Науково-дослідний інститут інформатики 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

№ 1(36)/2021

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

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

м. Київ

Scientific Research Institute of Informatics and Law
of the 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

№ 1(36)/2021

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

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

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * *

З М І С Т

Інформаційне право

Інформаційна і національна безпека

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

До відома читачів

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

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 17.0. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ "Видавничий дім "АртЕк".
04050, м. Київ, вул. Мельникова, буд. 63. Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІІП НАПрН України, протокол № 3 від 11.03.21 р.

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

Informative Law

Informative and National Safety

Information on other subject research directions by specializations in the field of knowledge 08 – "Law"

For the consideration of readers

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 3 dated 11.03.21.

Інформаційне право

УДК 342.951

КОРЖ І.Ф., *доктор юридичних наук, с.н.с.,* завідувач наукової лабораторії НДІ інформатики і права НАПрН України.

АБЕРАЦІЯ НОРМАТИВНО-ПРАВОВОЇ ІНФОРМАЦІЇ

Анотація. *В статті досліджується питання існування підґрунтя для прояву такого негативного явища в національному правовому полі, яким є "аберація" нормативно-правової інформації. Під терміном "аберація нормативно-правової інформації" у цій роботі розуміється свідоме, вмотивоване або несвідоме, невмотивоване викривлення змісту нормативно-правової інформації в порівнянні з його аналоговим текстом, тобто такої інформації, яка міститься в проектах чи в нормативно-правових актах, в судових рішеннях та в інших матеріалах, які є додатком до цих документів і використовуються при їх прийнятті. Робиться висновок щодо причин виникнення цього явища та необхідності застосування заходів щодо його мінімізації.*

Ключові слова: *аберація, викривлення змісту інформації, нормативно-правова інформація, правова культура, правова норма, судові рішення.*

Summary. *The article explores the question of the existence of grounds for the manifestation of such a negative phenomenon in the national legal field, which is the "aberration" of regulatory information. The term "aberration of regulatory information" in this study means a conscious, motivated or unconscious, unmotivated distortion of the content of regulatory information in comparison with its analogue text, that is, information contained in drafts or in regulatory legal acts, in court decisions and other materials that are annexed to these documents and used in their adoption. A conclusion is made about the causes of this phenomenon and the need to apply measures to minimize it.*

Keywords: *aberration, distortion of the content of information, legal information, legal culture, legal norm, court decisions.*

Аннотация. *В статье исследуется вопрос существования оснований для проявления такого негативного явления в национальном правовом поле, которым является "аберрация" нормативно-правовой информации. Под термином "аберрация нормативно-правовой информации" в этой работе понимается сознательное, мотивированное или бессознательное, немотивированное искажение содержания нормативно-правовой информации в сравнении с его аналоговым текстом, то есть такой информации, которая содержится в проектах или в нормативно-правовых актах, в судебных решениях и в других материалах, которые являются приложением к этим документам и используется при их принятии. Делается вывод о причинах возникновения этого явления и необходимости применения мер по его минимизации.*

Ключевые слова: *аберрация, искажение содержания информации, нормативно-правовая информация, правовая культура, правовая норма, судебные решения.*

Постановка проблеми. В сучасному інформаційному суспільстві створення, поширення, використання, узагальнення і зберігання інформації становить значну частину економічної, політичної та культурної діяльності. Водночас, нинішній світ, який є глобалізованим, розглядається як самоорганізуюча система, яка розвивається за допомогою інформаційно-комунікаційних технологій. Зростаюче значення зазначених технологій, різноманітних інформаційних ресурсів, як основи інтелектуальної діяльності людини в умовах нинішніх трансформаційних процесів сучасного суспільства, сприяє формуванню, насамперед, національного інформаційного простору.

Відповідно до еволюційних процесів, на базі національного, так само як і глобального, інформаційного простору, формуються необхідні інформаційні потреби людини.
Тим самим, формуються відповідні інформаційно-правові відносини між суб'єктами згаданих відносин. Визначним показником таких відносин є отримання адекватної інформації, насамперед, нормативно-правової інформації, за допомоги якої формується та активізується участь громадян в управлінні державними справами. Для отримання належної нормативно-правової інформації громадянами в державі мають ефективно функціонувати відповідні засоби і механізми напрацювання, зберігання та поширення згаданої інформації. В іншому випадку громадяни ризикують отримувати неточну, викривлену нормативно-правову інформацію, що не сприяє активізації їхньої життєвої позиції, негативно впливає на функціонування інформаційно-правових відносин, призводить до виникнення конфліктів в суспільному середовищі.

Даному питанню приділяли свою увагу такі науковці у даній сфері, як: Арістова І.В., Белєнцева В.В., Беляков К.І., Брижко В.М., Дзьобань О.П., Довгань О.Д., Доронін І.М., Золотар О.О., Калюжний Р.А., Кормич Б.А., Марущак А.І., Оніщенко Н.М., Пилипчук В.Г., Скулиш Є.Д., Фурашев В.М., Швець М.Я. та інші. Однак, саме дослідження явища "аберації" залишалося поза увагою дослідників.

Метою статті є визначення стану поширення, отримання та зберігання нормативно-правової інформації в Україні, недоліків функціонування нормативно-правової інформації, що, при її отриманні, викривляють її зміст та призначення, напрацювання пропозицій щодо мінімізації настання негативних наслідків дії викривленої інформації на суспільство.

Виклад основного матеріалу. Здійснювані в Україні реформи державної влади та місцевого самоврядування, спрямовані на демократичні перетворення та реалізацію курсу України на євроінтеграцію, не можуть бути успішними, без активної участі у цих процесах громадянського суспільства. Тому у суспільстві дедалі глибше укорінюється усвідомлення, що свобода і людська гідність, інформованість є не тільки загальнолюдськими цінностями, а й наріжним каменем процесів розбудови цивілізованої демократичної держави, вироблення та реалізації її зовнішньої і внутрішньої політики, політики національної безпеки. Тому важливим є питання подолання об'єктивно існуючих проблем в теорії і практиці комунікації публічної влади та громадянського суспільства, яке активізувалось в результаті здійснюваних в Україні реформ.

Розвиток демократії, незворотність проведення політико-правових перетворень, симетричні та дієві відповіді на загрози безпеці країни, поступ у реформах щодо європейської інтеграції – усе це в Україні було б неможливим без розвитку та зміцнення громадянського суспільства, підвищення інституційної спроможності неурядових організацій, активного впровадження волонтерських ініціатив.

Нові виклики розвитку та безпеці України породжують симетричні громадські ініціативи, покликані змінити ситуацію на засадах відкритої комунікації, діалогу та відповідального лідерства. Фактично в більшості секторів, які забезпечують формування порядку денного реформ, діють організації громадянського суспільства. Важливим аспектом розвитку громадянського суспільства є необхідність розвитку співпраці, партнерства між публічними органами державної влади та громадянським суспільством, які би сприяли вирішенню суспільно значущих проблем, розробленню та імплементації комплексних реформ, ефективному контролю за діями влади.

Пріоритети стосовно ролі держави у сприянні розвитку громадянського суспільства викладено в Національній стратегії сприяння розвитку громадянського

суспільства в Україні на 2016 – 2020 роки [1]. Її прийняття зумовлено необхідністю створення державою сприятливих умов для розвитку громадянського суспільства, різноманітних форм демократії участі, налагодження ефективної взаємодії громадськості з органами державної влади та органами місцевого самоврядування.

Активне, впливове і розвинене громадянське суспільство є важливим елементом будь-якої демократичної держави та відіграє одну з ключових ролей у впровадженні нагальних суспільних змін і належного врядування, в управлінні державними справами і вирішенні питань місцевого значення, розробці і реалізації ефективної державної політики у різних сферах, утвердженні відповідальної перед людиною правової держави, розв'язанні політичних, соціально-економічних та гуманітарних проблем.

Взаємодія органів державної влади, органів місцевого самоврядування з громадськістю буде залишатися малоефективною, якщо буде недостатньою прозорість діяльності цих органів та через забюрократизовані процедури такої взаємодії, через низький рівень взаємної довіри. Крім того, недосконаліть і малодоступність чинного законодавства створює штучні бар'єри для реалізації громадських ініціатив, утворення та діяльності окремих видів організацій громадянського суспільства, розгляду та врахування громадських пропозицій органами державної влади, органами місцевого самоврядування. Тому сприяння забезпеченню інформаційної прозорості і відкритості публічної влади, у тому числі питань залучення громадськості до підготовки проектів актів, що мають важливе суспільне значення, має бути пріоритетним для цих органів.

У розвинутих, демократичних країнах світу забезпечення громадянам доступу до публічної інформації, якою є нормативно-правова, є основним індикатором відкритості публічної влади. З огляду на зазначене, отримання громадськістю достовірної нормативно-правової інформації від публічної влади в нинішніх умовах є надзвичайно важливим. Це – право громадян, яке базується на правових актах ООН та Ради Європи, що регулюють основоположні права та свободи людини. Наприклад, 18 червня 2009 року, у м. Тромсо (Норвегія) Рада Європи прийняла Конвенцію про доступ до офіційних документів [2]. Цей документ вперше вивів тему доступу до публічної інформації на такий високий рівень. Положення Конвенції наша країна враховувала, розробляючи проект Закону "Про доступ до публічної інформації" [3], який свого часу увійшов у десятку найкращих у світі і зараз перебуває в першій десятці європейських законів. Україна підписала Конвенцію у квітні 2018 року і того ж року намагалась ратифікувати цей документ, проте для цього у парламенті не вистачило голосів і розуміння важливості такої ратифікації. І лише у 2020 році згадану Конвенцію вдалося ратифікувати [4].

Прагнення України приєднатися до сім'ї демократичних країн Європи, бажання налагоджувати та підтримувати на належному рівні міждержавні відносини, співпрацю у різних сферах життєдіяльності, у тому числі у галузі права, вимагає апроксимації (зближення, адаптації) законодавства України до законодавства країн Європейського Союзу та, у підсумку, його гармонізації (повної ідентичності) з останнім. Крім того, зазначене вимагає від держави забезпечення вільного, повного, безоплатного і швидкого доступу до реєстрів (баз даних) нормативно-правових актів публічної влади для будь-кого з громадян України. Зазначене дозволить, на наше переконання, вирішити питання щодо недопущення прояву такого негативного явища, яким є аберація нормативно-правової інформації (від лат. *aberratio* – " відхилення") [5, с. 6].

Згаданий термін має широкий вжиток в електроніці, астрономії, мікробіології, морфології та фізіології, оптиці, психології тощо. В довідковій літературі згаданий термін означає "хибне розуміння, відхилення від істини, помилка. Може мати місце, зокрема, при оцінці доказів у цивільному та кримінальному процесі, прийнятті

управлінських рішень тощо" [6, с. 9]. Таким чином, сутність згаданого явища полягає у відхиленні, викривленні індивідуальної побудови або функції будь-чого від норми, від відповідного зразка.

У відповідній статті [7] під "аберацією" в законодавстві розумілося викривлення змісту правової норми нормативно-правового акту нижчого рівня після імплементації в нього відповідної правової норми нормативно-правового акту вищого рівня. Згадане відбувається внаслідок корегування, наприклад, міжнародно-правової норми, здійснення свого роду інтерполяції (філологічне – зміна первинного тексту; вставка відсутніх у первинному документі слів, речень) в процесі імплементації згаданої норми в національне законодавство. Аналогічне явище може відбуватися, також, і у процесі нормотворчої діяльності при розробці, згідно з вимогою закону, підзаконних нормативно-правових актів, внаслідок чого змінюється (звужується або розширюється) дія правової норми підзаконного акту по відношенню до аналогічної правової норми закону, що є порушенням принципу верховенства закону, а також при ухваленні судових рішень в мотиваційній його частині, та при отриманні нормативно-правової інформації в цілому (неточний текст проекту чи змісту нормативно-правового акту та обґрунтування необхідності його прийняття, свідоме перекручення змісту акту чи аргументації його відповідності праву тощо).

З огляду на зазначене, під "аберацією" нормативно-правової інформації в цьому дослідженні потрібно розуміти свідоме, вмотивоване або несвідоме, невмотивоване викривлення змісту нормативно-правової інформації в порівняні з його аналоговим текстом, тобто такої інформації, яка міститься в проектах чи в нормативно-правових актах, в судових рішеннях та в інших матеріалах, які є додатком до цих документів і використовуються при їх прийнятті.

"Аберaційна" нормативно-правова інформація має певні спільні ознаки з "фейковою" інформацією (від англ. *fake information* – "липова/підроблена/шахрайська/фальшива інформація (дезінформація)", яку створено з метою впливу на свідомість великої кількості людей і яка не витримує перевірки на відповідність та реальність), як то: невідповідність реальності; призначена для досягнення певної мети; ігнорування певних формальних правил при її створенні; певний примітивізм; надмірно емоційне її подання тощо. Різняться вони між собою тим, що "аберaційна" нормативно-правова інформація створюється лише у нормотворчій сфері та у сфері судочинства, оскільки лише у зазначених сферах створюється нормативно-правова інформація, як при позитивній, так і при негативній нормотворчості.

Україна має багато прикладів, коли органи публічної влади, створюючи різні нормативно-правові акти та приймаючи судові рішення, закладають в їхні положення правові норми, сутність та напрям дії яких різняться від сутності та напряму дії аналогічних правових норм ратифікованих актів міжнародного права, Конституції та законів України, що викликає не лише непорозуміння у їх застосуванні та неоднозначне їх тлумачення, а й призводить до обмежень у відповідних правах та свободах громадян.

Явище аберації не є, як може здаватися на перший погляд, невинним явищем, що викликано відхиленням від вимог нормотворчої діяльності чи порушенням згаданих вимог. Як зазначалося вище, за ним можуть критися грубі порушення прав і свобод людини і громадянина, які держава зобов'язалася неухильно забезпечувати, ратифікувавши міжнародні угоди або приєднавшись до них. Зазначене проявляється, наприклад, при розгляді судами різних рівнів питання поновлення порушених прав громадян України. Як свідчить практика, зазначене питання залишається на сьогоднішній день актуальним.

Прикладом зазначеного слугує прийнятий Українським парламентом Закон України "Про очищення влади" [8], в пояснювальній записці до якого щодо доцільності його прийняття зазначено: "Діяльність органів влади останніх років призвела до зневіри громадян у владних органах. Влада як на центральному рівні, так і на місцевому, повністю знівелювала себе, оскільки асоціюється нерозривно з порушенням прав та законних інтересів громадян, вчиненням корупційних діянь, недотриманням у своїй діяльності положень Конституції України та законів. Останніми роками посадові (службові) особи органів державної влади (державних органів), виконуючи свої посадові (службові) обов'язки, керувались не законами, а незаконними вказівками вищого керівництва держави. Саме тому одним із нагальних кроків діючої влади має стати очищення влади.

Запровадження в Україні обов'язковості проходження процедури перевірки при призначенні/обранні на посади у органах державної влади (державних органах), а також осіб, які вже займають ці посади, дасть змогу сформувати апарат управління з осіб, які не скомпрометували себе співучастю у злочинах попередньої політичної системи, а також очистити апарат управління від осіб, які причетні до злочинів попередньої влади, у тому числі, й влади, яка панувала до проголошення незалежності України.

Законопроектом запроваджується проведення процедури відповідної перевірки при вирішенні питання про можливість призначення особи, як суб'єкта перевірки, на посаду в органах влади, а також організація процедури перевірки осіб, які є суб'єктами перевірки на відповідність визначеним законопроектом критеріям, з метою вирішення питання щодо можливості їх подальшого перебування на відповідній посаді".

Всупереч зазначеним у пояснювальній записці відповідним моральним та безпековим напрямам законопроекту, прийнятий парламентом закон вже містив не відповідні зазначеним принципам правові норми, які йшли в розріз з положеннями Конституції України, ратифікованими Україною міжнародних угод та в цілому українському законодавству, на що звертала увагу керівництва країни Венеціанська комісія. Внаслідок застосування правових норм Закону потерпіли тисячі громадян України, які були примусово звільнені з посад або змушені самі звільнятися з державної служби. При цьому особиста вина цих громадян в негативній діяльності зазначеній в Законі, в судовому порядку не доказувалася.

На сьогодні, тобто в 2020 році, згаданий Закон знаходиться на розгляді в Конституційному Суді України, в якому перевіряється його відповідність Конституції України (з 22 березня 2016 року Суд завершив усне слухання і перейшов до закритої частини розгляду). Коли Закон буде розглянутий – нікому невідомо, а десятки тисяч громадян України продовжують чекати на свою реабілітацію.

Наступний приклад. Печерський районний суд 19.02.18 р., виправдовуючи підсудного у справі № 757/7651/16-к, зазначив, що держава не вправі застосовувати до особи процесуальний примус у вигляді кримінальної відповідальності за відсутність дозволу, передбаченого законом, поки немає закону, який передбачає отримання цього дозволу [9]. І зазначене, на наше переконання, є цілковитою правовою позицією суду, оскільки відповідає загальновизнаній правовій засаді *"nullum crimen sine lege"* ("немає злочину і покарання без наперед установленого закону"). Зазначимо, що зазначений принцип закріплений в статті 7 Міжнародної Конвенції [10]: "Нікого не може бути визнано винним у вчиненні будь-якого кримінального правопорушення на підставі будь-якої дії чи бездіяльності, яка на час її вчинення не становила кримінального правопорушення згідно з національним законом або міжнародним правом…".

Однак, 31 травня 2018 року колегія суддів Другої судової палати Касаційного кримінального суду Верховного Суду у своїй постанові (справа № 127/27182/15-к, провадження № 51-3305км18) зазначила, що поняття "закон"**,** вжите законодавцем у ст. 263 КК України**,** має розширене тлумачення і включає в себе законодавство у цілому, в тому числі нормативні акти, що регулюють відповідні правовідносини, порушення яких утворює об'єктивну сторону складу злочину, передбаченого цією статтею кримінального закону. Під розширеним поняттям "закон" Верховний Суд має на увазі відповідний наказ Міністерства внутрішніх справ України [11], прийнятий на підставі Закону України "Про міліцію", який втратив чинність 2 липня 2015 року.

На наше переконання, хибність даної позиції Суду полягає у наступному:

По-перше, об'єктивна сторона злочину за статтями 263 і 263-1 КК України полягає у незаконному поводженні зі зброєю, бойовими припасами або вибуховими речовинами та у незаконному виготовленні, переробці чи ремонті вогнепальної зброї або фальсифікації, незаконному видаленні чи зміні її маркування, або незаконному виготовленні бойових припасів, вибухових речовин чи вибухових пристроїв. Таким чином, законодавець визначив функціонування (наявність) закону, предметом регулювання якого є регулювання суспільних відносин, пов'язаних із зазначеним вище, і яким передбачено отримання дозволу на зазначене, тобто, призначення згаданого закону полягає у здійсненні регулятивної функції. У свою чергу, відповідно до ч. другої ст. 178 Цивільного кодексу України [12]: "Види об'єктів цивільних прав, перебування яких у цивільному обороті не допускається (об'єкти, вилучені з цивільного обороту), мають бути прямо встановлені у законі. Види об'єктів цивільних прав, які можуть належати лише певним учасникам обороту або перебування яких у цивільному обороті допускається за спеціальним дозволом (об'єкти, обмежено оборотоздатні), встановлюються законом".

Основна ж функція кримінального права – це охоронна функція. Саме кримінальне право через КК України покликано стояти на сторожі найважливіших суспільних відносин від їх порушення, застосовувати до винних найсуворіші заходи примусу – покарання. Як зазначає відомий науковець П. Фріс [13] кримінальне право, охороняючи нормами Особливої частини КК України суспільні відносини, не регулює їх, а для визначення факту порушення в ряді випадків відсилає через бланкетну норму до регуляторних актів інших галузей права, у даному випадку до закону, якого не існує. У свою чергу, Конституційний Суд України зазначає, що бланкетна диспозиція кримінально-правової норми лише називає або описує злочин, а для повного визначення його ознак відсилає до інших галузей права [14].

По-друге, тлумачення Судом терміну "закон" в широкому сенсі, що включає в себе усі нормативно-правові акти публічної влади, не відповідає положенням загальної теорії держави і права і національному законодавству. Закон є творінням законодавчої влади. В Україні використовується в широкому сенсі термін "законодавство", але не "закон", оскільки в країні не запроваджено делеговане законодавство (були декрети Кабінету Міністрів України, що видавалися в період з 2 грудня 1992 р. по 20 травня 1993 р.), як це передбачено в конституціях інших країн, як то: Російська Федерація, окремі країни Європи.

Таким чином, вищезазначене дає підстави констатувати факт відсутності на сьогодні в Україні закону, що здійснює регуляцію суспільних відносин в сфері обороту зброї, боєприпасів та вибухових речовин, що у свою чергу не дає можливості визначати законність чи незаконність тих чи інших дій із зазначеними предметами. Тим не менш органи досудового розслідування продовжують реєструвати кримінальні провадження

та здійснювати попереднє розслідування, а суди виносити обвинувальні вироки за ст.ст. 263 і 263-1 КК України. При цьому вони посилаються на порушення особами порядку обороту цих предметів, врегульованого підзаконними актами.

Викликає, м'яко кажучи, подив твердження Суду, що законодавець, використовуючи термін "закон", мав на увазі його розширене тлумачення – "законодавство у цілому". Зазначене є перекручуванням термінологічного змісту з певним умислом (можливо будь-якою метою заповнити існуючий вакуум правового регулювання даної сфери, а за таким рішенням явно проглядається певна корупційна "змова" судової та виконавчої гілок державної влади), оскільки законодавець чітко знає свої повноваження щодо врегулювання суспільних відносин шляхом прийняття ним законів, як це і передбачено Конституцією України.

Таким чином, факт притягнення громадян до кримінальної відповідальності у згаданих випадках є грубим порушенням Конституції України.

За відсутності прийнятого українським парламентом відповідного закону, державна влада не вправі застосовувати до громадян процесуальний примус у вигляді кримінальної відповідальності.

Також термінологічні маніпуляції Суду з метою надання вироку певного вигляду законності – це прийняття завідомо неправосудного рішення і створення великої загрози правовій безпеці суспільства, а також державі. Крім того, зазначене є ігноруванням загальновизнаних принципів права, дискредитацією євроінтеграційних процесів України, нівелювання процесу демократизації суспільного життя в Україні.

Висновки.

Під "аберацією" нормативно-правової інформації маємо розуміти свідоме, вмотивоване або несвідоме, невмотивоване викривлення змісту нормативно-правової інформації в порівнянні з його аналоговим текстом, тобто такої інформації, яка міститься в проектах чи в нормативно-правових актах, в судових рішеннях та в інших матеріалах, які є додатком до цих документів і використовуються при їх прийнятті.

На нашу думку явище аберації у процесі отримання та застосування нормативно-правової інформації є, свого роду, хворобою становлення молодої національної правової системи України, яка прагне створити демократичне, правосвідоме, соціальне, громадянське суспільство. Згадане викликане, насамперед, недостатньою правовою культурою певної частини суспільства, включаючи і представників державної влади, для подолання якої необхідний певний час, а також застосування відповідних санкцій держави щодо авторів її продукування з метою його мінімізації.

Для "лікування згаданої хвороби" потрібна більш активна правова та громадянська позиція нетерпимості до зазначених фактів як з боку науковців, так і практиків. Вони мають активно доводити згадані негативні факти до громадянського суспільства та до міжнародної спільноти, роз'яснювати їх неконституційність і шкідливість для суспільних відносин і тим самим виховувати у суспільства нульову толерантність до зазначеного.

Використана література

1. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26.02.16 р. № 68/2016. *Офіційний вісник Президента України.* 2016. № 703 (берез.).

2. Про доступ до офіційних документів: Конвенція Ради Європи від 18.06.09 р. (офіційний переклад). URL: https://cedem.org.ua/library/konventsiya-rady-yevropy-pro-dostup-do-ofitsijnyh-dokumentiv-ofitsijnyj-pereklad (дата звернення: 10.11.2020).

3. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

4. Про ратифікацію Конвенції Ради Європи про доступ до офіційних документів: Закон України від 20.05.20 р. № 631-IX. *Відомості Верховної Ради України*. 2020. № 39. Ст. 299.

5. Советский энциклопедический словарь / гл. ред. А.М. Прохоров. 4-е изд., испр. и доп. Москва: СОВЕТСКАЯ ЭНЦИКЛОПЕДИЯ, 1990. 1632 с.

6. Юридична енциклопедія: в 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. Т. 1. Київ: Вид. "Українська енциклопедія" ім. М.П. Бажана, 1998. 672 с.

7. Корж І.Ф. Явище аберації в українському законодавстві. *Право України.* 2006. № 11. С. 89-94.

8. Про очищення влади: Закон України від 16.09.14 р. № 1682-VII. *Відомості Верховної Ради України*. 2014. № 44. Ст. 2041.

9. Відсутність закону щодо порядку надання дозволу на носіння зброї не унеможливлює притягнення особи до кримінальної відповідальності (ВС/ККС, справа № 127/27182/15-к, 31.05.18). URL: https://protocol.ua/ru/vs_kks_vidsutnist_zakonu_shchodo_poryadku_nadannya_dozvolu_ na_nosinnya_zbroi_ne_unemoglivlyue_prityagnennya_osobi_do_kriminalnoi_vidpovidalnosti_(s_kks_spr ava (дата звернення: 13.11.2020).

10. Про захист прав людини і основоположних свобод: Конвенція РЄ від 04.11.1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 13.11.2020).

11. Про затвердження Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів: наказ Міністерства внутрішні справ України від 21.08.98 р. № 622. URL: https://zakon.rada.gov.ua/laws/show/z0637-98 (дата звернення: 13.11.2020).

12. Цивільний кодекс України від 16.01.03 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № № 40-44. Ст. 356.

13. Щодо кримінальної відповідальності за незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (ст. 263 КК України). URL: https://lexinform.com.ua/yuridychna-praktyka/shhodo-kryminalnoyi-vidpovidalnosti-za-nezakonne-povodzhennya-zi-zbroyeyu-ojovymy-prypasamy-abo-vybuhovymy-rechovynamy-st-263-kk-ukrayiny (дата звернення: 13.11.2020).

14. Рішення Конституційного Суду України у справі за конституційним поданням 46 народних депутатів України щодо офіційного тлумачення положень статті 58 Конституції України, статей 6, 81 Кримінального кодексу України (справа про зворотну дію кримінального закону в часі) від 19.04.00 р. № 6-рп/2000. URL: https://zakon.rada.gov.ua/laws/show/v006p710-00 (дата звернення: 13.11.2020).

15. Делеговане законодавство в Україні: що, як і чому? *Юридична Газета* (online). URL: https://yur-gazeta.com/dumka-eksperta/delegovane-zakonodavstvo-v-ukrayini-shcho-yak-i-chomu.html (дата звернення: 13.11.2020).

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

УДК 316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, с.н.с.*
ORCID: https://orcid.org/0000-0002-3941-1013.
ПИЛИПЧУК В.Г., *доктор юридичних наук, професор,*
академік НАПрН України.
ORSID: https://orcid.org/0000-0002-3754-4592.

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВІ СТАНДАРТИ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА СУЧАСНІ ПРИКЛАДНІ ПРОБЛЕМИ

Анотація. *Стаття є продовженням низки наукових праць щодо стану, тенденцій і подальшого забезпечення безпеки персональних даних в умовах цифрової трансформації та пов'язаних з нею проблем правового регулювання нових суспільних відносин у цій сфері. Розглядаються та оцінюються ключові аспекти документів ЄС, затверджених останніми роками, зокрема, Регламенту GDPR, Директиви NIS і проекту правового акту про e-Privacy. Висвітлено основні критерії й актуальні проблемні питання, що потребують врегулювання в контексті імплементації правових норм ЄС та розвитку національного законодавства з питань захисту персональних даних.*

Ключеві слова: *безпека, персональні дані, правові стандарти, ЄС.*

Summary. *The article is a continuation of a number of scientific works on the state, trends and further ensuring security of personal data in the context of digital transformation and related problems of legal regulation of new social relations in this area. The key aspects of the EU documents approved in recent years, in particular, the GDPR Regulation, the NIS Directive and the draft legal act on e-Privacy, are considered and evaluated. The main criteria and topical issues that need to be addressed in the context of the implementation of EU law and the development of national legislation on personal data protection are highlighted.*

Keywords: *protection, security, personal data, European legal standards.*

Аннотация. *Статья является продолжением ряда научных работ, касающихся состояния, тенденций и перспектив дальнейшего обеспечения безопасности персональных данных в условиях цифровой трансформации, а также связанной с ней проблемой правового регулирования новых общественных отношений в этой сфере. Рассматриваются и оцениваются ключевые аспекты документов ЄС, утвержденных в последние годы, в частности, Регламент GDPR, Директива NIS и проект о e-Privacy. Освещены основные критерии и актуальные проблемы, которые требуют урегулирования в контексте имплементации правовых норм ЄС и развития национального законодательства по вопросам защиты персональных данных.*

Ключевые слова: *безопасность, персональные данные, правовые стандарты ЄС.*

Постановка проблеми. Пошуки у вирішенні правових проблем щодо природи людських цінностей здійснюються з часів римського права й донині. Це пояснюється поступовими і доволі тривалими змінами у розумінні демократичних цінностей і прав людини, зокрема, у сфері захисту персональних даних. Формування теоретичних поглядів і правових приписів з питань недоторканності приватного життя має менш тривалий історичний шлях, який розпочався з кінця XVII століття [1].

В останні десятиліття прийнято значну кількість міжнародних актів (резолюцій, конвенцій, директив, протоколів, рекомендацій) Організації Об'єднаних Націй, Ради Європи, Європейського Парламенту і Ради Європейського Союзу, які безпосередньо або опосередковано стосуються правового регулювання захисту персональних даних

(наприклад, див. у [2]). Наявність великого переліку галузевих та інших документів, а також їх обсяги вражають і навіть можуть сприяти уявленню про послідовність та глибину наукових розробок у регулюванні суспільних відносин у цій сфері. Однак, як свідчить аналіз, практика сучасного життя ще залишається досить далекою від наявних теоретичних здобутків і нормативно-правової бази, а головне – від розуміння глибини суспільних трансформацій та потреби кардинального перегляду питань врегулювання суспільних відносин, які нині динамічно змінюються.

Сьогодні новітні інформаційні технології, які спочатку мали конкретне функціонально-цільове призначення, в умовах цифрової трансформації інтегруються з іншими технологіями і можуть надавати не лише нову якість результатів їх сумісного (сумарного) використання, але й створювати нові загрози та більші можливості для несанкціонованого отримання й використання персональних даних людини.

Проблеми розбудови та ефективності систем захисту персональних даних є предметом активних наукових розвідок та висвітлені у працях іноземних та українських вчених [3], але продовжують викликати багато правових та нормативних питань.

Метою статті є оцінка низки актуальних теоретичних та прикладних проблем у сфері захисту та безпеки персональних даних людини.

Виклад основних положень. У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних – General Data Protection Regulation (далі – GDPR, з англ. "Пакет захисту даних"), який передбачає умови забезпечення узгодженої нормативно-правової бази на європейському рівні.

Головним документом, який визначає на території держав-членів ЄС застосування обов'язкових правил, є Регламент (ЄС) 2016/679 "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви № 95/46/ЄС (Загальні Положення про захист даних)" від 27 квітня 2016 р. (див. [4, с. 2-103]).

Регламент GDPR має понад 100 стор. тексту, з яких Преамбула-роз'яснення наступних приписів складає 44 стор. (173 роз'яснення), де йдеться про підходи до правового регулювання захисту персональних даних у контексті раніше прийнятих документів ЄС та намаганнями врахування проблем щодо нових технологічних досягнень.

Важливою новацією Регламенту GDPR є те, що вперше у документах сфери захисту персональних даних офіційно констатовано (п. 1 Преамбули): *"**Захист** фізичних осіб у зв'язку з обробкою персональних даних **є основоположним правом**"* (курсів – *Авт.*). Далі, у п. 11 Преамбули, зазначено: "*Ефективний захист персональних даних на усій території ЄС вимагає зміцнення та детального визначення прав суб'єктів даних* та обов'язків осіб, які визначають та здійснюють обробку персональних даних". А згідно з п. 10 Преамбули щодо удосконалення законодавства встановлена така рекомендація – "*надати державам-членам можливість …введення національних положень з метою подальшого уточнення застосування правил, передбачених цим Регламентом,…більш точно визначаючи умови, за яких обробка персональних даних є законною*".

До GDPR включено Директиву (ЄС) 2016/680 "Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень або виконання кримінальних покарань, та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД" [4, с. 104-156], а також Директиву (ЄС) 2016/681 "Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину" [4, с. 157-176].

Питання скасування Директиви 1995 р. та Рамкового рішення 2008 р. пов'язано з проблемами наявності правової невизначеності у зв'язку з діяльністю у мережі Інтернет (п. 9 Преамбули).

Крім зазначеного, у 2016 р. Європейським Парламентом також була затверджена Директива ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive) [5], а з 2017 р. почалась робота над проектом ЄС ЄС про ePrivacy [6].

Вважаємо за доцільне розглянути деякі актуальні, на наш погляд, ключові аспекти згаданих документів.

1. Регламент GDPR.

Першим ключовим аспектом, зокрема у будь-якої науці, – це питання визначення та тлумачення термінів. У сфері захисту та безпеки персональних даних це, поперед усього, стосується термінів "персональні дані" та "ідентифікація" (для порівняння розбіжностей наведено Таблицю визначень), а також розуміння термінів "контролер" та "обробник".

Конвенції РЄ № 108 від 28.01.81 р.	**Директива 95/46/ЄС** від 24.10.95 р.	**Регламент GDPR** від 27.04.16 р.	**Закон України** від 01.06.10 р. № 2297-VI (ред. від 04.03.20 р.)
персональні дані – означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною ("суб'єкт даних") [2, с. 66].	**персональні дані** – означає будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити ("суб'єкт даних"); особою, яку можна встановити, є така, яка може бути встановленою прямо чи опосередковано, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, ізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості [2, с. 281].	**персональні дані** – означає будь-яку інформацію, що стосується фізичної особи, що ідентифікована або може бути ідентифікована ("суб'єкта даних"); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як: ім'я, ідентифікаційний номер, дані про місце розташування, онлайн-ідентифікатор, один чи декілька специфічних факторів фізичної особи щодо: фізичної, фізіологічної, генетичної, ментальної, економічної, культурної і соціальної ідентичності [4, с. 45].	**персональні дані** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

У загально-теоретичному плані поняття *"персональні дані"* охоплює об'єктивні та суб'єктивні відомості про особисте, сімейне чи публічне життя фізичної особи-людини, що виражені у формі літер, чисел, графіки, фото, звуку чи відео, якщо вони дозволяють ідентифікувати таку особу, тобто обов'язково стосуються конкретної особи.

В інформаційних системах під *"ідентифікацією"* звичайно розуміють процес присвоєння як суб'єктам, так і об'єктам комунікації певних унікальних ідентифікаторів і їх порівняння з переліком привласнених ідентифікаторів. Для визначення особи-людини або об'єкту техніки, що застосовують інформаційні засоби, можна говорити не стільки про ідентифікацію, скільки про її автентифікацію. Саме автентифікація дозволяє

встановити відповідність названому нею ідентифікатору. Таким чином, при ідентифікації користувач Інтернету "визначає себе" інформаційній системі, підключеної до мережі, а завдяки автентіфікації встановлюється відповідність особи (або об'єкта) названому нею ідентифікатору, зокрема шляхом застосування пароля.

На практиці встановити наявність зв'язку між літерами і/або цифровими позначеннями та конкретною фізичною особою достатньо складно, оскільки за різних умов позначення можуть розглядатися як персональні дані, так і не бути ними, наприклад – набір цифр ідентифікатора окремо не є персональними даними. Якщо ж додати до нього, наприклад ПІБ, то виникають персональні дані.

За GDPR вирішення питання, чи є відомості про особу персональними даними залежить від поглядів та можливостей конкретного *контролера* (означає *фізичну чи юридичну особу, державний орган, агенцію або іншу установу, яка, самостійно чи спільно з іншими, визначає мету, засоби збирання та обробки персональних даних* (п. 7 ст. 4 Регламенту) ідентифікувати людину за наявних у нього відомостей, у тому числі за рахунок поєднання таких відомостей з інформацією, яку він може отримати від третіх осіб з урахуванням "доцільної ймовірності". Разом з умовністю (тобто наявності випадковості) вказане передбачає (згідно п. 26 Преамбули та ст. 25 Регламенту GDPR) оцінку фінансових витрат, існуючих технологій та часу, що необхідні для ідентифікації особи. При цьому, обробку даних за дорученням контролера може здійснювати *обробник* (означає *фізичну чи юридичну особу, державний орган, агенцію або іншу установу, яка здійснює обробку персональних даних від імені контролера* (п. 8 ст. 4 Регламенту)*, який також, як представляється, може слідувати "доцільної ймовірності".

Для збирання персональних даних сьогодні звичайно використовуються не лише аккаунти щодо онлайн ідентифікації, а й IP-адреса – набір чисел, що присвоюється приладу, забезпечує його ідентифікацію та зв'язок з іншими приладами через мережу Інтернет. Для провайдерів електронних комунікацій щодо Інтернет-послуг IP-адреси вважаються персональними даними, оскільки можна пов'язати IP-адресу з конкретною людиною. Стосовно контролерів, які не є провайдерами Інтернет-послуг, то вони використовуючи IP-адресу, можуть створювати профіль звичок людей та розрізняти їх один від одного (за аналогією з файлами cookie). Головне у тому, що коли людину можна ідентифікувати, поєднавши IP-адресу з додатковою інформацією, то IP-адреса може вважатися персональними даними. До того ж, інформація, отримана за допомогою файлів cookie, в більшості випадків буде вважатися персональними даними.

Таким чином, фізичні особи можуть асоціюватися з онлайн-ідентифікаторами, що надаються їх пристроями, застосуваннями, інструментами та протоколами, такими як адреси Інтернет-протоколів, ідентифікатори файлів cookie або інші ідентифікатори, наприклад, ідентифікаційні мітки радіочастоти. Це може спричинити появу електроних слідів, які, зокрема у комбінації з унікальними ідентифікаторами та іншими даними (відомостями), отриманими серверами, можуть бути використані для створення профілів фізичних осіб та їх ідентифікації, що визначається у Регламенті GDPR (п. 30 Преамбули).

---

* *Примітка.* Закон України "Про захист персональних даних" застосовує терміни *володілець персональних даних* – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом та *розпорядник персональних даних* – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Регламент GDPR зобов'язує – для того, *щоб визначити, чи є фізична особа такою, що може бути ідентифікована*, необхідно врахувати *усі засоби*, які можуть бути використані з достатнім ступенем ймовірності, наприклад, виокремлення контролером або іншою особою, прямо чи опосередковано. Для того, *щоб встановити, чи можуть засоби з достатнім ступенем ймовірності бути використані для ідентифікації фізичної особи*, необхідно врахувати *усі об'єктивні фактори*, такі як витрати та кількість часу, необхідного для ідентифікації, з урахуванням технологій, наявних на момент обробки, та технічних розробок (п. 26 Преамбулт). Ідентифікація повинна включати в себе цифрову ідентифікацію суб'єкта даних, наприклад, через механізм автентифікації, такий як реєстраційні дані, що використовуються суб'єктом даних для авторизації в системі онлайн-послуг, що пропонує контролер даних (п. 57 Преамбула).

Наступним ключовим аспектом у сфері захисту та безпеки персональних даних є визначення принципів та умов їх обробки.

Згідно положень Регламенту GDPR обробка має здійснюватися на основні таких принципів (ст. 5 Глави II Регламенту GDPR):

1) *законність, справедливість і прозорість* – персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб'єкта даних;

2) *цільове обмеження* – збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою;

3) *зведення до мінімуму даних* – бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються;

4) *точність* – бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілей, для яких вони обробляються, слід видаляти або виправляти без затримки;

5) *обмеження зберігання* – зберігається у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілей, для яких вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно з метою архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей;

6) *цілісність і конфіденційність*[**] – оброблятися так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів;

7) *підзвітність* – будь-яка установа (компанія тощо) несе відповідальність перед наглядовими органами і повинна бути здатна довести дотримання положень Регламенту.

У загальному плані правові новації Регламенту GDPR свідчать про спрямованість на подальше посилення захисту прав суб'єктів персональних даних. Це знайшло відображення у ст. 17 Регламенту GDPR яка встановлює за суб'єктом персональних

[**] *Примітка*. Поняття "конфіденційність" згадується у Регламенті GDPR у пп. 39, 49, 75, 83, 85, 163 Преамбули та у ст. 14, 28, 32, 38, 54, 76 Регламенту, але *юридичного* його *визначення та ознак сутності не наведене*. У законодавстві України чинним є Державний стандарт "Технічний захист інформації. Терміни та визначення" (ДСТУ 3396.2-97), який *визначає це поняття та надає його суттєві ознаки застосування* крізь тріаду повноважень права власності (див. [7]), але практично їх не використовують. Сенс тлумачення "конфіденційності" може розумітися як "таємно-довірче" властивість об'єкта, зокрема, інформації, яка обумовлює умови її використання, тобто надані особам можливості по відношенню до об'єкта конфіденційності.

даних “право бути забутим” (англ. – *right to be forgotten*). Стаття уточнює “право на видалення даних” і визначає його умови, включаючи обов’язок володільця, який оприлюднив персональні дані, повідомляти треті сторони про вимогу суб’єкта даних щодо усунення будь-яких посилань на відповідні персональні дані, а також видалення будь-яких копій чи примірників таких персональних даних. Вона також передбачає право на обмеження обсягів обробки в певних випадках, уникаючи при цьому використання двозначності терміну “блокування даних”.

У Розділі 4 Регламенту GDPR передбачено право суб’єкта даних не бути предметом заходів, які ґрунтуються на “профілюванні”, що розвиває (з відповідними змінами та додатковими запобіжними заходами) положення ч. 1 ст. 15 Директиви № 95/46/ЄС щодо автоматизованих рішень та враховує численні рекомендації Ради Європи щодо запобігання профілювання.

Значна увага у Регламенті GDPR приділена правилам передачі персональних даних в межах ЄС та у треті країни або міжнародні організації, з урахуванням умов передачі з однієї системи електронної обробки до іншої (пп. 6, 48, 50, 68, 101, 107 та ін. Преамбули, а також у ст. 14, 15, 20 та ст. 44-49 Глави V Регламенту GDPR).

Нові правила-приписи мають застосовуватися до обробки даних фізичних осіб у компаніях, закладах, установах, організаціях та підприємствах, розташованих не тільки на території держав-членів ЄС, але і тих, що здійснюють свою діяльність за його межами і пов’язані з обробкою персональних даних в рамках ЄС. Правила не поширюються на обробку даних про юридичних осіб, а також на дані, які відносяться до анонімної інформації і померлих осіб (п. 26, 27 Преамбули).

Правила Регламенту GDPR не застосовуються до обробки персональних даних фізичною особою для особистої чи побутової діяльності та без зв’язку з професійною або комерційною діяльністю В то же час Регламент застосовується до контролерів чи осіб, що здійснюють обробку даних, які забезпечують засоби для обробки персональних даних у ході такої особистої чи побутової діяльності (п. 18 Преамбули, ст. 2 Регламенту). Особиста або побутова діяльність може включати, зокрема, листування, використання особистої адреси (е-пошта), здійснення онлайн діяльності в інформаційно-комунікаційних мережах тощо у зазначеному контексті діяльності. Суб’єкт даних повинен мати можливість передавати свої персональні дані з однієї системи електронної обробки до іншої без втручання інших осіб.

Згідно з положеннями Регламент GDPR не застосовується до обробки персональних даних в інтересах забезпечення національної безпеки та діяльності правоохоронних органів (для цілей попередження і розслідування протиправних дій), а також до обробки персональних даних державами-членами ЄС щодо загальної зовнішньої політики і політики безпеки ЄС (п. 16 Преамбули).

Персональні дані, які обробляються державними органами з метою запобігання, розслідування, виявлення чи судового переслідування злочинів або виконання покарань, зокрема, щодо запобігання загрозам суспільній безпеці та вільному переміщенню таких даних, регулюються іншим правовим актом ЄС, а саме – Директивою (ЄС) 2016/680 Європейського Парламенту і Ради.

У зв’язку з використанням нових технологій та з урахуванням характеру, обсягу, контексту та цілей обробки, що ймовірно, призведе до високого ризику для прав і свобод фізичних осіб, контролер повинен перед початком обробки провести *оцінку впливу* операцій з захисту та безпеці даних які передбачаються, тобто до початку проведення ризикованих операцій з обробки даних (п. 83, 84, 91, 94 Преамбули; ст. 35 Регламенту GDPR).

При цьому кожна держава-член ЄС може мати свої особливі погляди та відповідний зміст національного законодавства, але коли справа стосується та пов'язана зі співпрацею з будь-якими організаційними структурами держав-членів ЄС (зокрема, бізнес-діяльністю) слід керуватися приписами, що визначаються у Регламенті GDPR. У разі недодержання зазначеного можуть бути накладені такі *санкції*:

- *попередження у письмовій формі у разі першого й не навмисного недотримання приписів щодо захисту персональних даних;*
- *призначення регулярних або періодичних перевірок діяльності щодо захисту даних;*
- *призначення санкцій (в межах ЄС, на організацію, компанію та ін.) – штрафів у розмірі до 20 млн. EUR або до 4 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше);*
- *призначення санкцій (при транскордонній передачі персональних даних) – штрафів у розмірі до 10 млн. EUR або до 2 % від загального річного обсягу фінансування (від показників поточного і попереднього фінансового року, виходячи з того, яка сума більше).*[***]

2. Директива ЄС "Про безпеку мережевих та інформаційних систем" (NIS Directive).

Основне завдання NIS Directive – забезпечення високого рівня інформаційної безпеки для операторів критичної інфраструктури і провайдерів цифрових послуг [5]. Тобто, йдеться не лише про захист персональних даних, але й про безпеку даних взагалі.

Для виконання цього завдання державам-членам ЄС запропоновано підвищити свою готовність і поліпшити співробітництво один з одним, а також зобов'язати операторів, які надають критично важливі послуги, пов'язані з певними об'єктами інфраструктури, і провайдерів окремих цифрових послуг вжити відповідних заходів з керування ризиками безпеки й повідомляти про серйозні інциденти компетентним національним органам.

Національні особливості існують при реалізації будь-яких міжнародно-правових актів. Проте, NIS Directive безпосередньо пов'язана з проблемами її практичного застосування, оскільки більшою мірою визначає дії, які необхідно виконати державам-членам ЄС, залишаючи деталі на розсуд таких країн.

Водночас, нагальною залишається проблема як саме держави-члени мають реалізовувати вимоги щодо організації співробітництва з метою забезпечення скоординованої відповіді на різні інциденти за наявності різних підходів до цих питань.

3. Проект ЄС про e-Privacy.

Сьогодні, поряд з GDPR, в Європейському Союзі діє Директива 2002/58/ЄС "Про обробку персональних даних та захист таємниці ("privacy") в секторі електронних комунікацій" від 12 липня 2002 року [2, с. 379-392]. Водночас, планується прийняття нового акту на рівні рекомендацій-директиви або правового стандарту (Регламенту ЄС) – "e-Privacy Regulation".

[***] *Примітка.* В Україні за *порушення законодавства у сфері захисту персональних даних* передбачається накладення штрафу: на громадян та посадових осіб від 100 до 500 неоподатковуваних мінімумів їх доходів; на громадян-суб'єктів підприємницької діяльності від 200 до 2000 неоподатковуваних мінімумів доходів (ст. 188^{39} Кодексу України про адміністративні правопорушення). *Порушення недоторканності приватного життя* караються штрафом від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до 2 років, або арештом на строк до від 3 до 6 місяців, або обмеженням чи позбавленням волі на строк від 3 до 5 років (ст. 182 Кримінального кодексу України).

