконалення правового регулювання	Красноступ Г.М.	1(44)/2023, с. 58-66
6	Трансформація правових систем – засаднича умова сталого розвитку	Баранов О.А.	2(45)/2023, с. 9-32
7	Міжнародні правові стандарти національного регулювання прав людини	Жиляєв І.Б.	2(45)/2023, с. 33-41
8	Правові основи обмеження конституційних прав і свобод людини в Україні	Корж І.Ф.	2(45)/2023, с. 42-49
9	Дезінформація як фактор маніпулювання свідомістю	Брижко В.М., Дзьобань О.П.	2(45)/2022, с. 50-63
10	Становлення національного законодавства про інформацію: врахування найкращих європейських практик	Красноступ Г.М.	2(45)/2023, с. 64-72
11	Відкрита наука та інтелектуальна власність	Капіца Ю.М., Шахбазян К.С.	2(45)/2023, с. 73-87
12	Безпека людини: некласична рефлексія загроз у філософії модерну й постмодерну	Дзьобань О.П., Брижко В.М.	3(46)/2023, с. 9-24
13	Цивілізаційна місія цифрових трансформацій	Баранов О.А.	3(46)/2023, с. 25-41
14	Дотримання верховенства права та прав і свобод людини в умовах війни в Україні: проблеми теорії та практики	Ірха Ю.Б.	3(46)/2023, с. 42-54
15	Правове регулювання забезпечення доступу до публічної інформації під час правового режиму воєнного стану в Україні	Красноступ Г.М.	3(46)/2023, с. 55-63
16	Теоретичні та історико-правові засади трансформації інформаційного суспільства в суспільство знань	Пилипчук В.Г.	4(47)/2023, с. 9-17
17	Теоретико-методологічні засади інформаційно-комунікаційних, психологічних та гібридних війн	Бебик В.М.	4(47)/2023, с. 18-26
18	Права людини та корупція, як прояв їх порушення	Корж І.Ф.	4(47)/2023, с. 27-39
19	Особливості визначення правового статусу робота із штучним інтелектом	Баранов О.А.	4(47)/2023, с. 40-54

42	Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни	Мануілов Я.С.	1(44)/2023, с. 154-167
43	Стратегічне планування у сфері державної безпеки як прикладна проблема	Гордієнко С.Г., Доронін І.М.	1(44)/2023, с. 169-176
44	Сучасні тренди виявлення та протидії застосуванню шпигунських та шкідливих програм	Поляков О.М.	2(45)/2023, с. 125-138
45	Особливості застосування шкідливого програмного забезпечення спецслужбами країни-агресора	Білан І.А.	2(45)/2023, с. 139-152
46	Blackout і фейки російської пропаганди: кримінологічний погляд на проблему симбіозу	Батиргареєва В.С.	2(45)/2023, с. 153-162
47	Засади формування ворожої пропаганди та заходи протидії їй в умовах воєнного стану в Україні	Горун О.Ю.	2(45)/2023, с. 163-171
48	Інститут секретних винаходів у забезпеченні національної безпеки держави: проблемні питання	Андрощук Г.О., Копил Я.В.	2(45)/2023, с. 172-185
49	Інформаційно-комунікаційні війни та інформаційно-комунікаційні війська	Бебик В.М.	3(46)/2023, с. 86-97
50	Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм	Нетеса Н.В., Мокляк В.В.	3(46)/2023, с. 98-107
51	Особливості протидії кіберзлочинності під час воєнного стану	Гуцалюк М.В.	3(46)/2023, с. 108-117
52	Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану	Красніков С.А.	3(46)/2023, с. 118-128
53	Системний вимір інформаційно-психологічної консцієнтальної війни	Качинський А.Б.	3(46)/2023, с. 129-134
54	Правове та організаційне забезпечення кіберзахисту систем детекції брехні від кібератак в умовах воєнного стану	Казьмірук С.Д., Леонов Б.Д.	3(46)/2023, с. 135-141
55	Загрозливі тенденції використання державою-агресором шкідливого програмного забезпечення в умовах правового режиму воєнного стану	Федієнко О.П.	3(46)/2023, с. 142-153
56	Загрозливі тенденції використання криптовалют з метою фінансування терористичної діяльності в умовах війни	Білан І.А.	3(46)/2023, с. 154-163
57	Протидія фінансуванню тероризму з використанням криптовалют	Лук’янчук Р.В.	3(46)/2023, с. 164-175
58	Організаційно-технічний аспект протидії фішингу	Гуржій С.В.	3(46)/2023, с. 176-186
59	Формування антитерористичних компетентностей фахівців національної системи кібербезпеки	Кудінов С.С.	3(46)/2023, с. 187-192
60	Інформаційна безпека: міжнародно-правовий аспект	Ковальов К.Є.	4(47)/2023, с. 159-167
61	Правове забезпечення кібербезпеки об’єктів критичної інфраструктури.	Алексеєва О.А.	4(47)/2023, с. 168-176
62	Кримінально-правова протидія фінансуванню тероризму в контексті ратифікації Додаткового протоколу до Конвенції РЄ про запобігання тероризму	Леонов Б.Д.	4(47)/2023, с. 177-186
63	Кіберзлочини, як загроза державній безпеці: кримінологічні та організаційні особливості обліку	Ковальчук А. Ю., Гавловський В.Д.	4(47)/2023, с. 187-196
64	Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України	Малахов Г.Б.	4(47)/2023, с. 197-206
65	Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки	Гуржій С.В.	4(47)/2023, с. 207-216

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

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 – Ph.D. та доктора наук з проблем права та інформаційного законодавства, інформаційних технологій, цифрової трансформації, 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 та законодавство, цифрова трансформація, 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. та англ. 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, первинної та редакторської оцінки наданих на публікацію матеріалів, виправлення помилок, узгодження змісту текстів з авторами, коректування, реєстрації наукової публікації згідно з міжнародною ідентифікацією цифрового об'єкта DOI, форматування, дизайн, тиражування чергового номера та ін. роботи, які пов'язані з публікацією статей і виданням журналу, **пропонується здійснити оплату в розмірі 550 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

- Редакційна колегія та Вчена рада НДІІП НАПрН України не завжди поділяють 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.
- Редакція журналу 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(47)/2023

DOI: https:// .....

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:	04053, Україна, м. Київ, пров. Несторівський, 4. 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:	04053, Ukraine, Kyiv, Nestorivsky lane, 4. 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.