Процес розробки проекту розпочався ще в 2017 році [6], коли у ЄС затвердили GDPR та дійшли висновку, що Директива 2002/58/ЄС вже не відповідає вимогам цифрового суспільства, а її приписи, які були розроблені у розвиток Директиви 95/46/ЄС, в деяких питаннях не узгоджуються з приписами GDPR. Зазначимо, що на відміну від Директив ЄС, Регламент ЄС є правовим актом-стандартом Європейського Союзу, який негайно набирає чинності як закон в усіх державах-членах одночасно. Проте, "e-Privacy Regulation" може бути документом загального характеру, без необхідності імплементації його положень до національного законодавства кожної країни-учасниці ЄС.

Нині положення "e-Privacy Regulation" активно дискутуються, а погляди сильно різняться. До основних проблем, які розглядаються, можна віднести:

– конфіденційність комунікацій та посилення контролю за нею в умовах електронної згоди, застосування браузерів, файлів-cookie, не обмежуючись приватністю під час надсилання голосових та текстових повідомленнях в мережі Інтернет, крім обмеження щодо контролю "чутливих" персональних даних;

– необхідність позбавлення власників веб-ресурсів отримувати згоду щодо файлів-cookie, які використовуються для покращення роботи в Інтернеті, а також спрощення можливості для користувачів налаштовувати браузери в частині згоди або відмови від обробки файлів-cookie;

– надання фізичним особам можливості погоджувати отримання маркетингових листів, які надсилаються за допомогою SMS, електронної пошти або в будь-який інший спосіб (захист від спаму);

– доцільності збереження таких важливих прав споживачів, як "право на заперечення" та "оцінки впливу на захист даних", обробки даних про особу для різних цілей без згоди осіб тощо.

Водночас, розробники проекту e-Privacy висловлюють надію про те, що метою регулювання має бути посилення довіри та безпеки в умовах єдиного ринку цифрових технологій [8].

Загалом, можна зробити припущення, що "e-Privacy Regulation" може бути або окремим документом, який діятиме узгоджено з GDPR, або окремим спеціальним положенням, який в деяких частинах буде доповнювати та уточнювати приписи Регламенту GDPR щодо захисту та безпеки персональних даних [9].

4. Підготовка нової редакції Закону України "Про захист персональних даних".

В Україні, як свідчить аналіз, здійснюються певні заходи щодо удосконалення законодавства у сфері захисту персональних даних. Сьогодні це стосується проектів змін до Закону України "Про захист персональних даних" щодо форм та умов надання згоди на обробку персональних даних в органах влади (від КМ України - реєстр. № 2671 від 23.12.2019, та альтернативний законопроект - від народних депутатів - реєстр. № 2671-1, кер. Королевська Н.Ю.).

Не торкаючись деталей пропозицій щодо упорядкування відносин, висловимо свою загальну точку зору на сутність предмету пропозицій.

У контексті захисту та безпеки існують такі категорії персональних даних:

перша – це відомості, які необхідні органам державної влади та місцевого самоврядування для здійснення повноважень у вирішенні загальних суспільно-економічних питань. У такому разі "згода суб'єкта даних на обробку" не потрібна;

друга – це відомості про особисту приватність та приватність сімейного життя. Приватність – це право людини "на недоторканність її особистого життя", що передбачає наявність права на "самітність та самоту", "бути наданій самої собі", "бути забутою та

залишеною у спокої", "мати у житті особистий простір" тощо. Вона (приватність) не може бути предметом обробки органами державної влади та місцевого самоврядування. Водночас, право приватності повинно бути гнучким та здатним прилаштовуватись до потреб сьогодення, зокрема, воно не повинно забороняти публікацію матеріалів, що становлять суспільний або державний інтерес, зокрема щодо розслідувань, виявлення та судових переслідувань кримінальних правопорушень;

третя – це особливі відомості щодо персональних даних людини ("чутливі" дані**)**. Стосуються расового, етнічного і національного походження, політичних, релігійних, світоглядних вірувань, членства у політпартіях, профспілках, стану здоров'я, біометричні, генетичні дані, статева орієнтація. Чим більша " чутливість" цих даних, тим більший ризик порушення прав і свобод людини і тим більш надійними мають бути правові гарантії. Тому вони заслуговують на особливий захист. Однак, обробка зазначених даних може бути необхідною для забезпечення суспільних інтересів у сферах охорони здоров'я, правоохоронної діяльності тощо без згоди суб'єкта даних. Якщо в ході електоральної діяльності робота демократичної системи держави-члена потребує від політичних партій компіляції персональних даних щодо політичних переконань населення, обробка таких даних може бути дозволена з міркувань суспільних інтересів, за умови встановлення відповідних гарантій.

Зазначене, вважаємо, повинно отримати відображення у Законі України "Про захист персональних даних", наприклад у вигляді формулювання: *персональні дані приватного характеру не є предметом обробки у ході діяльності органів державної влади та місцевого самоврядування.* При цьому, вказане може бути додатком до п. 4 ст. 10 Закону та сформульовано таким чином – *відомості про приватне життя людини не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості*.

Одночасно з вказаним, слід звернути увагу на те, що в державі триває робота щодо оцінки ефективності законодавства у сфері захисту персональних даних та визначення перспектив в його удосконаленні.

Так, у листопаді 2020 р. відбулися консультації з цих питань з представниками-експертами від ЄС та РЄ. При цьому зазначалося, що проект нової редакції Закону України "Про захист персональних даних" слугуватиме основою для захисту персональних даних у державному і приватному секторах, а також для ухвалення правових актів, що регулюють обробку і безпеку персональних даних [10].

У презентації до законопроекту представники-експерти від ЄС та РЄ відзначали, що: *"...для отримання якісного законодавства дуже важливо дотримуватися загальної мети внесення поправок та оцінити їхній вплив на права і свободи людини, а також на вільний рух персональних даних"*.

Рекомендації та пропозиції експертів від ЄС та РЄ стосувалися необхідності вирішення таких *проблемних питань*, а саме:

- *"уникнення положень законопроекту, які є занадто складними й навіть неможливими для реалізації на практиці, оскільки вони не матимуть жодної цінності для захисту прав і свобод людини;*
- *зобов'язання державних органів, залучених до законотворчого процесу, включати до правових актів, що регулюють обробку персональних даних, ціль обробки, про яку йдеться, та іншу необхідну інформацію залежно від обставин;*
- *передбачення процедури здійснення контролерами даних оцінки впливу на захист даних у процесі ухвалення законодавчих актів;*

- *встановлення основних принципів обробки персональних даних органами державного і недержавного секторів;*
- *визнання в законопроекті застосування механізмів ЄС з боку українських контролерів даних і операторів даних, передбачених у GDPR – кодексу поведінки (стаття 40) і зобов'язальних корпоративних правил (стаття 47);*
- *створення незалежного контролюючого органу з питань захисту персональних даних".*

В цілому, з огляду на викладене та стан сучасних процесів цифрової трансформації та євроінтеграції України, вкрай актуальною постає проблема кардинального перегляду поглядів та підходів щодо правового врегулювання новітніх суспільних відносин, які активно формуються і розвиваються в українському суспільстві.

З цього приводу, слушними видаються оцінки стану національного законодавства, надані першим заступником Голови Верховної Ради України, академіком НАПрН України Р. Стефанчуком: *"Кількість діючих нормативно-правових актів уже набагато перевищила один мільйон. 90 % законопроектів, які розглядаються українським парламентом, – це зміни й доповнення до чинного законодавства. Велика кількість законів обернено пропорційна їх якості. І якщо такі тенденції збережуться, то ми й надалі без єдиного системного підходу будемо робити величезну кількість нормативно-правових актів, які не забезпечують головного – якості українського законодавства. В Україні необхідно змінити підхід до правотворчої діяльності"* [11].

Висновки.

1. Реальні та потенційні ризики можливих порушень прав суб'єктів персональних даних (фізичної особи, людини і громадянина) залишаються вкрай актуальною прикладною проблемою в сучасних умовах розвитку інформаційних (цифрових) технологій, зокрема, впровадження "хмарних" технологій та технологій "великих даних" з їх конвергенцією, Інтернету речей, штучного інтелекту, розвитку ринку електронних комунікацій тощо. При цьому визначення та трактування терміну "персональні дані" є одним з головних аспектів, який безпосередньо пов'язаний з проблемами захисту прав та безпеки людини в умовах глобальних трансформаційних процесів та необхідності імплементації європейських правових стандартів в національне законодавство України.

2. До системних проблем у сфері захисту та безпеки персональних даних в сучасних умовах суспільних та цифрових трансформацій слід віднести такі:

– незважаючи на значну кількість прийнятих в установах Європейського Союзу і Ради Європи актів, законодавство про захист персональних даних у європейських країнах перебуває на етапі становлення. Повна відповідність національних законодавств держав-членів ЄС з питань захисту персональних даних європейським правовим стандартам також не досягнута. Вкрай актуальною ця проблема залишається й для України;

– реалізація положень нового європейського порядку захисту персональних даних, зокрема, GDPR, Директиви NIS, а у майбутньому – регламенту (або положення) про e-Privacy вимагає пошуку нових підходів та комплексних змін ділової практики у державах-членах ЄС та в країнах-партнерах ЄС. При цьому, потребує дуже значної уваги проблема суттєвого зростання розриву між стрімким розвитком інформаційних (цифрових) технологій та змінами законодавства у цій сфері;

– в сучасних умовах актуалізується проблема зміни концептуальних поглядів і правового регулювання з питань захисту прав в інформаційній сфері, тобто ***зміни існуючої правової модальності***. Передусім це стосується проблем забезпечення захисту та безпеки приватності персональних даних людини.

3. Виходячи з того, що людина, її життя і здоров'я, недоторканність та безпека віднесені до найвищих цінностей демократичного суспільства, у національному законодавстві мають бути відображені базові критерії з питань захисту та безпеки персональних даних за такою можливою формулою: *право приватної власності людини і громадянина (фізичної особи) на персональні дані – це право володіння, користування та виключного розпорядження своїми персональними даними, за умов збалансованості та узгодженості цього права з правами інших громадян та потребами суспільства і держави у безпеці.*

При цьому, володіння, користування та розпорядження персональними даними мають передбачати: *а) володіння персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення приватності персональних даних в незмінному вигляді; *б) користування персональними даними* – наявність можливості людини та нормативно-правових умов для забезпечення використання відомостей про себе на власний розсуд; *в) розпорядження персональними даними* – наявність можливості та нормативно-правових умов для забезпечення виключного права людини щодо порядку доступу до своїх персональних даних.

Запропоновані формули, як вважаємо, відповідають здобуткам історико-правової науки щодо загальної ідеї прав людини на життя, приватну власність і свободу, корелюється з приписами п. 1 Преамбули Регламенту GDPR, що ***захист персональних даних фізичних осіб є основоположним правом***, а також можуть визначати основу для законотворчості, правозастосування та оцінки ефективності діяльності у сфері захисту персональних даних.

4. Сьогодні продовжує існувати проблема імплементації приписів європейських правових стандартів щодо сфери захисту персональних даних у законодавство України. Це, поперед усього, стосується повної узгодженості законодавства з правовими приписами Регламенту GDPR, який є обов'язковим у виконанні для усіх держав-членів ЄС.

Роботу можна почати з запровадження у базовий Закон України (у ст. 2. Визначення термінів) дефініцій, сформульованих у ст. 4 Регламенту GDPR. Потім здійснити розміщення термінів у тексті Закону, з урахуванням потреби внесення в статті відповідних виправлень і змін.

Навіть з вищевказаного видно, що існує багато різнобічних проблем щоб привести законодавство України у відповідність до приписів Регламенту GDPR. Це можливо за наявності умов формування системності у організаційних та правових питаннях, вирішення яких потребує створення окремого у державі незалежного наглядового органу (згідно положень Глави VI Регламенту GDPR), який повинен сприяти послідовному впровадженню та застосуванню цього Регламенту.

Використана література

1. Защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. Київ: Национальное агентство по вопросам информатизации при Президенте Украины, 1998 г. 128 с.; Права человека и защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. – (Государственный комитет связи и информатизации Украины). Харьков: Фолио, 2000. 280 с. С. 11-36; Становлення і розвиток правових основ та системи захисту персональних данихв Україні: монографія ; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017 р. 226 с. С. 9-19.

2. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності": посібник. Кн. 2 / В. Брижко, М. Швець та ін. Київ: ТОВ "Пан Тот", 2006 р. 509 с.

3. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*: зб. наук. праць. № 3(90)/2017. С. 36-50; Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних. *Інформація і право*. № 1(32)/2020. С. 33-46; Брайчевський С.М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* № 4(31)/2019. С. 61-67; Брайчевський С.М. Проблема персональних даних при використанні систем Інтернету речей в галузі охорони здоров'я. *Інформація і право.* № 2(33)/2020. С. 69-76; Брайчевський С.М. Персональні дані та мультимедіа. *Інформація і право.* № 4(35)/2020. С. 82-91; Сенюта І.Я. Обробка персональних даних за новими правилами: захист чи порушення прав людини. – (*Стосовно упорядкування відносин, пов'язаних з коронавірусною хворобою COVID-19*). URL: https://www.hsa.org.ua/blog/obrobka-personalnyh-danyh-v-umovah-covid-19-zahyst-chy-porushen nya-prav-lyudyny

4. Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних / І. Майстренко – переклад з англ.; В. Брижко – редагування тексту. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.

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

6. ePrivacy Regulation. URL: https://en.wikipedia.org/wiki/EPrivacy_Regulation; Proposal for a Regulation on Privacy and Electronic Communications (2017). URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

7. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. № 4(19)/2016. С. 67.

8. Підготувались до GDPR? Тепер готуйтесь до ePrivacy regulation. URL: https://legalit group.com/eprivacy-regulation

9. Council of the EU Released a (New) Draft of the ePrivacy Regulation (2021). URL: https://www.lexology.com/library/detail.aspx?g=21a1516a-4682-4403-a828-5cf761438d41; Opinion 5/ 2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the com petence, tasks and powers of data protection authorities. URL: https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_en; Confidentiality of electronic communicatio ns: Council agrees its position on ePrivacy rules. URL: https://www.consilium.europa.eu/en/press/press-releases/ 2021/02/ 10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy- rules; The EU ePR (ePrivacy Regulation). A proposed regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). URL: https://www.itgovernan ce.co.uk/eprivacy-regulation-epr

10. Новий законопроект про захист персональних даних – експертні консультації за підтримки спільного проекту ЄС та Ради Європи. – (Україна). URL: https://www.coe.int/uk/web/ kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join -eu-and-coe-project

11. Стефанчук Р. Про необхідність змін у підходах до правотворчої діяльності. URL: https://www.rbc.ua/rus/news/otmenyayut-svyshe-tysyachi-aktov-sssr-rade-1614027171.html

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

УДК 343.412

КАРЄВ І.Ю., *магістр права.*
ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент,* КПІ ім. Ігоря Сікорського.

КІБЕРСТАЛКІНГ: ВІДОБРАЖЕННЯ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ

Анотація. *Стаття присвячена кіберсталкінгу – виду специфічного кіберзлочину, при якому психологічний тиск на жертву відбувається за допомогою ІТ-технологій, та його відображення у національному законодавстві.*
Ключові слова: *інформаційне суспільство, соціальні мережі, кіберсталкінг, закон.*

Summary. *The article is devoted to cyberstalking – a type of specific cybercrime in which psychological pressure on the victim occurs with the help of IT-technologies, and its reflection in national legislation.*
Keywords: *information society, social network, cyberstalking, law.*

Аннотация. *Статья посвящена кіберсталкингу – виду специфического киберпреступления, при котором психологическое давление на жертву происходит с помощью ІТ-технологий, и его отображение в национальном законодательстве.*
Ключевые слова: *информационное общество, социальные сети, кіберсталкинг, закон.*

Постановка проблеми. Кіберсталкінгом, або онлайн-сталкінгом називають переслідування в соцмережах Інтернету [1]. Кіберсталкінг – це відносно нове явище, яке виникло з розвитком інформаційних технологій. Сам термін уперше з'явився на початку 2000-х років, а в 2015 році був офіційно внесений у нову редакцію словника Уебстера, який уважається самим повним сучасним американським словником англійської мови. По суті кіберсталкінг являє собою нав'язливе переслідування в Інтернеті з боку однієї людини або групи осіб, яке несе в собі потенційну погрозу психологічному, фізичному або матеріальному стану жертви. Воно може містити в собі прямі або непрямі погрози, шантаж, несанкціоноване використання персональних даних, поширення наклепу та ін. Кіберсталкери географічно не обмежені деяким районом, країною – вони можуть переслідувати жертв, навіть перебуваючи в інших країнах з такою ж легкістю, якби вони знаходились по сусідству. Більше того, новітні технології дозволяють віртуальному переслідувачеві не тільки загрожувати іншій особі, але й підбурювати до таких дій третю сторону. І це вкрай складно відстежити. Кіберсталкінг може проявлятися не тільки в несанкціонованому використанні персональних даних з метою заплямувати честь жертви або вкрасти майно, але й в психологічному тиску, що припускає контакт із переслідувачем.

Згідно даним Міністерства юстиції США, щорічно жертвами Інтернет-переслідування стають більш 1 мільйона жінок і 370 тисяч чоловіків. Кожна 12-та жінка й кожний 45-й чоловік зіштовхуються із проявами кіберсталкінгу, спрямованого проти них. Онлайн-сталкери можуть, зокрема, зламувати акаунти, читати листування жертви, погрожувати в приватних повідомленнях, розсилати іншим знайдені в переписці інтимні світлини ("чутливі дані") тощо. Ці цифри й фактори виглядають досить тривожно. Особливо враховуючи той факт, що поки не існує достатнього досвіду боротьби з кіберсталкінгом, що утрудняє притягнення злочинців до відповідальності. Важливим є те, що віртуальне переслідування нерідко плавно перетікає в реальне. І наслідки цього можуть бути абсолютно непередбачуваними [2].

До вказаного слід зазначити, що кіберсталкінг, як сучасний поширений у світі вид злочину у сфері ІТ-технологій, поки що, на превеликий жаль, не має відображення у законодавстві України.

Метою статті є дослідження кіберсталкінгу як об'єкту інформаційної загрози.

Виклад основного матеріалу. Кіберсталкінг – вид правопорушення в інформаційній сфері, який передбачає переслідування людини в мережі з агресивним або сексуальним підтекстом, поширення неправдивих обвинувачень в Інтернеті, плітки й наклеп [3]. Він став можливим завдяки появі та розвитку декількох факторів, а саме: цифрових технологій, комп'ютерних мереж, соціальних мереж та окремої науки – соціальної інженерії [4]. Кіберсталкінг, як і його "брат" з реального світу – сталкінг (від англ. *stalk* – "переслідувати") не розглядається правоохоронцями як певний вид правопорушення (злочину), але у даному діянні існує як потерпіла сторона, так і сторона, яка певним чином створює для потерпілої сторони умови, при яких вона відчуває страх та ін. Кіберсталкерами можуть бути будь-хто, навіть просто угруповання тих, хто робить це для розваги, але легше за все виконати певні дії, коли вже маєш необхідні початкові дані.

Як зазначається у [2], США стали першої у світі країною, що розробила закон про сталкінг. Це відбулося ще 30 років тому, в 1990 році. Там кіберпереслідування підпадає під статтю закону про наклеп і утиск. Залежно від ваги злочину, розміру економічного збитку, заподіяного діянням, кримінального минулого підсудного й багатьох інших факторів порушникові може бути призначений штраф і тюремне ув'язнення. Навіть нетривалий доведений кіберсталкінг, який задав фізичної, фінансової, репутаційної або емоційної шкоди жертві, карається кримінальним судом США. Але труднощі полягають у тому, що довести такі злочини буває складно. Головні труднощі виникають в пошуку злочинця, оскільки кіберсталкери найчастіше використовують спеціальні програми, які маскують справжню IP-адресу комп'ютерного обладнання.

Механізм кіберсталкерської атаки можливий у кількох сценаріях:

1. Взаємодія безпосередньо з жертвою – варіант шантажу. Такий вид кіберсталкерської атаки проводять у тому випадку, коли жертву починають шантажувати та примушувати до здійснення певних дій, або з метою отримання певних благ як матеріального, так і не матеріального характеру для себе або третьої особи. Результату добиваються завдяки погрозам оприлюднити певну приватну інформацію про жертву, завдяки якій остання опиниться у вразливому становищі. Інструментами такої взаємодії є: листи з погрозами на електронну пошту від анонімних джерел, листи з погрозами від новостворених акаунтів у соціальних мережах, телефонні дзвінки та СМС-повідомлення. Такий варіант можливий за умови, що атакуюча сторона не впевнена у стійкості жертви, або відсутністю певної інформації, яку можливо оприлюднити. Зазвичай даний метод використовують починаючі кіберсталкери бо вони можуть бути досить швидко ідентифіковані за електронними адресами, номерами телефонів.

2. Взаємодія безпосередньо з жертвою – варіант з метою отримання контролю над соціальним життям жертви у комп'ютерній мережі. Це – видозмінений варіант шантажу. Даний вид правопорушення здійснюється за умов наявності певних технологічних навичок у нападника, зокрема, злам профілю у соціальних мережах, анонімні дзвінки, отримання контролю над усіма можливими пристроями жертви та виконання певних програм по залякуванню. Для прикладу роздрукування на принтері будь-яких словосполучень або "гра" зі світлом за умови отримання доступу до системи "розумний дім". Використання такого варіанту можливе з метою отримання коштів від жертви у обмін на залишення у спокої або для спонукання до певних дій.

3. Жорсткий пресинг жертви. Сам варіант такої взаємодії можливий за умови, що кіберсталкер має певну команду професіоналів у цій сфері або замовив виконання визначених дій "зовнішнім" професіоналам. У такому випадку інформація, яка може бути оприлюднена, у разі не досягнення визначеної мети, дійсно існує. Вона була отримана від самої жертви або іншим шляхом – з реєстрів, банків даних, або навіть інформація з обмеженим доступом. Існує вірогідність, що жертва має цінну інформацію або має зробити дещо, що має серйозне значення для замовника. Кожен крок людини у цифровій мережі відслідковується. Зловмисники отримають доступ та викрадають не тільки профілі соціальних мереж, та паролі до електронних скриньок, а ще починається фаза стеження та взаємодія у реальності. У жертви зникають гроші з розрахункових рахунків, до неї доставляють певного роду предмети, досить часто крадуть авто. Іноді для повного розпечення самої жертви зламують телефон та блокують його вихідні дзвінки або навіть створюють DDOS-атаку за допомогою СМС-повідомлень, або анонімних телефонних дзвінків.

4. Використання контактної інформації соціальної мережі. Варіант, коли у соціальних мережах певні акаунти розповсюджують завідомо неправдиву інформацію, покликану викликати огиду до жертви. У даному варіанті кіберсталкер створює велику кількість профілів у соціальній мережі, певні веб-сайти з фіктивною інформацією про жертву (при чому оплату за хостинг та ім'я сайту вносить анонімним методом або за допомогою кардінгу). Жертві пишуть у соціальні мережі та на електронну пошту свої вимоги для зупинення акції залякування. При такому варіанті ніколи не відбувається контактів у реальному світі кіберсталкера та жертви.

5. Взаємодія з знайомими з реального життя. Досить цинічний вид кіберсталкера, коли жертва не отримує погроз у прямий спосіб. Уся взаємодія проходить з жертвою через рідних та знайомих, яких починають тероризувати телефонними спам-дзвінками з анонімних номерів та наговорювати на жертву. У соціальних мережах на сторінці кожного знайомого чи рідного будуть з'являтися спам-повідомлення від новостворених акаунтів. Іноді, як варіант, замість дзвінків використовують СМС-спам. Взаємодія напряму з жертвою не відбувається. Усі вимоги зловмисники надають у СМС-повідомленнях або на сторінках у соціальних мережах усіх знайомих та рідних.

6. Масовий пресинг. Варіант жорсткого пресингу жертви, але існує досить серйозна відмінність – абсолютно усі знайомі з соціальних мереж та реального життя будуть знаходитися під атакою кіберсталкера. Можливий варіант, що і найближчі родичі втратять кошти з розрахункових рахунків.

Для виконання будь-якого з варіантів необхідно пройти кілька стадій підготовки правопорушення, але за умови, що коли вони будуть проходити у кіберпросторі, то будуть мати свої особливості та специфіку:

1). Вибір жертви. За умови, що жертва вже знайома, тоді дана стадія переходить у наступну. Якщо жертва не знайома – обирається з соціальних мереж за певним критерієм, який визначений вже кіберсталкером.

2). Стадія розвідки. Вся інформація, яку можливо отримати з соціальних мереж – збирається та класифікується. Спочатку збирається інформація про електронну адресу, контактну інформацію, місце життя, контакти у соціальних мережах, з'ясовується ступінь взаємовідносин, роль у взаємовідносинах. Найбільший пріоритет надається рідним та тим, з ким людина взаємодіє постійно, де працює та детальна інформація про хобі. Якщо людина не відома, то збирається інформація про її матеріальний стан.

3). Стадія слідкування. Можливий варіант коли винаймається приватний детектив, що починає слідкувати за потерпілою особою. Але основне слідкування йде у соціальних

мережах. До сфери інтересів входить – персональні дані, приватне життя, часто відвідувані місця, рухоме майно, інформація про номери рахунків та банки, клієнтом яких є жертва та ін.

4). Тиха взаємодія або глибинне слідкування. Відбувається злам профілю соціальної мережі та електронного поштового ящику. Отримується доступ до карткових та розрахункових рахунків жертви, якщо така дія є у плані кіберсталкера.

5). Активна фаза. Початок обраного сценарію нападу на жертву. Отримання перших погроз.

Існує й інший вид кіберзлочину – кібербуллінг співзвучний з кіберсталкінгом. Є думка, що кіберсталкінг та кібербуллінг – одне й те саме, але це зовсім різні методи впливу та взаємодії з жертвою. Об'єднує ці два вида правопорушень використання одних і тих же засобів – апаратно-програмних засобів, таких як месенджер, соціальна мережа, також існує жертва та нападник. Але природа та кінцева мета досить різні. Якщо кіберсталкінг – це систематичний, моральний та психологічний тиск на жертву для отримання певного результату, то кібербуллінг – цькування для задоволення певних морально-психологічних потреб нападника [5 – 7].

На жаль, до цього часу національним законодавством не розглядається сталкінг та кіберсталкінг як окремий вид правопорушень. Не створені механізми фіксації, підтвердження та збору доказів, а також захисту жертви. Але при цьому слід враховувати, що кіберсталкінг – це кіберзлочин, тобто складне правопорушення, що складається з кількох дій, які мають певний сценарій та використовують апаратно-програмні засоби. Також слід враховувати, що певні закони поки ще не адаптовані під сучасні реалії, тому у них не означена юридична відповідальність за здійснення подібних діянь. Тому досить важко визначити ступінь вини організатора діяння, але такий злочин необхідно розглядати по частинах, адже він виконується у залежності від сценарію.

Основна ідея кіберсталкінгу – втручання у життя певної фізичної особи за допомогою комп'ютерної мережі для створення умов морального, матеріального впливу та психологічного страждання жертви. Кримінальним законодавством України зазначені дії не визначаються [8]. Крім цього, у випадку, коли людині не погрожують видати певні про неї матеріали або не наказують перевести кошти для зупинення акції, немає вимог виконати певні дії – лише цькування та постійне життя у страху, то такий випадок законодавцем, на жаль, також не визначено. Також не визначено протиправними діяння осіб, які за допомогою комп'ютерної мережі та смартфонів здійснюють надокучливі дзвінки або СМС-повідомлення з погрозами, шантажем, вимаганнями тощо, які повинні розглядатися як явний злочин в інформаційній сфері.

Немає чіткого розуміння, що таке DDOS-атака на пристрій зв'язку потенційної або реальної жертви за допомогою великої кількості телефонних дзвінків. По своїй суті таке порушення, як залякування особи завдяки засобам зв'язку, не визначено жодним законом.

В умовах розвитку цифровізації поняття "персональні дані" та його сприйняття що існує у чинному у законодавстві України, стає дедалі більш "розмитим" та неоднозначним. Більш того, відсутня чітка межа між поняттями "персональні дані" та "конфіденційна інформація" (яке у законодавстві взагалі не визначено), а також немає чіткої юридичної відповідальності за недбалість поводження з персональними даними на всіх етапах роботи з ними – збору, обробки, поширення, збереження та знищення [9].

Якого плану інформацію про особу треба вважати конфіденційною інформацією?

Якщо інформація взята з соціальних мереж, тобто та, яку особа власноруч виклала, то така інформація вже є публічною та загальнодоступною.

Якщо особу шантажують розповсюдженням інформації еротичного характеру або розповсюдженням інформації та доказів стосовно її приватного життя, яку б вона хотіла б приховати, то отримаємо ситуацію, коли відсутність реагування на це з боку правоохоронних органів "відштовхують" людину і провокують злочинців на кіберсталкерську активність. Як приклад інформації, з якою людина за власним бажанням не звернеться до правоохоронних органів – докази її участі в кримінальному правопорушенні, які не були отримані правоохоронцями, матеріали еротичного характеру, певний компромат та інші.

Фізичну особу, яка являє собою потерпілу сторону, такий підхід як законодавця, так і правоохоронців ставить у заздалегідь програшне положення, адже відсутній механізм правового захисту від злочинних дій подібного роду. Досить часто інформацію використовують як товар (що також у законодавстві не визначено), як засіб для маніпуляції, і у жодному випадку немає варіанту заборонити та вилучити інформацію у злочинця.

Для отримання контролю над соціальними мережами, електронною адресою та комп'ютерним обладнанням зловмисники проводять певні заходи, а саме процес зламу. Навіть за умови, що людина певним чином запідозрить спроби зламу – потерпілому нікуди звернутися з даною проблемою, адже жодна відповідна правоохоронна структура не працює з злочинами на етапі спроби зламу. Навіть після зламу електронної пошти, зламу та отримання контролю за розрахунковим рахунком жертва не може зробити майже нічого. Служба безпеки банку – буде відписуватися, що клієнт повинен самостійно дбати про власну безпеку, при зверненні до кіберполіцію – там теж активних дій не проглядається. Доказування через суд – справа не одного місяця, навіть якщо вдасться довести свою позицію, то завдяки інфляції людина отримає вже збитки та витрачений час.

Проблема кіберсталкінгу загострюється і надалі буде загострюватися в умовах подальшого активного розвитку комп'ютерних мереж та активного інтегрування комп'ютерних технологій у суспільне та приватне життя. Якщо вчасно не провести модернізацію законодавства у сфері захисту інформації та персональних даних, не створити державну службу, обов'язком якої буде робота щодо правопорушень, у ході яких за допомогою програмно-апаратного комплексу виконуються операції з отримання доступу та контролю над програмним забезпеченням постраждалої сторони, то з подальшою інтеграцією комп'ютерних технологій у приватне та соціальне життя отримаємо зростання кількості кіберзлочинців, які зможуть вільно тероризувати населення, відчуваючи свою безкарність.

Висновки.

Сучасні юридичні проблеми у сфері електронно-інформаційної комунікації пов'язані з тим, що техніко-технологічна взаємодія з реальним світом здійснюється через віртуальний простір за допомогою певного програмно-апаратного комплексу.

У зв'язку зі швидким розвитком ІТ-технологій та повільним розвитком законодавства щодо сфери комп'ютерних технологій маємо реальну ситуацію, коли злочинці діють безкарно, за умов недосконалості законодавства.

Складність вияву злочинця та отримання допомоги від кіберполіції, відсутність законодавчого визначення понять "кіберсталкінг" та "кібербуллінг" разом з визначенням механізмів протидії, надає злочинцям можливість безкарно виконувати дії, які вони обирають за певним сценарієм. Саме велика кількість варіацій дій злочинця не дає можливості чітко визначити ступінь його вини, а потерпілій стороні – навіть можливості на мінімальний захист від зловмисника. Зокрема це стосується відсутності сталих механізмів взаємодії та нормативних важелів щодо банківських структур, які

зобов'язують забезпечувати більше тісну взаємодію з правоохоронними структурами у частині розслідування втрати коштів з розрахункового рахунку потерпілих.

У підсумку, масштаб та поява нових способів і методів кіберзлочинів зумовлює потреби подальших досліджень з цієї тематики, спрямованих на удосконалення та розвиток національного законодавства, створення спеціальних програмних засобів захисту прав людини та відповідного методичного забезпечення для сфери протидії кіберзлочинності.

Використана література

1. Про сталкінг… URL: https://bit.ua/2020/01/pro-stalking

2. Меня преследуют в Интернете: что такое кибersталкинг, и как от него защититься. URL: https://www.marieclaire.ru/stil-zjizny/menya-presleduyut-v-internete-chto-takoe-kiberstalking-i-kak-ot-nego-zaschititsya

3. Кібersталкінг. URL: https://stop-ugroza.ru/life/kiberstalking-i-kak-ot-nego-zashhititsya

4. Соціальна інженерія: виклики та перспективи боротьби в українському контексті. *Інтернет ресурс – Українське право*.URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain (дата звернення: 25.01.2021).

5. Workplace Violence. United state department of labor. URL: https://www.osha.gov/workplace-violence (дата звернення: 25.01.2021).

6. The Involvement of Girls and Boys with Bullying: An Analysis of Gender Differences. US national library of medicine. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3881143 (дата звернення: 25.01.2021).

7. Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress, Research Press, 2007. – ISBN 0878225374.

8. Кримінальний Кодекс України: Закон України від 05.04.01 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n744 (дата звернення: 30.01.2021).

9. Закон України "Про захист персональних даних" від 01.06.10 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 30.01.2021).

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

УДК 341:316.774

ЗАБАРА І.М., *кандидат юридичних наук, доцент.*
Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка.

СВОБОДА ІНФОРМАЦІЇ: КОНЦЕПТУАЛЬНІ ПІДХОДИ У МІЖНАРОДНОМУ ПРАВІ

Анотація. *У статті розглядаються основні положення концепції свободи інформації. Автор досліджує доктринальні погляди на зміст свободи інформації. Розглядається сучасне трактування свободи інформації в міжнародному праві.*

Ключові слова: *інформація, доктрина, права людини, концепція, свобода інформації, міжнародне право.*

Summary. *Article deals with the contents of the information freedom concept. The author examines the doctrinal views on the content of information freedom. The author also examines a modern interpretation of the information freedom.*

Keywords*: information, doctrine, human rights, concept, freedom of information, international law.*

Аннотация. *В статье рассматриваются основные положения концепции свободы информации. Автор исследует доктринальные взгляды на содержание свободы информации. Рассматривается современная трактовка свободы информации в международном праве.*

Ключевые слова: *информация, доктрина, права человека, концепція, свобода информации, международное право.*

Постановка проблеми. Становлення і розвиток концептуальних засад інституту свободи інформації відбувається вже протягом майже сімдесятьох років, що охоплюють кілька періодів, протягом яких увага світового співтовариства зосереджувалась на широкому комплексі міжнародно-правових питань – від визначення змісту свободи інформації, до питань, пов'язаних з її реалізацією [1, с. 117-132; 2]. Інститут свободи інформації, виступаючи в якості стрижневого і ключового поняття, тим не менш, залишається одним із дискусійних і суперечливих явищ.

В сучасних умовах широкомасштабного розвитку інформаційно-комунікаційних технологій інститут свободи інформації набуває більшого значення і, відповідно, привертає більшу увагу, у зв'язку з чим постає питання щодо його сучасного бачення та перспективних напрямків розвитку. Його сучасне розуміння може бути доповнено врахуванням ключових основ, що свого часу визначили напрямки і пріоритети його розвитку в міжнародному праві. Розглянуті разом, вони, на нашу думку, дадуть комплексне бачення концепції інституту свободи інформації в сучасному міжнародному праві.

Результати аналізу наукових публікацій свідчать про те, що низкою дослідників були закладені основи для обґрунтування розвитку інституту свободи інформації в міжнародному праві. Загальнотеоретичну основу склали роботи А. Зануччи, Ю.М. Колосова, О.Г. Дніпровського, О.В. Єрмішиної, Т. Мендела, І.І. Мисика, Ф.В. Хондиуса та інших. Їх загальне бачення ґрунтується на досягненнях теорії міжнародного права та галузей міжнародного права. Тематика, розглянута в наукових роботах є доволі широкою, проте, залишаються питання щодо концептуального розвитку інституту свободи інформації в сучасному міжнародному праві.

Метою статті є оцінка основних положень концепції свободи інформації в міжнародному праві.

Виклад основного матеріалу. Ключові концептуальні положення щодо сучасного міжнародно-правового регулювання свободи інформації були закладені на універсальному рівні Резолюцією Генеральної Асамблеї ООН №59 (I) "Скликання міжнародної конференції з питання про свободу інформації" прийнятою 14 грудня 1946 року [3].

Спільне бачення світовим співтовариством ключових концептуальних положень цього інституту ґрунтувалось на загальновизнаному розумінні свободи інформації, а також розумінні її значення для міжнародно-правового регулювання тогочасних і майбутніх міжнародних інформаційних відносин. Таке бачення зводилось до низки принципових положень, що знайшло відображення в цій Резолюції і полягало, зокрема, у наступному:

- по-перше, було визначено загальне поняття свободи інформації. Зазначалось, що "свобода інформації є основоположним правом людини і являє собою критерій усіх видів свободи, захисту яких Об'єднані Нації себе присвятили" [3]. Варто звернути увагу на кілька принципових аспектів, що випливають з цього положення, а саме:

а) свобода інформації була віднесена до категорії основоположних прав людини (і розумілась виключно як право людини, а не право суб'єктів міжнародного права);

б) свобода інформації була визначена в якості критерію усіх видів свободи, що підлягають захисту ООН;

- по-друге, було визначено зміст свободи інформації і умови її реалізації. Так, було зазначено, що "свобода інформації визначається як право всюди і безперешкодно збирати, передавати і опубліковувати інформаційні відомості" [3].

Принциповим в цьому визначенні виступив комплекс прав, що поєднує різні види інформаційної діяльності – збирання, передавання і опублікування. При цьому, існує думка про те, що вказане "визначення стосується тільки однієї сторони питання про свободу інформації – права поширювати інформацію (це право віднесено до категорії основоположних прав людини) і нічого не говорить про право користування інформацією" [1, с. 118]. Однак на нашу думку, зміст визначення навпаки, таку можливість надає. Зауважимо, що важливими виступають і зазначені умови реалізації свободи інформації;

- по-третє, було визначено основний принцип свободи інформації. Визначалось, що "основним принципом її (свободи інформації) є моральний обов'язок прагнути до виявлення об'єктивних фактів і до поширення інформації без злісних намірів" [3]. Цим положенням фактично визначався загальний підхід до висвітлення подій, явищ і фактів, а також пов'язаних з ними коментарів і оцінок існуючого стану міжнародних відносин;

- по-четверте, була визначена роль інституту свободи інформації в міжнародних відносинах, як "основної передумови для будь-якої серйозної спроби сприяти досягненню миру та світовому прогресу" [3] (враховуючи можливість всюди і безперешкодно збирати, передавати і опубліковувати інформаційні відомості);

- по-п'яте, було підкреслено значення розвитку (інституту) свободи інформації і наголошено, що "взаєморозуміння і співробітництво між народами є неможливими за відсутності пильної і здорової світової суспільної думки, яка в свою чергу, цілком залежить від свободи інформації" [3].

Прийнята Резолюція, безперечно, надала можливість як загального бачення, так і наступного розвитку інституту свободи інформації в міжнародному праві. Подальшим

логічним і оптимальним шляхом було б прийняття міжнародної угоди на основі запропонованих Резолюцією положень. Проте, його реалізація наштовхнулась на розбіжності в підходах держав до розуміння і тлумачення положень щодо використання свободи інформації у міжнародних відносинах [1, с. 120-124; 4, с. 103-104; 5, с. 11-40]. Навіть досягнуті шляхом компромісу, залишились не повною мірою реалізовані результати роботи Конференції ООН з питання про свободу інформації 1948 року, а вони склали три проекти міжнародних конвенцій (Конвенції про свободу інформації, Конвенції про збір та міжнародну передачу новин, Конвенції про міжнародне право спростування), а також 43 резолюції за зазначеною тематикою [4, с. 103].

Подальший розвиток інституту свободи інформації відбувся в інший спосіб – шляхом включення його ключових положень до міжнародно-правових актів з прав людини. Цьому, головним чином, посприяв розвиток міжнародно-правового регулювання захисту прав людини і основоположних свобод. Зокрема, інститут свободи інформації було закріплено у низці міжнародних універсальних і регіональних угод – Всесвітній декларації прав людини 1948 року, Конвенції про захист прав людини і основоположних свобод 1950 року, Міжнародному пакті про громадянські і політичні права 1966 року, Американській конвенції про права людини 1969 року, Африканській хартії прав людини і народів 1981 року, Конвенції ООН про права дитини 1989 року, Міжнародній конвенції про захист прав всіх трудящих-мігрантів та членів їхніх сімей 1990 року, Арабській хартії прав людини 2004 року, Конвенції ООН про права інвалідів 2006 року.

Зазначимо, що міжнародні угоди дозволили не тільки закріпити, але й значно розширити і доповнити положення інституту свободи інформації.

Включений до цілої низки міжнародно-правових актів з прав людини, інститут свободи інформації отримав розвиток у складі права на свободу переконань і вільне їх виявлення *(“the right to freedom of opinion and expression”* (англ.), *“derecho a la libertad de opinión y de expressión”* (icп.), *“право на свободу убеждений и на свободное выражение их”* (рос.), *“a droit à la liberté d’opinionet d’expression”* (фр.)).

Початок цьому було покладено статтею 19 Всесвітньої декларації прав людини 1948 року, якою було визначено, що “Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватись своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів” [6].

Наступні міжнародно-правові акти, базуючись на запропонованій юридичній конструкції, додали до цього низку уточнюючих положень, в тому числі і термінологічних і, у подальшому, деталізували як зміст самого права, так і визначили місце свободи інформації. Так, враховуючи аналогічну статтю 19 Міжнародного пакту про громадянські і політичні права 1966 року [7], фактично було визначено два складові елементи, а саме:

(1) право дотримуватись переконань (ст. 19 Всесвітньої Декларації) (“дотримуватись поглядів” – в п. 1, п. 2 ст. 19 Пакту 1966 р.) [7], а також

(2) право на вільне вираження свого погляду (п. 2 ст. 19 Пакту 1966 р.) (“виявлення”– в ст. 19 Всесвітньої Декларації).

Право дотримуватись переконань і право вільно їх виражати, на думку Комісії (з 2006 року – Ради) з прав людини ООН, різняться [8, с. 8].

Варто зауважити, що саме право на вільне вираження свого погляду (відповідно до п. 2 ст. 19 Пакту 1966 р.) включає в себе свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї *(“the freedom to seek, receive and impart information and ideas”* (англ.), *“la libertad de bescar, recibir y difundir informationes e ideas”* (icп.),

“свободу искать, получать и распространять всякого рода информацию и идеи” (рос.), *“la liberté de rechercher, de recevoir et de répandre des information et des ideés”* (фр.)), тобто свободу інформації.

Аналіз змісту і обсягу свободи інформації, які характеризують її сучасний стан і розвиток у контексті запропонованої вище юридичної конструкції, на нашу думку, варто здійснити з позицій як самої *природи феномену свободи*, так і з позицій *правового інституту свободи інформації*, а саме – складу свободи інформації, умов, засобів і форм її реалізації, відповідальності та випадків її можливого обмеження.

Природа феномену свободи.

Сучасне розуміння свободи, враховуючи як положення міжнародно-правових актів, так і позицію, викладену в щорічних доповідях Спеціального доповідача ООН з питання про заохочення і захист права на свободу переконань та їх вільне виявлення (1993 – 2015 рр.), базується на низці базових положень. Визначаючи природу феномену “свобода” в сенсі ст. 19 Всесвітньої декларації прав людини 1948 року та ст. 19 Міжнародного пакту про громадянські і політичні права 1966 року, він зазначає: “Суттєвим аспектом права на свободу переконань і їх вільне вираження є двоєдина концепція свободи, що лежить в основі цього права. Ця двоєдина концепція свободи значною мірою визначає ті області, на які поширюється захист цього права. Двома основними елементами концепції свободи є “свобода доступу до держави” і “свобода від держави”.

Перший елемент стосується участі індивідуума у справах держави. В ньому присутній додатковий відтінок “колективності”, із нього випливають права індивідуума на зібрання і на створення своїх організацій.

Другий елемент стосується особистого життя індивідуума і передбачає її всебічну охорону від будь-якого неправомірного зовнішнього втручання. В даному випадку держава в принципі не зобов’язана забезпечувати це право шляхом застосування позитивних заходів. Державні органи зобов’язані втрутитись лише у тих випадках, коли вільне вираження переконань безпосередньо зачіпає права інших індивідуумів або представляє собою пряму загрозу для суспільства” (п. 19) [8].

Таке твердження має сенс і підтверджується тим, що на сьогодні склалось дві концепції свободи, які визначають як ліберальну і соціалістичну. В основі такої спорідненості концепцій лежать гуманістичні погляди філософів XIX сторіччя.

Спеціальний доповідач ООН в якості аргументу на користь такого підходу наводить думку Джона Стюарта Мілля з його “Есе про свободу” (1859 рік), в якій автор, розглядаючи сферу свободи людини, зауважив: “По-перше, вона охоплює внутрішню область свідомості, що обумовлює необхідність свободи совісті в найбільш широкому сенсі слова, свободу думки і відчуттів, абсолютної свободи переконань і переконань з будь-яких питань, включаючи практичні, теоретичні і наукові питання, а також питання моральності та богослов’я. Свобода переконань і публікацій своїх думок може, на переконання, підпасти під дію і цього принципу, оскільки вона відноситься до тієї області поведінки індивідуума, яка стосується інших людей; проте, оскільки вона має майже таке ж важливе значення, як свобода думки, і ґрунтується на тому ж фундаменті, вона практично складає з нею єдине ціле.

По-друге, даний принцип припускає свободу смаків і спрямувань, свободу будувати своє життя з врахуванням свого характеру, свободу чинити на свій розсуд, нести відповідальність за наслідки своїх вчинків, не зазнаючи при цьому жодних ускладнень з боку інших людей до тих пір, поки наші вчинки не заподіюють їм

шкоди, навіть якщо вони вважають нашу поведінку безглуздою, спотвореною або неправильною.

По-третє, з цієї свободи кожного індивідууму, в межах тих самих обмежень, випливає свобода спільного існування індивідуумів, свобода об'єднуватись з будь-якою метою, не заподіюючи шкоди іншим, за умов, що особи, що об'єднуються, є повнолітніми і ніхто їх не примушує і не вводить в оману" (п. 20) [8].

Такий погляд на свободу переважно пов'язується з ліберальною концепцією.

В той же час соціалістична концепція передбачає розглядати свободу як певний припис, вказівку або "директиву, що прописує свободу, спрямовану не стільки на попередження втручання держави в особисте життя індивідуума, скільки на його соціальну інтеграцію у суспільне життя" (п. 21) [8].

Разом з тим, незважаючи на той факт, що концепції свободи були предметом маніпуляцій і використовувались для досягнення політичних цілей, "обидві концепції свободи, якщо розглядати їх позитивні сторони, сприяли розумінню того, що для захисту і заохочення прав людини держава повинна і, з точки зору права, зобов'язана вживати заходів або утримуватись від їх вживання у тих випадках, коли цього потребують інтереси захисту прав людини, або в цілях захисту індивідуумів від неправомірного втручання держави або третіх сторін, або в цілях забезпечення їх ефективної участі в соціальному, культурному, цивільному, економічному і політичному житті суспільства. Таке розуміння стало результатом поєднання ліберальних і соціалістичних ідей в тих областях, де вони зачіпали питання прав людини" (п. 23) [8].

Зазначений підхід до розуміння феномену свободи надає можливість уявити як її природу, так і визначити притаманні їй властивості і межі. Це є суттєвим для розуміння свобод людини, в тому числі і свободи інформації, що є предметом розгляду.

Правовий інститут свободи інформації.

Запропонована свого часу ООН юридична конструкція інституту свободи інформації, що врахувала попередні філософські підходи і визначила базові концептуальні основи її розвитку, була значно розширена і доповнена низкою положень міжнародно-правових актів щодо умов, засобів і форм її реалізації, відповідальності і випадків її можливого обмеження. Проте, склад інституту свободи інформації – свобода шукати, одержувати і поширювати інформацію – протягом тривалого часу залишається незмінним.

Ключовим у цьому питанні є положення про те, що свобода інформації передбачає можливість використовувати у відносинах будь-яку інформацію та ідеї (ст. 19) [7], (п. 31) [8].

Для реалізації цього положення міжнародно-правовими актами передбачено поширення дії свободи на три окремі види інформаційної діяльності. Зокрема йдеться про свободу ведення діяльності з пошуку, одержання і поширення інформації. Підкреслимо той факт, що з усіх можливих видів інформаційної діяльності, міжнародно-правовими актами з прав людини визначено тільки ці зазначені три види.

Свобода використання зазначених видів інформаційної діяльності, а саме – пошуку, одержання і поширення інформації, надає можливість в повному обсязі реалізовувати право на вільне вираження свого погляду (п. 2 ст. 19 Пакту 1966 р.) [7]. При цьому здатність особи в повному обсязі реалізовувати свободу інформації є можливою тільки за умов сукупного використання цих видів інформаційної діяльності.

Варто звернути увагу на те, що міжнародно-правовими актами визначаються види інформаційної діяльності на які поширюється свобода, але не визначаються умови і

способи її реалізації щодо кожного з цих видів. У той же час, ці види інформаційної діяльності – пошук, одержання і поширення інформації, мають відмінності, різну спрямованість і правову природу, що є предметом окремого дослідження.

Сьогодні ці види інформаційної діяльності – пошук, одержання і поширення інформації – продовжують відігравати важливу роль у реалізації права на вільне вираження свого погляду в новітніх умовах широкомасштабного використання інформаційно-комунікаційних технологій та, окрім того, сприяють формуванню нових поглядів, підходів і концепцій. І, якщо свобода поширення інформації пов'язується в умовах глобального інформаційного суспільства із подальшим розвитком таких категорій, як "свобода слова" (додаток. до Пакту 1966 р.), "свобода преси" (п. 13) [9], а також "правом на вільне вираження свого погляду" (ст. 19 Пакту 1966 р.), то свобода шукати та свобода одержувати інформацію пов'язуються із становленням і розвитком в міжнародному праві нової концепції – концепції права на інформацію (п. 36) [10].

Разом із питаннями щодо складу, інститут свободи інформації характеризують і інші елементи, зокрема умови, засоби і форми реалізації, відповідальності і випадки можливого обмеження.

Умови реалізації свободи інформації передбачають передумови та обставини, що обумовлюють її дотримання. За загальними умовами реалізація свободи інформації (свободи шукати, одержувати і поширювати інформацію), відповідно до положень міжнародно-правових актів, повинна відбуватись незалежно від державних кордонів (ст. 19) [7].

Це означає, що:

- свобода шукати інформацію надає можливість особі самостійно і без обмежень вести пошук інформації не тільки на території держави, але й за її межами;
- свобода одержувати інформацію надає можливість самостійно і без обмежень отримувати інформацію від будь-яких національних та іноземних фізичних і юридичних осіб та держав;
- свобода поширювати інформацію надає можливість самостійно і без обмежень поширювати інформацію на території держави та за її межами.

Передбачається, що умови реалізації свободи інформації не повинні залежати від засобів і форм її реалізації.

Засоби реалізації свободи інформації визначають сукупність способів для її здійснення. Загалом, міжнародне право не обмежує особу у використанні засобів реалізації свободи інформації для пошуку, одержання і поширення інформації (ст. 19) [6]. В якості таких виступають друковані видання, мовні (радіо і телевізійні) і цифрові засоби інформації. Зрозуміло, що із подальшим розвитком і вдосконаленням інформаційно-комунікаційних технологій, такі умови щодо засобів будуть тільки сприяти розвитку свободи інформації.

Форми реалізації свободи інформації визначають різновиди і способи прийомів для її реалізації. Універсальні міжнародно-правові акти надають широкий перелік форм реалізації свободи інформації. Зокрема, передбачається, що свобода шукати, одержувати і поширювати інформацію може реалізовуватись в усній, письмовій чи друкованій формі, у формі творів мистецтва (художніх формах вираження) чи за допомогою інших засобів на свій вибір (ст. 19) [7], (ст. 13) [11], (ст. 13) [12].

Розширений перелік форм реалізації свободи інформації в міжнародному праві передбачено для окремої групи осіб – інвалідів. Зокрема, "на власний вибір всіма

формами спілкування (що включає використання мов, текстів, абетки Брайля, тактильного спілкування, великого шрифту, доступних мультимедійних засобів, так само як і друкованих матеріалів, аудіо засобів, звичайної мови, декламаторів, а також посилюючих і альтернативних методів, способів і форматів спілкування, включаючи доступну інформаційно-комунікаційну технологію" (ст. 2) [13], що включає "a) забезпечення інвалідів інформацією, призначеної для широкої публіки, в доступних форматах і з використанням технологій, що враховують різні форми інвалідності, своєчасно і без додаткової платні; b) прийняття і сприяння використанню в офіційних зносинах: жестових мов, абетки Брайля, посилюючих і альтернативних способів спілкування і усіх інших доступних способів, методів і форматів спілкування за вибором інвалідів; c) активне спонукання приватних підприємств, що надають послуги широкій публіці, в тому числі через Інтернет, до надання інформації і послуг в доступних та придатних для інвалідів форматах; d) спонукання засобів масової інформації, в тому числі таких, що надають інформацію через Інтернет, до перетворення своїх послуг в доступні для інвалідів; e) визнання та заохочення використання жестових мов" (ст. 21) [13].

Зазначені форми реалізації свободи інформації відображають сучасний стан і рівень розвитку міжнародно-правового регулювання з цього питання.

Користування свободою інформації (свободою шукати, одержувати і поширювати інформацію) накладає на особу певні обов'язки та особливу відповідальність.

Це положення ґрунтується на нормі щодо встановлення особливих обов'язків та особливої відповідальності за реалізацію права на вільне виявлення своїх переконань (п. 3 ст. 19 Пакту 1966 р.) [7]. Враховуючи, що інститут свободи інформації включено до складу права на вільне виявлення своїх переконань (п. 2 ст. 19 Пакту 1966) [7], на нього, відповідно, поширюються ці зазначені положення щодо обов'язків і відповідальності (п. 2 ст. 19 Пакту 1966 р.) [7], (п. 3 ст. 13 МК-1990) [12].

Варто зауважити, що будучи результатом компромісу, ця норма розглядається в якості такої, що на відміну від більшості інших норм Пакту 1966 р., накладає особливі обов'язки та особливу відповідальність саме за користування правом (п. 37) [8].

Реалізація свободи інформації пов'язана і з певними обмеженнями. Характеризуючи необхідність і доцільність їх застосування до свободи інформації, варто звернути увагу на кілька наступних положень.

Важливим, при визначені необхідності введення того чи іншого обмеження, є принцип пропорційності (п. 44) [8]. Принциповим є те, що "правилом у цьому відношенні повинен бути захист свободи, а виключенням – обмеження такої свободи" (п. 44) [8]. При цьому "обмеження не повинно ставити під загрозу саме право, а співвідношення між правом і обмеженням, а також між нормою і виключенням не повинно бути змінено у зворотну сторону" (п.17) [14].

Свобода інформації повинна обмежуватись в тій мірі, яка необхідна для досягнення однієї з визначених міжнародно-правовими актами цілей. Обмеження не повинно зводитись лише до заборони з будь-якого конкретного питання.

Кожне з обмежень, сукупність яких визначена міжнародно-правовими актами повинно відповідати визначеним умовам, а саме повинно:

- бути встановлено законом,
- слугувати одній з перерахованих цілей і
- бути необхідним для досягнення такої цілі (п. 41) [8], (п. 15) [14].

Беззастережною є вимога у міжнародно-правових актах про те, що будь-які обмеження повинні бути офіційно закріплені в (національному) законі [7; 11; 12].

І “такий закон повинен містити конкретну вказівку на можливість втручання з боку правоохоронних органів. Важливе значення має характер нормативного акту. Будь-яке втручання, на підставі лише адміністративних положень, *prima facie* є порушенням статті 19 (Пакту)” (п. 42) [8].

Будь-яке з обмежень свободи інформації, крім того, що повинно бути визначено законом, також повинно слугувати і бути спрямовано для досягнення наступних цілей:

- для поваги прав та репутації інших осіб;
- для охорони державної безпеки;
- для охорони суспільного порядку;
- для охорони здоров’я населення;
- для охорони моральності населення [7; 11; 12].

Зазначимо, що цей перелік стосовно трудящих-мігрантів та членів їх сімей доповнено кількома пунктами, що визначають додаткові умови і є необхідними [12]:

- для цілей попередження будь-якої пропаганди війни;
- для цілей попередження будь-якого виступу на користь національної, расової або релігійної ненависті, що представляє собою підбурювання до дискримінації, ворожнечі або насиллю.

За сучасних умов масштабного розвитку інформаційно-комунікаційних технологій спостерігається тенденція до можливого розширення кола випадків щодо обмеження свободи інформації на універсальному рівні. На сьогодні, актуальними постають питання щодо свободи шукати, одержувати і поширювати будь-яку інформацію у відношенні Інтернету в контексті права на вільне вираження свого погляду. Запропоновано проводити різницю між вираженням поглядів які, зокрема, [14]:

(а) є порушенням міжнародного права, можуть бути кримінально караними та належатимуть забороні (дитяча порнографія; пряме і публічне підбурювання до скоєння геноциду; виступи на користь національної, расової та релігійної ненависті (підбурювання до дискримінації, ворожнечі або насилля); підбурювання до тероризму), (додамо, що низка з них є вже забороненими міжнародним правом);

(б) не є кримінально караними, проте можуть бути підставами для обмежень та цивільних позовів та

(в) не є кримінально караними, проте викликають занепокоєння з приводу терпимості, моралі і поваги по відношенню до інших.

Отже, такими на сьогодні виступають новітні положення концепції свободи інформації, що ґрунтуються на більш ніж сімдесятирічному міжнародному досвіді розвитку свободи шукати, одержувати і поширювати інформацію.

Варто додати, що тематика, пов’язана з подальшим майбутнім розвитком концептуальних основ свободи інформації, виявилось актуальною і стала одним з ключових тем для дослідження Комісії (з 2006 р. – Ради) з прав людини ООН. Призначення і надання повноважень Спеціальному доповідачу з питання про заохочення і захист права на свободу переконань та їх вільне виявлення (1993 – 2015 рр.) сприяє розвитку концепції свободи інформації.

Важливе значення для її доктринального розвитку мають щорічні доповіді спеціальних доповідачів міжнародних організацій, а також їх щорічні спільні декларації, що разом приймаються Спеціальним доповідачем ООН з питання про заохочення і захист права на свободу переконань та їх вільне виявлення, Представником Організації з безпеки і співробітництва у Європі (ОБСЄ) з питання свободи засобів масової інформації, Спеціальним доповідачем Організації американських держав (ОАД) з питань свободи вираження поглядів та Спеціальним доповідачем Африканської комісії з

прав людини і народів (АКПЛН) з питань свободи вираження поглядів і доступу до інформації (1999 – 2014 рр.).

Сьогодні значну роль у дотриманні положень щодо свободи шукати, одержувати і поширювати інформацію продовжують відігравати міжнародні судові інституції, зокрема Європейський Суд з прав людини, Міжамериканський Суд з прав людини, Африканський Суд з прав людини.

Вартими уваги для розвитку концепції свободи інформації є і пропозиції міжнародних неурядових організацій. Вагомим є внесок міжнародної неурядової організації "Article 19" (Стаття 19), що запропонувала комплекс принципів під назвою "Право суспільства знати: принципи законодавства про свободу інформації" [2].

Висновки.

Розглянувши питання, пов'язані із основними положеннями концепції свободи інформації в міжнародному праві, варто зазначити наступне:

- розвиток сучасної концепції інституту свободи інформації відбувається протягом останніх сімдесятьох років;
- загальні концептуальні положення були сформульовані в рамках ООН і полягають у визначенні свободи інформації, її основного принципу, ролі інституту, значенні інституту в розвитку сучасних міжнародних відносин;
- розвиток інституту свободи інформації відбувається в рамках міжнародно-правового регулювання захисту прав людини і основоположних свобод;
- інститут свободи інформації характеризується з позицій складу свободи інформації, умов, засобів і форм її реалізації, відповідальності та випадків її можливого обмеження.
- важливим аспектом для розвитку свободи інформації виступає зміст інформації;
- на стан міжнародно-правового регулювання інституту свободи інформації впливатиме розвиток інформаційно-комунікаційних технологій і зміст поширюваної інформації.

Використана література

1. Колосов Ю.М. Массовая информация и международное право. Москва: "Международные отношения", 1974. 168 с.

2. Мендел Т. Свобода информации: сравнительно-правовое исследование. 2-е изд., доп. Париж, ЮНЕСКО, 2008. 176 с.

3. Созыв международной конференции по вопросу о свободе информации: Резолюция Генеральной Асамблеи ООН 59 (I) от 14 декабря 1946 г. URL: //www.daccess-dds-ny.un.org/doc/ RESOLUTION/GEN/NR0/033/ 10/IMG/NR003310.pdf?OpenElement

4. Ермишина Е.В. Международный обмен информацией: правовые аспекты. Москва: "Международные отношения", 1988. 144 с.

5. Днепровский А.Г. Правовые проблемы нового международного информационного порядка. Москва: "Наука", 1989. 142 с.

6. Всемирная декларация прав человека 1948 г. URL: //www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/045/84/IMG/NR004584.pdf?OpenElement

7. Международный пакт о гражданських и политических правах 1966 г. URL: //www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NL6/600/01/IMG/NL660001. pdf?OpenElement

8. Поощрение и защита права на свободу убеждений и их свободное выражение : доклад Специального докладчика г-на Абида Хуссейна, подготовленный в соответствии с Резолюцией 1993/45 Комиссии по правам человека. 19 декабря 1994 г. E/CN.4/1995/32. URL: //www.daccess-ods.un.org/TMP/7821679.71134186.html

9. Гражданские и политические права, включая вопрос свободы выражения мнений: доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное их выражение г-на Абида Хуссейна. 29 января 1999 г. E/CN.4/1999/64. URL: //www.daccess-ods.un.org/TMP /980569.4222450 26.html

10. Право на свободу мнений и их свободное выражение : доклад Специального докладчика г-на Амбейи Лигабо, представленный в соответствии с Резолюцией 2003/42 Комиссии. 12 декабря 2003 г. E/CN.4/2004/62. URL: //www.ap. ohchr.org/documents/dpage_e.aspx?m=85

11. О правах ребенка: Конвенция ООН 1989 г. URL: //www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/552/66/IMG/NR055266.pdf?OpenElement

12. О защите прав трудящихся-эмигрантов и членов их семей: Международная конвенция 1990 г. URL: //www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/570/63/IMG/NR057063.pdf?OpenElement

13. О правах инвалидов: Международная конвенция 2006 г. URL: //www.daccess-dds-ny.un.org/doc/UNDOC/GEN/N06/500/81/PDF/N0650081.pdf?OpenElement

14. Право на свободу мнений и их свободное выражение: доклад Специального докладчика г-на Амбейи Лигабо, представленный в соответствии с Резолюцией 16/4 Совета по правам человека. 11 августа 2011 г. A/66/290. URL: //www.daccess-ods.un.org/TMP/4055686.59305573.html

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

УДК 004.89:347.78

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

ТЕКСТИ, МУЗИКА, ЗОБРАЖЕННЯ, ЩО СТВОРЮЮТЬСЯ ШТУЧНИМ ІНТЕЛЕКТОМ: ДО ВИЗНАЧЕННЯ МОДЕЛІ ПРАВОВОЇ ОХОРОНИ

Анотація. *Розглядаються підходи до охорони прав на об'єкти, що створюються штучним інтелектом, авторським правом, суміжними правами, правом sui generis, правом на інформацію.*

Ключові слова*: штучний інтелект, авторське право, суміжні права.*

Summary. *Approaches to the protection of rights to objects, created by artificial intelligence by copyright, related rights, sui generis right and rights on information are considered.*

Keywords*: artificial intelligence, copyright, related rights, information law.*

Аннотация. *Рассматриваются подходы к охране прав на тексты, музыку, изображения, которые создаются искусственным интеллектом, авторским правом, смежными правами, правом sui generis, правом на информацию.*

Ключевые слова*: искусственный интеллект, авторское право, смежные права.*

Постановка проблеми. Розвиток застосування систем штучного інтелекту (далі – AI) є знаковою подією XX1 століття. Системи штучного інтелекту використовуються в автоматизованій журналістиці, підготовці фінансових оглядів, аналізів ринку, при створенні музичних, літературних, образотворчих творів, фільмів, ігор, а також в деяких випадках генерують без безпосередньої участі фізичної особи тексти, зображення, музику та інші об'єкти.

Характерною для 2015 – 2021 рр. є активна дискусія фахівців щодо можливості охорони об'єктів створених штучним інтелектом, авторським правом або іншими правовими інститутами.

З врахуванням робіт з оновлення Цивільного кодексу України в рамках рекодифікації цивільного законодавства, а також наближення законодавства України до законодавства ЄС, актуальним є подальше дослідження правового режиму об'єктів, що створюються за допомогою або безпосередньо системами AI, з оцінкою можливостей охорони прав на такі об'єкти в рамках наявних правових інститутів або через введення спеціального режиму охорони.

Результати аналізу наукових публікацій. Проблематика застосування авторського права щодо об'єктів, створених за допомогою AI, розглядалася De Cock M., Ginsburg J., Guadamuz A., Hetmank S.; Lauber-Rönsberg A., Michaux B.; Perry M, Margoni T., Ramalho A., Yanisky-Ravid S., Pearlman R., Schönberger D. та ін.

На замовлення Європейської комісії, у 2019 р. підготовлено огляд "Інтелектуальна власність та штучний інтелект" [1], а також у 2020 р. звіт "Тенденції та розвиток штучного інтелекту. Виклики врегулюванню прав інтелектуальної власності" [2].

Офісом з патентів та торговельних марок США у 2019 р. було проведено публічні консультації щодо охорони правами інтелектуальної власності інновацій штучного інтелекту та у 2020 р. оприлюднено результати "Публічна думка щодо штучного інтелекту та політики з інтелектуальної власності" [3].

Також, у 2020 р. Офісом інтелектуальної власності Великої Британії ініційовані публічні консультації "Штучний інтелект та інтелектуальна власність" [4].

AIPPI у 2019 р. було проведено дослідження практики різних країн та прийнято резолюцію "Авторське право стосовно творів, створених штучно" [5].

ВОІВ в рамках обговорень питань інтелектуальної власності та AI підготовлено переглянутий концептуальний документ з питань політики у сфері інтелектуальної власності та AI [6].

В Україні проблематика правового режиму об'єктів, створених за допомогою AI, розглядалася Андрощуком Г., Дубняк М., Міліциною К., Ситницькою А., Тимошенко Є. Уткіною М. та ін.

У зазначених публікаціях ставляться питання: чи є можливим застосування охорони прав на об'єкти, які створюються за допомогою або безпосередньо системами AI, авторським правом; які інші правові інститути можуть бути застосовані; чи мають такі об'єкти бути у загальному доступі.

Наукова дискусія та результати консультацій свідчать про істотні концептуальні відмінності пропозицій, а також відсутність на цей час прийнятої на національному рівні як в ЄС, так і в США концепції правової охорони таких об'єктів.

Метою статті є розгляд підходів з охорони прав на тексти, зображення, музику, що створюються за допомогою або безпосередньо системами AI, а також визначення доцільності внесення змін до законодавства з метою врегулювання суспільних відносин щодо їх використання.

Виклад основного матеріалу. Основні вихідні положення авторів наукових публікацій та респондентів публічних консультацій становлять:

(1) оцінка неможливості в рамках діючого *acquis* з авторського права ЄС, законодавства США застосовувати інститут авторського права стосовно об'єктів, створених безпосередньо AI, у зв'язку з відсутністю в ЄС для таких об'єктів дотримання вимоги оригінальності; в США охорона авторським правом надається лише для творів, створених людиною [2; 3];

(2) відсутність можливості наділяти AI правом авторства. Національні закони держав-членів ЄС, США передбачають, що немайнове право авторства належить фізичній особі. Водночас, певні національні режими не передбачають немайнові права для комп'ютерних програм, дизайну шрифтів, службових творів тощо (ст. 79 CDPA, Велика Британія тощо). Також, зазначимо, що Бернська конвенція зазначає можливість застосування охорони, що надається конвенцією, лише для авторів (які є або не є громадянами країн Союзу), тобто для фізичних осіб (ст. 3). Вказане свідчить про неможливість застосування положень конвенції для результатів діяльності AI, де неможливо визначити фізичну особу як автора;

(3) пропозиції, що твори, створені AI, мають набувати охорону авторським правом лише за умови участі людини у створенні твору та за умови дотримання інших умов захисту [5];

(4) слід розділяти випадки створення об'єктів авторського права і суміжних прав, де AI використовується як інструмент, та коли об'єкти створюються AI без участі людини.

Автори звіту "Тенденції та розвиток штучного інтелекту" вказують на судову практику в ЄС (*Painer,* 2011 [7]), що стосується визначення, що об'єкт авторського права має бути інтелектуальним творінням автора, яке відображає його особистість та виражає його "вільний та творчий вибір". При створенні об'єктів за допомогою AI ними виділяються три фази: концепції, виконання (генерування версій) та фіналізації

(редагування, вибір остаточної версії). За думкою авторів звіту, роль творчого внеску фізичної особи є істотним на стадії концепції та, в багатьох випадках, під час фіналізації. З врахуванням творчого вибору, що здійснює особа, та якщо такий вибір втілено в об'єкті, кінцевий об'єкт слід кваліфікувати як об'єкт авторського права. Проте, якщо AI запрограмований автоматично створювати контент без участі у процесі фіналізації особи, що здійснює творчий вибір, в цьому випадку, на думку авторів звіту, авторське право на такі об'єкти не має розповсюджуватися.

У зв'язку з цим зазначається, що авторство при створенні об'єктів за допомогою AI має належати особі (особам), яка зробила творчий внесок у результат (користувач системи AI або розробник системи, або зазначені особи спільно). Як проблема визначається, що особи можуть фальшиво заявляти про авторство стосовно об'єктів, які не мають кваліфікуватися як твори, у зв'язку з відсутністю творчого внеску фізичної особи.

В США, якщо твір створено фізичною особою з використанням машини, права на твір будуть охоронятися авторським правом, якщо виконано інші умови, зокрема, що стосується демонстрації фізичною особою творчості під час такого використання [8]. Для набуття охорони авторським правом, у творі має бути відображено творче вираження фізичної особи (*creative expression*) [3];

(5) зазначається можливість кризи авторського права, оскільки в деяких випадках результати, створені за допомогою AI, можуть бути більш привабливими для використання, ніж твори, створені фізичними особами, а також користуватися більшим комерційним попитом [9].

(6) за результатами консультацій USPTO, відсутня єдина думка стосовно можливості припинення порушень авторського права, що заподіяно твором створеним за допомогою AI. Разом з наявністю у законодавстві США щодо авторського права (Title 17, United States Code) відповідальності за порушення авторського права, одні фахівці вважають, що така відповідальність може наставати, якщо власник має право та здатність контролювати діяльність AI. Інші вважають, що через те, що загально-правова доктрина щодо творів, створених за допомогою штучного інтелекту, є незрозумілою та суди мають розглядати нові питання стосовно контролю та передбачуваності дій пристрою. Оскільки AI стає дедалі більш автономним, можуть бути необхідні зміни до законодавства.

На можливість порушення авторського права внаслідок діяльності AI звертається увага також у документі GBIPO. Зазначається, що як і людина, AI може створювати та розповсюджувати копії пісень. Якщо авторське право порушується, відповідальною, за думкою авторів документу, має бути людина, яка контролює порушення. Якщо порушення відбувається під час "навчання" AI, тоді відповідальною особою буде особа, яка "навчає" AI. Якщо AI створює твір, який порушує авторське право, то відповідальною особою буде той, хто вчинив необхідні заходи, які змусили AI порушити авторське право. Це, швидше за все, буде користувач AI [4].

Відзначимо, що на цей час у законодавстві як Великої Британії так і інших країн відсутні особливості визначення суб'єктів, що мають нести відповідальність у зазначеному випадку;

(7) важливим питанням, з нашої точки зору, є визначена у документі GBIPO потреба внесення змін до законодавства для простішого отримання особами, яким належить авторське право, право *sui generis* стосовно баз даних, винагороди за використання їх творів та даних для "тренування" систем AI та створенням AI відповідних об'єктів. Пропозиції включають або обмеження існуючих винятків для

використання, або введення нових прав стосовно використання вхідних даних та заходи з полегшення ліцензування [4].

Переважна кількість авторів та респондентів вважають, що використання AI фізичною особою в якості інструменту, якщо наявним є творчий внесок фізичної особи в отримання результату, не має призводити до проблем визначення автора або сторони, яка набуває майнові авторські права.

Проте, на наш погляд, не є достатньо дослідженими конкретні випадки використання AI. Так, відомим випадком використання AI є створення портрету Едмон де Беламі та його продаж на аукціоні Christie's 25.11.2018 р. за 432,5 тис. дол. Портрет було створено французькою арт-групою Obvious з використанням технології Generative Adversarial Network (GAN). Технологія полягає в використанні двох нейронних мереж, що навчаються, використовуючи копії створених художниками картин. До системи було введено зображення 15 000 портретів, написаних у період з XIV по XX століття. Генератор створює нове зображення з заданого набору зображень та дискримінатор намагається виявити різницю між рукотворним зображенням та зображенням, створеним генератором на основі набору зображень. Якщо при порівнянні відповідь на запитання, чи створено портрет людиною, є негативною, варіант системою відхиляється.

Зазначається художня цінність портрета. Вказується, що такий стиль живопису може становити новий напрям, як, наприклад, Чорний квадрат Малевича. Також зазначається, що портрет відходить від традиційного уявлення про портрет XVIII століття. Та в ньому є щось сучасне [10].

Особливістю наведеного прикладу є те, що людиною було створено алгоритм відбору згенерованих зображень, що відповідає певним вимогам (їх має бути неможливим відрізнити від зображення, створеного людиною). Також було задано тематику відбору зображення. Проте, з урахуванням наведених вище критеріїв оригінальності принципові рішення щодо відбору (фіналізації) вирішувала не людина, а алгоритм. В цьому сенсі вклад людини у появу конкретного предмету живопису є дуже опосередкованим та не впливає на вибір конкретного кінцевого результату.

В той же час, як вказує A. Elgammal, керівник лабораторії мистецтва та штучного інтелекту при Університеті Рутгерса в Нью-Джерсі, різниця у сприйнятті людиною живопису, створеного людиною, та результатів, отриманих за допомогою системи GAN, є невеликою, а в деяких людей мистецтво, створене машиною, навіть надихає більше. Зазначимо, що поруч з оприлюдненим зображенням портрету вказується: Image © Obvious.

Наведений приклад очевидно свідчить, що можлива поява об’єктів, в отримання яких вкладено значні кошти та зусилля. Вони можуть мати художню та значну комерційну цінність та, у зв’язку з цим (як і у випадку захисту від використання нетворчого змісту баз даних правом *sui generis*), потребують захисту від несанкціонованого використання з метою окупити інвестиції. В той же час, для таких об’єктів критерій оригінальності, визначений у справі Суду ЄС Case C-145/10, Painer, може бути неочевидним або відсутнім. Таким чином питанням є винайдення адекватної форми правової охорони таких об’єктів.

Пропозиції щодо правової охорони об’єктів, створених за допомогою AI, у наукових публікаціях, документах Єврокомісії, USPTO, GBIPO, AIPPI узагальнено у наступних варіантах.

Підхід 1. Охорона суміжними правами для окремих об’єктів. Оскільки щодо суміжних прав, за думкою Hartmann C. та ін., відсутнє визначення немайнових прав фізичних осіб-творців фонограм, відеограм, а також вимога оригінальності, то права

виробників фонограм можуть застосовуватися для надання охорони звуковим сигналам (аудіо даним); права виробників перших записів фільмів – для аудіовізуальних об'єктів; права організацій мовлення – відносно записів передач, які створюються за допомогою AI. Без правової охорони, на думку авторів, залишаються об'єкти, створені AI, у літерно-цифровій формі, тобто тексти [2, с. 7-9].

Аналогічний підхід наводиться у документі GBIPO, з зазначенням (з врахуванням специфіки законодавства Великої Британії), що для низки об'єктів (звукозаписи, фільми, передачі мовлення) відсутні вимоги щодо оригінальності. Права на такі об'єкти належать продюсерам, виробникам, видавцям, незважаючи на їх творчий внесок. Вказане можливо застосовувати для охорони прав на дотичні результати, отримані AI. У Резолюції 2019 р. AIPPI також визначається можливість застосування суміжних прав, а також авторського права не у значенні Бернської конвенції.

Підхід 2. Охорона авторським правом з особливим правовим режимом об'єктів, створених AI. Відповідно до запропонованих у Великій Британії ще у 1987 р. положень: стаття 9 "Авторство на твір" Закону про авторське право, промислові зразки та патенти [11]. визначається, що: "у випадку літературного, драматичного, музичного чи художнього твору, який створений комп'ютером, автором вважається особа, якою здійснюються заходи, необхідні для створення твору". Ст. 12 визначає що, якщо твір генерується комп'ютером, авторські права втрачають силу в кінці періоду 50 років з кінця календарного року, в якому твір було створено. Також ст. 79, що стосується виключень із моральних прав, визначає, що положення ст. 77 "Право бути визначеним автором або режисером" не стосуються будь-яких творів, що генеруються комп'ютером, також, зокрема, комп'ютерних програм.

Аналогічні положення визначено Законом Ірландії про авторське право і суміжні права, Законом Нової Зеландії про авторське право, Законом Південно-Африканської республіки про авторське право, Законом Індії про авторське право.

За думкою Guadamuz A., положення британського законодавства є найкращим рішенням стосовно результатів, отриманих за допомогою AI – вказаний підхід вносить ясність у невизначену правову сферу. Він використовується у законодавстві низки країн та дозволяє не вирішувати проблему належності авторського права або лише програмісту або користувачу, а виходити з конкретних випадків створення твору. Вказаний підхід застосовується тривалий час без виявлення ускладнень судовою практикою [12].

Підхід 3. Запровадження нового права, розширення меж застосування права sui generis стосовно баз даних. Lauber-Rönsberg, Hetmank S. звертають увагу на потенційну можливість більш широкого тлумачення видів контенту, на який розповсюджується право *sui generis* Директиви 96/9/ЄС про правову охорону баз даних, маючи на увазі, що база даних є збірником самостійних творів, даних або інших матеріалів (ст. 1), а також на рішення Суду ЄС *Esterbauer,* 2015, яким визначено, що "автономна інформативна цінність матеріалу, який було вилучено із збірки, повинна оцінюватися з урахуванням цінності інформації не для звичайного користувача колекції, але для кожної третьої сторони, зацікавленої у вилученому матеріалі". На цій підставі, Суд вважав, що аналогова топографічна карта складає базу даних у значенні ст. 1 (2) Директиви. Виходячи з цього, автори вважають, що збірки навіть коротких звукових послідовностей, створених за допомогою AI, можуть охоронятися правом *sui generis*, як і окремі кадри фільму, а також карти, створені за допомогою AI [9].

Пропозиції щодо застосування для об'єктів, створених за допомогою AI, нового права *sui generis* наводяться Ginsburg J. [13], De Cock M. [14], Lauber-Rönsberg [9] та ін.

Британською групою AIPPI запропоновано що твори, створені за допомогою AI, можуть охоронятися новим суміжним правом, що триває 25 років та яке має сприяти відшкодуванню інвестицій, вкладених у розробку AI [15]. Таке право пропонується застосовувати до творів, які підпадають під існуючі визначення літературного, драматичного, художнього та музичного твору, проте, відсутня можливість застосування авторсько-правової охорони у зв'язку з відсутністю фізичної особи, яка безпосередньо пов'язана з втіленим у творі результатом творчості. Для забезпечення охорони, твори мають відповідати певним кваліфікаційним критеріям.

Для уникнення проблеми копіювання, пропонується особливий тест на оригінальність творів, створених за допомогою AI. Твір, створений комп'ютером, є оригінальним, якщо створення такого ж самого твору фізичною особою потребує власного інтелектуального творіння автора. Щодо набуття нового суміжного права, пропонується два альтернативних підходи, а саме: особа/організація, яка найтісніше пов'язана з результатом "навченого" AI (підхід близькості), або фізична чи юридична особа, якою здійснюються заходи, необхідні для створення твору (інвестиційний підхід).

Підхід 4. Відсутність правової охорони. Результати, створені за допомогою AI, не мають набувати правової охорони та мають використовуватися без обмежень [2; 16 – 18].

Звернемо увагу на певні методологічні питання визначення правового режиму об'єктів, що створюються за допомогою AI.

1. Інвестиції у штучний інтелект мають окупатися. Це може мати місце при продажу систем штучного інтелекту користувачам або розробки власних систем AI для, наприклад, цілей автоматизованої журналістики (застосовується такими медіа-компаніями, як Associated Press, Forbes, The New York Times, Los Angeles Times та ProPublica [19], генерування фінансових звітів, аналізів ринку (Narrative Science); створення саундтреков (AIVA, Flow Machines); зображень (мережі GAN та CAN) тощо.

З врахуванням комерційного попиту на об'єкти, які отримуються людиною за допомогою або безпосередньо AI, безумовно мають бути винайдені рішення, що дозволяють захищати такі об'єкти від недозволеного використання та сприяти, аналогічно моделі *sui generis* для баз даних, патентної охорони винаходів, авторського права, поверненню інвестицій та компенсації витрат на створення таких об'єктів.

З врахуванням наведеного, пропозиції деяких авторів стосовно відсутності необхідності запровадження охорони об'єктів створених за допомогою AI не є, на наш погляд, обгрунтованими.

2. Стосовно підходу, що передбачає виявлення при створенні AI об'єктів творчого внеску людини та, на підставі цього, їх віднесення до об'єктів авторського права, його запровадження, як свідчать окремі приклади, наведені у опублікованих працях, а також судова практика*, може призвести в умовах відсутності альтернативних форм охорони таких об'єктів, до штучного винайдення вкладу людини* у створення об'єкту та до звуження розуміння критерію оригінальності.

Так, наприклад, проблема охорони прав на нетворчі фотографії та відеозаписи (зокрема, застосування фото- або відеокамери, що здійснює зйомку природи або вулиць через певний проміжок часу тощо) у певних країнах вирішується через невіднесення таких фотографій до фотографічних творів та запровадження відносно них спеціального режиму охорони (Іспанія, Італія, Австрія, Данія, Фінляндія) [20].

В той же час, як свідчить рішення Суду інтелектуальної власності Пекіну від 2.04.2020 р. у справі *Gao Yang v. Youku* стосовно фотографічного твору, створеного з використанням AI, поняття творчого внеску людини при здійсненні фотографії було тлумачено судом досить широко. У цьому випадку, позивач прикріпив до повітряної

кулі спортивну камеру яка автоматично фотографувала поверхню Землі. Суд визначив, що, незважаючи на те, що камера знаходилася поза контролем людини – роль людини була у виборі та оцінці таких факторів, як вибір камери та кута зйомки, режимі відеозйомки, форматі відображення відео, чутливості та інших параметрах зйомки та, таким чином, є фотографічним твором.

З врахуванням, що в певних країнах ЄС віднесення аналогічних фотографій до об'єктів авторського права навряд чи можливо – вказане є свідченням можливості довільного тлумачення критерію творчості при створенні твору. Це стосується й рішення у справі *Shenzhen Tencent v. Shanghai Yingxun*, прийнятого 24.12.2019 р. Nanshan District People's Court, Shenzhen, Guangdong Province щодо визнання об'єктом авторського права фінансової статті, згенерованої штучним інтелектом, що була розміщена на веб-сайті Tencent Securities, з зазначенням "Ця стаття була автоматично написана роботом Tencent's Dreamwriter" [21]. Чи було б прийняте аналогічне рішення в ЄС з врахуванням критеріїв оригінальності, що вироблені судовою практикою в ЄС?

3. Стосовно використання інституту суміжних прав, зазначимо, що "суміжні права" є умовним терміном, що не застосовується договорами ВОІВ 1961, 1971, 1996 рр., які врегульовують використання виконань, фонограм та телерадіопередач. Історично, виникнення охорони прав на виконання, фонограми та телерадіопередачі та віднесення цих питань до компетенції ВОІВ було пов'язано з творчим характером створення зазначених об'єктів.

Зникнення у конвенціях ВОІВ, на відміну від Бернської конвенції, людини, яка безпосередньо створює фонограму, передачу організацій мовлення, було пов'язано з інтересами сторін, які ініціювали прийняття конвенцій.

Відсутність критерію оригінальності стосовно фонограм та відеограм у національних законах з авторського права і суміжних прав та передбачення набуття прав безпосередньо виробниками фонограм, виробниками відеограм, на перший погляд, надає змогу використовувати вказаний інститут для певної частки об'єктів (звукозаписи, відеозаписи), створених як безпосередньо, так і за допомогою АІ, без вирішення складних проблем з'ясування оригінальності, як це має місце для об'єктів авторського права. Вказані пропозиції висловлюються певними дослідниками.

Проте, іншою стороною такого підходу є насичення ринку об'єктами, де відсутня можливість відрізнити: чи вони створені людиною або АІ. Також система охорони авторського права і суміжних прав перетворюється з інструменту охорони результатів творчості людини на засіб охорони прав на нетворчі об'єкти, для яких не знайшлося місця в межах діючого правового регулювання.

4. Щодо текстів вбачається можливим конструювання спеціальної системи охорони авторським правом, або суміжним правом, або правом *sui generis*, де не передбачається вимога оригінальності стосовно таких об'єктів та визначення автора, проте, передбачаються інші критерії, якими, зокрема, може бути істотне інвестування у створення АІ або у створенні за допомогою АІ певного об'єкту, або інші критерії. Така система має передбачати, зокрема, критерії, за якими запроваджується охорона прав, визначення сторін, які набувають права, моменту набуття прав, терміну дії прав, винятків з права, можливості існування аналогічних текстів, створених за допомогою АІ, якщо такий текст або схожий текст є єдиним можливим варіантом письмового опису інформації (наприклад, письмовий опис даних графіків фінансових індексів).

Проте знову, беручи до уваги спрямованість міжнародного та національного законодавства з авторського права і суміжних прав на об'єкти творчої діяльності людини, найбільш доцільним було б відокремлення врегулювання використання

об’єктів, створених за допомогою AI, від авторського права і суміжних прав з утворення права *sui generis*.

5. Особливість України та інших країн, які визначають інформацію об’єктом цивільних прав, є можливість застосування права на інформацію для врегулювання відносин щодо об’єктів, створених за допомогою AI. Зауважимо, що в інших країнах, з врахуванням наведеного вище, скоріше аналогом права на інформацію може бути утворення права *sui generis*.

У ЦК України містяться важливі для застосування цього підходу положення част. 2 ст. 200 щодо можливості суб’єкта інформаційних відносин вимагати усунення порушення його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями. Також, оскільки інформація є об’єктом цивільних прав, особи можуть застосовувати способи захисту права на інформацію відповідно до ст. 16 ЦК України.

У ЦК України, Законі України “Про інформацію” може бути визначено особливості застосування права на інформацію для об’єктів, створених за допомогою AI. Вказане може включати: визначення критеріїв, відповідність яким надає змогу застосування особливого режиму охорони прав; підставі набуття майнових прав на інформацію; обсяг прав, термін дії прав, випадки вільного використання тощо. Відносно таких об’єктів не має передбачатися визначення немайнових прав. Вказаний підхід може бути застосовано для нетворчих фотографій, відеозаписів, об’єктів, що створюються AI без участі людини або, якщо участь людини при створенні таких об’єктів не відповідає критеріям для об’єктів авторського права і суміжних прав.

Також доцільним є визначення вимоги щодо зазначення особою, що застосовує особливий режим охорони, відповідного повідомлення або символу, що вказує на дату виникнення охорони та особу, якій належать майнові права на такий об’єкт.

В контексті наведеного вище доцільним, на наш погляд, для України є мати більш активну роль у процесі розпочатих у 2019 р. публічних консультацій ВОІВ щодо AI та політики у сфері інтелектуальної власності [22].

6. Зазначимо, що при загальному відсиланні на початку багатьох публікацій до різних прикладів створення об’єктів за допомогою AI висновки та аргументація здебільшого не спираються на аналіз, наскільки запропоновані у публікаціях конструкції можуть ефективно працювати для конкретних на цей час відомих прикладів створення об’єктів AI. Значна частина пропозицій має теоретичний характер, не апробований на конкретних прикладах діяльності AI.

7. Одним з істотних питань, чи буде визнаватися в інших країнах той чи інший вид національної охорони прав на об’єкти, створені AI без участі людини або, якщо така участь не відповідає критерію оригінальності інших країнах. Звісно, якщо для таких об’єктів буде використано інститут авторського права або для текстів буде запропонована охорона суміжними правами, вказане не має підпадати під дію Бернської конвенції, договору ВОІВ про авторське право та конвенцій ВОІВ стосовно творів, виконань, фонограм і телерадіопередач з врахуванням або відсутності оригінальності або внаслідок того, що такі нові об’єкти суміжних прав не будуть підпадати під дію відповідних міжнародних конвенцій.

Один з напрямків вирішення цього питання – запровадження охорони прав на такі об’єкти, створені в іноземних країнах, з дотриманням принципу взаємності або на підставі двосторонніх або багатосторонніх договорів. Перше, зокрема, було запропоновано ЄС стосовно права *sui generis* щодо баз даних Директивою 96/9/ЄС про правову охорону баз даних.

Висновки.

Аналіз обговорення проблематики визначення правового режиму текстів, музики, зображень, що створюються за допомогою AI, свідчить про знаходження переважно на етапі вивчення проблеми з відсутністю рішень, ефективність яких була б засвідчена практикою. Слід враховувати світовий феномен використання AI та малу вірогідність, що країнами світу буде застосовуватися значна кількість різних моделей охорони прав на такі об'єкти. Актуальність винайдення ефективної форми охорони пов'язана з необхідністю компенсації інвестицій, часу та зусиль, що витрачаються на створення систем AI та/або об'єктів, які створюються AI безпосередньо або за участю людини. Слід зазначити суттєві ризики звуження вимог до оригінальності твору при намаганні відносити в деяких країнах до об'єктів авторського права тексти, зображення, музика, де роль людини не є значною.

На наш погляд, слід підтримати напрям, що передбачає застосування права *sui generis* стосовно текстів, звукозаписів та відеозаписів, що створюються AI, з виключенням вимог щодо оригінальності та ідентифікації автора.

В Україні та інших країнах, де інформацію віднесено до об'єктів цивільних прав, об'єкти, що створюються за допомогою AI, можуть розглядатися, як інформація. З врахуванням тенденцій розвитку систем AI у ЦК України, Законі України "Про інформацію" може бути визначено підстави набуття майнових прав на інформацію, що створюється AI, обсяг прав, термін дії прав, випадки вільного використання тощо.

Використана література

1. Iglesias Portela M., Shamuilia S. and Anderberg A. Intellectual Property and Artificial Intelligence - A literature review. European Commission, 2019, doi:10.2760/2517. 29 p.

2. Trends and Developments in Artificial Intelligence. Challenges to the Intellectual Property Rights Framework. Final report / C. Hartmann, J. E.M. Allan, P. B. Hugenholtz, João P. Quintais, D. Gervais. European Commission. 2020. 175 p.

3. Public Views on Artificial Intelligence and Intellectual Property Policy. USPTO. 2020. 56 p.

4. Artificial intelligence call for views: copyright and related rights. Consultation. Intellectual Property Office. Great Britain. 7.09.2020. URL: https://www.gov.uk (Last accessed: 12.03.2021).

5. Resolution "Copyright in artificially generated works". 2019 AIPPI World Congress. September 18, 2019.

6. Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence. WIPO/IP/AI/2/GE/20/1. May 21, 2020.

7. Judgment of the Court (Third Chamber) of 1 December 2011. Eva-Maria Painer v Standard VerlagsGmbH and Others. Case C-145/10.

8. Burrow-Giles Lithographic Company v. Sarony, 111 U.S. 53 (1884). U.S. Supreme Court.

9. Lauber-Rönsberg, A., Hetmank, S., 'The concept of authorship and inventorship under pressure: Does artificial intelligence shift paradigms?', *Journal of Intellectual Property Law & Practice*, Vol. 14, No 7, 2019. URL: https://doi.org/10.1093/jiplp/jpz061 (Last accessed: 12.03.2021).

10. Is artificial intelligence set to become art's next medium? Christie's. 12.12.2018. URL: https://www.christies.com/features/A-collaboration-between-two-artists-one-human-one-a-machine-9332-1.aspx (Last accessed: 12.03.2021).

11. Great Britain Copyright, Designs and Patents Act, 1988 amended.

12. Guadamuz A. Do androids dream of electric copyright? Comparative analysis of originality in artificial intelligence generated works. *Intellectual Property Quarterly*, 2017 (2). P. 169-186.

13. Ginsburg J. People not machines: authorship and what it means in the Berne Convention, *International Review of Intellectual Property and Competition Law.* Vol. 49. No 2. 2018. P.131-135.

14. De Cock M. Artificial intelligence and the creative industry: new challenges for the EU paradigm for art and technology, in Research Handbook on the Law of Artificial Intelligence, Edward Elgar Publishing, 2018.

15. Great Britain. 2019 Study Question. Copyright in artificially generated works. AIPPI. 2019. 22 p.

16. Perry M., Margoni T. From music tracks to google maps: who owns computer-generated works? *Computer Law & Security Report.* Vol. 26. 2010, Pp. 621-629.

17. Schönberger D. Deep Copyright: Up – And Downstream Questions Related to Artificial Intelligence (AI) and Machine Learning (ML). *Droit d'auteur 4.0/Copyright 4.0, Schulthess Editions Romandes*, 2018. P. 145-173. URL: https://ssrn.com/abstract=3098315 (Last accessed: 12.03.2021).

18. Дубняк М.В. Проблеми визначення правового режиму об'єктів, створених за допомогою технологій нейромереж. *Інформація і право*. № 4(31)/2019. С. 45-53.

19. Andreas G. Guide to Automated Journalism. 7.01.2016. *TOW reports*. URL: https://www.cjr.org/tow_center_reports/guide_to_automated_journalism.php (Last accessed: 12.03.2021).

20. Капіца Ю.М., Ступак С.К., Жувака О.В. Авторське право і суміжні права в Європі. Київ: Логос, 2012. С. 216-221.

21. Zhou Bo Artificial Intelligence and Copyright Protection. *Judicial Practice in Chinese Courts.* WIPO conversations in intellectula property and artificial intelligence. 2020. URL: https://www.wipo.int

22. WIPO Begins Public Consultation Process on Artificial Intelligence and Intellectual Property Policy. PR/2019/843. Geneva. 13.12.2019. URL: https://www.wipo.int (Last accessed: 12.03.2021).

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

УДК 34:316.774-043.2](045)

САМЧИНСЬКА О.А., викладач кафедри інформаційного права та права інтелектуальної власності, КПІ ім. Ігоря Сікорського.
ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент*, КПІ ім. Ігоря Сікорського.

ІНФОРМАЦІЙНЕ НАСИЛЬСТВО, ІНФОРМАЦІЙНА МАНІПУЛЯЦІЯ ТА ПРОПАГАНДА: ПОНЯТТЯ, ОЗНАКИ ТА СПІВВІДНОШЕННЯ

***Анотація**. У статті досліджено поняття "інформаційно-психологічний вплив", "інформаційне насильство", "інформаційні маніпуляції" та "пропаганда", їх основні ознаки та співвідношення.*

***Ключові слова:** інформаційний вплив, психологічний вплив, інформаційно-психологічний вплив, інформаційне насильство, інформаційні маніпуляції, пропаганда.*

***Summary.** The article examines the concepts "information and psychological influence", "information violence", "information manipulation" and "propaganda", their main features and relationships.*

***Keywords:** informational influence, psychological influence, informational and psychological influence, information violence, information manipulations, propaganda.*

***Аннотация.** В статье исследованы понятия "информационно-психологическое воздействие", "информационное насилие", "информационные манипуляции" и "пропаганда", их основные признаки и соотношение.*

***Ключевые слова:** информационное воздействие, психологическое воздействие, информационно-психологическое воздействие, информационное насилие, информационные манипуляции, пропаганда.*

Постановка проблеми. Безпека завжди була, є і буде однією з найголовніших передумов розвитку людини, суспільства, держави та усього міжнародного співтовариства. Недарма видатний психолог Абрахам Маслоу [1] у своїй піраміді потреб, суть якої полягає у розділенні головних людських потреб на так звані рівні, де перехід на вищий рівень можливий лише після задоволення потреби нижчого рівня, визначив безпеку другою, після основних фізіологічних потреб. Суспільство та держава як складні механізми здатні ефективно функціонувати лише за налагодженої взаємодії їх елементів, головним з яких є окремий індивід. В свою чергу, лише людина, яка відчуває себе захищеною, здатна повною мірою здійснювати комунікацію з іншими членами соціуму, створювати сім'ю, працювати, поважати інших, критично та неупереджено сприймати факти, брати участь у політичних, економічних, соціальних, правових та культурних суспільних процесах, а це в свою чергу є запорукою ефективного розвитку сучасної держави.

Саме тому вже досить тривалий проміжок часу одним із найголовніших завдань будь-якої демократичної, спрямованої на розвиток держави є забезпечення безпеки, як держави в цілому, так і її громадян. Поряд із забезпеченням так званої традиційної, фізичної безпеки, сьогодні значна роль віддається інформаційній безпеці.

Варто зазначити, що під безпекою слід розуміти не відсутність загроз, адже в сучасному світі знешкодити усі загрози просто неможливо. Стрімкий науково-технічний прогрес, глобальна інформатизація, розвиток існуючих та створення нових інформаційно-

комунікаційних технологій поряд із численними плюсами має низку мінусів. Так швидке збільшення кількості інформації та її обсягів призвело до інформаційного вибуху, наслідком якого стало інформаційне перевантаження – ідеальне підґрунтя для здійснення інформаційно-психологічного впливу.

Посиливши інформаційний інструментарій, людство майже нічого не зробило для того, щоб підготовити до цього населення. Несміливі слова про медіаграмотність не можуть допомогти вирішити проблему. Створивши небезпеку "полум'я" в інформаційних потоках, людство не потурбувалося про інститут нових інформаційних пожежних того ж рівня, що й можлива небезпека [2].

Безпека – це стан захищеності від загроз, тобто сукупність механізмів преференції, знешкодження, протидії, охорони та захисту від них.

Однією із запорук ефективної діяльності у сфері забезпечення будь-якої безпеки, зокрема інформаційної, є чітке розуміння, що являють собою загрози, їх сутності, поняття та основних ознак.

Гібридна війна, яку веде Російська Федерація проти нашої держави продемонструвала, що однією із найголовніших загроз не лише інформаційній, а й національній безпеці в наш час є інформаційно-психологічний вплив, зокрема такі його прояви як інформаційне насильство, інформаційні маніпуляції та пропаганда.

Результати аналізу наукових публікацій. Інформаційна безпека як й інформаційне право є специфічними галузями права, відмінною рисою яких є "проникнення" та тісний зв'язок не лише практично з усіма галузями права, а й практично з усіма сферами наукових знань. Саме тому низка понять інформаційної безпеки, до яких належить як інформаційно-психологічний вплив в цілому, так окремі його прояви, такі як інформаційне насильство, інформаційні маніпуляції та пропаганда, стало предметом наукових праць не лише вчених в галузі права, а й філософії, соціології, психології, політології, економіки, медицини, інформатики, національної безпеки, і це далеко не вичерпний перелік.

Зокрема вивчення питань сутності, змісту, структури та основних ознак інформаційно-психологічного впливу, інформаційного насильства, інформаційних маніпуляцій та його ролі у сучасному суспільстві здійснювали Г. Почепцов [2], В. Брижко [3], О. Дзьобань, О. Панфілов, С. Соболєва та О. Соснін [4; 5], І. Євченко [6], О. Золотар [7], О. Нємцева [8], Д. Павлов [9], Г. Сащук [10], О. Сищук [11], В. Фурашев [12] та інші вітчизняні та зарубіжні науковці.

Проте, незважаючи на досить велику увагу до даної проблеми з боку наукового товариства, досі не існує єдиного підходу до визначення понять та основних ознак понять "інформаційно-психологічний вплив", "інформаційне насильство", "інформаційна маніпуляція" і "пропаганда" та їх співвідношення між собою, що перешкоджає здійсненню ефективної протидії даним явищам.

Метою статті є з'ясування змісту та основних ознак таких феноменів як "інформаційно-психологічний вплив", "інформаційне насильство", "інформаційні маніпуляції" та "пропаганда" та визначення їх співвідношення.

Виклад основного матеріалу. Першочерговим завданням кожної сучасної демократичної держави, якою відповідно до Конституції являється і Україна, є забезпечення не просто безпеки громадян, а інформаційної безпеки громадян. Відповідно до положень статті 3 та статті 17 Основного закону людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю, а захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями

держави, справою всього Українського народу. Дані положення знайшли відгук в низці нормативно-правових актів, таких як Закон України "Про національну безпеку" від 21.06.18 р. № 2469-VIII, Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.20 р. № 392/2020, Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.17 р. № 47/2017, Стратегія кібербезпеки України, затверджена Указом Президента від 15.03.16 р. № 96/2016.

Однак, незважаючи на нібито розуміння правлячою верхівкою проблем і важливості інформаційної сфери та безпеки в системі національної безпеки та закріплення положень щодо її забезпечення в різних документах загальнодержавного значення, реальний стан речей вказує на недостатній рівень врегулювання даного питання в Україні.

Низький рівень медіаграмотності населення, здатності до критичного мислення, інформаційної культури засобів масової інформації, неврегульованість нових шляхів та методів поширення інформації та низький рівень довіри до традиційних засобів масової інформації стали основними перепонами, які постали на шляху здійснення ефективної політики держави в сфері інформаційної безпеки.

До того, справжнім викликом 2020 року для всієї світової спільноти та України, зокрема, стала коронавірусна інфекція COVID-19. Сучасний стан речей показав, що пандемія сколихнула не лише систему охорони здоров'я, її вплив вже відчутний практично в усіх сферах життя та діяльності людини, суспільства та держави. Не просто не стала винятком, а напевно однією із найбільш "постраждалих" від пандемії стала інформаційна сфера, як в аспекті реалізації основних цифрових прав людини, так і забезпечення інформаційної безпеки суспільства та держави. Підтвердженням тому слугує і пункт 11 Стратегії національної безпеки України, в якому першою сферою, де поширення коронавірусної хвороби (COVID-19) виявило критичні проблеми, вказана саме інформаційна [13].

В період пандемії, під час досі невідомої для людства тотальної ізоляції, як ніколи загострилася проблема захисту громадян від інформаційно-психологічного впливу у вигляді інформаційного насильства, інформаційних маніпуляції та пропаганди. Зміна звичного способу життєдіяльності, велика кількість суперечливої інформації, фейки, неактивна діяльність держави щодо поширення власного наративу та спростування дезінформації, відсутність можливості перевірки інформації так званими "незалежними" експертами – все це стало запорукою виникнення "ідеального" середовища для здійснення управління людьми та досягнення поставлених цілей за допомогою інформаційних та психологічних інструментів.

Одним із основних бар'єрів на шляху врегулювання даної проблеми є відсутність єдиного підходу до визначення понятійно-категорійного апарату таких явищ як інформаційно-психологічний вплив, інформаційне насильство, інформаційні маніпуляції та пропаганди в парадигмі інформаційної безпеки, їх основних ознак та відмінностей. Це в свою чергу унеможливлює законодавче закріплення даних термінів та розроблення ефективних механізмів захисту від них.

Варто зазначити, що у даному випадку мова йде не просто про інформаційно-психологічний вплив, адже сьогодні ті ж самі маніпуляції є елементом будь-якого процесу комунікації у відносинах батьки-діти, дружина-чоловік, між друзями та інших повсякденних соціальних зв'язках, який не завжди здійснюється навмисно, під час якого не використовуються сукупно інформаційні технології та психологічні прийоми, який не має глобальних цілей та зазвичай не завдає шкоди особі, на яку він спрямований. Стаття присвячена дослідженню цілеспрямованого, організованого впливу, який завжди

здійснюється завдяки одночасному використанню інформаційних та психологічних засобів, завжди має чітку ціль та спрямований проти волі та інформаційної свободи об'єкта впливу.

Саме тому, перш за все необхідно дати чітке визначення поняттю "інформаційно-психологічний вплив", який є предметом цієї роботи. Доречно почати з визначення поняття "вплив".

У найбільш широкому розумінні під "впливом" розуміється дія, яку певна особа чи предмет або явище виявляє стосовно іншої особи чи предмета. У традиційній психологічній літературі під цим явищем розуміють цілеспрямоване перенесення руху й інформації від одного учасника взаємодії іншому [14]. Відомі спеціалісти у галузі психології Г.О. Бал і М.С. Бургін під "впливом" розуміють певний процес, який реалізується в ході взаємодії двох і більше рівномірно упорядкованих систем і результатом якого є зміна в структурі (просторово-часових характеристиках), в стані хоча б однієї із цих систем, зміна, перебудова індивідуальних або групових психічних явищ (поглядів, відносин, мотивів, установок, станів тощо) [15].

Підсумувавши вказані визначення, можна зазначити, що в широкому значенні "вплив" являє собою втручання в природній перебіг певних процесів.

Вплив у психології, тобто психологічний вплив визначається як процес і результат зміни індивідуумом поведінки іншої людини, її установок, намірів, уявлень, оцінок і тому подібне в ході взаємодії з нею [16].

О.В. Сидоренко визначає дане поняття як вплив на психічний стан, думки, почуття й дії іншої людини за допомогою винятково психологічних засобів (вербальних, паралінгвістичних або невербальних), з наданням йому права й часу відповідати на цей вплив [17].

В.М. Куліков зазначає, що сутність такого впливу полягає в "проникненні" однієї особистості чи їх групи у психіку іншої особистості (чи групи осіб) [18].

Тобто, психологічний вплив – це цілеспрямований процес, який полягає у "проникненні" у психіку особи (або групи осіб) з метою зміни індивідуальних або групових психічних явищ таких як думок, відносин, поглядів, установок та станів та наслідки такого процесу. Основні ознаки такого процесу: а) цілеспрямованість; б) "проникнення" у психіку особи або групи осіб; в) використання психологічних прийомів; г) мета – зміна психічних явищ, як індивідуальних, так і групових.

Інформаційний вплив визначають як організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість населення (корекція поведінки) та (або) інформаційно-технічну інфраструктуру об'єкта [19].

Схоже, але дещо ширше визначення інформаційного впливу звучить як організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об'єкта впливу та (чи) фізичний стан людини [20].

Отже, основними особливостями інформаційного впливу є: а) організованість; б) цілеспрямованість; в) використання спеціальних інформаційних засобів та технологій; г) мета – внесення змін у свідомість або інформаційно-технічну структуру об'єкта.

Проаналізувавши основні особливості інформаційного та психологічного впливів, спробуємо дати визначення інформаційно-психологічному впливу як комплексному явищу, визначити його сутність, основні ознаки та відмінності від інших видів впливу.

Інформаційно-психологічний вплив – це цілеспрямований, переважно організований процес проникнення у свідомість людини (або групи осіб), який здійснюється за допомогою сукупного використання спеціальних інформаційних засобів та технологій і психологічних прийомів та спрямований на зміну індивідуальних та/або групових психічних явищ та (або) психічний або фізичний стан людини (або групи осіб). Це цілеспрямоване втручання у природний перебіг психічних процесів, основним інструментом якого є – інформація та інформаційні технології, способи поводження з інформацією, а також вербальні, невербальні та паралінгвістичні психологічні засоби.

Інформаційно-психологічний вплив спрямований на індивідуальну або суспільну свідомість, здійснюється інформаційно-психологічними або іншими засобами та викликає трансформацію психіки, зміну поглядів, думок, відносин, ціннісних орієнтацій, мотивів, стереотипів особистості з метою впливу на її діяльність і поведінку. Кінцевою його метою є досягнення певної реакції, поведінки (дії або бездіяльності) особистості, яка відповідає цілям такого впливу [8].

Тобто, основною відмінністю інформаційно-психологічного впливу від психологічного є його організованість та використання поряд із психологічними засобами спеціальних інформаційних засобів та технологій. Від суто інформаційного впливу він відрізняється перш за все засобами – поряд з інформаційними використовуються і психологічні та об'єктом такого впливу, так як інформаційно-психологічний вплив спрямований на свідомість та зміну саме психічних явищ, то його об'єктом може бути виключно особа або ж група осіб. При цьому наслідком такого впливу може бути як зміна свідомості, психічного та фізичного стану як людини та групи осіб, так і як побічний результат такої зміни – зміна інформаційної інфраструктури об'єкта.

Варто зазначити, що інформаційно-психологічний вплив має певні складові такі як суб'єкт впливу (кому це потрібно?), об'єкт впливу (на кого він спрямований?), мета (задля чого?), методи, способи та засоби (яким чином?) та результат такого впливу.

Щодо суб'єкта впливу – це може бути будь-хто, хто володіє достатніми засобами для здійснення такого впливу – держава, група держав, орган, організація (державна, недержавна, міжнародна), конкретна особа, група осіб – цей перелік невичерпний. Адже основною передумовою для здійснення такого впливу є чітке поставлення цілей та наявність інструментів для їх досягнення.

Якщо говорити про об'єкт, то основним об'єктом завжди виступає людина або група осіб, однак варто зазначити і про додаткові, так звані опосередковані об'єкти такого впливу, якими можуть виступати настрій в суспільстві, соціально-психологічні процеси, ставлення до того чи іншого явища, система цінностей та навіть діяльність конкретної держави, органу чи підприємства.

Так як інформаційно-психологічний вплив завжди є цілеспрямований, тобто здійснюється для досягнення конкретної цілі та організований, тобто заздалегідь підготовлений, обов'язковим його компонентом є мета його здійснення.

Варто зазначити, що організованість інформаційно-психологічного впливу не означає складання плану дій, який не змінюється протягом всього часу його здійснення. Так як такий процес може бути досить тривалим, його організованість полягає у складенні плану дій, підбору способів та засобів для перших етапів його здійснення.

Не менш важливим елементом є засоби, методи та способи здійснення інформаційно-психологічного впливу. Тобто, які саме психологічні та інформаційні засоби та технології використовуються

З першого погляду виникає питання для чого так детально розглядати структуру такого впливу. Відповідь досить проста – лише повний розбір складових частин може забезпечити розуміння сутності феномену інформаційно-психологічного впливу, а це є головною умовою побудови не просто стратегії, а ефективної стратегії протидії такому впливу та втілення її у життя.

Встановивши поняття, основні ознаки та структуру інформаційно-психологічного впливу, перейдемо до розгляду таких понять як інформаційне насильство, інформаційні маніпуляції та пропаганда. Розпочнемо з розгляду поняття "інформаційне насильство".

У широкому розумінні під насильством розуміють застосування сили для досягнення чого-небудь; примусовий вплив на когось або щось [21, с. 303].

У більш широкому визначенні насильство – це енергетичний вплив на органи і тканини організму людини, їх фізіологічні функції, шляхом використання матеріальних факторів зовнішнього середовища (механічних, фізичних, хімічних і біологічних) та/або вплив на її психіку шляхом інформаційного впливу, що вчиняється всупереч або поза її волею, здатний заподіяти смерть, фізичну та/або психічну травму, а також обмежити свободу волевиявлення або дій людини [22].

Особливостями такого виду інформаційно-психологічного впливу є те, що він:

а) може бути як явним так і прихованим для об'єкта впливу;

б) завжди здійснюється примусово, тобто проти волі людини та спонукає до дій, які суперечать її інтересам;

в) порушує інформаційну свободу особи (групи осіб);

г) незважаючи на нефізичний характер впливу, здатний заподіяти шкоду життю та здоров'ю людини.

Наступним розглянемо поняття "інформаційна маніпуляція".

Поняття "маніпуляція" походить від латинського терміна *manipulus* та має два значення: а) "пригорща" (*manus* – "рука" та *ple* – "наповнювати") [3, С. 43-49]; б) маленька група, купка (*manus* – "рука" та *pi* – "слабка форма кореня"). У другому значення це слово означало невеликий загін воїнів (близько 120 осіб) у римському війську. У загальному значенні "маніпуляція" розуміється як використання об'єктів із спеціальними намірами, особливою метою, як ручне управління, як рух, що здійснюється руками, ручні дії [23].

Основною особливістю інформаційної маніпуляції, яка відрізняє її від інформаційного насильства, є її завжди прихований та неочевидний характер. Під час такого впливу особа не підозрює про його здійснення та впевнена, що рішення, яке вона приймає, є її власним. Якщо розглядати ці явища в аспекті суспільно-шкідливих наслідків, то інформаційні маніпуляції подібні проступкам, а інформаційне насильство можна співвіднести зі злочинами у кримінальному праві. Маніпуляції спрямовані на виникнення бажання, в результаті чого людина вважає, що вона самостійно прийняла те чи інше рішення. А, отже, хоча такі дії і впливають на її волевиявлення та порушують її свободу, зазвичай не здатні завдати шкоду життю та здоров'ю особи або групи осіб, на яких здійснюється такий вплив.

І останній вид інформаційно-психологічного впливу, який ми розглянемо у даній статті – це пропаганда.

Слово "пропаганда" походить від латинських слів *pro* – "для", "на користь" та *paganus* – "язичник, обиватель, сільський житель, простий, невчений", *propagatio* – "розповсюдження, розширення меж". Отже, етимологічно слово "пропаганда" означає розповсюдження деякої інформації серед простих, невчених людей, язичників [9].

Сьогодні немає єдиного підходу до визначення вказаного явища. Так, відповідно до одного визначення "пропаганда" – це будь-яка систематична спроба впливу на думку чи позицію великої кількості людей, перш за все використовуючи символічні знаки. Це певна форма комунікації, яка спрямована на засвоєння або відкидання певної інформації з метою впливу на організацію, групу, індивіда. Інші ж говорять про пропаганду як про поширення інформації – фактів, аргументів, чуток, напівправди чи брехні – для впливу на публічну думку [24].

Специфічними рисами цього виду інформаційно-психологічного впливу є: а) масовий характер, тобто, пропаганда завжди спрямована не на конкретного індивіда, а на їх групу; б) тривалий характер – пропаганда завжди є тривалим процесом, який складається з певної послідовності дій; в) чітко визначена мета – здійснюється задля формування певного ставлення до того чи іншого явища, події, особи, держави тощо. Тобто, якщо говорити про інформаційні маніпуляції, наприклад, під час передвиборчої кампанії, то її кінцевою метою є отримання голосу виборця за конкретного кандидата, в той час як ціллю пропаганди є не просто отримання голосу, а формування позитивного ставлення та підтримки цього кандидата не лише під час виборів, а взагалі.

Так як процес пропаганди досить тривалий та має зазвичай глобальніші цілі ніж маніпуляції та насильство, він вимагає набагато більшої підготовки та засобів. Саме тому здійснювати такий вплив може собі дозволити далеко не кожен. Яскравим прикладом даного явища слугує російська пропаганда, яка здійснюється з метою створення негативного образу та ставлення населення до України, Сполучених Штатів Америки, Європейського Союзу, НАТО та інших країн та організацій, які на думку правлячої верхівки є головними загрозами та перепонами розвитку Російської Федерації.

Першою особливістю такої діяльності є створення великої кількості інформаційних ресурсів, в тому числі і нібито іноземних, для створення враження різноманітності джерел інформації, що підтримують дану позицію. Періодичний характер діяльності таких засобів. Залучення думки "незалежних експертів" та підтримки відомих "незаінтересованих" осіб зі сфери шоу-бізнесу – це лише невеликий перелік засобів, які використовує російська пропаганда і які, незважаючи на абсурдність поширюваних ідей, досягають зазначеної мети.

З'ясувавши визначення та основні ознаки понять "інформаційного насильства", "інформаційної маніпуляції" та "пропаганди", можна зробити висновок, що і інформаційна маніпуляція і пропаганда, по своїй суті є інформаційним насильством, адже має всі його ознаки, проте є конкретизованим щодо способу, кінцевої мети та об'єкта впливу.

Так як в силу подібності даних явищ досить складно провести чітку межу між ними, розглянемо їх співвідношення на конкретному прикладі.

З початком епідемії, коли коронавірус був поширений переважно на території Китаю та лише починав свою "мандрівку" світом, в засобах масової інформації, онлайн-ресурсах та соціальних мережах почала поширюватися досить значна кількість інформації про хворобу, її походження, симптоми, перебіг, лікування, статистику хворих та померлих. Цим скористалися багато так званих "нетрадиційних" засобів масової інформації, серед яких особливо виділилися так звані телеграм-канали та пабліки в інстаграм, які перейменовувалися в гучні назви "Коронавірус.інфо" або "Koronalife" або ж і без такого перейменування та розміщували сенсаційні заголовки статей, для прочитання повного тексту яких необхідно було перейти на їх сторінку –

таким чином такі ресурси підвищували переходи та збільшували свою аудиторію. У даному випадку можна говорити про маніпуляцію, по-перше, є чітко визначена ціль – збільшення переглядів та аудиторії, по-друге, використовується один із психологічних прийомів такий як гучний заголовок, інформаційна складова – платформа, на якій група, канал чи паблік здійснює свою діяльність (телеграм, інстаграм тощо) та впевненість особи, на яку спрямований такий вплив, що вона переходить за таким посиланням виключно за власним бажанням. Також, варто зазначити, що негативних наслідків для життя та здоров'я особи, яка перейшла за таким посиланням не буде.

Наступний етап – активне поширення вірусу за межами Китаю та введення карантинних заходів в різних країнах світу. Тут знову ж таки активувалися усі можливі джерела інформації – поширення даних про повне закриття магазинів, в тому числі і продуктових, аптек, фото переповнених лікарень та моргів, інформація про дефіцит продуктів та засобів гігієни, закриття кордонів, заборона роботи транспорту, періодичне нагадування про велику кількість хворих, критичних та летальних випадків в європейських державах, ненадання об'єктивної інформації з боку державних органів – це лише маленький перелік шляхів, якими здійснювалося "чисте" інформаційне насильство, адже у даному випадку мова іде саме про це явище. Деякі з цих прийомів не були явні для людей, в деяких випадках люди чітко розуміли, що це на них здійснюється цілеспрямований вплив, в будь-якому випадку наслідки були однакові – це поширило серед населення страх і паніку, яка в тій чи іншій мірі вплинула на здоров'я населення. Погане самопочуття, яке нагадувало симптоми того самого "смертоносного вірусу", страх соціального контакту та перебування в громадських місцях – з одного боку, та скептичне ставлення до вірусу, зневага та в деяких випадках ненависть до людей, які його бояться – з іншого. Все це не лише вплинуло на свідомість індивідів, а спонукало до фізичного насильства та порушення сталих соціальних зв'язків.

Якщо відповісти на питання, кому такий стан був вигідний, то тут можна висувати лише припущення. Державі? Для того, щоб запровадити жорсткі карантинні обмеження, які явно порушували конституційні права людей? Фармацевтичним компаніям та продуктовим магазинам? Які отримали заробіток від панічного скуповування медикаментів та продуктів? Чи можливо суб'єкти та цілі впливу набагато глобальніші? Ці питання залишаються відкритими, адже встановити прямий взаємозв'язок між ними досить складно.

Щодо пропаганди, то хоча "інформаційний бум" припав саме на першу хвилю пандемії, діяльність засобів масової інформації, онлайн-ресурсів та соціальних мереж, які є упередженими та все-таки схиляють до певного ставлення до ситуації – підтримують всесвітню теорію змови, впевнені в особливій небезпеці коронавірусу або ж скептичне ставлення до нього, продовжують свою діяльність, знаходячи все нові підтвердження власних поглядів. Така діяльність і може вважатися пропагандою, так як здійснюється протягом тривалого часу, спрямована на масову аудиторію і має конкретну ціль – формування конкретного ставлення до пандемії коронавірусу COVID-19.

На основі вказаного прикладу, можна зазначити про подібність, взаємопов'язаність та взаєпроникність усіх трьох видів впливу. Між ними не можливо провести чітку межу, яка б розділяла один вплив від іншого та залежно від конкретних обставин одна і та ж ситуація може розглядатися як інформаційне насильство, інформаційна маніпуляція або пропаганда.

Висновки.

Підводячи підсумки, зазначаємо, що основним завданням будь-якої держави є забезпечення безпеки. В силу постійного розвитку інформаційних технологій, а також їх цінності в сучасному соціумі саме інформаційна безпека стала однією із пріоритетних складових національної безпеки, яка в силу своєї "новизни" та постійного вдосконалення вимагає особливого вивчення та врегулювання.

Основною загрозою інформаційній сфері, яка набуває просто масового характеру, є інформаційно-психологічний вплив – цілеспрямований, переважно організований процес проникнення у свідомість людини (або групи осіб), який здійснюється за допомогою сукупного використання спеціальних інформаційних засобів та технологій і психологічних прийомів та спрямований на зміну індивідуальних та/або групових психічних явищ та (або) психічний або фізичний стан людини (або групи осіб).

Найпоширенішими термінами, які вживаються сьогодні в аспекті інформаційно-психологічного впливу, є інформаційні насильство, маніпуляція та пропаганда.

Інформаційне насильство – це цілеспрямований вплив на свідомість людини (групи осіб) поза її волею, який здійснюється за допомогою інформаційних засобів, інформаційних технологій та психологічних прийомів в результаті якого порушується інформаційна свобода об'єкта впливу та який здатний заподіяти шкоду життю та здоров'ю людини (групі осіб) на яку впливають.

Інформаційна маніпуляція – це цілеспрямований прихований вплив на свідомість особи (групи осіб), який здійснюється за допомогою інформаційних та психологічних засобів, який здійснюється поза волею особи (групи осіб) та спрямований на досягнення певного, заздалегідь визначеного результату, а саме викликати бажання вчиняти певні дії або утримуватися від таких дій, підтримувати певні погляди або навпаки тощо.

Пропаганда – це тривалий, цілеспрямований, організований вплив на масову свідомість, що здійснюється за допомогою інформаційних та психологічних засобів та спрямований на формування певного, заздалегідь передбаченого, настрою в суспільстві та ставлення до явища, події, особи, держави тощо.

На підставі аналізу та співвідношення вказаних понять та їх основних ознак можна зазначити наступне:

1. Всі, досліджувані процеси спрямовані проти волі та інформаційної свободи особи (або групи осіб), мають конкретну кінцеву мету, є організованими, здійснюються за допомогою інформаційних та психологічних прийомів та інформаційних технологій та мають наслідки у вигляді зміни індивідуальних або групових психічних явищ.

2. Інформаційна маніпуляція та пропаганда є видами інформаційного насильства, специфічними ознаками яких є прихований характер впливу та спрямованість на виникнення бажання вчинити певні дії або утриматися від них – для маніпуляції та масовий характер, тривалий період впливу і конкретна ціль – формування конкретного ставлення чи уявлення про явища, події, осіб тощо – для пропаганди.

3. Не існує конкретної межі між інформаційним насильством, інформаційною маніпуляцією та пропагандою. Залежно від конкретних обставин відповідно до яких розглядається один і той же процес, він може бути як інформаційною маніпуляцією, інформаційним насильством, так і пропагандою.

Використана література

1. В UX потребности важнее, чем желания – пирамида Маслоу и иерархия потребностей. URL: https://www.ux-ui.top/ux-education/v-ux-potrebnosti-vazhnee-chem-zhelaniya-piramida-maslou-i-ierarhiya-potrebnostej.html; URL: http://psychclassics.yorku.ca/Maslow/motivation.htm

2. Почепцов Г. Пропаганда 2.0. Харків: Фоліо, 2018. 796 с.

3. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія ; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. – ISBN 978-966-96731-6-9.

4. Дзьобань О.П., Панфілов О.Ю., Соболєва С.М. Інформаційне насильство: змістовний аспект. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/47745-95745-1-PB.pdf (дата звернення: 07.11.2020).

5. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/drsk_2015_4_11.pdf (дата звернення: 07.11.2020).

6. Євченко І.М. Інформаційно-психологічний вплив ЗМІ на особистість: матеріали ІІІ Всеукраїнської конференції з міжнародною участю *Психологічні виміри особистісної взаємодії суб'єктів освітнього простору в контексті гуманістичної парадигми* / ред. С.Д. Максименко, м. Київ, 31 бер. 2020 р. Київ: Інститут психології імені Г.С. Костюка НАПрН України, 2020. С. 59-61.

7. Золотар О.О. Пропаганда в соціальних мережах – загроза інформаційній безпеці держави. URL: http://sci.ldubgd.edu.ua:8080/bitstream/handle/123456789/6139/konf_04_04_2019.pdf?sequence=1&isAllowed=y#page=48 (дата звернення: 10.11.2020).

8. Нємцева О.О. Структура інформаційно-психологічного впливу. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39499/09-Nikolaienko2.pdf?sequence=1 (дата звернення: 07.11.2020 р.).

9. Павлов Д. Політична пропаганда: до визначення поняття. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/gileya_2013_79_102.pdf (дата звернення: 10.11.2020).

10. Сащук Г.М. Інформаційне насильство в сучасному суспільстві. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/gileya_2016_111_84.pdf (дата звернення: 08.11.2020).

11. Сищук О.А. Інформаційно-психологічний компонент "гібридної війни". URL: https://core.ac.uk/download/pdf/33693038.pdf (дата звернення: 08.11.2020).

12. Фурашев В.М., Самчинська О.А. Маніпуляції свідомістю людини як основний спосіб ведення передвиборчих кампаній. *Інформація і право*. № 3(30)/2019. С. 119-125.

13. Стратегія національної безпеки: Указ Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 10.11.2020).

14. Ніколаєнко С.О., Ніколаєнко С.І. Категорія психологічного впливу в психології. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39499/09Nikolaienko2.pdf?sequence=1 (дата звернення: 07.11.2020).

15. Балл Г.А., Бургин М.С. Аналіз психологических воздействий и его педагогическое значение. *Вопросы психологии.* 1994. № 4.С. 56-66.

16. Куций О.А. Види психологічного впливу у діяльності спеціалістів ризиконебезпечних професій. URL: https://nuczu.edu.ua/sciencearchive/ProblemsOfExtremeAndCrisisPsychology/vol7/031.pdf (дата звернення: 08.11.2020).

17. Сидоренко Е.В. Личностное влияние и противостояние чужому влиянию. *Психологические проблемы самореализации личности*. СПб.: СпбГУ, 1997. С.123-142.

18. Куликов В.Н. Прикладне исследование социально-психологического воздействия. *Прикладные проблемы социальной психологии.* 1983. 158-172.

19. Остроухов В. До проблеми забезпечення інформаційної безпеки України. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/59848/14-Ostroukhov.pdf?sequence=1 (дата звернення: 07.11.2020).

20. Захаренко К. Інформаційні впливи як джерела загострення інформаційної небезпеки. URL: http://enpuir.npu.edu.ua/bitstream/123456789/22362/1/Nchnpu_7_2015_34_24.pdf (дата звернення: 07.11.2020).

21. Новий тлумачний словник української мови: у 3 т.: 42000 сл. / уклад. В. Яременко, О. Сліпушко. Київ: Аконіт, 2003. Т. 2. 926 с. – ISBN 966-7173-23-2.

22. Ігнатов О.М. Насильство як спосіб вчинення злочину: поняття та сутність. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/FP_index.htm_2010_3_21.pdf (дата звернення: 10.11.2020).

23. Лукасевич О.А., Титар Ю.В. Маніпулятивні прийоми: особливості використання у міжособистісному спілкуванні. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/pspz_2017_2_22.pdf (дата звернення: 09.11.2020).

24. Колтик О. Підходи до визначення терміну “пропаганда”. URL: file:///C:/Users/%D0%9A%D1%81%D1%8E%D1%88%D0%B0/Downloads/znpkhnpu_zntndr_2015_45_5.pdf (дата звернення: 10.11.2020).

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

УДК 37.014:355.233.11

САНДУЛ В.С., СТАРОВА С.Б., загальноосвітній заклад
“Слов’янська гімназія”, м. Київ.

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ЩОДО ДИСТАНЦІЙНОГО НАВЧАННЯ В УМОВАХ КАРАНТИНУ

***Анотація**. В статті досліджується питання удосконалення нормативно-правового упорядкування інформаційних відносин щодо форм та методів дистанційного навчання, зокрема в середніх загальноосвітніх закладах, у тому числі при вивченні предмета “Захист України”, в умовах світової пандемії та тимчасової окупації частини території України.*

***Ключові слова:** пандемія коронавірусу, дистанційне навчання, електронні освітні платформи, предмет “Захист України”,“гібридна війна”.*

***Summary.** The article examines the issue of improving the legal regulation of information relations on the forms and methods of distance learning, in particular in secondary schools, including the study of the subject “Defense of Ukraine”, in a global pandemic and temporary occupation of Ukraine.*

***Keywords:** coronavirus pandemic, distance learning, electronic educational platforms, subject “Defense of Ukraine”, “hybrid warfare”.*

***Аннотация.** В статье исследуется вопрос совершенствования законодательства, форм и методов дистанционного обучения в средних общеобразовательных учреждениях, в том числе при изучении предмета “Защита Украины” в условиях мировой пандемии и временной оккупации части территории Украины.*

***Ключевые слова:** пандемия коронавируса, дистанционное обучение, электронные образовательные платформы, предмет “Защита Украины”, “гибридная война”.*

Постановка проблеми. Пандемія коронавірусу, яка охопила світ у 2020 році, докорінно змінила життя українців. Зміни торкнулися таких речей, як спосіб життя, в тому числі шкільного навчання.

Протягом тисячоліть людство виживало завдяки своєму вмінню своєчасно та адекватно реагувати на зовнішні виклики, шляхом зменшення негативного впливу на соціум або вмінню пристосовуватися до таких змін.

Від початку першої фази карантину, яку український уряд запровадив у березні 2020 року, минуло майже 10 місяців. За цей короткий строк у системі освіти проведена велика робота з удосконалення дистанційного навчання, процесу організації навчання та користування відповідними електронними ресурсами як викладачами, так і здобувачами освіти. Водночас виявилась деяка недосконаліть чинного законодавства України в системі освіти.

Для врегулювання зазначених відносин необхідно провести відповідні роботи з аналізу й оцінки законодавства України в системі освіти та вжити заходів з його вдосконалення в тій частині, що відповідає ситуації, яка склалася в державі Україна.

Як вважаємо, є потреба у необхідності нових поглядів та підходів до викладання предметів (у тому числі предмета “Захист України”) у формі дистанційного навчання з використанням електронних освітніх платформ, онлайн-сервісів та інструментів, розроблених та запропонованих Міністерством освіти і науки України (далі – МОН України) для, зокрема, закладів загальної середньої освіти.

Метою статті є удосконалення чинного законодавства України стосовно форм та методів дистанційного навчання в умовах карантинних обмежень.

Виклад основних положень. Масштабні негативні наслідки пандемії, а також її згубний вплив на добробут людей і держав, не залишилися поза увагою провідних міжнародних інституцій. Організація Об'єднаних Націй зайняла центральну роль у справі активізації та координації глобальних заходів з недопущення і стримування поширення захворювання. 2 квітня 2020 р. Генеральна Асамблея ООН ухвалила Резолюцію № 74/270 "Глобальна солідарність у боротьбі з коронавірусним захворюванням 2019 року (CoVID-19)", в якій звернено увагу в тому числі на:

- наслідки кризи в результаті пандемії, що можуть знівелювати успіхи, досягнуті у сфері розвитку, та обмежити прогрес у досягненні цілей сталого розвитку людства;
- заходи, що пом'якшили б соціальні наслідки, та увагу, необхідну для всеохоплюваного відновлення.

13 квітня 2020 р. ВР України затвердила Закон України "Про внесення змін до Закону України "Про захист населення від інфекційних хвороб" щодо запобігання поширенню коронавірусної хвороби (CoVID-19)" [1].

Постановою Кабінету Міністрів України "Про запобігання поширенню на території України гострої респіраторної хвороби CoVID-19, спричиненої коронавірусом SARS-CoV-2" від 11.03.20 р. № 211 на всій території України з 12 березня 2020 року введено карантин та визначено низку заходів протидії поширенню цієї небезпечної хвороби.

Незважаючи на такі негативні зовнішні виклики, обов'язком держави залишається забезпечення громадян гідними умовами життя, що гарантовані Конституцією України.

У преамбулі Конституції [2] задекларовано, що Верховна Рада України від імені Українського народу-громадян України всіх національностей, дбаючи про забезпечення прав і свобод людини та гідних умов її життя, приймає цю Конституцію – Основний Закон України. У статті 46 Конституції встановлено, що пенсії, інші види соціальних виплат та допомоги, що є основним джерелом існування, мають забезпечувати рівень життя, не нижчий від прожиткового мінімуму, встановленого законом. Водночас нормативно-правовим актом найвищої юридичної сили до цієї пори не визначено, чи відповідає прожитковий мінімум загальноприйнятим світовим показникам якості життя та що взагалі позначає таке словосполучення, як "якість життя".

Тож, "якість життя" – це загальний добробут людей та суспільства, що окреслює негативні та позитивні риси життя. Якість життя включає все: від фізичного здоров'я, сім'ї, освіти, зайнятості, багатства до безпеки, свободи, релігійних переконань та навколишнього середовища [3]. Таким чином, ведучи мову про якість життя, на третьому місці серед основних складових цієї соціальної категорії стоїть освіта.

Отже, якість життя однозначно перебуває в тісній кореляції з якістю освіти. Навіть більше того, між цими двома соціальними категоріями існує позитивний зворотній зв'язок. Адже від якості освіти залежить, в недалекому майбутньому, рівень наукового, технічного, технологічного та соціального розвитку і добробуту суспільства.

Із досить нехитрих викладок напрошується висновок, що суспільство, яке знехтувало якістю освіти своїх громадян сьогодні, вже завтра буде приречене на долю світового аутсайдера.

Пунктом 29 частини першої статті 1 Закону України "Про освіту" [4] передбачено, що якість освіти – це відповідність результатів навчання вимогам, встановленим законодавством, відповідним стандартом освіти та/або договором про надання освітніх послуг.

Одним із важливих показників якості освіти можна вважати Індекс рівня освіти (далі – Індекс) в країнах світу (Education Index) – це комбінований показник Програми розвитку Організації Об'єднаних Націй (ПРООН).

Індекс стандартизується у вигляді числових значень від 0 (мінімальний) до 1 (максимальний). Прийнято вважати, що розвинені країни повинні володіти мінімальним показником 0.8, хоча багато з них мають показник 0,9 або вище. Усього зазначеним індексом оцінено якість освіти 188 країн світу. При визначенні місця у світовому рейтингу всі країни ранжуються на основі Індексу, де місця з меншими числовими показниками відповідають вищому значенню цього показника, а з більшими – нижчому [5]. Нижче наведена порівняльна таблиця (Таблиця) для деяких суб'єктів колишнього СРСР.

Отож, у порівнянні з 2016 роком, у 2019 році Індекс України зменшився з 0.803 до 0.797, що змістило нашу державу з 40 на 47 місце у світовому рейтингу та у свою чергу призвело до виключення України з "клубу" розвинених країн світу.

Як видно з Таблиці, у більшості країн зміни Індексу призвели до втрати високого рейтингу. Водночас Індекс Латвії та особливо Грузії, яка, як і Україна, зазнала втрат внаслідок російської агресії, в 2019 році "зміцнився" в порівнянні з 2016 роком на 7 позицій.

Таблиця

Країна	**2016 рік**		**2019 рік**	
	Місце в таблиці рейтингу	Індекс рівня освіти	Місце в таблиці рейтингу	Індекс рівня освіти
Україна	40	0.803	47	0.797
Казахстан	39	0.805	38	0.817
Росія	34	0.816	33	0.832
Білорусь	26	0.834	30	0.837
Латвія	25	0.835	22	0.817
Грузія	43	0.794	26	0.856

На наш погляд, чинником, що призвів до зазначених змін, є якість освітньої діяльності, яка у свою чергу залежить від рівня організації, забезпечення та реалізації освітнього процесу. Рівень організації освітнього процесу залежить від професійних якостей педагогів, професіоналізму та компетентності керівництва МОН України, а також наявності зовнішніх викликів, що негативно впливають на якість освітнього процесу. До зовнішніх викликів можна віднести карантинні обмеження, пов'язані з епідемією коронавірусу, вплив військової агресії Росії проти України та тимчасову окупацію тією ж Росією частини території України. Зважаючи на таке, держава змушена використовувати значні фінансові, матеріальні та людські ресурси для нейтралізації зазначених негативних явищ, що призводить до збитковості у фінансуванні інших, також важливих соціальних напрямків людської діяльності, в тому числі і освітнього процесу.

Відповідно до постанови Кабінету Міністрів України "Про внесення змін до деяких постанов Кабінету Міністрів України" від 26.02.20 р. № 143 та наказу МОН України "Про внесення змін до типової освітньої програми закладів загальної середньої освіти ІІІ

ступеня" від 31.03.20 р. № 464 назву навчального предмета "Захист Вітчизни" змінено на "Захист України". Тож, коли ведеться мова про навчальний предмет "Захист Вітчизни", маємо на увазі "Захист України".

Питання щодо вдосконалення законодавства та навчальної програми викладання предмета "Захист Вітчизни" в середніх загальноосвітніх закладах та необхідності підвищення ролі військово-патріотичного виховання молоді у відповідь на збройну агресію з боку Росії на Сході України, анексію Криму та подальше розгортання Росією гібридної війни на усіх можливих напрямках, розглянуте нами раніше в [6; 7]. Важливість цього питання стає дедалі більшою.

За висновками військових спеціалістів та аналітиків, українські військові розглядають кілька можливих сценаріїв вторгнення Росії в Україну на різних частинах кордону, навіть одночасно [8]. Водночас, Російська Федерація стягує до кордонів з Україною війська, літаки й танки, розраховуючи на помилку української сторони, аби використати це як привід для повномасштабного вторгнення [9].

Виходячи з вищенаведеного, проблема національної безпеки є однією з ключових у розвитку будь-якого суспільства, а з урахуванням загрозливих чинників, потребує більшої уваги на рівні держави. У Методичних рекомендаціях про викладання предмета "Захист України" у 2020/2021 навчальному році, згідно Додатку до листа Міністерства освіти і науки України від 11.08.20 р. № 1/9-430 [10] (далі – Додаток) зазначено, що суспільна система, що не здатна забезпечити власну національну безпеку, завжди перебуває на межі ризику свого припинення. Готовність Збройних сил України до виконання своїх функцій значною мірою залежить від її особового складу, зокрема підготовленості молоді до проходження військової служби.

Звідси, незважаючи на таке вразливе для всього суспільства соціальне явище, як пандемія, важливість вивчення всіх предметів, у тому числі шкільного предмета "Захист України", з урахуванням можливості повномасштабного військового вторгнення з боку Росії на територію України, зростає.

У цій складній ситуації, в якій опинилась Україна, тішить те, що МОН України досить оперативно відреагувало на такий зовнішній фактор, як пандемія, та своїм Наказом від 08.09.20 р. № 1115, зареєстрованим у Міністерстві юстиції України 28.09.20 р. за № 941/35224 своєчасно затвердило нове Положення про дистанційну форму здобуття повної загальної середньої освіти (далі – Положення) [11] та одночасно були внесені зміни до Положення про дистанційне навчання, затвердженого наказом Міністерства освіти і науки України від 25.04.13 р. № 466, зареєстрованого в Міністерстві юстиції України 30.04.13 р. за № 703/23235 (зі змінами) [12].

У Положенні особливо велика увага приділяється технологіям дистанційного навчання, особливо використанню інформаційно-комунікаційних (цифрових) технологій, з урахуванням новітніх технологічних досягнень.

Водночас, МОН України своїм листом від 02.11.20 р. № 1/9-609 (далі – Лист) [13] надало рекомендації закладам загальної середньої освіти щодо організації освітнього процесу під час дистанційного навчання.

У Листі декларується право закладів середньої освіти в межах своєї автономії в тому числі, визначати форми організації освітнього процесу та обирати (схвалювати педагогічною радою закладу освіти) конкретні електронні освітні платформи, онлайн-сервіси та інструменти, за допомогою яких організовується освітній процес під час дистанційного навчання (Moodle, Google Classroom, Zoom тощо).

У Додатку [10] визначено мету навчального предмета "Захист України" та встановлено, що "вибір форм, методів та засобів навчання, зокрема і підручників,

розподіл кількості годин, що відводяться на вивчення розділів та окремих тем (це стосується як порядку вивчення тем, так і розподілу часу на їх вивчення), учитель визначає самостійно".

Враховуючи вищенаведене, для успішного освоєння навчальних програм закладу загальної середньої освіти, в тому числі предмета "Захист України", МОН України створені майже всі необхідні умови. У той же час, у зазначеному Додатку не акцентується увага на тому, що російськими найманцями продовжується окупація частини території України і що в таких умовах потрібно запроваджувати вивчення більш агресивних форм супротиву факторам впливу "гібридної війни" [6] на підростаюче покоління, а не замовчувати факт окупації та не пропагувати заходи примирення у вигляді "нового стратегічного способу ведення бойових дій", як то – "відведення сил та засобів".

Щодо способу викладання, то Положенням [11] встановлено, що "під час дії карантинних обмежень освітній процес у закладі освіти може організовуватися у спосіб, за якого окремі теми з навчального предмету частиною учнів класу вивчаються очно, іншою частиною учнів класу – дистанційно (в асинхронному режимі, з можливістю надання учням підтримки шляхом проведення консультацій у синхронному режимі)".

Практика викладання шкільної програми предмету "Захист України" показала, що найбільш ефективним способом викладання є поєднання дистанційних форм та очної форми навчання з метою проведення консультацій та практичних занять.

Дистанційне навчання проводилося в асинхронному режимі з використанням електронної освітньої платформи GSuite у Google Classroom. При цьому в навчальному закладі були створені умови для реалізації синхронного режиму з використанням технологій Meet, Moodle та Zoom.

Використовувалися відеофільми, створені для дистанційного вивчення такої теми, як "Орієнтування на місцевості", "Ведення вогню з місця по нерухомих цілях і цілях, що з'являються".

При очній формі навчання, що передбачала розподіл класу на дві зміни, проводились практичні заняття з тактичної, стройової підготовки та практичні стрільби з пневматичної гвинтівки.

Як очно, так і дистанційно проводилось поточне, тематичне та семестрове оцінювання.

При організації дистанційного навчання, у школі було створено умови для використання учителями системи технічного забезпечення комп'ютерною технікою.

Водночас виникає необхідність навчання учителів комп'ютерній грамотності та вмінню використовувати під час освітнього процесу сучасні електронні освітні платформи, що, при відповідальному підході керівництва школи, було реалізовано майже на 100 відсотків. При цьому потрібно враховувати, що змінюються технології освітнього процесу, тому навчання учителів повинно проводитися постійно та безперервно.

Частиною другою статті 8 Закону України "Про освіту" [4] надано визначення, що таке "Формальна освіта". При цьому не згадується про можливість використання дистанційної форми навчання при здобутті такої освіти.

Також практика проведення дистанційних форм навчання передбачає використання електронних освітніх платформ, онлайн-сервісів та інструментів, за допомогою яких організовується освітній процес під час дистанційного навчання, що не передбачено чинним законодавством України.

Виникає необхідність приведення у відповідність реаліям сьогодення норм чинних Законів України, а саме:

- частина перша статті 1 Закону України "Про освіту" потребує визначення такої формі навчання, як "дистанційна форма навчання", та визначення "інформаційно-комунікаційних технологій дистанційного навчання", у розумінні, що наведено в Положенні [11].
- частина друга статті 8 Закону України "Про освіту" потребує змін в частині, що стосується визначення "Формальна освіта", та викладення її визначення у формі, що передбачає використання дистанційної освіти.

Висновки.

Враховуючи вищезазначене та потреби, з метою пом'якшення соціальних наслідків пандемії зусилля держави мають бути спрямовані на:

1. Вдосконалення чинного законодавства України шляхом внесення змін до частини першої статті 1 Закону України "Про освіту" в частині, що стосується надання визначення термінів, а саме:

а) дистанційне навчання (доповнити пунктом 4^{-1}, в якому надати визначення поняття "дистанційне навчання" у такому формулюванні: "дистанційне навчання – організація освітнього процесу (за дистанційною формою здобуття освіти або шляхом використання технологій дистанційного навчання в різних формах здобуття освіти) в умовах віддаленості один від одного його учасників та їх, як правило, опосередкованої взаємодії в освітньому середовищі, яке функціонує на базі сучасних освітніх, інформаційно-комунікаційних (цифрових) технологій", – що буде відповідати змісту, наведеному в Положенні [11];

б) інформаційно-комунікаційні (цифрові) технології дистанційного навчання (доповнити пунктом 11^{-1} у такому формулюванні: "інформаційно-комунікаційні (цифрові) технології дистанційного навчання – технології створення, накопичення, зберігання та доступу до електронних освітніх ресурсів з навчальних предметів (інтегрованих курсів), а також забезпечення організації та супроводу освітнього процесу за допомогою спеціалізованого програмного забезпечення та засобів інформаційно-комунікаційного зв'язку, у тому числі мережі Інтернет", – та привести у відповідність до вимог Положення [11];

2) Внесення змін до частини другої статті 8 Закону України "Про освіту" в частині, що стосується визначення терміну "формальна освіта", та викласти у такій редакції:

"Формальна освіта – це освіта, яка здобувається, у тому числі з використанням ***дистанційного навчання***, за освітніми програмами відповідно до визначених законодавством рівнів освіти, галузей знань, спеціальностей (професій) і передбачає досягнення здобувачами освіти визначених стандартами освіти результатів навчання, відповідного рівня освіти та здобуття кваліфікацій, що визнаються державою".

3) Постійне та безперервне підвищення "комп'ютерної грамотності" педагогічних працівників з метою освоєння інформаційно-комунікаційних (цифрових) технологій дистанційного навчання.

4) Використання електронних освітніх платформ, онлайн-сервісів та інструментів при організації освітньої діяльності в режимі дистанційного навчання.

5) Поєднання дистанційного навчання з очною формою навчання в умовах карантинних заходів у масштабах держави.

6) Приділення особливої уваги нейтралізації факторів "гібридної війни" при викладанні предмета "Захист України".

Використана література

1. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін.; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса: Фенікс, 2020. 260 с. – ISBN 978-966-928-618-5.

2. Конституція України: Закон України від 28.06.96 р. № 254/96-ВР. URL://www.rada.gov.ua

3. Якість життя. Визначення. URL: https://uk.wikipedia.org/wiki/%D0%AF%D0%BA%D1%96%D1%81%D1%82%D1%8C_%D0%B6%D0%B8%D1%82%D1%82%D1%8F

4. Про освіту: Закон України від 05.09.17 р. № 2145-VIII. *Відомості Верховної Ради України.* 2017. № 38-39. Ст. 380.

5. Світовий рейтинг загальноосвітніх шкіл. URL: https://www.bbc.com/ukrainian/science/2015/05/150513_vj_education_rankings_it

6. Сандул В.С. Удосконалення законодавства та навчальної програми викладання предмета "Захист Вітчизни" в середніх загальноосвітніх закладах. *Інформація і право*. № 2(29)/2019. С. 123-128.

7. Сандул В.С., Сікорський В.А. Військово-патріотичне виховання при викладанні навчального предмета "Захист Вітчизни" в середніх загальноосвітніх закладах. *Інформація і право*. № 3(30)/2019. С. 126-131.

8. Наєв С.І. Росія, Крим, вторгнення Росії в Україну. URL: https://lb.ua/news/2020/07/10/461556_naiev_rozpoviv_pro_stsenarii_mozhlivogo.html

9. Денис Богуш. Ексклюзивне інтерв'ю. URL: https://wz.lviv.ua/article/385543-zahroza-povnomasshtabnoho-vtorhnennia-rosii-v-ukrainu-zberihaietsia

10. Методичні рекомендації про викладання предмета "Захист України" у 2020/2021 навчальному році: додаток до листа Міністерства освіти і науки України від 11.08.20 р. № 1/9-430. URL: https://www.schoollife.org.ua/shhodo-metodychnyh-rekomendatsij-pro-vykladannya-navchalnyh-predmetiv-u-zakladah-zagalnoyi-serednoyi-osvity-u-2020-2021-navchalnomu-rotsi

11. Положення про дистанційну форму здобуття повної загальної середньої освіти: наказ МОН України від 08.09.20 р. № 1115, зареєстровано в Міністерстві юстиції України 28.09.20 р. за № 941/35224. URL https://zakon.rada.gov.ua/laws/show/z0941-20#Text

12. Положення про дистанційне навчання: наказ МОН України від 25.04.13 р. № 466, зареєстрованого в Міністерстві юстиції України 30.04.13 р. за № 703/23235. URL: https://zakon.rada.gov.ua/laws/show/z0703-13#Text

13. Щодо організації дистанційного навчання: лист МОН України від 02.11.20 р. № 1/9-609. URL: https://mon.gov.ua/ua/npa/shodo-organizaciyi-distancijnogo-navchannya

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

Інформаційна і національна безпека

УДК 342.7:004

ЗОЛОТАР О.О., *доктор юридичних наук, старший науковий співробітник,*
завідувач науковим сектором НДІ інформатики і права
НАПрН України.

ПОНЯТТЯ ТА ЗМІСТ КАТЕГОРІЇ “ІНФОРМАЦІЙНА БЕЗПЕКА ЛЮДИНИ”

Анотація. *У статті аналізуються доктринальні підходи до визначення наукової категорії “інформаційна безпека людини”, а також розуміння її змісту.*
Ключові слова*: інформаційна безпека людини, структура інформаційної безпеки людини.*

Summary*. Doctrinal approaches to the definition of the scientific category of “Human Information Security”, as well as understanding of its content, are analyzed.*
Keywords*: sociological research, electoral process, democracy, information influence.*

Аннотация*. В статье анализируются доктринальные подходы к определению научной категории “информационная безопасность человека”, а также ее понимание.*
Ключевые слова*: Human Information Security, structure of Human Information Security.*

Постановка проблеми. Розвиток науки про безпеку в напрямку інформаційної безпеки істотно залежить від стану формування інформаційного суспільства в конкретній державі. Рівень розвитку і використання інформаційно-комп’ютерних технологій (далі – ІКТ) в світі дуже нерівномірний – наприклад, доступ до Інтернету має близько 60 % жителів планети, при цьому найвищі показники більш 90 % – в Південній Кореї та Австралії, і найнижчі – менше 10 % – в деяких африканських країнах.

Це означає, що в залежності від рівня розвитку ІКТ, інформаційні проблеми населення суттєво відрізняються. Однак, це не означає, що вони не існують. Людина завжди “приречена” на пошук, оцінку і захист інформації (різниця полягає лише за своїм змістом – інформація про місця для полювання, джерела води, інше плем’я або про комерційну таємницю, авторські права і персональны даны), тобто, інформаційну діяльність, яка нерозривно пов’язана з інформаційною безпекою. Тільки ось за умови формування інформаційного суспільства значення останньої неухильно зростає.

Інформаційна діяльність сучасної людини є необхідною умовою її самореалізації та задоволення різноманітних потреб та інтересів – матеріальних, соціальних і духовних. Кількість і якість існуючої і доступної інформації, а також інтенсивність впливу інформаційного простору на людину абсолютно змінилася за останні півстоліття, в т.ч. в зв’язку з останньою інформаційною революцією – винаходом і повсюдним використанням інтернету. “Інтернет ...набагато більше схожий на інформаційну супермагістраль з пробками, ніж на інформацію” [1]. І в цьому величезному потоці інформації людина змушена не тільки лавірувати в цілях пошуку необхідної інформації, але також і захищати свої інтереси, зберігати і відстоювати свої цінності, а також протистояти негативному впливу і загрозам інформаційного простору.

Переважна кількість наукових досліджень категорії “інформаційна безпека” спрямована на вирішення питань, пов’язаних або з інформаційною безпекою держави, або з національною інформаційною безпекою, в яких проблематика інформаційної безпеки

людини розглядається частково і виключно як складова ширшого об'єкта безпеки. Таким чином, інформаційна безпека людини, в цілому, є актуальним предметом досліджень не тільки правових наук, а й соціологічних та психологічних, а також теорії управління та науки про безпеку. Попри те, слід відзначити у всіх цих науках відсутність чіткої і загальновизнаної термінологічної системи у сфері інформаційної безпеки, що впливає на розбіжність у доктринальному та практичному тлумаченні цієї важливої категорії.

Метою статті є дослідження наукових підходів до розуміння інформаційної безпеки людини і формулювання визначення цієї наукової категорії на основі її істотних складових.

Результати аналізу наукових публікацій. Інформаційна безпека як наукова категорія передбачає доктринальні, енциклопедичні та нормативно-правові визначення. При цьому методологічні підходи, логічні способи їх утворення і закріплення, сфери існування і прикладного використання істотно відрізняються. Це пов'язано також з тим, що категорія безпеки неоднозначна і визначається в залежності від наукової області, в якій вона вивчається.

В основі будь-якої безпеки як системи мають місце життєве важливі інтереси особистості, нації, держави або міжнародної спільноти. Так, Ярочкин В.І. визначає безпеку як стан захищеності особистості, суспільства і держави від зовнішніх і внутрішніх небезпек і загроз, заснована на діяльності людей, суспільства, держави, світового співтовариства щодо виявлення (вивчення), попередження, послаблення, ліквідації та відображенню небезпек і загроз, здатних їх знищити, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку [2, с. 253].

У цьому, як процесі, проявляється розуміння, сенс, необхідність усвідомленого оволодіння ідеєю безпечного існування заради подальшого існування або розвитку соціальної системи.

Розкриваючи філософські проблеми безпеки як соціального явища, слід зазначити, що поняття про безпеку і усвідомлення її необхідності проявляється як на чуттєвому (підсвідомому), так і на раціональному рівні. У дослідженнях польський вчений К. Лідерман, стверджує, що в той час як забезпечення стосується більшою мірою заходів (технічних, організаційних, правових і т.д.), то безпека – суб'єктивного відчуття. Передчуття, негативні емоції, відчуття небезпеки, відчуття необхідності самозахисту з подальшим усвідомленим формуванням системи охорони і захисту є проявом багатства різноманітності людської природи, невичерпності людських якостей. Тобто, безпеку знаходить відображення в свідомості суб'єкта суспільних відносин як динамічний процес, який має ряд варіативних детермінант – стан, рівень розвитку системи, в тому числі культурності і цивілізованості. Тому обґрунтованою є постановка проблеми виявлення і розкриття сутнісних ознак безпеки як соціального феномена. До таких можна віднести: усвідомлена самодостатність, здатність до самозбереження, захищеність від загроз, гарантованість власного існування і т.д. У практичній діяльності (в політичній, економічній, правовій, культурній сферах) мають місце статичні ознаки: визначення стану захищеності від загроз в просторі, часі та за колом осіб.

Російська вчена, одна з "піонерів" інформаційного права Бачило І.Л. акцентувала увагу на багатоплановості поняття "інформаційна безпека" [3, с. 253]. Більшість українських вчених, визначаючи інформаційну безпеку, розглядає її системно, наприклад, як "стан захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх і внутрішніх викликів і загроз, який

забезпечує їх сталий розвиток" [4, с. 150]. Подібну позицію підтримують Бєляков К.І. [5, с. 28], Баранов О.А. [6, с. 160], Довгань А.Д. [7, с. 165], Нижник Н.Р. [8, с. 45].

Петрик В.Н. відзначає, що природні явища "безпека" і "небезпека" існують в діалектичному взаємозалежності, тобто в природі не існує окремо "стану безпеки" і "стану небезпеки" [9, с. 25].

Богуш В. ставить акцент на інформаційне середовище суспільства і визначає, що "інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави" [10, с. 42].

Виклад основних положень. Більш розширений аналіз змісту категорії "безпека" дозволяє стверджувати, що в суспільній свідомості це поняття ототожнюється не стільки з об'єктивними ознаками – відсутністю загроз, скільки з суб'єктивними – станом, почуттями і переживаннями людей [16]. І тому в тріаді "людина, держава, суспільство" небезпідставно на першому місці як об'єкт інформаційної безпеки має визначатися людина, в т.ч. реалізація її конституційних прав на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також захист інформації, що забезпечує особисту безпеку.

В останні десятиліття актуалізувалося питання захисту інформаційних прав і свобод людини в зв'язку з інтенсифікацією інформаційних процесів. І в науковому обігу, а також в окремих нормативно-правових актах, з'явилася як самостійна категорія "інформаційна безпека людини (особистості, особи)". При цьому, як правило, категорії осіб, особистість і фізична особа як правило ототожнюються, коли мова йде про інформаційну безпеку.

Розглядаючи зміст інформаційної безпеки людини, слід звернути увагу на вже існуючі підходи. Так, наприклад, російський вчений Баринов С.В. розглядає такі аспекти інформаційної безпеки особистості як інформаційно-технічна безпека, інформаційно-ідеологічна безпека, інформаційно-психологічна безпека особистості, а також інформаційно-правова безпека особи [11].

Такий підхід значною мірою відображає сфери, в яких можуть бути реалізовані негативні інформаційні впливи – технологічна, психологічна (в складі якої може бути виділена ідеологічна, емоційна, сфера самоідентифікації і самореалізації, релігійна та ін.), Правова, економічна, соціальна (адаптаційна, етнокультурна, національна та ін.), екологічна та інші.

Галатенко В.А. визначає інформаційно-технічну безпеку, як "захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести до завдання шкоди власникам або користувачам інформації і підтримуючої інфраструктури" [12, с. 39]. Не цілком згодні з таким визначенням, оскільки автор, називаючи цю складову "інформаційно-технічною" у визначенні описує "інформаційно-технологічну".

Ковальова М.М., виділяє інформаційно-ідеологічну безпеку, як захищеність від навмисного або ненавмисного інформаційного впливу, в результаті якого порушуються права і свободи в області створення, споживання та поширення інформації, користування інформаційною інфраструктурою і ресурсами, що суперечить моральним і етичним нормам, який чинить деструктивний вплив на особистість, що має негласний (неусвідомлений) характер, що впроваджує в суспільну свідомість антисоціальні установки [13, с. 109]. Не вважаємо за доцільне розглядати інформаційно-ідеологічну

безпеку як категорію, що стосується окремої особистості, оскільки, метою будь-якої ідеології є вплив на суспільство в цілому або окремі соціальні групи.

Більш обґрунтованим є підхід у пропозиціях Осторухова В.В., який пропонує розглядає інформаційно-психологічну безпеку особистості у вузькому і широкому розумінні. У першому випадку, на його думку, це стан захищеності психіки людини від негативного впливу, який здійснюється шляхом впровадження деструктивної інформації в свідомість і (або) в підсвідомість людини, що призводить до неадекватного сприйняття нею дійсності. У більш широкому розумінні, під інформаційно-психологічною безпекою особистості, він пропонує розуміти: по-перше, належний рівень теоретичної та практичної підготовки особистості, при якому досягається захищеність і реалізація її життєве важливих інтересів і гармонійний розвиток незалежно від наявності інформаційних загроз; по-друге, здатність держави створити умови для гармонійного розвитку і задоволення потреб особистості в інформації незалежно від наявності інформаційних загроз; по-третє, забезпечення, розвиток і використання інформаційного середовища в інтересах особистості; по-четверте, захищеність від різного роду інформаційних загроз [14, с. 456].

Грачов Г.В. також звертає увагу на багатофакторність категорії, визначаючи інформаційно-психологічну безпеку як "стан захищеності психіки від дії різноманітних інформаційних факторів, що перешкоджають чи ускладнюють формування і функціонування адекватної інформаційно-орієнтовної основи соціальної поведінки людини (і в цілому життєдіяльності в суспільстві), а також адекватної системи його суб'єктивних (особистісних, суб'єктивно-особистісних) відносин до навколишнього світу і самому собі" [15, с. 15].

Лихачов С.В. вважає, що проблеми інформаційно-психологічної безпеки неможливо розглядати окремо від проблем розвитку суспільства, оскільки система забезпечення такої безпеки неможлива без визначення стратегій розвитку того чи іншого суспільства, без розробки відповідних моделей цивілізаційного розвитку, моделей розвитку культури [16, с. 106].

Важливим фактором інформаційно-психологічної безпеки особистості є та частина інформаційного середовища суспільства, яка неадекватно відображає навколишній світ. Тобто інформація, яка вводить людей в оману, в світ ілюзій, не дозволяє адекватно сприймати навколишній і самого себе [17, с. 543]. Наслідком такого сприйняття може стати неможливість ефективно брати участь в житті суспільства, реалізовувати свої права і виконувати обов'язки, починаючи від правового нігілізму і аж до злочинної діяльності. Виходячи з подібної точки зору російський дослідник Панарін І.М. робить більший акцент на ролі політичної еліти, яка може протистояти інформаційному впливу. На його думку, "інформаційна безпека – стан інформаційного середовища суспільства і політичної еліти, яка забезпечує її формування та розвиток в інтересах керівництва країни, громадян і суспільства" [18, с. 9].

Враховуючи вищезазначене, вважаємо, що зміст інформаційної безпеки людини як наукової і правової категорії повинен ґрунтуватися на осмисленні комплексності цього соціального явища, а також враховувати інформаційні права і свободи людини, які є змістовним наповненням, що визначає сутність даної категорії.

Наукове розуміння актуальності та комплексності проблеми інформаційної безпеки людини є необхідною умовою її правового та організаційного забезпечення. Не можемо не погодитись з Пилипчуком В.Г. і Брижко В.М., що "повага і неухильне забезпечення прав, свобод і безпеки людини – гарантія від несанкціонованого втручання у її приватне життя та одна із головних функцій держави" [19, с. 61]. З метою ефективної державної

політики інформаційної безпеки людини необхідно науково обґрунтувати правові способи збалансування інформаційних прав людини і необхідного державного втручання в інформаційні відносини.

Висновки.

Таким чином, виходячи з розуміння, що інформаційна безпека людини є складовою будь-якого виду інформаційної безпеки – чи то держави, чи суспільства, чи міжнародного співтовариства, а також має місце у складі інших сфер безпеки – продовольчої, екологічної, економічної, соціальної тощо, а її забезпечення є необхідною умовою реалізації прав і законних інтересів людини в кожній сфері її життєдіяльності пропонуємо таке визначення цієї наукової категорії: *"під* ***інформаційною безпекою людини*** *слід розуміти стан і процес захищеності людини від інформаційних загроз і викликів, що забезпечує можливість людини як біологічного організму і соціальної істоти функціонувати, розвиватись, задовольняти свої потреби і досягати бажаних для себе результатів в інформаційному суспільстві".*

Зміст інформаційної безпеки людини, на нашу думку, становлять інформаційні права і свободи людини, а в її структурі можна виділити інформаційно-психологічну, інформаційно-технологічну та інформаційно-правову складові.

Використана література

1. Карафано Д. Понимание социальных сетей и национальная безопасность / пер. с англ. Савина Л. URL: https://www.geopolitica.ru/article/ponimanie-socialnyh-setey-i-nacionalnaya-bezopa snost (дата звернення: 09.03.2021).

2. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности. Москва, 2000. С. 28.

3. Бачило И.Л. Информационное право: основы практической информатики. Москва, 2001. С. 253.

4. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти; за заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2011. 244 с.

5. Бєляков К.І. Внутрішня безпека України і шляхи її забезпечення: наук. вид. Київ: МНДЦ, 2005. С. 26-32.

6. Баранов А.А. Информационная безопасность и экономические преобразования: мат. междунар. конф. *Углубление рыночных реформ и стратегия экономического развития Украины до 2010 года.* Ч. 2. Т. 1. Киев, 1999. С. 160.

7. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ, 2015. 388 с.

8. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч.посібн. Ірпінь, 2000. 304 с.

9. Забезпечення інформаційної безпеки держави: підручник / В.М. Петрик та ін.; за заг. ред. О.А. Семченка. Київ: Книжкова палата України, 2015. 665 с.

10. Богуш В., Юдин А. Информационная безопасность государства. Москва: "МК-Пресс", 2005. 432 с.

11. Баринов С.В. О правовом определении понятия "информационная безопасность личности". *Актуальные проблемы российского права*. 2016. № 4 (65). URL: https://cyberlen inka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti (дата звернення: 01.03.2021).

12. Галатенко В.А. Информационная безопасность. *Открытые системы*. 1996. № 1 (15). С. 38-43.

13. Ковалева Н.Н. Информационное право России: учеб. пособие. Москва: Дашков и Ко, 2007. С. 109.

14. Інформаційна безпека (соціально-правові аспекти): підручник / В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк та ін.; за заг. ред. Є.Д. Скулиша. Київ: КНТ, 2010. 776 с.

15. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. Москва: Изд-во РАГС, 1998. С. 15.

16. Лихачов С.В. Інформаційно-психологічна безпека як складова національної безпеки України. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 2(1). С. 103-108.

17. Политическая психология: учеб. пособие для вузов / Деркач А.А., Жуков В.И., Лаптев Л.Г. (ред.). Екатеринбург: Деловая книга, 2003. 858 с.

18. Панарин И.Н. Информационная безопасность. URL: http://panarin.com/ info_voina/86-informacionnaya-bezopasnost.html. (дата звернення: 01.03.2021).

19. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. № 4(19)/2016. С. 60-70.

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

УДК 343.9.024:004.056

ГУЦАЛЮК М.В., *кандидат юридичних наук, старший науковий співробітник, доцент*, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

НОВІТНІ ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.*
Ключові слова: *кіберзлочинність, кібератака, COVID-19, шахрайство.*

Summary*. The article deals with current trends in cyber crime, including its organized forms, and proposes to strengthen the counteraction to this phenomenon.*
Keywords*: cyber crime, cyber attack, COVID-19, fraud.*

Аннотация*: В статье исследуются современные тенденции киберпреступности, в том числе ее организованные формы, представлены предложения по усилению противодействия этому явлению.*
Ключевые слова*: киберпреступность, кибератака, COVID-19, мошенничество*.

Постановка проблеми. Відповідно до Конституції України забезпечення інформаційної безпеки відноситься до найважливіших функцій держави, справою всього Українського народу. У зв'язку з динамічним розвитком інформаційних технологій та розширенням сфери їх застосування постійно зростає вплив кіберзагроз на сталий розвиток суспільства. Водночас на характер кіберзагроз та методи і способи вчинення кіберзлочинів впливають не тільки технологічні новації, але й різноманітні соціальні процеси. В статті досліджуються новітні тенденції кіберзлочинності, у тому числі пов'язані з впливом пандемії COVID-19.

Результати аналізу наукових публікацій. Вплив кіберзлочинності на цифрове суспільство досліджувалось багатьма закордонними Maras Marie-Helen, Eoghan Casey, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar та вітчизняними вченими Н. Ахтирська, П. Біленчук, В. Бутузов, В. Гавловський, О. Кравцова, А. Марущак, К. Тітуніна, В. Шеломенцев, В. Хахановський, О. Юрченко та інші.

В той же час сьогодні ще не достатньо досліджені особливості діяльності кіберзлочинців та кіберугруповань під час суттєвого збільшення кількості працівників, що працюють дистанційно та збільшення часу використання мережі Інтернет, що збільшило кількість кібератак та Інтернет-шахрайства.

Виклад основного матеріалу. Найбільш значуща подія 2020 року, яка вплинула на увесь світ, була безперечно пандемія COVID-19. Понад 100 мільйонів випадків інфікування коронавірусом було виявлено у майже всіх країнах та територіях світу. Унаслідок захворювання понад 2,5 млн осіб померли. Стрімке поширення світом вірусу позначилось на діяльності державних установ, промислових підприємств та громадян абсолютної більшості країн світу.

Значний вплив коронавірусної пандемії на інформаційну сферу України підкреслено у Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020. У документі зокрема зазначено про

виявлення критичних проблем в інформаційній сфері, системах охорони здоров'я та соціального захисту.

Внаслідок введення комплексних заходів соціального дистанціювання суттєво зросла кількість онлайн-комунікацій між державними органами, підприємствами та приватними особами. Зріс попит на програмне забезпечення для домашнього офісу, таке як Zoom, Microsoft Teams і їх аналоги. Значно зросла й кількість часу, який люди проводять в мережі Інтернет.

Інтернет-провайдери фіксованого та мобільного широкосмугового зв'язку, контенту та "хмарних обчислень", а також пункти для обміну трафіком (IXP) відзначили збільшення Інтернет-трафіку на 60 % у порівнянні з доковідним періодом.

Поява нових обставин, пов'язана з поширенням вірусу COVID-19 створила нові можливості для вчинення злочинів. Як окремі злочинці, так і організовані злочинні угруповання, надзвичайно швидко адаптувалися до змін у суспільстві для підвищення рівня кримінального прибутку та почали використовувати дану проблему у своїх цілях.

Через зростання кількості корпоративних клієнтів американської компанії Zoom Video Communications, що надає послуги віддаленого конференц-зв'язку, у порівнянні з аналогічним періодом 2019 року на 458 %, цей сервіс привернув увагу злочинців. У Даркнеті зявилися понад 500 000 облікових записів Zoom, які продаються на форумах менше, ніж за копійку кожен, а в деяких випадках даруються безкоштовно. Ці облікові дані збираються за допомогою кібератак. Потім успішні логіни та паролі складаються у списки, які продаються іншим хакерам [1].

Таку поведінку злочинців слід називати опортуністичною, адже під терміном опортунізм (франц. *opportunism* – пристосовництво, від лат. *opportunus* – зручний, вигідний, слушний) слід розуміти поведінку, метою якої є отримання вигоди нечесним шляхом [2].

Серед ключових передумов виникнення загрози кібербезпеці на фоні розгортання пандемії COVID-19 Національний інститут стратегічних досліджень виділяє наступні [3]:

1. Збільшення кількості людей, які працюють віддалено (використовуючи IT, але не маючи належних знань та досвіду).

2. Збільшення кількості та обсягів електронних платежів.

3. Загальна атмосфера кризи та паніки.

Згідно з даними міжнародного розробника програмного забезпечення в сфері кібербезпеки ESET, за 2020 рік в Україні вдвічі збільшилась кількість веб-загроз та кібератак, пов'язаних з пандемією COVID-19, в тому числі через електронну пошту (шкідливе програмне забезпечення, програми-вимагачі сімейства WannaCryptor, завантажувачі та криптомайнери, експлойти EternalBlue і т.п.).

Втрати світової економіки через кіберзлочини і витрати на забезпечення захисту від них у 2020 році ***перевищили 1 трлн. доларів***. Тоді як ще два роки тому ця сума становила близько 600 млрд. доларів. Про це йдеться у звіті виробника антивірусного програмного забезпечення McAfee [4].

Кіберзлочинці почали більш ефективно використовувати традиційні методи кіберзлочинності, такі як соціальна інженерія, фішинг (спеціальна методика маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані) та шахрайство.

Зазначимо, що поняття кіберзлочину було введено в чинне законодавство Законом України "Про основні засади забезпечення кібербезпеки України" як 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. У цьому аспекті перш за все слід мати на увазі Конвенцію про кіберзлочинність 2001р. (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV).

Водночас на сьогодні у чинному законодавстві України не існує чіткого переліку таких видів злочинів, які слід віднести до кіберзлочинів, що призводить до певних труднощів, адже небезпечні діяння у кіберпросторі виходять за рамки XVI розділу КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Тому деякі науковці і практики паралельно з кіберзлочинами використовують термін "злочини, учинені із використанням високих інформаційних технологій" та інші назви [5].

За повідомленням Департаменту кіберполіції НП України в Україні кількість злочинів, учинених із використанням високих інформаційних технологій у 2020 зросла на 22,9 % у порівнянні з попереднім роком(2019 - 4263, 2020 - 5240). Найбільшу питому вагу серед них становлять ***кримінальні правопорушення***, передбачені чч. 3 і 4 ст. 190 КК України – 25,9 %, які ***зросли на 70,2 %*** (2018 - 796, 2020 - 1355).

При цьому слід зазначити високу латентність такого виду злочинів. Так, 80 % від всіх звернень громадян до кіберполіції становлять повідомлення про шахрайські дії в Інтернеті [6].

За словами фахівців, найбільш поширеними видами шахрайства у віртуальному просторі є продаж неіснуючих товарів, а також фішингові онлайн-магазини.

Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або в соцмережах. Як правило, в таких випадках головна умова покупки – повна передоплата за товар, після чого "продавець" перестає контактувати з покупцем.

Кіберзлочинці дедалі частіше використовують в своїх цілях страх людей перед вірусом COVID-19: виставляють на продаж в Інтернеті підроблені лікарські препарати, неіснуючі дезінфікуючі засоби, засоби індивідуального захисту, медичні апарати і засоби гігієни. Інші види шахрайства включають пропозиції щодо інвестиційного консультування, в тому числі по криптовалюті, а також неправдиві медичні консультації і діагностику.

Особливо значний сплеск фішингових атак з використанням проблематики COVID-19 відбувся відразу після початку пандемії [7].

За один чотиримісячний період (з січня по квітень 2020 року) одним з партнерів приватного сектору INTERPOL було виявлено близько 907 000 спам-повідомлень, 737 випадків, пов'язаних зі шкідливим програмним забезпеченням, та 48 000 шкідливих URL-адрес – усіх, пов'язаних із пандемією COVID-19 [8].

Вплив COVID-19 на злочинність змінювався з часом, зокрема підвищення обізнаності громадян зменшило вплив, який мали деякі види злочинів, водночас за інформацією Європолу кількість шкідливих програм, які використовують COVID-19 як приманку і сьогодні продовжує зростати.

Крім правоохоронців певну роботу щодо протидії спекулятивній діяльності намагаються проводити власники майданчиків електронної торгівлі.

Зокрема, на платформі OLX модераторами видаляється контент з відповідним змістом, що містить назви товарів, заборонених до продажу на цій платформі та зупиняється можливість публікації інформації про товари, що вимагають особливих умов зберігання і збуту, у тому числі тих, що використовуються для боротьби з коронавірусом, щоб не наражати на небезпеку користувачів.

На порталі Prom.ua також обмежуються можливості продавців, які використовують підвищений інтерес до теми коронавірусу для отримання надприбутку шляхом видалення з каталогу товарів, у ключових словах, тегах і назвах яких є слова "коронавірус", COVID-19 та їх синоніми. Особливо це стосується профілактичних препаратів, БАДів. Наприклад, продавати "антисептик" можна без проблем, а от "антисептик для профілактики коронавірусу".

Як повідомляє BBC, соціальна мережа Facebook ввела заборону на розміщення реклами гігієнічних масок і дезінфікуючих засобів для рук з метою перешкодити ажіотажному попиту на них і зростанню цін.

Крім того, соцмережа посилила контроль за появою в мережі дезінформації про засоби, які нібито сприяють лікуванню від вірусу, а також про товари, на які нібито виник дефіцит.

"Ми уважно спостерігаємо за ситуацією навколо Covid-19 і в разі потреби будемо вносити зміни в нашу політику, якщо виявимо, що люди експлуатують цю надзвичайну ситуацію", – заявив директор з контролю за продуктами Facebook Роб Літерн [9].

Оскільки велика кількість громадян та бізнес шукали інформацію та джерела допомоги під час пандемії, кіберзлочинці активно використовують соціальну інженерію.

Фахівці Національного координаційного центру кібербезпеки (далі – НКЦК) зазначають, що на початку пандемії у світі щодня реєструвалося понад 18 мільйонів фішингових повідомлень, пов'язаних з темою COVID-19.

Із середини 2020 року їх кількість поступово зменшувалась, а фішингові атаки стали більш направленими, їхня тематика змінювалася: від доступності масок і тестів до розробки вакцин.

Наприкінці січня 2021 року НКЦК виявив фішингову кібератаку, спрямовану на українських користувачів Інтернету, основною темою якої був початок вакцинації від COVID-19 в Україні.

Під час атаки на популярній хостинговій платформі було створено фейкову веб-сторінку, що імітувала сайт Міністерства охорони здоров'я України. Для розміщення сторінки атакуючі зареєстрували кілька доменів, які нагадували офіційний домен МОЗ України – moz.gov.ua.

На цій фейковій сторінці було розміщено інформацію щодо початку з 25 січня обов'язкової вакцинації від COVID-19 із пропозицією завантажити файл (документ Word) із подробицями.

У цей документ було вбудовано шкідливий код (макрос), який при відкритті файлу приховано від користувача завантажує та виконує інший шкідливий скрипт, що забезпечує віддалене управління зараженим комп'ютером. Таким чином, атакуючі отримували повний доступ до комп'ютера жертви [10].

Кримінальне правопорушення у червні 2020 року викрили працівники управління протидії кіберзлочинам Харківщини спільно зі слідчим управлінням обласної поліції та регіональним управлінням СБУ.

Встановлено, що до шахрайських дій причетні сім мешканців Кривого Рогу віком від 20 до 30 років.

Зловмисники діяли за декількома шахрайськими схемами. Так, члени групи телефонували клієнтам одного з мобільних операторів, видаючи себе за представників внутрішньої служби безпеки. Під приводом підтвердження верифікації користувача мобільного номеру отримували інформацію щодо останніх трьох номерів телефонів, з якими абонент спілкувався. Далі цю інформацію використовували для відновлення і перевипуску відповідної sim-карти та оформлювали онлайн-кредити.

За іншою злочинною схемою правопорушники від імені співробітника кредитної організації телефонували громадянам та повідомляли, що на його ім'я нібито здійснюється оформлення кредиту. У такий спосіб зловмисники переконували потерпілого назвати надісланий пароль доступу до особистого кабінету у фінансовій установі. Після цього вони подавали від його імені заявку на видачу кредиту.

Отримані гроші злочинці розподіляли між собою. Від протиправних дій постраждали близько 40 осіб, загальна сума збитків сягає 500 тисяч гривень.

Фігурантам було оголошено про підозру за ч. 1, ч. 2 ст. 255 (створення злочинної організації, керівництво такою організацією, а також участь у ній), ч. 4 ст. 28, ч. 1, ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, вчинене членами злочинної організації), ч. 4 ст. 28, ч. 3 ст. 190 (Шахрайство, вчинене членами злочинної організації) Кримінального кодексу України [11].

Можливості для кіберзлочинності збільшуються завдяки поширенню дезінформації. Наявність дезінформації стала вирішальною рисою в загальному ландшафті загроз під час кризи COVID-19. Хибна і недостовірна інформація щодо вірусу продовжує поширюватися, головним чином, через соціальні мережі, а також через сервіси із зашифрованою передачею повідомлень.

Фейкові повідомлення сприяють злочинцям, які продають предмети, що, начебто допомагають запобігти або вилікувати COVID-19. Такі засоби продаються як через звичайний Інтернет так і через Даркнет. Кількість нових доменів та веб-сайтів, пов'язаних із COVID-19, значно зросла на початку пандемії.

Поряд з традиційними видами кіберзлочинності, продовжують удосконалюватися і використовуватися загрози підвищеної складності (APT – Advanced Persistent Threats) для отримання вигоди із ситуації з пандемією COVID19. Основною метою APT атак є критичні об'єкти інфраструктури, включаючи лікарні та лабораторії по розробці вакцин. При цьому застосовуються шкідливі програми, програми-вимагачі, а також DDoS-атаки. Мотивом для подібних атак є не тільки отримання прибутку, але і можливість доступу до персональних даних та іншої конфіденційної інформації, що представляє цінність.

Наприклад, за повідомленням Національної служби розвідки Південної Кореї Північна Корея намагалася отримати технологію, що стосується вакцини проти коронавірусу та його лікування, за допомогою кібератаки проти Pfizer. КНДР збиралася продати отримані дані про вакцину, а не запустити власне виробництво.

Також у ЗМІ потрапила інформація з конфіденційної доповіді експертної комісії ООН про те, що хакери з Північної Кореї протягом 2020 року викрали в однієї з неназваних країн віртуальні активи на суму 316,4 млн. доларів на свою ядерну програму [12].

Успіх більшості кіберзлочинів, пов'язаних з COVID-19, заснований на фішингових атаках по електронній пошті, в якості початкового вектора зараження. Як тільки люди переходять по посиланню або завантажують документ, обліковий запис стає зкомпрометованим. Компрометація облікового запису може бути помітна жертві, але частіше всього вона залишається прихованою і дозволяє встановити довгостроковий доступ до облікового запису, організації із схожим програмним забезпеченням. Крім збору конфіденційної інформації, APT атаки можуть зашкодити роботі веб-сайтів, вносити зміни в документи, видаляти дані, а також поширювати неправдиву інформацію.

Управління ООН з наркотиків та злочинності рекомендує урядам країн і представникам приватного сектору активно проводити кампанії з підвищення рівня

інформованості населення, з урахуванням культурної специфіки. Також рекомендується регулярне оновлення системи безпеки і резервне копіювання даних [13].

Значних збитків продовжують завдавати кібератаки на банківський сектор.

Експерти з кібербезпеки прогнозують, що в 2021 році кібератаки будуть відбуватися кожні 11 секунд. Це майже вдвічі більше, ніж було в 2019 році (кожні 19 секунд), і в чотири рази більше, ніж п'ять років тому (кожні 40 секунд в 2016 році) . Значно збільшуються збитки від кібератак.

У США трьох північнокорейців звинувачено у викраденні та вимаганні понад 1,3 мільярда доларів у банків та підприємств усього світу.

Містер Парк, Джон Чанг Хьок та Кім Ір звинувачуються у змові з метою банківського шахрайства.

Міністерство юстиції заявляє, що обвинувачені працюють в Генеральному бюро розвідки, агентстві військової розвідки Північної Кореї.

Вважається, що всі троє перебувають у Північній Кореї, яка не видає своїх громадян для звинувачення США [14].

Упродовж 2020 року підрозділами Національної поліції України у сфері протидії злочинам у банківській сфері виявлено 2110 правопорушень (1079 у 2019 році) Також правоохоронними органами України у 2020 році суттєво посилилась робота щодо виявлення організованих кіберугруповань, у тому числі міжнародних.

Зокрема було викрито транснаціональну групу хакерів, які розповсюджували найнебезпечніший у світі комп'ютерний вірус EMOTET.

Хакери за допомоги вірусного програмного забезпечення здійснювали масові втручання в роботу серверів приватних та державних установ країн Європи та Сполучених Штатів Америки.

За даними слідства, група хакерів з України з 2014 року, використовуючи шкідливе програмне забезпечення, так званий вірус-шифрувальник ("банківський троян"), призначений для викрадення персональних даних – паролів, логінів та платіжних даних, здійснювала масові втручання в роботу серверів приватних та державних банківських установ Великої Британії, Німеччини, Австрії, Швейцарії, Нідерландів, Литви та США.

Інфраструктура "EMOTET" включала сервери, розташовані по всьому світу, і фактично була БОТ-мережею. Вірус поширювався шляхом спам-розсилок, через документи Word, Excel тощо. Електронні листи виглядали як попередження про безпеку облікового запису, запрошення на вечірку і навіть як застереження від поширення COVID-19.

Проникнувши у програмне забезпечення, вірус використовував "інфіковану" техніку для подальшої розсилки, а також встановлював на пристрій додаткові віруси. У результаті шкідливе програмне забезпечення викрадало персональні дані користувачів, зокрема паролі, логіни, історію браузера, платіжні та банківські дані тощо. У подальшому зловмисники перераховували гроші на свої підконтрольні рахунки.

Слідчі викрили двох громадян України, які забезпечували належну роботу інфраструктури розповсюдження вірусу та підтримували його безперебійну діяльність.

На даний час підтверджено, що вірус завдав збитків банкам і фінансовим установам США та Європи на 2,5 мільярда доларів.

Кіберполіцейські спільно з правоохоронцями іноземних держав одночасно провели обшуки на території України, Нідерландів, Німеччини, Франції, Литви, Канади, США та Великобританії.

Зазначається, що наразі повністю заблоковано діяльність БОТ-мережі "EMOTET", яка розташовувалася на більш ніж 90 серверах у різних країнах світу [15].

За повідомленням прес-служби СБУ кіберфахівці Служби безпеки України заблокували діяльність транснаціонального злочинного хакерського угруповання. Багаторівнева масштабна спецоперація проводилася в рамках міжнародного співробітництва з компетентними органами США і Франції. Зазначається, що з вересня 2020 року цими хакерами було уражено понад 150 компаній країн Європи і США. Збитки від діяльності угруповання становлять понад 80 млн доларів США.

У ході розслідування співробітники спецслужби встановили, що на території України діяла група осіб, яка використовувала шкідливе програмне забезпечення Egregor. З його допомогою хакери:

- шифрували комп'ютерні мережі іноземних компаній;
- викрадали персональні дані своїх клієнтів і працівників;
- викрадали інформацію про фінансові показники і технологічні розробки;
- блокували роботу вебресурсів.

Потім зловмисники вимагали великі суми грошей, найчастіше в криптовалюті, за дешифрування уражених комп'ютерних мереж і нерозголошення викрадених персональних даних [16].

Всього за минулий рік СБУ було розкрито 20 хакерських угруповань.

Значних збитків банківським установам можуть завдавати і окремі правопорушники. Так вже у 2021 році правоохоронці України викрили зловмисника – жителя Тернопільщини, який розробляв небезпечні онлайн-сервіси для атаки на банки та пошти.

У результаті використання таких зловмисних програм постраждали фінустанови 11 країн світу – США, Італії, Іспанії, Мексики, Чилі, Великої Британії, Нідерландів, Швейцарії, Австралії, Франції та Німеччини. Їхні збитки сягають понад $10 млн.

Встановлено, що правопорушник розробив спеціальну адмінпанель, що контролювала облікові записи користувачів, які вводили платіжні дані. В подальшому ці дані отримували зловмисники.

Окрім цього, зловмисник створював шахрайські сервіси для зламу пошти, яку використовують понад 1,5 млрд. користувачів.

Для продажу своїх розробок хакер створив інтернет-магазин у DarkNet, де було понад 200 покупців шкідливого програмного забезпечення [17].

Слід зазначити, що майже 98 % всіх кібератак ґрунтуються на тій чи іншій формі соціальної інженерії для доставки корисного навантаження, такого як шкідливі програми та програми-вимагачі. Один з найбільш успішних форматів атак, які кіберзлочинці регулярно використовують для проведення атак соціальної інженерії, – це фішингові електронні листи. Таким чином, зловмисники розповсюджують шкідливе ПО по електронній пошті приблизно в 92 % випадків [18].

Наприклад, у січні 2021 року було зафіксовано понад 400 тисяч фішингових атак. Зокрема, було виявлено масове розсилання електронних листів по державних установах нібито від Адміністрації Держспецзв'язку.

Файл, який містився в цих електронних листах, надавав доступ зловмисникам для дистанційного управління зараженим комп'ютером. Тобто особа, яка отримала доступ, мала можливість знищувати, копіювати, змінювати дані, що містяться на таких комп'ютерах.

Зазначається, що в більшості випадків вдалося уникнути негативних наслідків, але в деяких держустановах зловмисникам все-таки вдалося отримати доступ до комп'ютерів [19].

Для атак на об'єкти критичної інфраструктури організовані злочинні кіберугруповання використовують ***компрометацію постачальників*** засобів захисту інформації.

Так федеральні цивільні відомства США отримали розпорядження Американського агентства з питань кібербезпеки та інфраструктури проаналізувати свої мережі та негайно відключити продукти фірми SolarWinds Orion після кібератаки на неї.

Компанія SolarWinds, що базується в Остіні (США), допомагає своїм клієнтам керувати комп'ютерними мережами та контролювати їх на предмет можливого порушення даних. В своїх продуктах компанія використовує складні системи виявлення, включаючи доступ, події та управління журналами, щоб допомогти IT-командам легше контролювати та забезпечувати кібербезпеку.

SolarWinds продає технологічну продукцію великому переліку організацій критичної інфраструктури, включаючи всі п'ять родів американської армії. За межами США, SolarWinds уклав контракти з Національною службою охорони здоров'я Великобританії, Європейським Парламентом та НАТО, згідно з деталями на своєму веб-сайті. Компанія заявила, що має понад 300 000 клієнтів по всьому світу, включаючи велику кількість організацій з Fortune 500 [20].

Механізми вчинення кібератак постійно вдосконалюються. Починаючи з лютого 2021 року Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони фіксує масовані DDoS атаки на український сегмент Інтернет, переважно на веб-сайти сектору безпеки і оборони.

Зокрема атаки здійснювалися на сайти Служби безпеки України, Ради національної безпеки і оборони України, ресурси інших державних установ та стратегічних підприємств.

Встановлено, що джерелом цих атак були IP-адреси, які належать певним російським мережам обміну трафіком. Фахівці виявили, що зловмисники використовували новий механізм кібератак, який не спостерігався раніше під час подібних інцидентів.

Під час атаки вразливі веб-сервери державних органів інфікуються вірусом, який приховано робить їх елементом бот-мережі, що використовується для DDOS-атак на інші ресурси. При цьому системи безпеки Інтернет-провайдерів визначають скомпрометовані веб-сервери як джерело атак, та починають блокувати їх роботу шляхом автоматичного внесення до "чорних списків". Таким чином, навіть після закінчення фази DDoS атаковані веб-сайти залишаються недоступними для користувачів [21].

Особливо небезпечні тенденції спостерігаються останнім часом у сфері сексуального насильства та експлуатації дітей (Child Sexual Abuse Material – далі CSAM), що посилювалися значним збільшенням кількості людей, які працювали вдома, а також з тим, що діти проводять більше часу в Інтернеті, внаслідок чого збільшується попит на CSAM, що становить значну суспільну загрозу.

Співробітниками Департаменту кіберполіції України у 2020 році затримано 13 педофілів, що вдвічі більше за попередній період – 5.

Крім того діти шкільного віку, як нові, так і вже активні користувачі Інтернету, все частіше стають мішенню різноманітних нових видів онлайн-злочинів. Зокрема, злочинці проникають в онлайн класси, явище, що отримало назву "Zoom-бомбінг", і використовують грумінг і сексуальний шантаж по відношенню до дітей.

Також під час пандемії коронавірусу значно посилилася діяльність в соціальних мережах так званих "груп смерті" таких, як "Синій кит", "Море китів", "Біжи або вмри", "Розбуди мене в 4.20" та інші, які є вкрай небезпечні для дітей та підлітків.

Висновки.

Кіберзлочинність залишається однією з найбільш динамічних форм злочинності, яка постала перед правоохоронними органами усіх розвинутих країн. Хоча сьогодні програми-вимагачі, компрометація ділової електронної пошти та соціальна інженерія є звичними загрозами кіберзлочинності, їх виконання постійно еволюціонує та ускладнює цю злочинну діяльність для виявлення та розслідування. Технічний рівень інструментарію реалізації таких кіберзагроз постійно зростає. Особливе занепокоєння викликає використання для вчинення кібератак технологій штучного інтелекту, що призведе до зростання збитків від кіберзлочинності.

Сталий розвиток інформаційного суспільства залежить від багатьох чинників, до основних з яких слід віднести кіберзахист інформаційних систем та протидію кіберзлочинності.

Зважаючи на подальше зростання кількості кіберінцидентів Європейською Комісією 16 грудня 2020 року була представлена Нова Стратегія кібербезпеки. В документі, зокрема, зазначається, що питання до кібербезпеки є головним стримуючим фактором для використання Інтернет-послуг. Близько двох п’ятих користувачів із ЄС стикалися з проблемами безпеки, і три п’ятих відчувають, що не в змозі захиститися від кіберзлочинності. Третина отримувала шахрайські електронні листи або телефонні дзвінки з проханням ввести особисті дані за останні три роки, але ***83% ніколи не повідомляли про кіберзлочини***. Кожен восьмий бізнес постраждав від кібератак. Понад половина персональних комп’ютерів для бізнесу та споживачів, які інфікувалися шкідливим програмним забезпеченням, інфікуються повторно протягом року. Щорічно через витік даних втрачаються сотні мільйонів записів; середня вартість витоку для одного підприємства зросла до понад 3,5 млн EUR у 2018 році. Вплив кібератаки часто неможливо ізолювати, і він може спричинити ланцюгові реакції в економіці та суспільстві, охоплюючи мільйони людей [22].

Прийняття у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні планування у сфері забезпечення кібербезпеки та протидії кіберзлочинності [23]. Важливим етапом розвитку національної системи кібербезпеки стало прийняття Закону України “Про основні засади забезпечення кібербезпеки України”, який визначив завдання для основних суб’єктів національної системи кібербезпеки [5].

Водночас стан реалізації цієї стратегії був не на належному рівні. Багато запланованих завдань залишилися невиконаними [24]. Тому на заміну Стратегії 2016 року, яка діяла до 2020 року, постала необхідність підготувати новий стратегічний документ.

Відповідно до Рішення Ради національної безпеки і оборони України “Про Стратегію національної безпеки України” від 14.09.20 р., введеним в дію Указом Президента України від 14.09.20 р. № 392/2020, основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

Враховуючи світові тренди в глобальному кіберсередовищі як фактори впливу на розбудову національної системи кібербезпеки, робочою группою при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України було розроблено проєкт Стратегії кібербезпеки України на 2021 – 2025 роки, який схвалено 3 березня 2021 року, у якому визначено пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Основою для розроблення цього документу стали досвід кращих світових практик; ряд соціологічних опитувань та емпіричних досліджень, які були проведені наприкінці 2020 та на початку 2021 року.

Зокрема відповідно до зазначеного дослідження загальний рівень безпечного функціонування національного кіберпростору респонденти оцінюють на рівні 42 %. Рівень спроможності суб'єктів кібербезпеки протидіяти кіберзагрозам в державному секторі оцінюється як низький (на рівні 36 %), а для приватного сектора ця оцінка становить близько 62 %. При цьому головним недоліком в державному і в приватному секторах вважається їх недостатня забезпеченість технічними засобами.

Проведений аналіз доводить, що ландшафт загроз за останні роки суттєво не змінився і загрозами високого рівня залишаються: шкідливе програмне забезпечення, фішинг та інші прояви соціальної інженерії, DoS/DDoS-атаки та APTатаки. На найближчі 3 роки очікується збільшення ризиків за всіма типами загроз на рівні 41 %.

Отже, на сучасному етапі розвитку інформаційного суспільства слід суттєво посилити спроможності у протидії кіберзлочинності, задля чого необхідно:

провести аудит імплементації в українське законодавство положень Конвенції про кіберзлочинність та завершити цей процес шляхом внесення необхідних змін до законів України;

врегулювати на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики та підхід країн-членів ЄС з цих питань;

вдосконалити законодавство України, передбачивши внесення необхідних змін з урахуванням сучасних викликів та тенденцій у сфері кібербезпеки;

запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

врегулювати на законодавчому рівні правовий статус криптовалют, визначити правові механізми щодо операцій із криптовалютами та створення ринків;

проводити інші заходи задля створення відкритого, вільного, стабільного і безпечного кіберпростору, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток.

Використана література

1. Понад 500 000 облікових записів Zoom продано на форумах хакерів, темної мережі. URL: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web

2. Словник іншомовних слів ; за ред. члена-кореспондента АН УРСР О.С. Мельничука. Київ: Головна редакція "Українська радянська енциклопедія". 1977. 776 с.

3. Ускладнення COVID-19: пандемія дезінформації і загроза кібербезпеці. URL: https://nv.ua/ukr/biz/experts/pandemiya-covid-19-chas-dlya-kiberatak-i-feykiv-yak-zahistiti-sebe-i-biznes-ostanni-novini-50123696.html

4. The Hidden Costs of Cybercrime. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

5. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 01.01.19 р. / М.В. Гуцалюк та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

6. З початку 2020 року до кіберполіції надійшло понад 25 тисяч звернень щодо Інтернет-шахрайства. URL: https://cyberpolice.gov.ua/news/z-pochatku--roku-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-internet-shaxrajstva-6472

7. Гуцалюк М.В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*. № 3(34)/2020. С.75-87. URL: http://il.ippi.org.ua/article/view/220997

8. INTERPOL report shows alarming rate of cyberattacks during COVID-19. URL: https://www.interpol.int/News-and-Events/News/2020/COVID-19-crime-INTERPOL-issues-new-guideli nes-for-law-enforcement

9. Як на хвилі коронавірусу спекулянти намагаються збагатитися на eBay, Amazon, OLX, Prom.ua, Rozetka, Tabletki.ua та Liki24.com. URL: https://www.epravda.com.ua/publications/2020/03/19/658264

10. Фішингові атаки від фейкового МОЗ на тему вакцинації зафіксували в Україні. URL: https://www.pravda.com.ua/news/2021/02/12/7283229

11. На Харківщині судитимуть членів злочинної організації за шахрайські схеми оформлення онлайн-кредитів на громадян. URL: https://www.cyberpolice.gov.ua/news/na-xarkivshhyni-sudytymut-chleniv-zlochynnoyi-organizacziyi-za-shaxrajski-sxemy-oformlennya-onlajn-kredy tiv-na-gromadyan-5881

12. North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report. URL: https://edition.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk/index.html

13. CYBERCRIME AND COVID19: Risks and Responses. URL: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

14. US charges three North Koreans over $1.3bn theft. URL: https://www.bbc.com/news/technology-56103921

15. Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі комп'ютерного вірусу "EMOTET". URL: https://www.pravda.com.ua/news/2021/01/27/7281395

16. СБУ ліквідувала транснаціональне хакерське угруповання. URL: https://ua.korrespondent.net/ukraine/4328488-sbu-likviduvala-transnatsionalne-khakerske-uhrupovannia

17. Кіберполіція викрила найбільший у світі сервіс для атак на банки. URL: https:// fakty.com.ua/ua/proisshestvija/20210204-kiberpolitsiya-vykryla-najbilshyj-u-sviti-servis-dlya-atak-na-banky

18. Исследование: ущерб от киберпреступности в 2020-м по всему миру составил более 1 триллиона долларов. URL: https://internetua.com/issledovanie-usxerb-ot-kiberprestupnosti-v-2020-m-po-vsemu-miru-sostavil-bolee-1-trilliona-dollarov

19. В Україні з початку року вже майже 14 млн. кіберінцидентів. URL: https://ua.korrespondent.net/ukraine/4321796-v-ukraini-z-pochatku-roku-vzhe-maizhe-14-mln-kiberintsydentiv

20. Suspected Russian Hackers Gained Edge Through Tech Firm Attacks. URL: https://www.bloomberg.com/news/articles/2021-01-29/solarwinds-attackers-hit-strategic-targets-cyber-and-tech-firms

21. У РНБО попередили про новий механізм атак на українську інфраструктуру. URL: https://lb.ua/news/2021/02/22/478317_rnbo_poperedili_pro_noviy_mehanizm.html

22. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

23. DR Mykhaylo Gutsalyuk Ukraine's Cybersecurity strategy and ways to implement it. *European Cybersecurity journal*. Volume 2 (2016). The Kosciuszko Institute. Poland. P. 65-69.

24. Гуцалюк М.В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик. *Інформація і право*. № 2(29)/2019. С. 90-99.

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

УДК 343.3/.7

КУЧЕРИНА С.Є., *кандидат військових наук, доцент,* провідний науковий співробітник науково-дослідної лабораторії військового права, права національної та міжнародної безпеки НДІ інформатики і права НАПрН України.
ОЛЄЙНІКОВ Д.О., *кандидат юридичних наук,* начальник відділу наукової та науково-дослідної роботи ІПЮК для СБУ НЮУ ім. Ярослава Мудрого.
ORCID: https://orcid.org/0000-0002-8515-5241.

СУЧАСНИЙ СТАН КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *У роботі здійснено науковий аналіз сучасного стану норм кримінального права, які встановлюють кримінальну відповідальність за посягання на об'єкти критичної інфраструктури чи на їх інформаційну інфраструктуру, та оцінено їх ефективність з точки зору системності кримінально-правової охорони. Виявлено, що наразі рівень кримінально-правової охорони об'єктів критичної інфраструктури є недостатнім та безсистемним. Це обумовлено: відсутністю у законодавстві, яке встановлює кримінальну відповідальність за суспільно небезпечні діяння, індивідуалізованого підходу до критичної інфраструктури взагалі та її об'єктів зокрема; не врахуванням у кримінальному праві сучасного розвитку організаційно-правових засад критичної інфраструктури та ін. Авторами запропоновані конкретні кроки, що сприятимуть захищеності вітчизняної критичної інфраструктури кримінально-правовими засобами.*

Ключові слова: *об'єкти критичної інфраструктури, об'єкти критичної інформаційної інфраструктури, кримінальна відповідальність, кримінально-правова охорона.*

Summary. *The scientific analysis of the current state of criminal law, which establishes criminal liability for encroachment on critical infrastructure or their information infrastructure, and evaluates their effectiveness in terms of systemic criminal law protection. It is revealed that currently the level of criminal protection of critical infrastructure is insufficient and unsystematic. This is due to: the lack of legislation that establishes criminal liability for socially dangerous acts, an individualized approach to critical infrastructure in general and its facilities in particular; not taking into account in criminal law the modern development of organizational and legal principles of critical infrastructure, etc. The authors propose concrete steps that will contribute to the protection of domestic critical infrastructure by criminal law.*

Keywords: critical infrastructure facilities, critical information infrastructure facilities, criminal liability, criminal law protection.

Аннотация. *В работе осуществлен научный анализ современного состояния норм уголовного права, устанавливающих уголовную ответственность за посягательство на объекты критической инфраструктуры или на их информационную инфраструктуру, и оценена их эффективность с точки зрения системности уголовно-правовой охраны. Выявлено, что существующий уровень уголовно-правовой охраны объектов критической инфраструктуры является недостаточным и бессистемным. Это обусловлено: отсутствием в законодательстве, которое устанавливает уголовную ответственность за общественно опасные деяния, индивидуализированного подхода к критической инфраструктуры вообще и ее объектов в частности; игнорированием уголовным правом современного развития организационно-правовых основ критической инфраструктуры и др. Авторами предложены конкретные шаги, которые поспособствуют защищенности отечественной критической инфраструктуры уголовно-правовыми средствами.*

Ключевые *слова: объекты критической инфраструктуры, объекты критической информационной инфраструктуры, уголовная ответственность, уголовно-правовая охрана.*

Постановка проблеми. Реалії сьогодення переконливо демонструють удосконалення й переорієнтацію форм і методів глобального деструктивного впливу в площину кіберпростору, що дозволяє досягати більш руйнівного злочинного результату із задіянням новітніх технологій. З цього приводу О.П. Єрменчук підкреслює, що "…Україна протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки. Військовий конфлікт на сході країни, торгівельні війни, економічна експансія, різке посилення тероризму, небувалий ріст злочинності, руйнування та пошкодження численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, втрата новітніх технологій – все це та інші ризики вимагають від держави нових підходів до завчасного виявлення загроз та їх попередження і припинення" [1, с. 5]. При цьому, як зауважує О.М. Суходоля, система захисту критичної інфраструктури має будуватися виходячи з необхідності реагування на комплекс загроз та їх узгоджену реалізацію і спрямовуватися на забезпечення стійкості функціонування системи життєдіяльності суспільства, національної економіки та держави. Це завдання не може бути забезпечене лише заходами посилення фізичної охорони окремих об'єктів [2, с. 74].

Як свідчить попередній аналіз, кримінально-правова охорона критичної інфраструктури в Україні значно відстає від темпів розвитку злочинності у кіберпросторі та сфері інформаційної безпеки держави взагалі. Означена обставина, а також окремі нормотворчі ініціативи щодо об'єктів критичної інфраструктури обумовлюють необхідність активізації наукового аналізу в напрямку вироблення дієвого та сучасного механізму кримінально-правової охорони критичної інфраструктури в Україні.

Результати аналізу наукових публікацій. В принципі, наукові роботи, які досліджують ті або інші питання забезпечення безпеки об'єктів критичної інфраструктури, можна поділити на декілька напрямів:

- організаційно-правові засади забезпечення кібербезпеки об'єктів критичної інфраструктури. В зазначеному напрямі наукові розвідки здійснювали такі фахівці як В. Абрамов, В. Білоус, О. Довгань, І. Доронін, О. Насвіт, А. Пашков, А. Тарасюк, Т. Ткачук, І. Уряднікова, Л. Щаслива та інші;

- кримінально-правова охорона об'єктів критичної інфраструктури. Цей напрям досліджували Д. Пашнєв, О. Сандул, Т. Созанський, О. Суходоля, А. Таран та інші.

Наукові здобутки та висновки вказаних вчених покладено в основу дослідження, окремі положення набули подальшого розвитку. Разом з цим, динаміка соціальних, політичних та технічних перетворень в суспільстві є настільки гострою, а нормотворчі ініціативи численними, що обрана тематика навряд чи втратить свою актуальність найближчими роками.

Метою статті є аналіз сучасного стану кримінально-правової охорони об'єктів критичної інфраструктури та вироблення пропозицій щодо її удосконалення.

Виклад основного матеріалу. Рішенням Ради національної безпеки і оборони України "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29.12.16 р. введеним в дію Указом Президента України від 16.01.17 р. № 8/2017, Кабінету Міністрів України було доручено поетапно: 1) розробити за участю Національного інституту стратегічних досліджень і схвалити концепцію створення державної системи захисту критичної інфраструктури та план заходів з її

реалізації; 2) після схвалення концепції створення державної системи захисту критичної інфраструктури розробити за участю Служби безпеки України, Служби зовнішньої розвідки України і Національного банку України та внести в установленому порядку на розгляд Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист", в якому передбачити врегулювання питань, зокрема, щодо:

- створення державної системи захисту критичної інфраструктури;
- визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;
- визначення функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;
- запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;
- запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації;
- засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури;
- міжнародного співробітництва у сфері захисту критичної інфраструктури.

Трохи менше, ніж через рік, після вказаного вище Рішення РНБО України було прийнято Закон України "Про основні засади забезпечення кібербезпеки України", в якому міститься законодавча дефініція об'єктів критичної інфраструктури. Так, відповідно до п. 16 ч. 1 ст. 1 вказаного Закону, до критично важливих об'єктів інфраструктури (об'єктів критичної інфраструктури) віднесені підприємства, установи та 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.

Наступний термін, який в контексті досліджуваної теми має важливе значення, визначений у п. 19 згаданої норми. Так, об'єкт критичної інформаційної інфраструктури – це комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Таким чином, ми маємо дворівневий об'єкт, що складається власне з об'єкта критичної інфраструктури та його комунікаційної або технологічної системи, яка є уразливою для кібератак. Іншими словами, інформаційна інфраструктура є захисною надбудовою над об'єктом критичної інфраструктури, призначення якої – захищати сам об'єкт від деструктивного впливу в кіберпросторі. О.П. Єрменчук вказує, що провідні світові держави, поряд з фізичною інфраструктурою, виділяють та здійснюють захист кіберкритичної інфраструктури [2, с. 13]. І дійсно, наприклад, у Плані захисту критичної інфраструктури США від 2015 р. закріплено, що забезпечення безпеки та стійкості фізичної та кіберкритичної інфраструктури сприяє мінімізації наслідків від дії загроз та сприяє її швидкому відновленню [3].

Механізм формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури в Україні визначається Порядком формування переліку

об'єктів критичної інформаційної інфраструктури, затвердженим постановою Кабінету Міністрів України від 9 жовтня 2020 року № 943. Зазначеним Порядком безпека об'єкта критичної інфраструктури визначається як стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг. Під захистом об'єктів критичної інформаційної інфраструктури розуміються організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інформаційної інфраструктури [4].

Причини створення дворівневого об'єкта на базі об'єкта критичної інфраструктури мають свою логіку в контексті того, що "захист критичної інфраструктури поєднує три основні напрями: 1) захист від загроз у сфері державної безпеки; вони можуть включати внутрішні загрози та фізичне знищення КІ; 2) захист від кіберзагроз; 3) захист від надзвичайних ситуацій" [1, с. 14]. Враховуючи технологічні особливості окремих об'єктів критичної інфраструктури, їх власники змушені створювати технологічні системи як для управління циклом діяльності, так і з метою попередження зупинки чи руйнування об'єкта внаслідок, наприклад, помилки, техногенної аварії чи стихійного лиха. З одного боку, така ускладнена структура забезпечує захист об'єкта від зазначених вище загроз, з іншого ж боку, об'єкт стає більш уразливим за рахунок необхідності захищати також і саму інформаційну інфраструктуру.

Переходячи до суті кримінально-правової охорони, погодимось із В.В. Кузнецовим, який визнає її як, по-перше, певну систему кримінально-правових засобів, до яких слід включити кримінально-правові норми (заборонні, роз'яснювальні, заохочувальні та обмежувальні) та методи кримінально-правової політики (криміналізація та декриміналізація, пеналізація та депеналізація), за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин [5, с. 109]. Чим обумовлені особливості вітчизняної кримінально-правової охорони критичної інфраструктури?

По-перше, існуючі норми розраховані, перш за все, на протидію внутрішнім загрозам, та є мало орієнтованими на сучасну динаміку та еволюцію злочинної діяльності як у кіберпросторі, так і в реальному середовищі.

По-друге, вітчизняним законодавцем так і не сформовано ефективний кримінально-правовий інститут, який би поєднував багаторівневий захист об'єктів критичної інфраструктури та їх інформаційної інфраструктури як від внутрішніх, так і від зовнішніх загроз.

Об'єкти критичної інфраструктури як окремий об'єкт злочину не розглядаються наукою кримінального права, тому їх кримінально-правова охорона здійснюється через відповідні кримінально-правові норми, які розміщені законодавцем в різних розділах Особливої частини Кримінального кодексу України (далі – КК України). Так, існуючі норми КК України в контексті кримінально-правового захисту об'єктів критичної інфраструктури встановлюють кримінальну відповідальність за:

1) умисне знищення чи пошкодження майна (ст. 194 КК України).

М.І. Мельник та М.І. Хавронюк називають основним безпосереднім об'єктом цього злочину право власності. Додатковим факультативним об'єктом, на їх думку, можуть виступати громадський порядок, екологічна безпека, життя і здоров'я людини. Що стосується предмету злочину, то ним може бути будь-яке майно як рухоме, так і нерухоме, крім окремих його видів, знищення чи пошкодження яких передбачено КК України як спеціальний вид знищення чи пошкодження майна [6, с. 531]. Ця норма є

“базовою”, оскільки виключає наявність спеціальних ознак суб’єктивної сторони складу злочину.

Проте, необхідно враховувати, що здійснення особою суспільно небезпечної діяльності, яка виразилась в посяганні на об’єкти критичної інфраструктури, в більшості випадків матиме досить специфічну мету чи мотиви. Так, якщо кінцевою метою посягання на об’єкт критичної інфраструктури є, наприклад, масове знищення рослинного або тваринного світу, отруєння атмосфери або водних ресурсів, які відбудуться внаслідок знищення такого об’єкта, вчинене додатково слід кваліфікувати за ст. 441 КК України. У разі, коли посягання на об’єкт критичної інфраструктури вчиняється в контексті надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України, то вчинене додатково має кваліфікуватись за ч. 1 ст. 111 КК України.

2) Враховуючи, що, відповідно до п. 1 ч. 1 ст. 6 Закону України “Про основні засади забезпечення кібербезпеки”, до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, умисне пошкодження або руйнування об’єктів електроенергетики, якщо ці дії призвели або могли призвести до порушення нормальної роботи цих об’єктів, або спричинили небезпеку для життя людей, може кваліфікуватись за ст. 194-1 КК України;

3) диверсію (ст. 113 КК України), в тому випадку, коли особа, яка вчинила посягання на об’єкт критичної інфраструктури, прагнула ослабити державу. При цьому автори Науково-практичного коментаря до Розділу І Особливої частини КК України відносять об’єкти, які є невід’ємними складовими національної безпеки України та мають важливе народногосподарське чи оборонне значення, до предмету диверсії [7, с. 140]. Погоджуючись із означеною точкою зору, зауважимо, що, за відсутності мети ослабити державу та наявності іншої мети кримінально-правова оцінка посягання на сам об’єкт критичної інфраструктури буде іншою;

4) терористичний акт (ст. 258 КК України), якщо посягання на об’єкт критичної інфраструктури було вчинено з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста).

В контексті розглядуваного злочину необхідно згадати про термін “кібертероризм”, який введено Законом України “Про основні засади забезпечення кібербезпеки України”. Кібертероризм вважають одним із видів технологічного тероризму – злочинів, 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, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, 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 [8, с. 21]. Разом з цим в КК України відсутні спеціальні норми (чи частини статей), які б виділяли кібертероризм в окремий склад злочину;

5) напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення (ст. 261 КК України) – напад на об'єкти, на яких виготовляються, зберігаються, використовуються або якими транспортуються радіоактивні, хімічні, біологічні чи вибухонебезпечні матеріали, речовини, предмети, з метою захоплення, пошкодження або знищення цих об'єктів;

6) пошкодження шляхів сполучення і транспортних засобів (ст. 277 КК України) ядерної енергетики [9, с. 62].

В принципі, наведений перелік варіантів кримінально-правової оцінки суспільно небезпечних діянь, пов'язаних із посяганнями на об'єкти критичної інфраструктури, не є вичерпним, та, в залежності від конкретних ситуацій, може бути продовжений в багатьох напрямках. Означена обставина чітко вказує на розпорошеність відповідних норм, які можуть бути застосовані як засіб кримінально-правової охорони об'єктів критичної інфраструктури. Причина цього, як вказувалось вище, полягає в тому, що об'єкти критичної інфраструктури не розглядаються наукою кримінального права як окремі об'єкти злочину.

Що стосується спеціальної кримінально-правової охорони критичної інформаційної інфраструктури, то на її необхідності, "зважаючи на зростання негативних наслідків для держави, які завдаються кібератаками на інформаційну інфраструктуру органів державної влади, та на можливу шкоду, пов'язану з можливими кібератаками на промислові та інші об'єкти критичної інфраструктури, їх підвищену суспільну небезпечність" [10, с. 75], свого часу наголошував Д.В. Пашнєв.

У вітчизняному законодавстві містяться нереалізовані спроби впровадження кримінальної відповідальності за посягання на критичну інформаційну інфраструктуру. Так, Законом України "Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян" від 16.01.14 р. № 721-VII [11] були криміналізовані:

- несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури (ст. 361-3 КК України);

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що оброблюється в державних електронних інформаційних ресурсах (ст. 361-4 КК України);

- несанкціоновані дії з інформацією, що оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах критичних об'єктів національної інформаційної інфраструктури, вчинені особою, яка має право доступу до такої інформації (ст. 362-1 КК України).

Наведені вище норми так і не стали підґрунтям до кримінально-правової охорони критичної інформаційної інфраструктури, оскільки Закон України від 16.01.14 р. № 721-VII втратив чинність на підставі Закону України "Про визнання такими, що втратили чинність, деяких законів України" від 28.01.14 р. № 732-VII [12]. Разом з цим, навіть і з цих норм кримінально-правова охорона критичної інформаційної інфраструктури встановлювалась фактично лише ст. 361-3 КК України. Вказана норма передбачала кримінальну відповідальність за суспільно небезпечне діяння, яке виразилось в несанкціонованому втручанні в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури, що призвело до витоку,

втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Разом з цим, наприклад, в КК РФ передбачена кримінальна відповідальність за неправомірний вплив на критичну інформаційну структуру РФ (ст. 274.1), до якої може бути притягнуто особу за:

- створення, розповсюдження і (чи) використання комп'ютерних програм чи іншої комп'ютерної інформації, завідомо призначених для неправомірного впливу на критичну інформаційну інфраструктуру РФ, у тому числі для знищення, блокування, модифікації, копіювання інформація, яка в ній міститься, чи нейтралізації засобів захисту вказаної інформації;

- неправомірний доступ до охоронюваної комп'ютерної інформації, яка міститься в критичній інформаційній інфраструктурі РФ, у тому числі з використанням комп'ютерних програм чи іншої комп'ютерної інформації, які завідомо призначені для неправомірного впливу на критичну інформаційну інфраструктуру РФ, чи інших шкідливих комп'ютерних програм, якщо він призвів до завдання шкоди критичній інформаційній інфраструктурі РФ;

- порушення правил експлуатації засобів зберігання, обробки чи передачі охоронюваної комп'ютерної інформації, що міститься в критичній інформаційній інфраструктурі РФ, чи інформаційних систем, інформаційно-телекомунікаційних мереж, автоматизованих систем управління, мереж електрозв'язку, що відносяться до критичної інформаційної інфраструктури РФ, або правил доступу до вказаних інформації, інформаційних систем, інформаційно-телекомунікаційних мереж автоматизованих систем управління, мереж електрозв'язку, якщо це призвело до завдання шкоди критичній інформаційній інфраструктурі РФ [13].

Наразі ж перераховані вище дії, що розцінюються як неправомірний вплив на критичну інформаційну інфраструктуру, в вітчизняному законодавстві можуть бути кваліфіковані за відповідною нормою, яка міститься в Розділі XVI КК України (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку). В цьому контексті вважаємо абсолютно доцільним погодитись із окремими висновками Д.П. Пашнєва, які він зробив ще в 2014 році. Так, вказаний учений підкреслював, що зміст статей, які призвані охороняти інформаційно-телекомунікаційні системи від суспільно небезпечних посягань (ст. 361 – 363-1 КК України), суперечить підходу іноземних країн до кримінально-правової охорони державних інформаційних ресурсів, оскільки державні інформаційно-телекомунікаційні системи та інформаційні ресурси є лише окремим видом предмету складів цих злочинів, поряд з іншими, посягання на які мають значно нижчий ступінь суспільної небезпечності. Це не дозволяє виокремити особливості суспільно небезпечних діянь, вчинених з використанням комп'ютерних технологій проти інформаційно-телекомунікаційних систем державного та суспільного значення, індивідуалізувати відповідальність осіб, які їх вчинили [10, с. 79].

О.В. Таран і О.Г. Сандул, проаналізувавши стан кримінально-правової охорони об'єктів критичної інфраструктури в ядерній енергетиці, зауважили, що, "зважаючи на те, що наразі тільки відбувається формування спеціального законодавства, триває створення переліку об'єктів критичної інфраструктури, доцільно говорити про перспективи удосконалення КК України" [9, с. 65]. Такі удосконалення, на думку згаданих фахівців, мають полягати у "запровадженні окремої норми (норм), якою буде передбачено кримінальну відповідальність за посягання на об'єкти критичної інфраструктури. На теперішній час кримінально-правовою охороною охоплюється лише

частина таких об’єктів. Звичайно, у кримінально-правовій нормі не доцільно передбачати увесь перелік об’єктів критичної інфраструктури, адже по-перше, він значний за обсягом, а по-друге, зміни і доповнення до цього переліку, які будуть вноситись за результатами його періодичного перегляду, потребуватимуть відповідних змін до КК України. Тому диспозиція правової норми очевидно матиме бланкетний характер. У чинному КК України відповідні норми розміщені у різних його розділах, а отже мають різний родовий об’єкт, що не відповідає загальній концепції критичної інфраструктури. Отже, доповнення існуючих правових норм відповідними частинами з метою диференціації кримінальної відповідальності за такі злочини не вирішить зазначених проблем. Тому відповідну норму (норми) потрібно передбачити у Розділі І Особливої частини КК “Злочини проти основ національної безпеки України” [9, с. 65].

Можемо погодитись із висновками О.В. Тарана і О.Г. Сандула в частині того, що відсутність єдиного родового об’єкта не відповідає загальній концепції критичної інфраструктури. Одночасно заперечимо доцільність впровадження кримінальної відповідальності за посягання на об’єкт критичної інфраструктури (чи критичної інформаційної інфраструктури) у Розділі І Особливої частини КК України “Злочини проти основ національної безпеки України”, оскільки така норма буде спеціальною по відношенню до ст. 113 КК України, що навряд чи вирішить саму проблему в цілому.

Висновки та пропозиції.

Результати наукового аналізу свідчать про те, що рівень кримінально-правової охорони об’єктів критичної інфраструктури наразі є недостатнім та безсистемним. До основних недоліків відноситься: 1) у законодавстві, яке встановлює кримінальну відповідальність за суспільно небезпечні діяння, відсутній індивідуалізований підхід до критичної інфраструктури взагалі та її об’єктів зокрема. Як було доведено, кримінально-правова охорона об’єктів критичної інфраструктури здійснюється лише в контексті кримінально-правової охорони інших об’єктів більш загального характеру (власність, громадська безпека, економічна безпека і т.п.), а самі об’єкти розглядаються на рівні предмета злочину; 2) наразі посягання на об’єкт критичної інфраструктури, яке вчиняється у кіберпросторі шляхом втручання в інформаційну інфраструктуру, розглядається як сукупність злочинів, хоча, і це цілком очевидно, вони співвідносяться як суспільно небезпечне діяння та спосіб його вчинення. Означене досить яскраво вказує на спорадичність кримінально-правової охорони об’єктів критичної інфраструктури та в подальшому може призвести до формування неоднорідної слідчо-судової практики з цих питань; 3) законодавство про кримінальну відповідальність не враховує сучасний розвиток організаційно-правових засад критичної інфраструктури, внаслідок чого втрачає здатність повною мірою охороняти інтереси держави і суспільства, які реалізуються через можливості критичної інфраструктури.

Враховуючи наведене вище, вважаємо, що в першу чергу необхідно переглянути перелік загальних об’єктів кримінально-правової охорони, передбачений ст. 1 КК України, та визначити за вертикаллю роль і місце критичної інфраструктури на рівні, наприклад, видового об’єкту, а конкретних об’єктів критичної інфраструктури – безпосереднього. В залежності від виду родового об’єкту, до якого критична інфраструктура увійде як видовий об’єкт, надалі потрібно впровадити норму про кримінальну відповідальність за посягання на об’єкт критичної інфраструктури. Також, за необхідності доцільно передбачити в статтях інших розділів КК України (наприклад, ст. 194, 258 і т.і.) посягання на об’єкт критичної інфраструктури в якості кваліфікуючої обставини, яка обтяжує покарання.

Ці та подальші кроки, на нашу думку, безперечно, сприятимуть захищеності вітчизняної критичної інфраструктури кримінально-правовими засобами та нададуть можливість в подальшому зрушити з місця застарілі нормативно-правові конструкції законодавства про кримінальну відповідальність.

Використана література

1. Єрменчук О.П. Основні підходи до орґанізації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

2. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62-76.

3. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication

4. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, затверджений постановою Кабінету Міністрів України від 9.10.20 р. № 943URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

5. Кузнецов В. В. Кримінально-правова охорона: проблеми визначення поняття. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2015. Вип. 30(2). С. 107-110.

6. Науково-практичний коментар Кримінального кодексу України ; за ред. М.І. Мельника, М.І. Хавронюка. 7-ме вид., переробл. та допов. Київ: Юридична думка, 2010. 1288 с.

7. Сичевський В.В., Харитонов Є.І., Олєйніков Д.О. Науково-практичний коментар до Розділу І Особливої частини Кримінального кодексу України (Злочини проти основ національної безпеки України). Харьків: Право, 2016. 232 с.

8. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 1.01.19 р. / М.В. Гуцалюк та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

9. Таран О.В. Сандул О.Г. Проблеми кримінальної відповідальності за посягання на об'єкти критичної інфраструктури в ядерній енергетиці. *Ядерна та радіаційна безпека*. 2019. Вип. 3. С. 58-67.

10. Пашнєв Д.В. Необхідність спеціальної кримінально-правової охорони критичної інформаційної. *Вісник Кримінологічної асоціації України*. 2014. № 6. С. 73-82.

11. Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян: Закон України від 16.01.14 р. № 721-VII. *Голос України*. № 10. (21.01.2014 р.). URL: https://zakon.rada.gov.ua/laws/show/721-18#Text

12. Про визнання такими, що втратили чинність, деяких законів України: Закон України від 28.01.14 р. № 732-VII. *Голос України*. № 19. (01.02.2014 р.). URL: https://zakon.rada.gov.ua/laws/show/732-18#Text

13. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 27.10.2020 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_10699

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

УДК 343.14:004

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid/0000-0002-2488-7377.
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid/0000-0003-3302-1601.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ З КЛАСИФІКАЦІЇ, ІДЕНТИФІКАЦІЇ ТА ФІКСАЦІЇ КІБЕРЗЛОЧИНІВ

Анотація. *Стаття присвячена аналізу напрямів удосконалення методичного забезпечення експертних досліджень програмних засобів, призначених для негласного доступу до комп'ютерної інформації. В межах статті досліджуються актуальні питання методичного забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів на базі запропонованих методичних підходів у сфері протидії кіберзлочинності.*

Ключові слова*: інформаційна безпека, кібербезпека, кіберзлочинність, комп'ютерний злочин, механізм слідоутворення, шкідливі програмні засоби, спеціальний програмний засіб негласного отримання інформації.*

Summary*. The article is devoted to the analysis of directions of improvement of methodical maintenance of expert researches of the software intended for obtaining covert access to the computer information. Within the limits of the article the topical questions of methodical support of measures on classification, identification and fixing of cybercrimes on the basis of the offered methodical approaches in the field of counteraction to cybercrime are investigated. The approach proposed in the article on the study of software involves the integrated application of various research methods, including methods of monitoring the activity of software and the implementation of appropriate types of expert tasks in computer technical expertise and area of expertise of special technical means of covert access to information. It is noted that one of the important areas of improving the methodological support for combating cybercrime is the introduction of methodological materials to ensure the conduct of expert research on special software designed for obtaining covert access to information. The article concludes that the proposed approaches can serve as a methodological basis for the development of methods, tools and identification technology, fixation of cybercrime in the field of combating cybercrime*

Keywords*: information security, cybersecurity, cybercrime, computer crime, tracing mechanism, harmful software, special software for covert access to information.*

Аннотация*. Статья посвящена анализу направлений усовершенствования методического обеспечения экспертных иследований програмных средств, предназначеных для негласного доступа к компьютерной информации. В рамках статьи исследуются актуальные вопросы методического обеспечения мер по класификации, идентификации и фиксации киберпреступлений на основе предложенных методических подходов в сфере противодействия киберпреступности.*

Ключевые слова*: информационная безопасность, кибербезопасность, киберпреступность, компьютерное преступление, механизм следообразования, вредные програмные средства, специальное программное средство негласного получения информации.*

Постановка проблеми. Кіберзлочинність є сьогодні однією з найгостріших проблем захисту інформаційної безпеки держави. Глибокі зміни, спричинені переходом на цифрові технології, триваюча глобалізація комп'ютерних мереж, розробка новітніх телекомунікаційних пристроїв створюють умови для зростання кіберзлочинності як в Україні, так і за її межами.

Сьогодні більшість фахівців у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. У 2008 році щорічна шкода від кіберзлочинності оцінювалася експертами ОБСЕ приблизно у 100 млрд. доларів [1]. У 2020 році збитки світової економіки від кіберзлочинності оцінювались у $ 1 трлн., що складає понад один відсоток світового ВВП [2].

Революційне зростання кіберзлочинності з використанням сучасних інформаційних технологій на початку XXI століття можна порівняти з появою ядерної зброї, небезпечний руйнівний потенціал якої обумовив впровадження правових підстав її застосування. Масштаб та поява нових способів і методів кіберзлочинів зумовлює потребу подальших досліджень цієї тематики, спрямованих на удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності [3, с. 99].

Актуальність проблем протидії кіберзлочинності в умовах сьогодення потребує розробки криміналістичної теорії стосовно тактики проведення слідчих дій, методик та результативних методів, що спрямовані на збирання та дослідження криміналістичної значимої комп'ютерної інформації [4; 5].

Результати аналізу наукових публікацій. Основи криміналістичної теорії досліджень злочинів у сфері комп'ютерної інформації були закладені відносно недавно (наприкінці 1990-х – початку 2000-х років) у роботах Ю.М. Батурина, О.В. Ботвінкіна [4], В.Б. Вехова, О.П. Войтовича, В.Д. Гавловського [5], В.В. Голубєва [6], В.В. Крилова, С.А. Лапина, В.А. Мещерякова, В.В. Полякова, Н.А. Селиванова, Е.Р. Росинска, А.І. Усов, О.М. Черкуна, О.К. Юдіна та ін.

Особливе значення для криміналістичної теорії й практики мало запровадження в науковий обіг таких нових понять, як віртуальні сліди, електронні докази, формулювання базових принципів слідчих дій [6, с. 64]. При цьому широкий спектр комп'ютерних злочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховання або змін комп'ютерної інформації щодо слідів злочину.

У дослідженні судової комп'ютерно-технічної експертизи значну роль відіграли праці таких вчених, як Е.Р. Росинска та А.І. Усов. У той же час, малодослідженою залишається така важлива окрема криміналістична теорія, як доведення ознак, обставин, способів здійснення злочинів у сфері комп'ютерної інформації.

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96, зазначається, що боротьба з кіберзлочинністю повинна передбачати, зокрема, здійснення заходів з удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень [7]. Це обумовлює актуальність проведення досліджень криміналістичної характеристики злочинів у сфері комп'ютерної інформації, техніко-криміналістичних засобів і методів, тактико-криміналістичних та організаційно-криміналістичних прийомів слідчих дій [4; 8].

Слід підкреслити, що дослідження з позицій криміналістичної теорії зустрічаються зі значними труднощами, обумовленими як складністю цих високотехнологічних злочинів, високим рівнем їх латентності, так і відносно незначною кількістю їх судового

розгляду, що ускладнюють узагальнення слідчої, судової та експертної практики [6]. Є численні невирішені питання в сфері криміналістичної характеристики злочинів, пов'язаних з неправомірним доступом до комп'ютерної інформації, тактики проведення слідчих дій та методики їх експертного дослідження.

Метою статті є удосконалення методичного забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів.

Виклад основного матеріалу. Кіберзброя як інструмент кіберзлочинності характеризується такими ознаками, як цілеспрямованість, вибірковість, розосередженість, швидкість доставки, масштабність та досяжність впливу, комплексність впливу на технічні засоби, системи і людей, регулювання (дозування) "потужності" впливу, що зближує її зі зброєю масового ураження [3, с. 99].

Підвищення результативності протидії кіберзлочинності безумовно потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях [5, с. 110].

Одним із важливих напрямів забезпечення діяльності правоохоронних органів з розслідування кіберзлочинів є удосконалення нормативно-методичного забезпечення слідчих дій та експертних досліджень стосовно кіберзлочинів, зокрема удосконалення методів і технологій ідентифікації та фіксації кіберзлочинів за результатами практики застосування кримінально-правових норм та результатів експертних досліджень у цій сфері [3, с. 99].

Кіберзлочини завжди здійснюються з використанням засобів комп'ютерної техніки. До цих засобів відносяться комп'ютери в різноманітних варіантах їх виконання (ноутбуки, планшети, смартфони, тощо) з використанням телекомунікаційних технологій (бездротові Wi-Fi, Bluetooth, WiMAX тощо), а також комп'ютерне програмне забезпечення як загального використання, наприклад, Opera, Mozilla Firefox, так і програмне забезпечення, використання якого заборонено, наприклад, SpyEye, Zeus, Carberp тощо [9, с. 162].

Як свідчить сучасна практика слідчих дій, в переважній більшості випадків кіберзлочини (кібертероризм, кібершпигунство) здійснюються шляхом віддаленого несанкціонованого доступу до комп'ютерів, комп'ютерних систем, комп'ютерних мереж та мереж електрозв'язку за допомогою комп'ютерної техніки загального використання, на яку встановлюється спеціально розроблене програмне забезпечення, наприклад, Dugu, Wiper, Flame, Gauss, Madi, Narilam [9 с. 164].

Для визначення напрямків напрямків боротьби з кіберзлочинністю слід з'ясувати визначення поняття "кіберзлочинність", появу якого обґрунтовано пов'язують, перш за все, з рівнем її суспільно небезпечних загроз, що пов'язана з розширенням технічної бази інформатизації.

Кіберзлочинність як сукупність кіберзлочинів – суспільно небезпечних винних діянь у кіберпросторі та (або) з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та (або) які визнані злочинами міжнародними договорами України [10], є відносно новим антисоціальним явищем, яке швидко прогресує, але його характер і особливості в різних країнах практично не мають істотних відмінностей; етапи та зміст процесу становлення кримінально-правової системи боротьби з кіберзлочинністю в різних країнах практично повторюються [11].

Найбільш поширеним у вітчизняній юридичній літературі є підхід, згідно з яким до кола комп'ютерних злочинів слід відносити всі суспільно небезпечні посягання, при вчиненні яких комп'ютери використовуються як технічні засоби [12; 13]. Звідси випливає, що в основу такої класифікації злочинів покладено ознаки, що

характеризують засоби, які використовуються при їх вчиненні.

Визначення комп'ютерних злочинів як групи посягань, які характеризуються загальними ознаками способу, засобу чи знаряддя, може бути цілком затребуване з позиції криміналістики [13, с. 13]. В межах останньої йдеться про встановлення особливостей методики виявлення, розслідування злочинів цієї категорії, фіксації їх слідів тощо.

Сьогодні в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень носіїв цифрової інформації та комп'ютерної інформації, які використовуються у тому числі й для методичного забезпечення дослідження програмних продуктів, як засобів здійснення комп'ютерних злочинів [14 – 16].

Рекомендовані методи дослідження комп'ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його функцій. Встановлення та оцінка сукупності слідів дозволяє відтворити, тобто змоделювати, дії при здійсненні комп'ютерного злочину [17, с. 4].

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації (так званих "шпигунських" програм) в ІСТЕ СБ України було розроблено методичні рекомендації для проведення експертних досліджень програмних засобів, призначених для негласного отримання інформації (далі – ПЗ НОІ) [18].

Слід підкреслити, що віднесення програмного засобу до предмету злочину потребує встановлення за результатами дослідження необхідної сукупності ознак та властивостей, які є достатніми для визначення його призначеності для негласного отримання інформації [3, с. 102].

На відміну від вказаних методів дослідження комп'ютерної інформації, дослідження ПЗ НОІ повинно передбачати як аналіз слідів (ознак) реалізації функціоналу програмного засобу, так і безпосереднє дослідження дій комп'ютера чи телекомунікаційного пристрою, на який встановлено програмний засіб, зі визначенням причино-наслідкових зв'язків між виявленими діями з негласного отримання інформації та функціями ПЗ [18].

Розроблення методичних рекомендацій "Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації" базується на критеріях віднесення технічних та програмних засобів до спеціальних технічних засобів негласного отримання інформації та методичних матеріалів зарубіжних і вітчизняних фахівців у сфері комп'ютерно-технічної експертизи [14 – 18].

Новизною методичних рекомендацій є запропонований підхід щодо дослідження ПЗ, який передбачає комплексне застосування різних методів досліджень, зокрема методів контролю активності ПЗ та виконання відповідних видів експертних задач як в галузі комп'ютерно-технічної експертизи, так і в галузі експертизи СТЗ [18].

Предметом експертних досліджень ПЗ є факти й обставини, встановлені при дослідженні використання програмних засобів, що встановлені на технічні засоби загального користування (комп'ютери, телекомунікаційні пристрої тощо), та забезпечують реалізацію інформаційних процесів [8, с. 113].

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причино-наслідкових зв'язків між ними, дає підстави для:

– визначення можливості здійснення негласного отримання інформації з використанням наданого на дослідження програмного засобу;

– віднесення програмного засобу до ПЗ НОІ [18].

Як правило, при проведенні експертного дослідження вирішуються діагностичні та ситуаційні задачі, а також задачі групофікації ПЗ [15; 18].

Вирішення діагностичної задачі спрямовано на:

– встановлення загальної характеристики програмного засобу, з яких файлів та каталогів він складається, їх параметрів (обсяг, атрибути тощо);

– визначення функцій програмного засобу, які забезпечують виконання певних дій з негласного отримання інформації;

– встановлення типів апаратно-програмних платформ, що підтримують функціонування програмного засобу[3, с. 103].

При вирішенні ситуаційної задачі здійснюється зняття процесів (одномоментних станів) у режимі реального часу, встановлення й сприйняття яких можливо тільки з використанням спеціалізованих програмних засобів або в певних умовах (наприклад, у складі певної конфігурації технологічного устаткування, у складі комп'ютерної системи або мережі тощо) [9, с. 113].

Під час аналізу процесів у режимі реального часу виявляються ознаки функціонування спеціального ПЗ: читання/запис даних у файловій системі – створення, видалення, редагування файлів, каталогів; дописування інформації в файл; модифікації пам'яті – створення чи завершення процесів, створення прихованих процесів; зміни реєстру – створення нових записів в реєстрі, редагування або видалення існуючих; зовнішню мережеву активність – отримання чи відсилання інформації через мережу; внутрішню мережеву активність – отримання чи відсилання інформації через localhost; перехоплення хуків клавіатури; відкриття портів; запуск файлів в операційній системі; встановлення чи заміну драйверів [18].

Для виявлення ознак функціонування спеціального програмного засобу використовується спеціалізоване програмне забезпечення, наприклад, ThreatExpert, Process Monitor, Defense Wall HIPS, SafenSoft SysWatch Deluxe. При використанні зазначеного програмного забезпечення застосовується один з трьох основних методів контролю активності ПЗ: HIPS, VIPS та Пісочниця (sandbox) [17].

Проведення досліджень ПЗ в реальних умовах на стадії експертного експерименту спрямовано на визначення оцінки можливостей забезпечення виконання певних дій з негласного отримання інформації та виявлення необхідної сукупності функцій ПЗ, яка є достатньою для застосування його за призначенням.

При цьому дослідження ПЗ може організовуватися на базі технології "клієнт-сервер" телекомунікаційно-інформаційної системи, яка включає пункт управління об'єднаний телекомунікаційною мережею з абонентськими пристроями, на яких здійснюється перехоплення та передача дистанційно встановлених видів інформації [3, с. 104].

Висновок щодо віднесення ПЗ до ПЗ НОІ формується відповідно до встановлених критеріїв, а саме – наявності критеріальних ознак програмного засобу: придатності програмного засобу для негласного отримання інформації та призначеності програмного засобу для його застосування у прихований спосіб, який характерний для оперативно-розшукових заходів [18].

Запропонований в рекомендаціях метод аналізу виявлених слідів реалізації функцій ПЗ дозволяє з'ясувати спосіб функціонування ПЗ, його властивості з негласного

отримання інформації, а також визначити, в кінцевому підсумку, призначеність програмного засобу [18].

У свою чергу, аналіз та узагальнення результатів експертних досліджень надає можливість визначення ключових елементів криміналістичної характеристики кіберзлочинів, що здійснюються із застосуванням спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації, а саме: значущі ознаки ПЗ, спосіб його використання, механізм слідоутворення та типові сліди реалізації функцій ПЗ.

Висновки.

Актуальність проблеми протидії кіберзлочинності в умовах сьогодення потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях.

Одним із важливих напрямів удосконалення методичного забезпечення протидії кіберзлочинності є впровадження методичних матеріалів для забезпечення проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання інформації [9, с. 114].

Аналіз та узагальнення результатів експертних досліджень можуть бути використані для визначення криміналістичної характеристики кіберзлочинів, що здійснюються із застосуванням спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації.

Запропоновані підходи можуть слугувати методичним підґрунтям для розробки методів, засобів і технологій ідентифікації, фіксації кіберзлочинів у сфері протидії кіберзлочинності.

Використана література

1. Киберпреступность страшнее финансового кризиса. URL: https://www.crime-research.ru/news/03.12.2008/50 (дата звернення: 03.01.2021).

2. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://www.unn.com.ua/uk/news/1906706-kiberzlochintsi-u-2020-rotsi-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya (дата звернення: 19.02.2021).

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право*. № 4(31)/2019. С. 98-106.

4. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері. *Юридичний журнал.* 2007. № 2. С. 59-60.

5. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. № 1(28)/2019. С. 108-117.

6. Голубєв В.О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту.* 1997. № 2. С. 35-40.

7. Стратегія кібербезпеки України: Указ Президента України від 15.03.16 р. № 96. URL: https://www.president.gov.ua/documents/962016-19836. (дата звернення: 21.02.2020).

8. Серьогін В.С., Леонов Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов'язаних з неправомірним дистанційним доступом до комп'ютерної інформації. *Інформація і право*. № 2(21)/2017. С. 108-115.

9. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений: доклады ТУСУРа. 2014. № 2(32). Барнаул: Изд-во Алт. ун-та, 2014. С. 162-165.

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

11. Баранов О.А. Кримінологічні проблеми комп'ютерної злочинності. URL: http://www.bezpeka.com/ru/lib/spec/crim/art71.html

12. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні: монографія. Харків: Панов, 2016. 212 с.

13. Карчевский Н.В. "Киберпреступление" или преступление в сфере использования информационных технологий?: матеріали всеукр. наук.-практ. конф. *Кібербезпека в Україні: правові та організаційні питання,* м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. С. 10-14.

14. Дослідження інформації на цифрових носіях (методика): звіт про науково-досліду роботу / С.М. Бобрицький, О.В. Чишкало та ін. Харків. ХНДІСЕ. 2009. 2009. 34 с.

15. Методика дослідження комп'ютерної інформації / К.Ю. Усков, О.М. Пешехонова, Ю.М. Бєляк, В.А. Кореньок, А.О. Ружинський. Київ: КНДІСЕ. 2005. 37 с.

16. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж / О. Башкатов, Г. Дружинін та ін. Донецьк: ДНДІСЕ. 2010. 179 с.

17. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 3. С. 4-9.

18. Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації: методичні рекомендації. Київ: ІСТЕ СБУ. 2016. 31 с.

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

УДК 342.951

КУЗНЄЦОВ О.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0001-9242-0835.

ЄВРОПЕЙСЬКИЙ ДОСВІД ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Анотація. *Здійснено огляд новел європейського законодавства у сфері забезпечення кібербезпеки. Узагальнено перспективи діджіталізації в ЄС. Розглянуто положення Стратегії кібербезпеки ЄС на 2021 – 2027 роки та Дорожньої карти "Цифровий компас". Визначено засади та пріоритети спільної європейської цифрової політики. Деталізовано стратегічні цілі та напрями успішної цифрової трансформації Європи до 2030 року. Розкрито організаційно-правовий механізм запровадження режиму кіберсанкцій в ЄС. Визначено шляхи співпраці між Україною та ЄС у сфері забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, кіберзагроза, діджиталізація, цифрові технології, режим кіберсанкцій, штучний інтелект.*

Summary. *The novelties of the European legislation in the sphere of cybersecurity are reviewed. Prospects for digitalization in the EU are summarized. The provisions of the EU Cyber Security Strategy for 2021 – 2027 and the Digital Compass Roadmap are considered. Basic principles and priorities of a common European digital policy are defined. The strategy targets and avenues for a successful digital transformation of Europe by 2030 are detailed. The organizational and legal mechanism for introducing the cyber sanctions regime in the EU has been revealed. The directions of the cooperation between Ukraine and EU in the sphere of cybersecurity are identified.*

Keywords: *cybersecurity, cyberattack, cyberthreat, digitalization, digital technologies, cyber sanctions regime, artificial intelligence.*

Аннотация. *Осуществлено рассмотрение новел европейского законодательства в сфере обеспечения кибербезопасности. Обобщены перспективы диджитализации в ЕС. Рассмотрены положения Стратегии кибербезопасности ЕС на 2021 – 2027 года и Дорожная карта "Цифровой компас". Определены основы и приоритеты совместной европейской цифровой политики. Детализированы стратегические цели и направления успешной цифровой трансформации Европы до 2030 года. Раскрыто организационно-правовой механизм внедрения режима киберсанкций в ЕС. Определены направления сотрудничества между Украиной и ЕС в сфере обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, киберугроза, диджитализация, цифровые технологии, режим киберсанкций, штучный интеллект.*

Постановка проблеми. Цифрові технології відкривають унікальні можливості для розвитку економіки та підвищення якості життя громадян. У сучасному світі більшість країн світу вимушені "на ходу" адаптувати своє законодавство та впроваджувати державне регулювання сфери інформаційних технологій, у тому числі й цифрових, враховуючи появу нових викликів щодо забезпечення захисту прав людини та безпеки держави. Сучасний світ постійно змінюється. Поширення популярності цифрової економіки як принципово нової моделі розвитку глобальної економічної системи постійно зростає, що провокує необхідність розробки дієвих механізмів забезпечення надійного та безпечного середовища її функціонування. Саме тому кібербезпека являє

собою стратегічну комплексну проблему яка, передусім, стосується економіки країни, особливо електронної промисловості, в тому числі питань розвитку інфраструктури електронних комунікацій, технологій кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, визначення заходів боротьби з кіберзлочинністю та кібертероризмом тощо.

Враховуючи сучасні тенденції розвитку пріоритетних засад спільної політики провідних країн ЄС за напрямом протидії загрозам у кіберпросторі, динаміку змін у внутрішній інформаційній політиці цих держав, спостерігається прагнення швидкого та адекватного реагування на нові виклики сучасності. Проте кібернетичні загрози формуються та розвиваються досить швидко, стають дедалі складнішими та більш адаптивними. Саме тому забезпечення кібернетичної безпеки та кіберстабільності відносяться до основних пріоритетів Єврокомісії у рамках реалізації програми цифрової трансформації ЄС. На цьому фоні важливим завданням залишається забезпечення стабільності комунікаційних мереж, заснованих на технологіях 5G, з якими ЄС пов'язує швидкий цифровий розвиток європейської економіки. Невипадково вказані пріоритети знайшли своє відображення у бюджеті ЄС на 2021 – 2027 роки.

Прагнення політичного керівництва держав світу зміцнювати та посилювати систему забезпечення кібербезпеки нерозривно пов'язано із реагуванням на реальні та потенційні загрози, що передбачає вдосконалення законодавства, визначення стратегічних засад подальшого розвитку у базових програмних документах та їх реалізації. Враховуючи прагнення України інтегруватися у європейський інформаційний простір, актуальним та своєчасним є огляд новел сучасного законодавства ЄС, зокрема оновленої Стратегії кібербезпеки, яка визначає поступальні та дієві кроки спільної європейської інформаційної політики з метою посилення спроможності держав-членів ЄС у сфері забезпечення кібербезпеки, захисту надбань цифрової економіки.

Результати аналізу наукових публікацій. Правове забезпечення кібербезпеки України та висвітлення шляхів його удосконалення були предметом досліджень А. Баранова, М. Василенка, В. Гавловського, М. Гуцалюка, О. Довганя, Д. Дубова, А. Марущака, М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева та інших вітчизняних науковців. Більш детально аналізу європейських законодавчих ініціатив у сфері забезпечення кібербезпеки приділяли свою увагу такі фахівці як: О. Балуєва, Є. Боєр, С. Вдовенко, І. Забара, Т. Сліпченко, Р. Лук'янчук тощо. Водночас, слід констатувати, що дослідження процесів забезпечення кібербезпеки як важливої складової фарватеру цифрової економіки та її складових в контексті розбудови засад сучасної європейської інформаційної політики детально не розглядалося, що посилює актуальність обраної теми наукового дослідження. Масштабні збитки цифрової економіки провокують потребу пошуку шляхів мінімізації збитків, у тому числі й шляхом посилення кібербезпеки.

Метою статті є висвітлення й узагальнення кращих практик європейського досвіду щодо побудови та удосконалення системної протидії кіберзагрозам в сучасних умовах, проведення огляду новел європейського законодавства у сфері забезпечення кібербезпеки, зокрема Стратегії ЄС у вказаній сфері та висвітлення базових напрямків дорожньої карти "Цифровий компас", оприлюдненої Єврокомісією 9 березня 2021 року.

Виклад основного матеріалу. Останнім часом зусилля європейської спільноти спрямовані на узгодження та розвиток безпекової політики у кіберпросторі. Результатом цих узгоджених дій стала підготовка та оприлюднення 16 грудня 2020 року оновленої Стратегії кібербезпеки ЄС [1], ключовими завданнями якої є підвищення стійкості життєво необхідних структур та системна протидія масштабним зовнішнім кібератакам.

Пріоритетом визначено посилення колективної безпеки у кіберпросторі, забезпечення рівної можливості для усіх громадян у ЄС та представників бізнесу щодо використання надійних цифрових послуг та інструментів у повсякденному житті. Усі електронні мережі, банки, транспорт, лікарні, державні органи мають бути гарантовано захищеними від кібернетичних загроз та будь-яких ризиків у цій площині. У зв'язку з цим Єврокомісія запропонувала створити мережу Центрів оперативної безпеки по усій території ЄС, які будуть діяти на основі впровадження технологій штучного інтелекту та нададуть змогу створити реальний "щит кібернетичної безпеки" для зони ЄС. Згідно із цим задумом, система має розпізнавати кібернетичні атаки на ранніх стадіях та пропонувати алгоритми дій, спрямованих на їх упередження, викриття та ліквідацію.

На виконання цих стратегічних планів важлива роль відводиться інституційному удосконаленню складових кібербезпеки та її безперебійному забезпеченню. Зокрема, очікується створення нової структури ЄС – "Об'єднаний кібернетичний відділ", який у рамках своїх повноважень, має здійснювати координацію та консолідацію спільних дій та проведення операцій з метою виявлення та нівелювання хакерських атак, надання належної відсічі їм. Це також дозволить активізувати співпрацю між відповідальними структурами держав-членів ЄС, які є уповноваженими щодо виявлення кібератак та оперативного реагування на них. Кіберпідрозділ має посилити співробітництво у цій сфері між євроінституціями та державами-членами, включаючи цивільні структури та правоохоронні органи, дипломатичні установи та спеціалізовані підрозділи кібернетичного захисту.

Важливе місце в положеннях Стратегії посідає міжнародний напрямок діяльності, зокрема, це активізація взаємодії з міжнародними організаціями щодо розробки загальних методологічних підходів до кіберзахисту, зміцнення партнерства з державами світу в контексті розвитку глобального, відкритого, стабільного кібернетичного простору на основі засад верховенства права, дотримання та виконання фундаментальних свобод та демократичних цінностей. Запропоновано реформування у сфері забезпечення кібербезпеки мереж та інформаційних систем, що дозволить підвищити кібернетичну стійкість критичної інфраструктури ЄС, включаючи заклади охорони здоров'я, залізниці, центри зберігання даних, дослідницьких та виробничих установ, які можуть бути уразливими до швидких кібернетичних атак.

У рамках розбудови міжнародного вектору, Євросоюз тісно співпрацюватиме зі структурами ООН та іноземними партнерами, має використовувати "інститут санкцій" з метою захисту прав людини й громадянина, фундаментальних свобод в інформаційному просторі, розвивати міжнародні норми та стандарти безпеки у цій площині. Єврокомісія планує проведення поетапних переговорів з усіма зацікавленими суб'єктами у цьому контексті. Таким чином, започаткована активізація міжнародного співробітництва за ініціативи ЄС є ключовим моментом щодо ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози. Очікується, що міжнародне співробітництво також здійснюється з метою зміцнення взаємної довіри у сфері кібербезпеки, у першу чергу, між ЄС та ООН, іншими міжнародними організаціями та альянсами держав, надасть можливість вироблення спільних підходів у протидії кіберзлочинності, консолідації зусиль у розслідуванні та запобіганні транснаціональним кіберзлочинам. При цьому в основі реалізації європейської інтеграції та її просування знаходиться культура політичного компромісу.

З метою реалізації цього програмного документу Єврокомісія має намір залучити 4,5 млрд. євро-інвестицій з метою підвищення кібербезпеки на теренах ЄС протягом

2021 – 2027 років, завдяки спільним зусиллям євро-інституцій, країн-членів та промисловості. Очікується, що перспективні інвестиції у кібербезпеку сприятимуть покращенню та оздоровленню у майбутньому онлайн-простору та мінімізуватимуть ймовірні ризики для об'єктів критичної інфраструктури. У положеннях Стратегії окрема увага присвячена створенню в ЄС мережі оперативних центрів кібербезпеки з можливістю залучення та впровадження в практичну площину штучного інтелекту задля виявлення кібернападів та протидії їм.

Підготовка цього фундаментального документа на стратегічному рівні стала певною реакцією європейського співтовариства на збільшення кількості кібератак, які виникають на перманентній основі, підвищення уразливості та збитковості цифрової економіки ЄС. Також підставами для розробки цієї Стратегії стали такі виклики як: підвищення ризиків для критичної інфраструктури, перехід 40 % працівників в ЄС на віддалений формат роботи під час пандемії коронавірусу в 2020 році, масштабні щорічні збитки світової економіки від кіберзлочинності у розмірі 5,5 трильйонів EUR, офіційно зафіксованих 450 кібератак на європейські об'єкти критичної інфраструктури у 2019 році, недоукомплектовано 291 тис. посад фахівців у сфері інформаційної безпеки в ЄС. Також можна сюди добавити потужну хакерську кібератаку 9 грудня 2020 року на Європейське агентство з лікарських засобів, яке здійснює сертифікацію вакцин від коронавірусу. Хакери, які атакували Європейське агентство з лікарських засобів, отримали доступ до документів щодо вакцини Pfizer/BioNTech [2]. Одночасно з Стратегією кібербезпеки ЄС була схвалена Директива щодо забезпечення стабільності критично важливих об'єктів [3].

Тобто, удосконалення процесів з метою забезпечення кібербезпеки в ЄС передбачає адаптацію до нових викликів та кіберзагроз, які досить швидко поширюються та розвиваються, вбачається комплексним процесом, який вимагає посилення спроможності сектору безпеки і оборони, співпраці усіх зацікавлених суб'єктів, держав та інституцій ЄС, приватного сектору, правоохоронних органів з використанням дипломатії та міжнародного співробітництва з метою забезпечення гарантованого захисту громадян та усієї інфраструктури. Результатом практичного впровадження європейської політики у сфері забезпечення кібербезпеки має стати створення автономного щита кібернетичного захисту на теренах ЄС. Оновлена Стратегія кібербезпеки ЄС передбачає також розширення сфери дій правил, що вже працюють у Союзі. Раніше вони стосувалися об'єктів охорони здоров'я, банківської справи, питного водопостачання та енергетичної інфраструктури. Тепер до такого переліку внесене також держуправління, об'єкти харчової промисловості та фармацевтичне виробництво. Протягом 18 місяців з дати набуття чинності Стратегією кібербезпеки ЄС, усі країни-члени мають привести свої нормативно-правові акти у відповідність до положень цього програмного документа.

Слід зазначити, що попередня редакція Стратегії кібербезпеки ЄС була ухвалена ще в лютому 2013 року та передбачала кроки, націлені на нарощування потужності задля попередження кіберзагроз, включаючи кіберзлочинність та кібертероризм, при цьому боротьба з високотехнологічними злочинами була визначена як один із основних пріоритетів у діяльності Європейського поліцейського управління (European Police Office – Europol) [4].

Також слід акцентувати увагу, що в Євросоюзі запроваджено практичний механізм застосування санкцій за кібератаки, який передбачає запровадження обмежень та негативних наслідків для осіб, які підозрюються у їх скоєнні. Цей режим було розроблено на виконання рішення Євросоюзу від 12 червня 2017 року про створення механізму реагування на недружні дії у кібернетичному просторі, так званого

“Інструментарію кібернетичної дипломатії”. Так, у Європейському Союзі запроваджено санкції проти осіб, відповідальних за кібернапад на німецький Бундестаг у 2015 році. Таким чином, у ЄС вже існує певний досвід застосування режиму “кіберсанкцій”, який фактично було накладено на 8 фізичних та 4 юридичних осіб з РФ, КНР та Північної Кореї у 2020 році.

Режим кіберсанкцій являє собою дію правових рамок адресних обмежувальних заходів проти особи або установ, які залучалися до скоєння кібернетичних атак, що завдали значної шкоди та представляють зовнішню загрозу для ЄС або його країн-членів. Стратегією регламентовано, що ЄС може також застосовувати санкції у відповідь на кібернетичні атаки проти третіх країн або міжнародних організацій, якщо рішення про застосування таких обмежувальних заходів вважатиметься доцільним в рамках Спільної політики ЄС з безпеки й оборони. Кінцевою метою запровадження цих заходів є стримування та реагування на кібернетичні атаки, при цьому санкції можуть включати заборону на подорожі до держав ЄС, заморожування фінансових активів осіб та установ. Навіть особи й установи, які перебуватимуть у “санкційному списку” не матимуть доступу до жодних фондів від ЄС. Таким чином, “режим кіберсанкцій” створює для ЄС правову основу щодо можливостей застосування обмежувальних заходів проти фізичних осіб або установ, що залучаються до кібернетичних атак на Євросоюз або його держави-члени.

Окрім вищезгаданих санкцій, пропонується зміцнювати потенціал протидії зловмисній поведінці третіх країн у кіберпросторі. Передбачається створення робочої групи кіберрозвідки у складі Центру розвідки ЄС. На виконання положень Стратегії кібербезпеки, у майбутньому планується побудова та кооперація всередині ЄС щодо розвитку концептів кібероборони, створення спільних структур енергетичної та військової кібербезпеки у рамках постійної структурованої співпраці (PESCO).

Цифрові технології зіграли вирішальну роль у підтриманні економічного та соціального життя під час кризи, пов’язаної з короновірусом, та залишаються ключовим фактором в успішному переході до постпандемічної економіки у майбутньому. Тобто масштабна цифрова трансформація залишається пріоритетом створення умов для глобального впливу ЄС на світову геополітику та економіку.

9 березня 2021 року Колегія Єврокомісії схвалила дорожню карту “Цифровий компас” [5] – декларативний документ, який визначає перспективи та завдання у сфері розвитку глобальної цифрової трансформації до 2030 року. Як йдеться в документі, “Цифровий компас” відображає перспективи технологічного розвитку ЄС до 2030 року у чотирьох напрямах – цифрова освіта, цифрова інфраструктура, цифровий розвиток бізнесу, цифровий розвиток державного сектору.

Перший напрямок стосується цифрової освіти населення та підготовки досвідчених фахівців у сфері цифрових технологій. Це означає, що до 2030 року, 80 % усього населення ЄС повинні мати базові цифрові навички. При цьому в ЄС мають бути працевлаштовані не менше 20 мільйонів фахівців у цифровій сфері, серед яких має суттєво зрости доля зайнятості жінок.

Другий – передбачає розвиток безпечної, ефективної та захищеної цифрової інфраструктури. До 2030 року всі домогосподарства мають бути забезпечені комунікаціями гігабітного рівня, а всі населені регіони мають отримати покриття мережею 5G. На той час на Європу має припадати не менше 20 % світового обсягу виробництва напівпровідників, виробництво передових та стійких напівпровідників у Європі має становити 20 % світового виробництва. Передбачається створення не менше 10 тис. ефективних та екологічних передавальних вузлів. У Європі має з’явитися

перший квантовий комп'ютер до 2025 року. До 2030 року очікується створення конкурентних європейських підприємств з повними циклами роботи щодо постачання напівпровідників – від проектування компонентів до готових продуктів. Центром суцільної цифровізації стануть промислові підприємства з виробництва процесорів формату 5G. Також планується значно знизити залежність від поставок цифрових продуктів з Південно-Східної Азії та Китаю.

Третій – стосується цифрового розвитку для бізнесу. До 2030 року три з чотирьох компаній мають використовувати "хмарні" комп'ютерні послуги, бази "великих даних" та засоби штучного інтелекту. Очікується, що не менше 90 % малих та середніх промислових підприємств мають досягти принаймні базового рівня інтенсивності у застосуванні комп'ютерних технологій.

Четвертий – цифровий розвиток державного сектору передбачає, що до 2030 року всі ключові громадські та соціальні послуги мають бути доступними у форматі онлайн. Громадяни ЄС зможуть повноцінно використовувати засоби цифрової ідентифікації, мати безобмежений доступ до власних електронних даних.

Усі перераховані напрямки програми "Цифровий компас" ЄС будуть включені в Політичну програму, яка має пройти розгляд і затвердження на рівні Європейського Парламенту та Ради ЄС, після чого стане частиною скоординованих дій з цифрового розвитку у всіх державах-членах. Такі зусилля, на переконання Єврокомісії, мають допомогти ЄС у подоланні глобальних викликів, розвинути співпрацю з міжнародними партнерами та організаціями, які мають схожі цілі, розвинути стійке та ефективне цифрове партнерство. У цьому контексті ЄС вже запропонував створити нову Раду ЄС-США з питань торгівлі і технологій. ЄС має намір підтримувати інших міжнародних партнерів, зокрема, шляхом створення Фонду цифрових комунікацій [6].

Таким чином, "Цифровий компас" ЄС являє собою звіт правил амбіційного та динамічного розвитку цифрової сфери та суцільної діджиталізації на поточні 10 років, а його практичне впровадження надасть змогу піднятися Євросоюзу у рейтингу світового технологічного розвитку на лідерські позиції, налагодити масштабне промислове виробництво напівпровідників та встановити контроль над 20 % світових поставок мікросхем та процесорів у цьому сегменті.

В Україні все ще діє стратегія кібербезпеки, схвалена у 2016 році [7].

З цього приводу у [8, С. 135] слушно зазначається: "…*стан реалізації Стратегії кібербезпеки України є незадовільним, що негативно впливає на всю сферу кібербезпеки та кіберзахисту України та є свідченням формального підходу з боку відповідальних державних органів до стратегічного планування, формування та реалізації державної політики, а також здійснення стратегічного контролю у цій сфері. Фактично цей документ розроблявся на 5 років*".

Висновки.

Забезпечення цифрового суверенітету та цифрового благополуччя бізнесу та населення політичним керівництвом ЄС визначається пріоритетами у роботі.

Можна констатувати, що ЄС нарощує свій потенціал у сфері тотальної діджіталізації, максимально намагаючись впроваджувати цифрові технології у всі сфери життєдіяльності європейського суспільства. Основним базовим документом в ЄС, який регулюватиме сферу кіберзахисту, є оновлена Стратегія кібербезпеки на 2021 – 2027 роки. ЄС концептуально має намір та вживає заходів з метою оперативного реагування на виклики та загрози сучасності в інформаційній сфері, впроваджує у реалії життя на загальнонаціональному рівні концепти "ризик-менеджменту" в умовах пандемії, визначаючи при цьому цифрові права та свободи громадян, їх захист найвищою цінністю.

Аналіз положень Стратегії передбачає використання регуляторних та інвестиційних механізмів, політичних ініціатив за такими напрямами: забезпечення стабільності, технологічного суверенітету та лідерства; здатність попереджувати, стримувати та адекватно реагувати на кібератаки; розвиток міжнародного співробітництва з метою формування глобального та відкритого кіберпростору. Актуальним та важливим напрямом щодо створення надійного європейського "Кіберщита" є утворення об'єднаної спільноти (Joint Cyber Unit) з метою оперативного обміну інформацією про загрози та надання допомоги в реагуванні на них, підтримка життєдіяльності середніх та малих підприємств, перезавантаження та удосконалення "CERT-EU", запровадження дієвих заходів з метою забезпечення безпеки мереж 5G, законодавче врегулювання Інтернету речей (Internet of Secure Things).

Інноваційний підхід закладено у положеннях цієї Стратегії щодо запровадження механізму "кіберсанкцій". ЄС може застосовувати їх проти зовнішніх суб'єктів за дотримання певних умов: по-перше, має бути встановлено, що такі недружні дії зроблені з-поза кордонів ЄС; по-друге, здійснені атаки проводилися персонами та установами, які утворені або діють за межами ЄС, або здійснюються за підтримки організацій або персон, які знаходяться за межами ЄС. Санкції можуть бути спричинені навмисними кібернетичними атаками, які можуть потенційно завдати значної шкоди Євросоюзу або його державам-членам. Компетенція щодо ухвалення та продовження рішень про запровадження "режиму кіберсанкцій" належить виключно Раді ЄС. Для України є цікавим досвід ЄС у сфері запровадження "режиму кіберсанкцій", який можливо імплементувати у вітчизняне законодавство з урахуванням національних особливостей.

Як вважаємо, з набуттям чинності новою Стратегією національної безпеки України 2020 р. вітчизняна стратегія кібербезпеки має бути переглянута з урахуванням нових гібридних загроз та викликів у цій сфері, повинна деталізувати пріоритети національних інтересів у сфері кібербезпеки, а також основні підходи та напрями до формування питань кіберзахисту.

Враховуючі політичні реалії та сучасні спрямування, Україна має активізувати співробітництво у сфері забезпечення кібербезпеки за такими напрямами: створення механізму оперативної координації та взаємодії, обміну інформацією про кіберзагрози й кіберінциденти між компетентними органами України та ЄС; вдосконалення міжнародного співробітництва у сфері кібербезпеки; імплементація міжнародно-правових та європейських норм у національне законодавство України, особливо щодо запровадження режиму кіберсанкцій.

Використана література

1. New EU Cybersecuritu Strategy. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (дата звернення: 20.02.2021).

2. Кібератака на агентство ЄС: хакери викрали дані щодо вакцини Pfizer/BioNTech. URL: https://www.eurointegration.com.ua/news/2020/12/10/7117477 (дата звернення: 20.02.2021).

3. Directive Of The European Parliament And Of The Council on the resilience of critical entities. URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (дата звернення: 20.02.2021).

4. Яцишин М.Ю. Роль міжнародних організацій у протидії кіберзлочинності. *Українське право*. URL: https://ukrainepravo.com/international_law/public_international_law/rolmizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti (дата звернення: 20.02.2021).

5. Europe's Digital Decade: Digitally empowered Europe by 2030. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983 (дата звернення: 20.02.2021).

6. Єврокомісія визначила стратегічні цілі цифрового розвитку ЄС до 2030 року. URL: https://www.ukrinform.ua/rubric-world/3205020-evrokomisia-viznacila-strategicni-cili-cifrovogo-rozvitku-es-do-2030-roku.html (дата звернення: 20.02.2021).

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 20.02.2021).

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

9. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.02.2021).

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

УДК 342.951

ГРІБОЄДОВ С.М., головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0001-6389-0803.

УДОСКОНАЛЕННЯ ДЕРЖАВНОГО ПЛАНУВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Анотація. *Розглянуто засади державного стратегічного планування у сфері забезпечення кібербезпеки. Визначено шляхи удосконалення державного управління у сфері кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів. Проаналізовано та узагальнено недоліки Стратегії кібербезпеки України 2016 року. Розглянуто проєкт Стратегії кібербезпеки України на 2021 – 2025 роки та запропоновано напрями її удосконалення. Окреслено перспективи стратегічного державного планування у сфері забезпечення кібербезпеки в умовах поширення гібридних загроз.*

Ключові слова: *стратегічне планування, державне управління, кібербезпека, кіберзахист, організована кіберзлочинність, кібератака, кіберзагроза, цифрові технології, цифровий суверенітет.*

Summary.*The main principles of state strategic planning in the sphere of cybersecurity are considered. The directions of improvement of public administration in the field of cyber protection of a critical information infrastructure and state information resources are identified. The shortcomings of the Cyber Security Strategy of Ukraine in 2016 are analyzed and summarized. The draft of Cyber Security Strategy of Ukraine for 2021 – 2025 is considered and directions for its improvement are proposed. The prospects of strategic state planning in the sphere of cybersecurity in the context of the spread of hybrid threats are outlined.*

Keywords: *strategic planning, public administration, cybersecurity, cyberdefense, organized crime, cyberattack, cyberthreat, digital technologies, digital sovereignty.*

Аннотация. *Рассмотрены основы государственного стратегического планирования в сфере обеспечения кибербезопасности. Определены направления государственного управления в сфере киберзащиты критической информационной инфраструктуры, государственных информационных ресурсов. Проанализированы и обобщены недостатки Стратегии кибербезопасности Украины 2016 года. Рассмотрен проект Стратегии кибербезопасности Украины на 2021 – 2025 года и предложены направления его усовершенствования. Определены перспективы стратегического государственного планирования в сфере обеспечения кибербезопасности в условиях распространения гибридных угроз.*

Ключевые слова: *стратегическое планирование, государственное управление, кибербезопасность, киберзащита, организованная преступность, кибератака, киберугроза, цифровые технологии, цифровой суверенитет.*

Постановка проблеми. Побудова інформаційного суспільства в різних державах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя, з одного боку створюють підґрунтя для ефективного соціально-економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління. З іншого – перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів надзвичайно вразливими для

реалізації кібернетичних загроз. З огляду на це, функціонування національної системи кібербезпеки унеможливлюється без стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та забезпечення надійного кіберзахисту.

Державне стратегічне планування у сфері забезпечення кібербезпеки залишається важливою складовою реалізації державної безпекової політики виходячи із викликів та загроз в умовах поширення гібридних методів впливу. Саме завдяки державному стратегічному плануванню підвищується ефективність державного управління, визначаються необхідні планові поточні та перспективні заходи, реалізація яких дає змогу мінімізувати внутрішні й зовнішні кіберзагрози, визначати напрями комплексної взаємодії та спільних дій відповідальних суб'єктів забезпечення кібербезпеки. За таких умов державне стратегічне планування у сфері забезпечення кібербезпеки постає важливою складовою політики національної безпеки, виходячи положень Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.20 р. [1].

Стаття 25 Закону України "Про національну безпеку" від 21.06.18 р. [2] визначає засади планування у сферах національної безпеки і оборони, які встановлюються з метою забезпечення реалізації державної політики у цих сферах шляхом розроблення стратегій, концепцій, програм, планів розвитку органів сектору безпеки і оборони, управління ресурсами та ефективного їх розподілу. Планування у сферах національної безпеки і оборони поділяється на довгострокове (понад п'ять років), середньострокове (до п'яти років) та короткострокове (до трьох років). Нормативно встановлено, що одним із документів довгострокового планування виступає саме Стратегія кібербезпеки України. Адже існуюча Стратегія кібербезпеки України потребує перегляду та ухвалення її у новій редакції, виходячи із динамічних цифрових трансформацій та глобальних викликів сучасності, особливо щодо поширення у кіберпросторі гібридних загроз, появи нових форм організованої кіберзлочинності.

Результати аналізу наукових публікацій. Державне планування у сфері забезпечення кібербезпеки як важливу функцію державного управління розглядали у своїх наукових працях такі вчені як: В. Гурковський, О. Заярний, Р. Лук'янчук, А. Семенченко, О. Твердохліб, та ін. Організаційно-правовий аспект цих процесів досліджували: М. Гуцалюк, О. Довгань, Д. Дубов, І. Діордиця, Н. Ткачук.

Проте, у зв'язку із поширенням нових кіберзагроз гібридного характеру, постійного удосконалення цифрових технологій та їх проникнення у всі сфери життя суспільства ці питання потребують подальшого дослідження та ретельного вивчення як науково-теоретичної проблеми.

Метою статті є визначення на базі аналізу сучасних викликів та загроз у кіберпросторі шляхів удосконалення засад державного планування під час підготовки Стратегії кібербезпеки України з урахуванням запроваджених реформ складових сектору безпеки і оборони України

Виклад основного матеріалу. Світовий досвід переконливо засвідчує, що процес забезпечення кібербезпеки в обов'язковому порядку передбачає створення цілісної її системи, яка включає організаційно-правові, фінансові, технічні та оперативні заходи, спрямовані на створення надійного і дієвого кіберзахисту з використанням сучасних методів прогнозування, аналізу, моніторингу й моделювання ситуацій. З метою практичного виконання завдань з реалізації курсу України на європейську та євроатлантичну інтеграцію, впровадження в систему планування єдиних процедур та правил, необхідних для підвищення ефективності сектору безпеки і оборони, для нейтралізації реальних та потенційних загроз національній безпеці України Указом

Президента України від 16.05.19 р. № 225 було введено в дію рішення РНБО України "Про організацію планування в секторі безпеки і оборони України" [3], яким передбачалася підготовка: оборонного огляду; огляду громадської безпеки та цивільного захисту; огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом тощо.

З огляду на актуальність стратегічного завдання держави у сфері забезпечення кібербезпеки у 2019 році було заплановано підготовку Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів. Ретельний аналіз зазначеного рішення РНБО України дає змогу констатувати, що результатами підготовки вказаного огляду мали стати висновки щодо оцінки безпекового середовища на середньострокову перспективу на глобальному, регіональному та національному рівнях, а також оприлюднена інформація про досягнення стратегічних цілей за результатами проведення заходів реформування сектору безпеки і оборони, оцінку стану підпорядкованих структур сектору безпеки і оборони.

Лише Постановою Кабінету Міністрів України від 11.11.20 р. № 1176 [4] було затверджено порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дозволило нормативно визначити відповідний алгоритм. Метою проведення цього огляду є оцінювання стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та визначення готовності відповідальних підрозділів суб'єктів, до повноважень яких належить забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури. За результатами огляду визначаються напрями вдосконалення і розвитку національної системи кібербезпеки в частині кіберзахисту з урахуванням реальних і потенційних загроз у кіберпросторі та фінансово-економічних можливостей держави. Проте, жодних строків щодо проведення вказаного огляду нормативно не встановлено.

Загальновідомо, що державне стратегічне планування завершується розробкою плану дій, який стає початком стратегічного управління, яке умовно можливо поділити на управління функціонуванням та управління розвитком системи забезпечення кібербезпеки. При цьому головними напрямами державного стратегічного планування у сфері забезпечення кібербезпеки можна визначити такі: формування та розвиток системи стратегічного планування забезпечення кібербезпеки; визначення повноважень суб'єктів забезпечення кібербезпеки, у тому числі в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період; посилення прогностичної функції системи управління кібернетичною безпекою (стратегічний прогноз); підвищення ефективності моніторингу у сфері забезпечення кібербезпеки для своєчасного виявлення існуючих і нових типів внутрішніх і зовнішніх кіберзагроз, розробки дієвих заходів щодо їх нейтралізації та блокування; інформаційно-аналітичне забезпечення суб'єктів кібербезпеки; оцінка кібербезпеки, що потребує підготовки галузевих індикаторів її стану; визначення переліку об'єктів та порядку віднесення таких об'єктів до критичної інформаційної інфраструктури; нормативно-правове регулювання зазначеної сфери.

Саме стратегічне планування у сфері забезпечення кібербезпеки дає змогу підвищити ефективність та якість державного управління в зазначеному форматі. Стратегічне планування повинно розглядатися усіма органами державної влади, відповідальними складовими сектору безпеки і оборони України, як універсальний

інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення кібербезпеки, у тому числі й з використанням механізму державно-приватного партнерства. Більш того, як демонструє практика, відмова від державного стратегічного планування у важливих сферах життєдіяльності держави має ризики кризових проявів та негативних наслідків для розвитку суспільства та державних інституцій. Підвищення стратегічних спроможностей Уряду України та відповідальних за забезпечення кібербезпеки правоохоронних та інших державних органів потребує запровадження інституційних засад і стандартів системи стратегічного управління у сфері забезпечення кібербезпеки. Виходячи з аналізу положень Стратегії кібербезпеки України, реалізація заходів, спрямованих на її забезпечення, має здійснюватися чітко на планових засадах та з визначенням конкретних строків.

На жаль, все ще спостерігається висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею. Відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і незадекларованих функцій у такому обладнанні та звужують вітчизняні спроможності протидії кіберзагрозам.

За таких умов планування у сфері безпеки і оборони є важливим та стратегічним завданням держави, сферою відповідальності РНБО України. Оскільки Стратегія кібербезпеки України 2016 року [5] фізично та функціонально застаріла, не відповідає сучасним гібридним викликам та загрозам, то 12 жовтня 2020 року Президент України доручив Національному координаційному центру кібербезпеки розробити проект Стратегії кібербезпеки України та подати його у шестимісячний строк на розгляд РНБО України. З цією метою РНБО України було утворено робочу групу, до складу якої увійшли представники основних суб'єктів національної системи кібербезпеки, Верховної Ради України, Офісу Президента України, Секретаріату Кабінету Міністрів України, Міненерго, Мінінфраструктури, Національного інституту стратегічних досліджень. Основою для розроблення цього програмного документу стали, насамперед, Стратегія національної безпеки України [1], затверджена Указом Президента України від 14.09.20 р., прагнення посилити захист державних інтересів у кібернетичному просторі, адаптувати та впроваджувати кращі практики європейського та міжнародного досвіду у сфері забезпечення кібербезпеки.

Аналіз положень Стратегії кібербезпеки України 2016 року та досвід її практичного впровадження надав змогу сформулювати проблемні питання, які або ускладнювали, або унеможливлювали її ефективну її реалізацію. Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Об'єктивно, реалізація Стратегії кібербезпеки України 2016 року була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. Не були розроблені критерії оцінки стану кібербезпеки – індикатори виконання Стратегії, що ускладнило процес моніторингу її результативності та

виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади. Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства.

Нова Стратегія кібербезпеки України має враховувати цей досвід і проблеми та визначити механізми реалізації Стратегії на наступний п'ятирічний період. Стратегія є основою для розроблення інших нормативно-правових актів у сфері кібербезпеки України, а також для обґрунтування розподілу необхідних матеріальних, кадрових та інших ресурсів. Позитивним та прогресивним здобутком політикуму нашої держави стало схвалення проекту Стратегії кібербезпеки України на 2021 – 2025 роки [6], яка була представлена робочою групою при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України на початку березня 2021 року.

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

При цьому, у Стратегії закладено інноваційний підхід щодо визначення механізмів її реалізації та критеріїв вимірювання успіхів її практичного впровадження. Очікується, що у перший рік дії нової Стратегії планується невідкладне розроблені індикаторів оцінки стану кібербезпеки і кіберзахисту; огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, запровадження механізмів проведення оглядів стану національної системи кібербезпеки. Це дозволить у перспективі з урахуванням змін у безпековому середовищі вносити зміни до загального плану та щорічних планів заходів з реалізації Стратегії [7].

Проект Стратегії кібербезпеки України розкриває перспективні напрями щодо посилення спроможностей національної системи кібербезпеки. Пріоритетами забезпечення кібербезпеки України визначені: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації Стратегії.

Головним зовнішньополітичним пріоритетом у сфері кібербезпеки є поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. На цьому фоні, Україна приділятиме особливу увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти. Для цього наша держава планує розвивати на договірній основі з партнерськими спецслужбами країн-членів ЄС і НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовувати кращі світові практики, активно здійснювати інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки. За таких умов, Україна активно співпрацюватиме з міжнародними партнерами, організаціями та іншими заінтересованими сторонами.

Очікується, що протягом реалізації Стратегії Україна зробить кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна планує розвивати мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва.

Виходячи із викладеного, та аналізу базових положень проекту Стратегії кібербезпеки України доцільно звернути увагу на те, що, на жаль, поза увагою РНБО України, у рамках визначення планових засад, залишилося питання доцільності підготовки та щорічного оприлюднення на загальнодержавному рівні аналітичного звіту ІОСТА "Оцінка загроз від організованої злочинності в Інтернеті" [8], яка має готуватися на виконання Угоди між правоохоронним агентством ЄС та Україною щодо стратегічного співробітництва [9]. Як переконливо засвідчує європейський досвід, підготовка щорічного звіту ІОСТА є усталеною практикою країн-членів ЄС та залишається важливим інструментом управління та ухвалення політичних рішень, що використовуються фахівцями з протидії кіберзлочинності, у тому числі й транснаціональній, для розробки державних програм на стратегічному рівні, визначення пріоритетів та розподілу ресурсів на операційному рівні.

Підготовка аналітичного звіту ІОСТА мала б велике значення для виконання Угоди між правоохоронним агентством ЄС та Україною щодо стратегічного співробітництва. Також це відповідає Угоді про асоціацію між ЄС та Україною та допомогло б українській владі ефективно впроваджувати у практичну площину базові положення Закону України "Про основні засади забезпечення кібербезпеки в Україні" [10]. Також у документі були б окреслені основні сучасні кіберзагрози та шляхи їх подолання. У подальшому цю аналітичну та статистичну інформацію можна було би використовувати в майбутньому для прийняття стратегічних рішень, розподілу ресурсів та розбудови спроможності на національному рівні. Реагування правоохоронних органів на кіберзлочинність є одним із трьох основних блоків кібербезпеки, поряд із мережевою та інформаційною безпекою та кіберзахистом. На сьогодні в Україні бракує такого комплексного звіту на національному рівні про процеси, пов'язані із кіберзлочинністю, у якому могли б бути окреслені існуючі загрози та вказані рекомендації.

Як слушно зазначає М. Гуцалюк, для посилення боротьби з кіберзлочинністю Європол у 2013 році створив Європейський центр кіберзлочинності (англ. – European Cybercrime Centre, далі – ECC). Починаючи з 2014 року, ECC щорічно готує та оприлюднює Звіт про оцінку загроз організованої кіберзлочинності (англ. – Internet Facilitated Organised Crime Thread Assessment, далі – IOCTA), у положеннях якого досліджуються тенденції та нові загрози, які впливають на уряди, бізнес та громадян ЄС. У цьому звіті значна увага приділяється сферам злочинності, що належать до компетенції ECC, зокрема: кіберзлочини (кібератаки, зловмисне програмне забезпечення, ботмережі та ін.); сексуальна експлуатація дітей в Інтернеті; шахрайство з платіжними картками (викрадення даних карток – "кардінг", "скіммінг"). До інших напрямів, які аналізуються IOCTA, належать так звані наскрізні чинники злочинів, які охоплюють багато сфер злочинності, але самі по собі не завжди є кримінально караними діяннями. Зокрема, це зловживання криптовалютами, відмивання брудних коштів, отриманих злочинним шляхом, компрометація корпоративної електронної пошти тощо [11, с. 121].

За таких умов, завданням оприлюднення звіту IOCTA є інформування політикуму держав, пересічних громадян та представників бізнесу ЄС про здобутки та результати у сфері боротьби з організованою кіберзлочинністю, визначення нових форм та методів кіберзлочинності. Цей звіт має стимулювати відповідальні державні та правоохоронні органи схвалювати рішення на стратегічному, політичному та тактичному рівнях у сфері посилення спроможностей щодо боротьби з кіберзлочинністю та з метою подальшого удосконалення оперативної діяльності правоохоронних органів ЄС.

Висновки.

Саме на Національний координаційний центр кібербезпеки РНБО України покладається обов'язок здійснення та практичної реалізації Стратегії, розробки заходів щодо планування та її виконання, проведення оцінки ефективності впровадження тих чи інших заходів. Щороку Національний координаційний центр кібербезпеки РНБО має оприлюднювати публічний звіт про стан реалізації Стратегії, демонструючи оцінки ефективності проведених заходів. З метою створення умов для проведення оцінки стану забезпечення кібербезпеки необхідно прискорити на державному рівні розробку галузевих індикаторів стану кібербезпеки, що дозволить визначити ефективність реалізації положень Стратегії кібербезпеки.

Таким чином, державне стратегічне планування у сфері забезпечення кібербезпеки передбачає, насамперед, розробку першочергових та позачергових заходів у рамках реалізації положень Стратегії кібербезпеки, визначення організаційно-правового механізму гарантування цифрового суверенітету нашої держави, надійного кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Стратегічне державне планування у сфері забезпечення кібербезпеки має бути спрямоване на: формування та розвиток на державному рівні єдиної науково-технічної політики; вдосконалення нормативно-правової бази з питань кібербезпеки; створення єдиних реєстрів програмних та апаратних комплексів автоматизованої системи управління кібербезпекою; визначення переліку об'єктів критичної інформаційної інфраструктури; створення та функціонування дієвої системи постійного моніторингу кіберпростору; розробку методів та засобів своєчасного виявлення кібератак та кіберзагроз; розробку інформаційних у тому числі й квантових технологій, які дозволять на технологічному рівні покращити стан захисту інформації в інформаційно-телекомунікаційних системах; розробку та створення засобів протидії кіберзброї; розвиток та удосконалення програмно-технічних методів недопущення

витоків, перехоплення або знищення державних інформаційних ресурсів; використання технології нейронних мереж при побудові сучасної архітектури кібербезпеки, які характеризуються коефіцієнтом високої стабільності при пошкодженні своїх структурних елементів тощо.

Державне планування у сфері забезпечення кібербезпеки на виконання положень Стратегії має передбачати розробку щорічного плану заходів та контроль за його виконанням. Потребує вдосконалення система державного стратегічного планування з метою виявлення і запобігання виникненню кризових ситуацій, запровадження нових підходів до оцінки загроз у сфері забезпечення кібербезпеки, забезпечення ефективної координації та функціонування складових державної системи реагування на кібератаки та кіберзагрози. Також при визначенні ефективності національної Стратегії та плану її реалізації слід враховувати показники загального рівня кібербезпеки. Це зокрема, відсоток виконання зобов'язань, рівень прозорості витрат для цілей кібербезпеки (фінансовий аудит конкретних сфер діяльності щодо виконання плану дій з кібербезпеки), результати співробітництва з іншими державами в кіберпросторі тощо.

Також потребує удосконалення державне управління сектором безпеки і оборони, у тому числі системами забезпечення кібербезпеки, захисту інформації та безпеки інформаційних ресурсів; важливим є посилення спроможностей розвідувальних та контррозвідувальних органів шляхом створення організаційних, матеріально-технічних і фінансових умов для концентрації їх оперативних можливостей на пріоритетних напрямах оперативно-службової діяльності, посилення спроможностей суб'єктів забезпечення кібербезпеки для ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, зміцнення інституціональних та технічних можливостей таких суб`єктів, поглиблення міжнародного співробітництва у цій сфері.

Враховуючи викладене, вважаємо за потрібне передбачити у сучасній Стратегії кібербезпеки України на 2021 – 2025 роки положення стосовно доцільності щорічної підготовки загальнонаціонального аналітичного звіту "ІОСТА – Україна", що надасть змогу деталізувати ризики та загрози, здобутки та результати у сфері боротьби з кіберзлочинністю. Таким чином, можна констатувати, що реалізація системних заходів у сфері забезпечення кібербезпеки неможлива без її державного планування як важливої функції державного управління, без прийняття управлінських рішень на планових засадах, що передбачає розробку та вжиття необхідних заходів, визначення алгоритму спільних дій з боку державних органів та інших суб'єктів забезпечення кібербезпеки, встановлення конкретних строків та відповідальних за їх виконання структур, посилення відповідальності виконавців.

Використана література

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

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

3. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України": Указ Президента України від 16.05.19 р. № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2

4. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо

захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.20 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 96/2016.

6. Проект Стратегії кібербезпеки України (2021 – 2025). Безпечний кіберпростір – запорука успішного розвитку України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

7. Робоча група при НКЦК РНБО України схвалила проект Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4838.html

8. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

9. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.17 р. № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2

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

11. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. *Інформація і право.* № 1(28)/2019. С. 118-128.

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

УДК 343.14

ГРИЩЕНКО С.М., начальник підрозділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0002-5922-280X.
СТЕПАНОВ В.А., *кандидат технічних наук,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0002-5249-6883.

УМОВИ АВТОНОМНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ ПІД ЧАС ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

Анотація. *Стаття присвячена проблемі автономного доступу до інформації уповноважених органів під час зняття інформації з електронних комунікаційних мереж. Визначено поняття "єдина система технічних засобів". Запропонована структура єдиної системи технічних засобів. Наведені умови автономного доступу до інформації.*

Ключові слова: *автономний доступ, зняття інформації, електронна комунікаційна мережа, єдина система технічних засобів.*

Summary. *The article is devoted to the problem of autonomous access to information during interception of information from electronic communications network. The concept of "united system of technical means" is defined. Structure of united system technical means is proposed. The conditions for autonomous access are given.*

Keywords: *autonomous access, interception of information, electronic communication network, united system of technical means.*

Аннотация. *Статья посвящена проблеме автономного доступа к информации уполномоченных органов при снятии информации с электронных коммуникационных систем. Определено понятие "единая система технических средств". Предложена структура единой системы технических средств. Приведены условия автономного доступа к информации.*

Ключевые слова*: автономный доступ, снятие информации, электронная коммуникационная сеть, единая система технических средств.*

Постановка проблеми. У зв'язку з прийняттям Законів України "Про електронні комунікації" [1] та "Про розвідку" [2] актуальним стає питання автономного доступу уповноважених органів до інформації, що циркулює в електронних комунікаційних мережах, під час зняття інформації з використанням системи технічних засобів. В пункті 2 статті 121 Закону України [1] наведено, що зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством. В пункті 3 статті 15 Закону України [2] зазначається, що зняття інформації з транспортних телекомунікаційних мереж операторів телекомунікацій, які надають послуги мобільного та/ або фіксованого зв'язку, забезпечується системою технічних засобів, що використовується всіма розвідувальними органами на умовах автономного доступу до інформації у порядку, визначеному законодавством. На даний час в законодавстві та за результатами наукових досліджень не визначені умови автономного доступу до інформації в контексті зняття інформації з електронних комунікаційних (транспортних телекомунікаційних) мереж.

Результати аналізу наукових публікацій. Аспекти зняття інформації з телекомунікаційних мереж загального користування України досліджували Ю.Б. Балтер [3], А.В. Манжай [4], О.М. Мошков [3], С.В. Пеньков [4], І.К. Стішенко [5], інші науковці прикладних установ та фахівці уповноважених підрозділів. В більшості наукових робіт досліджувались теоретичні та прикладні проблеми побудови систем технічних засобів. Однак результати зазначених досліджень не відображають підхід з автономного доступу до інформації уповноважених органів, що планується забезпечувати єдиною системою технічних засобів зняття інформації з електронних комунікаційних мереж відповідно до Закону України [1], та як слід не визначені умови реалізації вказаного доступу.

Метою статті є визначення умов для реалізації уповноваженими органами автономного доступу до інформації під час проведення контррозвідувальних, оперативно-розшукових, розвідувальних заходів та негласних слідчих (розшукових) дій зі зняття інформації з електронних комунікаційних мереж з використанням єдиної системи технічних засобів.

Виклад основного матеріалу. Відповідно до статті 2 Директиви Європейського Парламенту і Ради (ЄС) [6] під "доступом" слід вважати забезпечення доступності засобів або комунікаційних послуг іншим суб'єктам господарювання на визначених умовах на виключній або невиключній основі, яка серед іншого охоплює доступ до мереж фіксованого, мобільного зв'язку та послуг віртуальних мереж, а також доступ до елементів мережі та пов'язаних засобів.

Згідно з розділом 2 наказу Держаної служби статистики України [7] "доступ до інформації" – це можливість одержання, оброблення, блокування та/чи порушення цілісності інформації. В той час в пункті 1.2 наказу Міністерства економіки України [8] визначено, що "доступ до електронних інформаційних ресурсів" є умовою отримання користувачем можливості обробляти і використовувати інформаційне наповнення ресурсу та правила обробки і використання цієї інформації.

Таким чином під доступом до інформації в контексті зняття інформації з електронних комунікаційних мереж слід розуміти не тільки можливість отримання інформації, а також її фіксацію та оброблення.

Термін "автономність" [9] має кілька значень. Одне із значень – незалежність від чого-небудь. Питанням стає визначення поняття "незалежність від чого-небудь або кого-небудь". В контексті єдиної системи технічних засобів О. Федієнко вважає [10], що автономний доступ – це доступ без участі оператора та система управління єдиною системою технічних засобів має знаходитися в Службі безпеки України. Автори статті не погоджуються з цією думкою та нижче надають пояснення іншої точки зору.

В пункті 2 статті 121 Закону України [1] введено поняття "єдина система технічних засобів", але визначення його не надається. Виходячи із практичного досвіду побудови та аналізу існуючих систем технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України, а також за результатами дослідження систем законного перехоплення телекомунікацій іноземного виробництва, пропонуємо вважати, що *єдина система технічних засобів є функціональним поєднанням засобів управління та обробки органів, уповноважених на зняття інформації з електронних комунікаційних мереж, засобів захищених транспортних мереж та мережного комплекту* (далі – МК), *що відноситься до категорії електронного комунікаційного обладнання.*

Вищезазначений МК призначений для забезпечення розпізнавання, відгалуження об'єктів зняття інформації (вмісту сеансів зв'язку абонентів спостереження – суб'єктів зняття інформації, даних про їх місцезнаходження та профілю послуг, що їм надаються), відбору та передачі даних до засобів управління та обробки кожного уповноваженого органу шляхом реалізації автономного доступу уповноважених органів до інформації. До складу МК будуть входити обладнання відбору об'єктів зняття інформації, що встановлюються у точках доступу (*access points*) – засобах електронної комунікаційної мережі (комутаційному обладнанні, шлюзових вузлах, регістрах та інших), та шлюзи, що встановлюються на сегменті електронної комунікаційної мережі постачальника послуг. Взаємодія обладнання відбору об'єктів зняття інформації з шлюзами здійснюється з використанням "внутрішнього" інтерфейсу, який у кожного виробника обладнання електронних комунікаційних мереж унікальний, та інтерфейсів на основі стандартизованих протоколів СКС-7, DIAMETER та SIP. Взаємодія шлюзів з засобами управління та обробки кожного уповноваженого органу здійснюється з використанням "зовнішнього" стандартизованого інтерфейсу.

Умови автономного доступу до інформації будуть забезпечені наступними факторами:

- наявністю у кожного уповноваженого органу окремих засобів управління та обробки;
- необхідністю проходження зазначеними засобами на шлюзах МК процедури автентифікації при кожному з'єднані з ними;
- формуванням кожним уповноваженим органом на підставі рішення суду, слідчого судді у випадках та порядку, передбачених законом, в окремих засобах управління та обробки індивідуальних ознак об'єктів зняття інформації;
- передаванням із зазначених вище засобів до шлюзів МК ознак об'єктів зняття інформації з використанням окремої захищеної транспортної мережі;
- керуванням процесом зняття інформації окремими командами управління кожним уповноваженим органом;
- наявністю в шлюзах МК у кожного уповноваженого органу окремої таблиці ознак об'єктів зняття інформації, при цьому технологічно зміст зазначеної таблиці не повинен бути доступним іншим уповноваженим органам;
- передаванням від МК до засобів управління та обробки кожного уповноваженого органу з використанням його захищеної транспортної мережі результатів зняття інформації, а саме: вмісту сеансів зв'язку абонентів спостереження (суб'єктів зняття інформації), даних про їх місцезнаходження та профілю послуг, що їм надаються;
- вибором в якості адміністратора роботи шлюзів МК структури, яка не залежить організаційно та фінансово від уповноважених органів (наприклад, підрозділ центрального органу виконавчої влади в сфері електронних комунікацій або постачальника послуг в відповідній електронній комунікаційній мережі);
- вибором кожним уповноваженим органом виробника засобів управління та обробки на конкурсній основі (виробником зазначених засобів має бути також відповідний підрозділ уповноваженого органу);
- проведенням оцінки засобів управління та обробки на відповідність вимогам нормативних документів у сфері електронних комунікацій, загальним вимогам, погоджених уповноваженими органами та державним органом виконавчої влади, що виконує функції технічного регулювання у сфері електронних комунікацій, вимогам

технічного регламенту за його наявністю та вимогам відповідних стандартів у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації за необхідністю;

- проведенням оцінки шлюзів МК на відповідність вимогам нормативних документів у сфері електронних комунікацій, загальним вимогам, які погоджені уповноваженими органами та державним органом виконавчої влади, що виконує функції технічного регулювання у сфері електронних комунікацій, та вимогам технічного регламенту за його наявністю.

Слід зазначити, що для організації доступу до будь-яких об’єктів зняття інформації з урахуванням характеристик та особливостей побудови електронних комунікаційних мереж необхідно використовувати технологічні можливості мереж при відгалуженні об’єктів зняття інформації. МК під час здійснення зняття інформації не повинні погіршувати якість послуг, що надаються споживачам послуг електронної комунікаційної мережі.

В пункті 3 статті 121 Закону України [1] введено поняття “точка підключення технічних засобів єдиної системи для автономного доступу до інформації в електронній комунікаційній мережі”, яку пропонуємо вважати шлюзом (шлюзами) МК, що виконує наступні основні функції:

- взаємодії з засобами управління та обробки кожного уповноваженого органу та з обладнанням відбору об’єктів зняття інформації;
- перетворення команд управління в команди взаємодії з електронною комунікаційною мережею;
- передавання в автоматичному режимі зазначених команд взаємодії;
- прийняття від обладнанням відбору об’єктів зняття інформації відгалужених об’єктів зняття інформації;
- зберігання ознак об’єктів зняття інформації в незмінному вигляді протягом терміну, необхідного для здійснення зняття інформації;
- захисту від несанкціонованого доступу до інформації, яка містить ознаки об’єктів зняття інформації, дані взаємодії з електронною комунікаційною мережею та об’єкти зняття інформації;
- буферизації (тимчасового проміжного зберігання інформації для запобігання її втрати) вмісту об’єктів зняття інформації у випадку пошкодження каналів захищених транспортних мереж між шлюзом та засобами управління та обробки.

Висновки.

Визначені поняття “єдина система технічних засобів” та “точка підключення технічних засобів єдиної системи для автономного доступу до інформації в електронній комунікаційній мережі” відповідають основним концептуальним вимогам технічного комітету “Законне перехоплення телекомунікацій” (TC LI) Європейського інституту телекомунікаційних стандартів (ETSI) та можуть бути рекомендовані для врахування в роботі фахівцям та науковцям, задіяним у заходах зі зняття інформації з електронних комунікаційних мереж.

Наведені умови автономного доступу до інформації доцільно враховувати під час розробки та побудови єдиної системи технічних засобів, проведенні оцінки відповідності мережного комплекту та підготовки відповідного порядку щодо зняття інформації з електронних комунікаційних мереж, який має бути затвердженим спільним наказом відповідних уповноважених органів та державного органу виконавчої влади, що виконує функції технічного регулювання у сфері електронних комунікацій.

Використана література

1. Про електронні комунікації: Закон України від 16.12.20 р. № 1089-IX. *Офіційний вісник України*. 2021. № 6 (26.01.2021). Ст. 306.

2. Про розвідку: Закон України від 17.09.20 р. № 912-IX. *Урядовий кур'єр* від 04.11.20 р. № 214.

3. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги: наказ Служби безпеки України і Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 04.09.18 р. № 1559/533. URL: https://zakononline.com.ua/documents/show/399084___399149 (дата звернення: 11.03.2021).

4. Манжай А.В., Пеньков С.В. Стандартизация в сфере законного перехвата телекомуникаций. *Legia si Vista*. 2017. № 5/2. С. 86-89. URL: https://www.researchgate.net/profile/Oleksandr_Manzhai/publication/337991533_Standartizatsiia_v_Sfere_Zakonnogo_Perekhvata_Telekommunikatsii_Standardization_in_the_Field_of_Lawful_Interception_of_Telecommunications/links/5df9211092851c8364854202/Standartizatsiia-v-Sfere-Zakonnogo-Perekhvata-Telekommunikatsii-Standardization-in-the-Field-of-Lawful-Interception-of-Telecommunications.pdf (дата звернення 11.03.2021).

5. Степанов В.А., Стішенко І.К. Особливості дозволеного законом перехоплення інформації з телекомунікаційних мереж. *Спеціальні телекомунікаційні системи та захист інформації*. 2005. № 10. С. 76-80.

6. Про запровадження Європейського кодексу електронних комунікацій: директива Європейського Парламенту і Ради ЄС від 11 грудня 2018 р. № 2018/1972. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text (дата звернення: 11.03.2021).

7. Методологічні положення щодо забезпечення статистичної конфіденційності в органах державної статистики: наказ Державної служби статистики України від 15.02.17 р. № 41. URL: http://www.dneprstat.gov.ua/diyalnist/Nakaz%2041.pdf (дата звернення: 11.03.2021).

8. Порядок планування, формування, створення, функціонування, супроводження, систематизації електронних інформаційних ресурсів Міністерства економіки України та доступу до них: наказ Міністерства економіки України від 16.07.10 р. № 854. URL: https://zakon.rada.gov.ua/rada/show/v0854665-10#Text (дата звернення: 11.03.2021).

9. Автономність. URL: https://uk.wikipedia.org/wiki/Автономність (дата звернення: 11.03.2021).

10. Олександр Федієнко. URL: https://mind.ua/publications/20220824-oleksander-fedienko-siloviki-vzhe-mayut-avtonomnij-dostup-do-mobilnih-merezh-bez-uchasti-operatora (дата звернення: 11.03.2021).

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

УДК 455:343.35

ГРЕСЬ О.М., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid.org/0000-0003-3642-4975.

КОРУПЦІЙНІ РИЗИКИ ПІД ЧАС ЗДІЙСНЕННЯ ОБОРОННИХ ЗАКУПІВЕЛЬ

Анотація. *У статті проведено аналіз чинних нормативно-правових актів у сфері оборонних закупівель, висвітлено деякі недоліки Закону України "Про оборонні закупівлі", а також проаналізовано корупційні ризики, які можуть з'явитися в результаті реалізації положень Закону "Про оборонні закупівлі".*

Ключові слова: *корупція, корупційні ризики, національна оборона, оборонні закупівлі, національна безпека.*

Summary. *The article is devoted to the analysis of current regulations in the field of defense procurement. The importance of the problem of corruption for the people of Ukraine is highlighted. The threat to national security caused by high levels of corruption is mentioned. A number of studies on the spread of corruption in the defense sector are processed, in particular by such public organizations as the Independent Anti-Corruption Committee on Defense, Transparency International UK, Transparency International Ukraine and others. Attention is drawn to the presence of a large number of corruption risks in the defense sector. The Law of Ukraine "On Defense Procurement", adopted by the Verkhovna Rada of Ukraine on July 17, 2020, was analyzed. Attention is paid to the fact that the Law of Ukraine "On Defense Procurement" provides for the purchase of goods, works and services for defense purposes, which is a state secret, through closed procurement, and it also regulates the absence of competitive procedures for procurement by import by making purchases directly through electronic trading platforms. Some aspects of the Law of Ukraine "On Public Procurement" used in defense procurement are considered. Based on the results of the analysis, it was concluded that the Law of Ukraine "On Defense Procurement" helps to overcome most of the corruption risks identified in the study of the Independent Anti-Corruption Committee on Defense, however, it also needs significant improvement, as some provisions contain gaps that lead to new corruption risks, if they are not corrected.*

Keywords: *corruption, corruption risks, national defense, defense procurement, national security.*

Аннотация. *В статье проведен анализ действующих нормативных документов в сфере оборонных закупок, приведены некоторые недостатки Закона Украины "Об оборонных закупках", а также проведен анализ коррупционных рисков, которые могут появиться в результате реализации положений Закона "Об оборонных закупках".*

Ключевые слова: *коррупция, коррупционные риски, национальная оборона, оборонные закупки, национальная безопасность.*

Постановка проблеми. Корупція для населення України є другою за значущістю суспільною проблемою після військових дій у Донецькій і Луганській областях. Такі результати опитування підприємців, експертів і населення презентували фахівці Антикорупційної ініціативи ЄС в Україні разом з Національним агентством з питань запобігання корупції [1]. Про високий рівень корупції в Україні також свідчить індекс сприйняття корупції, який опубліковано антикорупційною громадською організацією Transparency International Ukraine за 2019 рік [2].

Сьогодні на забезпечення національної безпеки та оборони в Україні виділяється значна частина фінансових ресурсів [3], оскільки наша держава повинна захищати свою

територіальну цілісність та незалежність, особливо у зв'язку з агресією з боку Російської Федерації. Проте необхідно зазначити, що корупція є ключовою загрозою національній безпеці та має системний характер. Це, в свою чергу, впливає на інші загрози у сфері безпеки, сприяючи діяльності організованої злочинності, та позбавляє державу можливостей виконувати покладені на неї функції, а також стримує економічний розвиток. Вочевидь, прояви корупції у оборонній сфері підривають авторитет влади і заважають ефективному управлінню державою, тим самим можуть завдати значної шкоди й обороноздатності України.

Результати аналізу наукових публікацій. Серед українських та зарубіжних науковців, у працях яких досліджувалася проблематика протидії корупції у сфері державних закупівель, варто назвати таких, як В. Трепак, В. Лунеєв, А. Закалюк, П. Чебоксаров, А. Кузьмін, К. Фрідріх, Д. Саймон, Д. Ейтцен, Дж. Най, С. Роуз-Аккерман, Т. Супрун [4], В. Гаращук, А. Мухатаєв, О. Пархоменко-Куцевіл [5], Л. Шестопалова [6], А. Кривенко [7].

Проте дослідження корупції в оборонній сфері України, у зв'язку з надмірною засекреченістю оборонних закупівель, здійснюють лише декілька недержавних (неурядових) громадських організацій, серед яких виділяються Незалежний антикорупційний комітет з питань оборони (далі – НАКО), Центр протидії корупції, Transparency International Україна. Тому дана сфера є невідомою для більшості науковців.

Метою статті є аналіз чинних нормативно-правових актів у сфері оборонних закупівель та виявлення корупційних ризиків, які можуть бути реалізовані виходячи з наявного законодавства.

Виклад основного матеріалу. За результатами дослідження НАКО було виявлено 12 основних корупційних ризиків [8]:

1) відсутність централізованої автоматизованої бази даних з інформацією про виробників озброєння та військової техніки;

2) брак сучасних засобів обробки інформації на етапі планування державного оборонного замовлення (далі – ДОЗ), доступу до інформації про потреби сектору оборони;

3) складність кваліфікації як виконавця ДОЗ;

4) неузгодженість законодавства в частині затвердження ДОЗ;

5) надмірна засекреченість ДОЗ;

6) відсутність конкурентних процедур у таємних закупівлях;

7) обмеження максимального прибутку постачальників;

8) відсутність конкурентних процедур при закупівлі за імпортом;

9) обмеження можливостей Управління військових представництв МО України щодо перевірки інформації під час реалізації оборонних закупівель;

10) зміна вартості продукції (послуг) під час виконання контракту;

11) розмитість відповідальності у сфері контролю за виконанням ДОЗ;

12) відсутність сучасних автоматизованих систем обробки інформації на етапі звітування про виконання ДОЗ.

Пропонуємо більш детально розглянути пункти 1 – 3, 5, 6, 8, 12, наведених у дослідженні НАКО.

З метою узгодження правил оборонних закупівель зі стандартами країн-партнерів ЄС та НАТО у частині, що стосується оборонної Директиви 2009/81/ЄС, а також Угоди про Асоціацію з ЄС, 17 липня 2020 року Верховною Радою України прийнято Закон України "Про оборонні закупівлі" (далі – Закон), яким визначено загальні правові засади планування, порядок формування обсягів та особливості здійснення закупівель товарів,

робіт і послуг оборонного призначення для забезпечення потреб сектору безпеки і оборони та інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони, а також порядок здійснення державного і демократичного цивільного контролю у сфері оборонних закупівель.

Постанова Кабінету Міністрів України "Питання державного оборонного замовлення" від 27 квітня 2011 року № 464 (далі – Постанова КМ України № 464) визначає державне оборонне замовлення як "засіб державного регулювання економіки для задоволення наукових та матеріально-технічних потреб із забезпечення національної безпеки і оборони шляхом планування обсягу фінансових ресурсів, визначення видів та обсягів продукції, робіт і послуг, а також укладення з виконавцями державних контрактів на постачання (закупівлю) продукції, робіт і послуг" [9]. Водночас з'являється юридична колізія, оскільки діюча Постанова КМ України № 464 містить посилання на вже не чинний Закон України "Про державне оборонне замовлення". При цьому в Законі України "Про оборонні закупівлі" не використовується поняття "державне оборонне замовлення", а вживається дещо інший термін, а саме "оборонні закупівлі", під яким пропонують розуміти здійснення державним замовником закупівель товарів, робіт і послуг, призначених для виконання державних програм у сферах національної безпеки і оборони, а також інших товарів, робіт і послуг для гарантованого забезпечення потреб безпеки і оборони" [10].

Слід зауважити, що прийнятий Закон України "Про оборонні закупівлі" скасовує застарілу радянську систему ціноутворення за розрахунково-калькуляційними матеріалами, що зменшує вірогідність корупційних ризиків, які наведені у дослідженні НАКО.

За результатами формування Міністерством економічного розвитку і торгівлі України електронного реєстру учасників відбору та виконавців державних контрактів, передбаченого Законом України "Про оборонні закупівлі", можливо усунути такі корупційні ризики, як: відсутність централізованої автоматизованої бази даних з інформацією про виробників озброєння та військової техніки; брак сучасних засобів обробки інформації на етапі планування ДОЗ; обмеження доступу до інформації про потреби сектору оборони. Згідно Закону електронний реєстр учасників відбору та виконавців державних контрактів (договорів) – це система накопичення, обробки, обліку, захисту та надання даних інформації про учасників відбору та виконавців державних контрактів (договорів) (далі – Реєстр).

Реєстр повинен забезпечувати систематизацію та здійснення ретроспективного аналізу даних щодо суб'єктів господарювання в оборонних закупівлях за такими класифікаційними ознаками:

1) номенклатура товарів, робіт, послуг оборонного призначення, що виробляється суб'єктом господарювання, робіт і послуг, що виконуються таким суб'єктом;

2) ціна на товари, роботи, послуги оборонного призначення, у тому числі, але не виключно, фіксована ціна на товари, роботи, послуги оборонного призначення, у тому числі за результатами попередніх закупівель, з додержанням законодавства про захист інформації;

3) фінансово-економічний стан підприємства;

4) наявність окремих видів виробничої діяльності підприємства;

5) наявність необхідних виробничих потужностей та технічної спроможності підприємства;

6) наявність необхідних об'єктів права інтелектуальної власності;

7) виконання або участь у виконанні науково-дослідних та інших робіт;

8) наявність потенційних підстав, передбачених Законом, для відмови в укладенні контракту (договору) за результатами торгів.

Проте не зрозуміло, як новостворений суб'єкт господарювання зможе потрапити до Реєстру (скільки часу на це витрачатиметься) та як часто він буде оновлюватися. Слід зазначити, що це ще не весь перелік питань, які залишаються на сьогодні невирішеними. Ці питання повинні бути врегульовані в підзаконних актах, що мали б бути впродовж шести місяців прийняті Урядом України та міністерствами на виконання вимог Закону. Проте, на даний час такі акти не прийнято.

У Стратегічному оборонному бюлетені України (введений в дію Указом Президента України від 06.06.16 р. № 240/2016 [11]) йдеться про необхідність зміни підходів до захисту державної таємниці та розсекречення оборонних закупівель.

Проте, прихильники старої системи закритих закупівель намагалися [12], та і досі намагаються згорнути, або хоча б загальмувати реформу оборонно-промислового комплексу країни [13]. Вважаємо, що таке "засекречування" відіграє свою роль в неефективному використанні бюджетних коштів та формуванні корупційних схем, що негативно впливає на обороноздатність та державну безпеку.

Новим Законом України "Про оборонні закупівлі" передбачено придбання товарів, робіт і послуг оборонного призначення, що становить державну таємницю, шляхом проведення закритих закупівель. Порядок проведення закритої закупівлі передбачає можливість проведення переговорів (поетапних переговорів) із суб'єктами господарювання, які внесені до Реєстру. Такий вид закупівель застосовується виключно до товарів, робіт і послуг оборонного призначення, що становлять державну таємницю, і здійснюється без застосування електронної системи закупівель.

У разі, якщо за результатами відбору встановлено, що визначеним критеріям відповідає лише один внесений до Реєстру суб'єкт господарювання або для участі у переговорах надійшла лише одна пропозиція, укладення державним замовником державного контракту (договору) здійснюється за результатами переговорів. Якщо ж вартість закупівлі у єдиного виконавця дорівнює або перевищує 200 мільйонів гривень, державний замовник скликає міжвідомчу комісію у складі відповідальних осіб державного замовника, представників інших державних замовників і центральних органів виконавчої влади.

Водночас, Законом передбачено, що порядок проведення переговорів, порядок укладення державного контракту (договору) з єдиним виконавцем, а також положення про міжвідомчу комісію та її склад розробляються головним органом у сфері здійснення оборонних закупівель і затверджуються Кабінетом Міністрів України. На даний час Міністерство оборони України та Міністерство з питань стратегічних галузей промисловості не забезпечили у визначений Законом термін розроблення та прийняття підзаконних актів, необхідних для реалізації положень Закону України "Про оборонні закупівлі" [14]. Це може привести до невиконання ДОЗ на 2021 рік.

Слід зауважити, що Закон врегульовує конкурентні процедури при закупівлі за імпортом шляхом здійснення закупівель напряму через електронні торговельні майданчики. Наприклад, у випадку відсутності потрібного обладнання в Україні або його імпортують в Україну посередники зі значними націнками. До таких торгівельних майданчиків належать, наприклад, NSPA та FMS [15]. Проте поки що не відомо, чи є ці майданчики публічними.

Закон чітко визначає умови, коли можна змінити вартість продукції (послуг) під час виконання контракту. Разом з цим у Законі визначено можливість замовника встановлювати такий критерій оцінки пропозиції учасника, як локалізація виробництва.

Це питома вага вартості сировини, матеріалів, вузлів, агрегатів, деталей і комплектуючих виробів вітчизняного походження, а також виконання робіт та надання послуг вітчизняними виробниками на митній території України у вартості товарів, робіт і послуг, що є предметом закупівлі. Державний замовник може особисто визначати – використовувати цей критерій чи ні, з урахуванням того, що питома вага локалізації виробництва повинна бути не менше 25 %. Отже, учасник з українським товаром отримає перемогу в аукціоні навіть тоді, якщо його ціна є вищою за ціну конкурентів. Проте Закон та інші чинні нормативно-правові акти не містять порядку визначення ступеня локалізації чи шляхів його підтвердження. Це, в свою чергу, створює додаткові нові корупційні ризики.

Необхідно також звернути увагу на торги з обмеженою участю, оскільки ані Закон "Про публічні закупівлі", ані Закон "Про оборонні закупівл" не визначають, у яких випадках замовник повинен обрати таку процедуру закупівлі, для яких товарів або очікуваної вартості тощо. Тож можна припустити, що обрання такої процедури – це виключно вибір замовника, який він може зробити без обмежень в будь-який час.

Є також і деякі дрібні розбіжності між Законом України "Про оборонні закупівлі" та Законом України "Про публічні закупівлі" [16] у частині, що стосується підстав для скасування процедур закупівель. За Законом України "Про публічні закупівлі" замовник скасовує торги (відкриті) у випадку подання менше двох пропозицій, а за Законом України "Про оборонні закупівлі" – у випадку неподання жодної пропозиції [17]. Отже, така норма дозволяє проводити замовникам спрощені торги із застосуванням електронної системи закупівель навіть у випадку подання лише однієї цінової пропозиції.

Висновки.

Підсумовуючи викладене, можна дійти висновку, що Закон України "Про оборонні закупівлі" потребує значного доопрацювання, оскільки його окремі положення містять прогалини, що мають бути обов'язково усунені. Зокрема, слід: Постанову 464 привести у відповідність до Закону України "Про оборонні закупівлі"; врегулювати порядок визначення ступеню локалізації виробництва та шляхів його підтвердження; визначити випадки, в яких можуть використовуватись торги з обмеженою участю; унормувати процес скасування відкритих торгів тощо. Також, потрібно прийняти нормативно-правові акти для реалізації положень Закону, ввести в дію Реєстр учасників відбору та виконавців державних контрактів (договорів) з оборонних закупівель.

З урахуванням наведеного, вважаємо, що сфера оборонних закупівель потребує подальших досліджень та удосконалення законодавства.

Використана література

1. Корупція в Україні 2020: розуміння, сприйняття, поширеність: презентація результатів дослідження *Антикорупційна ініціатива ЄС в Україні*. URL: https://euaci.eu/ua/news/prezentaciya-doslidzhennya-korrupciya-v-ua-2020 (дата звернення: 15.02.2021).

2. Індекс сприйняття корупції-2020. *Transparency International Ukraine*. URL: http://cpi.ti-ukraine.org/#/ (дата звернення: 15.02.2021).

3. Президент підписав закон про Державний бюджет України на 2020 рік. URL: https://www.president.gov.ua/news/prezident-pidpisav-zakon-pro-derzhavnij-byudzhet-ukrayini-na-58837 (дата звернення: 15.02.2021).

4. Супрун Т.М. Зарубіжний досвід запобігання та протидії корупції. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2017. № 2. С. 199-204.

5. Пархоменко-Куцевіл О. Теоретико-методологічні підходи до класифікації корупційних відносин в Україні. *Підприємництво, господарство і право.* 2018. № 9. С. 138-142.

6. Шестопалова Л. Відмежування корупційних правопорушень від правопорушень, пов'язаних із корупцією. *Підприємництво, господарство і право.* 2017. № 5. С. 193-197.

7. Кривенко А.Л. Шляхи протидії корупції у сфері державних закупівель. *Інформація і право*. № 3(34)/2020. С.104-109.

8. Реформа державного оборонного замовлення. – (НАКО). URL:https://nako.org.ua/publication/reforma-derzhavnoho-oboronnoho-zamovlennia-analitychna-zapyska (дата звернення: 24.02.2021).

9. Питання державного оборонного замовлення: Постанова Кабінету Міністрів України від 27.04.11 р. № 464. URL: https://zakon.rada.gov.ua/laws/show/464-2011-п#Text (дата звернення: 15.02.2021).

10. Про оборонні закупівлі: Закон України від 17.07.20 р. № 808-IX. URL: https://zakon. rada. gov.ua/laws/show/808-20#Text (дата звернення: 10.02.2021)

11. Про Стратегічний оборонний бюлетень України: Рішення Ради національної безпеки і оборони України від 20.05.16 р. URL: https://zakon.rada.gov.ua/laws/show/240/2016#n10 (дата звернення: 24.02.2021).

12. Чиновник з Мінекономрозвитку звільнився через "тиск і зловживання" у сфері оборонки. *Громадське Телебачення*. URL: https://hromadske.ua/posts/chynovnyk-z-minekonomrozvytku-zvilnyvsia-cherez-tysk-i-zlovzhyvannia-u-sferi-oboronky (дата звернення: 24.02.2021).

13. Укроборонпром звинувачує в зриві реформи ОПК міністерство Уруського. *Наголос.* URL: https://nagolos.com/news/ukroboronprom-zvinuvachuє-v-zrivi-reformi-opk-ministerstvo-uruskogo (дата звернення: 24.02.2021).

14. Два міністерства не виконали Указ Зеленського щодо оборонних закупівель. URL: https://zaxid.net/dva_ministerstva_ne_vikonali_ukaz_zelenskogo_shhodo_oboronnih_zakupivel_n1514527 (дата звернення: 24.02.2021)

15. . Завдяки приєднанню до організації NSPA, Міноборони може робити закупівлі без посередників. – (Міністерство оборони України). URL: https://www.mil.gov.ua/news/2020/01/22/zavdyaki-priednannyu-do-organizaczii-nspa-minoboroni-mozhe-robiti-zakupivli-bez-poserednikiv (дата звернення: 24.02.2021).

16. Про публічні закупівлі: Закон України від 25.12.15 р. № 922-VIII. URL: https://zakon. rada.gov.ua/laws/show/922-19#Text (дата звернення: 24.02.2021).

17. Що чекати від нового закону "Про оборонні закупівлі". *Наші Гроші*. URL: https://nashigroshi.org/2020/07/26/zakupivel-nyy-faq-shcho-chekaty-vid-novoho-zakonu-pro-oboronni-zakupivli (дата звернення: 24.02.2021).

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

УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, професор.*
НДІ інформатики і права НАПрН України.
ТАРАСЮК А.В., *кандидат юридичних наук*. НДІ інформатики і права НАПрН України.

НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В КІБЕРНЕТИЧНІЙ СФЕРІ

Анотація. *У статті проаналізовано основні засади розвитку національних інтересів України в кібернетичній сфері, а також визначені пов'язані із цим актуальні проблеми забезпечення кібербезпеки.Обґрунтовано, що нормативно-правова база – головна передумова забезпечення кібербезпеки держави. За результатами дослідження визначені можливі шляхи вирішення відповідних проблем та підвищення ефективності забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, національні інтереси.*

Summary. *The article analyzes the main principles of development of national interests of Ukraine in the cyber sphere, as well as identifies related current issues of cybersecurity. It is substantiated that the legal framework is the main prerequisite for ensuring cybersecurity of the state. According to the results of the study, possible ways to solve the relevant problems and increase the effectiveness of cybersecurity are identified.*

Keywords: *cybersecurity, information security, cyberspace, cyberthreats, national interests.*

Аннотация. *В статье проанализированы основные принципы развития национальных интересов Украины в кибернетической сфере, а также определены связанные с этим актуальные проблемы обеспечения кибербезопасности. Обосновано, что нормативно-правовая база – главная предпосылка обеспечения кибербезопасности государства. По результатам исследования определены возможные пути решения соответствующих проблем и повышения эффективности обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, информационная безопасность, киберпространство, киберугрозы, национальные интересы.*

Постановка проблеми. У другому десятилітті XXI ст. завдяки небувалому прогресу техніки й інформаційно-телекомунікаційних технологій наші традиційні уявлення про відстані та часовий простір зазнали докорінних змін, внаслідок яких сформувався новий тип цивілізації – інформаційна. Сутність інформаційної цивілізації полягає у розвитку Інтернет-технологій і розширенні супутникового зв'язку, у практично необмежених в обсязі взаєминах і спілкуванні поза просторовими рамками, у розробці та миттєвому поширенні інформації і новин, а також появі та розвитку цифрової дипломатії.

У зазначених умовах глобальний кіберпростір перетворюється на майданчик зіткнення економічних, політичних і культурних інтересів та центрів сили сучасного світу, на дієвий інструмент формування громадської думки та її спрямування в інтересах певних гравців. Слід визнати, що поряд із позитивними і конструктивними тенденціями, які забезпечують поінформованість про новітні досягнення людства у ході розвитку світового кіберпростору, можна помітити і негативні процеси, що містять ризики для кібербезпеки держав, зокрема й України.

З огляду на зазначене, забезпечення кібербезпеки України має бути головною метою і в межах реалізації та відстоювання цієї мети слід прикладати значні зусилля для виконання таких завдань:

– забезпечення адекватного і реального сприйняття широкою міжнародною громадськістю суті зовнішньої та внутрішньої політики України;

– сприяння створенню ефективних засобів інформаційного впливу на закордонну громадську думку з метою позитивного сприйняття України;

– здійснення активної міжнародної співпраці в інформаційній сфері;

– розширення можливостей засобів масової інформації країни в міжнародному кіберпросторі;

– своєчасна й ефективна протидія кіберзлочинам і кіберзагрозам державній незалежності та національним інтересам України, духовно-етичним цінностям українського народу та історичним святиням.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмету дослідження, а також творчий доробок відомих вчених, зокрема О. Сегеда, С. Харченко, Т. Ткачук, А. Носач, А. Баровська, Н. Литвин та ін.

Метою статті є визначення концептуальних засад правового співвідношення інформаційної та кібернетичної безпеки на сучасному етапі з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. Україна є прихильницею розробки комплексу міжнародних правових та етичних норм, націлених на забезпечення кібербезпеки, та їхнього всебічного дотримання у світовому кіберпросторі. Зважаючи на це, реалізація інформаційної дипломатії України спиратиметься на широке використання можливостей сучасних інформаційно-комунікаційних технологій [1, с. 141].

Аналіз актуальних загроз конфіденційній інформації, на основі якого формується система кібербезпеки і будується організація захисту інформації, розпочинається з усвідомлення та класифікації цих загроз. У зв’язку із цим підкреслимо, що теорія кібербезпеки оперує кількома формами класифікації інформаційних ризиків і загроз захисту інформації. Вважаємо за доцільне акцентувати увагу на поділі загроз кібербезпеці, що бувають зовнішніми і внутрішніми.

У разі зовнішніх атак супротивник відшукує слабкі місця в інформаційній структурі, що уможливлять доступ до ключових вузлів внутрішньої мережі, сховищ даних, локальних комп’ютерів співробітників. При цьому зловмисник використовує широкий набір інструментів і шкідливе програмне забезпечення для виведення з ладу систем захисту, шпигунства, фальсифікації або знищення даних, копіювання, завдання шкоди об’єктам власності тощо. З огляду на це не дивно, що у доповіді Всесвітнього економічного форуму “Глобальні ризики 2012” (“Global Risks 2012”) [2] кібератаки визначені як одна з основних загроз світовій економіці. За ймовірністю настання кібератаки входять до п’ятірки найбільших потенційних глобальних загроз. Зазначений висновок Всесвітнього економічного форуму доводить значну актуальність і велику небезпеку електронної злочинності. Спектр загроз кібербезпеці, викликаних застосуванням шкідливого програмного забезпечення, дуже широкий. Нині, наприклад, фахівці виокремлюють такі види загроз захисту інформації [3 – 5]:

– упровадження вірусів та застосування інших руйнівних програмних впливів;

– упровадження програм-шпигунів з метою аналізу мережевого трафіку й отримання даних про систему та стан мережевих з’єднань;

– аналіз і модифікація/знищення встановленого програмного забезпечення;

– розкриття, розкрадання та перехоплення секретних паролів і кодів;

– використання вразливостей ПЗ для виведення з ладу програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їхньої доступності;

– блокування роботи користувачів системи програмними засобами тощо.

Варто відзначити, що нами наведено базовий склад загроз кібербезпеці держави, у зв'язку з тим, що вичерпний перелік таких загроз зробити не можливо. Адже вони, значною мірою, залежать від динаміки розвитку суспільно-політичної та міжнародної обстановки. З огляду на це стали реальними загрози: а) створенню і розвитку національної індустрії інформації, зокрема й індустрії засобів інформатизації, зв'язку та телекомунікації, задоволенню потреб внутрішнього ринку в її продукції, а також забезпеченню накопичення, ефективного використання та збереження вітчизняних і зарубіжних інформаційних ресурсів; б) безпеці інформаційних і телекомунікаційних засобів та систем, як створюваних на території України, так і вже розгорнутих й упроваджуваних.

Згідно з теоретичними і практичними джерелами складовими кібербезпеки є:

– стан безпеки кіберпростору, за якого забезпечується його формування і розвиток в інтересах держави, організацій та громадян;

– стан безпеки інформаційної інфраструктури, за якого інформація використовується суворо за призначенням і при цьому не здійснює негативного впливу на об'єкт;

– стан безпеки самої інформації, за якого унеможливлюється або суттєво ускладнюється погіршення таких її характеристик, як конфіденційність, доступність, цілісність.

Нині ні в кого не викликає заперечень, що нормативно-правова база – *головна передумова забезпечення кібербезпеки держави*. А важливою складовою нормативно-правової бази забезпечення кібербезпеки є також сукупність правових норм, що регламентують відносини у сфері функціонування органів держави, які входять до складу системи забезпечення кібербезпеки України. Варто підкреслити, що останнім часом дедалі вагомішого значення набуває взаємодія державних органів із громадськими організаціями та громадянами. У цьому контексті розвиток державно-приватного партнерства має стати одним із пріоритетних завдань державної політики у забезпеченні кібербезпеки.

Інша проблема, яка потребує теоретичного осмислення та практичного вирішення це рівень інформаційно-просвітницької, ідеологічної й освітньої роботи із протидії радикальній ідеології та екстремізму. Така робота потребує значного посилення. Серед найбільших проблем можемо виокремити, зокрема такі:

– брак фахівців у галузі інформаційної протидії екстремізму і тероризму;

– недостатня кількість інформаційної та довідкової літератури стосовно екстремістських і терористичних організацій;

– спостерігається відсутність пропаганди та наочної агітації;

– слабка роль засобів масової інформації у запобіганні та профілактиці екстремізму, а також у висвітленні антитерористичної й антиекстремістської діяльності державних органів.

У розрізі зазначеного ми підтримуємо думку авторів статті "Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти", що запобігти екстремізму можна лише спільними зусиллями державних органів та громадськості, спрямованими на підвищення правової і загальної культури населення,

поліпшення соціально-економічних умов життя людей, формування позитивного іміджу держави [6, с. 43].

Зважаючи на це, необхідно вживати дієвих заходів із формування потужного ідеологічного корпусу, зміцнення його потенціалу в запобіганні радикалізації й екстремізму, із підготовки фахівців у напрямі інформаційної протидії тероризму й екстремізму, підвищення профілактичної ролі засобів масової інформації та інституційного забезпечення аналітичної, пропагандистської й інформаційної роботи в цій площині. Отже, питання забезпечення кібербезпеки, проблеми зовнішньої та внутрішньої загрози і протидії інформації, де пропагують релігійно-екстремістські і терористичні ідеї та явища в Україні, є одними з найактуальніших завдань суспільства й уряду на найближчу перспективу. Слід наголосити, що в нинішніх умовах радикальна ідеологія активніша, ніж будь-коли, і створює серйозну загрозу конституційному ладу держави. Дотепер в Україні таємно ведуть пропагандистську підривну діяльність рухи й організації релігійно-екстремістського напряму, що містять основну загрозу миру та стабільності держави.

До найнебезпечніших загроз безпеці в сучасній Україні в зазначеній сфері також належать:

– наявність зовнішніх і внутрішніх центрів політичної, релігійної, міжнаціональної та іншої напруженості у прикордонних районах суміжних Україні країн;

– збільшення на державному кордоні та прикордонній території масштабів розвідувально-підривної діяльності іноземних спецслужб;

– здійснення бандформуваннями бойових дій і терористичних акцій у прикордонній смузі та прикордонних територіях, зокрема проти військ й органів Державної прикордонної служби України.

Отже, з огляду на зазначене вище варто підкреслити, що державним органам необхідно вдосконалювати нормативно-правові акти, які регулюють питання протидії використанню Інтернету в терористичних й екстремістських цілях, а також забезпечують національні інтереси суверенної України в інформаційній сфері.

Іншим важливим напрямом державної політики у сфері правового забезпечення кібербезпеки України на сучасному етапі включення України у глобальні інформаційні процеси є міжнародний чинник.

Не викликає жодних сумнівів той факт, що виникнення нових засобів інформації і комунікації та їхнє поширення у країнах сучасного світу є одним із найвагоміших чинників процесу глобалізації. Стрімке розширення інформаційної та комп’ютерної павутини зменшило відстань між людьми в різних регіонах нашої планети ще більше, ніж розвиток шляхів наземної, повітряної та водної комунікації. Щоб уявити всю глибину інформаційної трансформації, яка відбувається останнім часом, і зрозуміти динаміку, необхідно усвідомити: в умовах глобальної інформатизації зникає географія, стираються межі між зовнішньою та внутрішньою політикою, що неминуче деформує не лише “національну”, але й “соціальну” ідентичності. Глобальна інформатизація розкриває багатопланові можливості для соціального інтегрування та транснаціональної взаємодії людей. Інтернет створює інші реалії для вільних контактів між людьми, які мешкають у різних країнах і є членами недержавних об’єднань.

Завдяки застосуванню сучасних інформаційно-комунікаційних технологій уявлення суб’єктів у реальному часі інтернаціоналізуються рідше, а їхню оцінку й відповідь на різні міжнародні події можна почути одразу ж після події. Усе це сприяє веденню дискусій на міжнародному рівні, створенню асоціацій між новими учасниками політичної інтерактивності.

Щоб розв'язати проблему "цифрового розриву", міжнародне співтовариство здійснює важливі кроки. На саміті "Великої вісімки", що проходив у липні 2000 р. в Японії (Окінава), наприклад, було ухвалено "Хартію глобального інформаційного співтовариства" [7]. У документі вперше у світовий контекст було введено поняття "цифровий розрив" й одним з основоположних принципів визначено імператив доступності інформаційних технологій для громадян усіх держав світу. Відповідно до основних положень Хартії було засновано міжнародну експертну раду "Група з можливостей цифрових технологій" (Digital Opportunity Task Force, G8DOT Force), головним завданням якої є пошук шляхів подолання існуючої нерівності між різними державами у доступі до новин та інформації. Рада також розробила програму дій і представила її очільникам держав "вісімки" на саміті, що проходив улітку 2001 р. в Генуї. Результати саміту уможливили вироблення плану конкретних рекомендацій (т. зв. "генуезька ініціатива") стосовно зазначеного питання [8]. Слід додати, що нині ініціатива з координації дій програми перейшла до Міжнародної експертної ради з інформаційно-комунікаційних технологій ООН, яку згодом було перетворено в Робочу (цільову) групу ООН з інформаційно-комунікаційних технологій (ІКТ). Виконання завдання подолання інформаційної нерівності в загальному контексті боротьби з бідністю нині покладено на ООН. Крім того, ООН у межах надання допомоги у впровадженні інформаційних технологій країнам, що розвиваються, ухвалила рішення про створення спеціального фонду обсягом 500 млн. дол. Звісно, цього поки що явно недостатньо для врегулювання проблеми. З огляду на це можна зробити висновок, що нині розвиток і поширення інформаційно-комунікативних технологій у державах світу проходить дуже незбалансовано, щоб стати переконливою передумовою для соціальної інтеграції та рівності у масштабі всієї планети. Подолання цифрової нерівності сьогодні стало пріоритетом у багатьох міжнародних організаціях. Проблема особливо посилилась з поширенням на планеті коронавірусної інфекції COVID-19 [9].У цій ситуації ми спостерігаємо й іншу сторону проблеми: протягом останнього року спостерігалося безпрецедентне впровадження цифрових технологій в усі сфери життя. Працівники почали виконувати свою роботу он-лайн, освітні заклади усіх рівнів перейшли на дистанційну форму навчання, що значно підвищило рівень обізнаності щодо інформаційно-комунікаційних технологій як учителів, викладачів так і тих, хто отримує знання, лікарі та пацієнти звернулися до телемедицини, політичні лідери почали відвідували віртуальні саміти, та багато інших прикладів.

Весь цифровий світ акумулював свої можливості для пошуку дієвих засобів протидії подальшому поширенню хвороби. Цифрові інструменти, такі як програми та дані смартфонів, також використовуються для перевірки розповсюдження вірусу, тоді як технічні компанії, включаючи Alibaba та Tencent в Китаї та IBM, Google і Microsoft в США, почали застосовувати свої високопродуктивні комп'ютерні можливості, щоб допомогти дослідникам у пошуку ліків від цієї хвороби.

Отже, процес глобальної інформатизації, поряд із розмиванням традиційних основ національно-державної ідентичності, може сприяти актуалізації інших форм об'єднання людей. Наслідком нерівномірної та експансіоністської інформатизації може бути посилення релігійної та етнічної ідентичності людей і їхнє об'єднання за ідеологічними принципами. Це, зі свого боку, може створити передумови для появи так званих конфліктів "нового покоління".

Оскільки останнім часом інформація перетворилася на особливий ресурс будь-якої діяльності, отже вона, як і будь-який інший ресурс, потребує захисту в забезпеченні її безпеки, цілісності та збереження. Проведений аналіз доводить, що членство в

регіональних організаціях дозволяє Україні виконувати актуальні завдання у сферах політичної комунікації та кібербезпеки. Україна на цій основі має гостру потребу у спільних із розвиненими державами діях, що можуть гарантувати їй безпеку на регіональному та глобальному рівнях. З огляду на це вона здійснює політику "відкритих дверей" та активно співпрацює з міждержавними об'єднаннями, що не пред'являють попередніх вимог до рівня її військової могутності (ООН, НАТО, ОБСЄ та ін.) та соціально-економічного розвитку.

Проте, визначальним у міжнародному співробітництві нашої держави з іноземними партнерами є російський чинник. Даний чинник досить вдало визначив голова Парламентської асамблеї НАТО Паоло Алліу своєму виступі на урочистому засіданні Верховної Ради, присвяченому 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північноатлантичного договору: *"Агресія Росії проти України в 2014 році відкрила нову главу в міжнародних відносинах. Україна і Східна Європа на сьогоднішній день є лінією фронту із захисту європейської безпеки і захисту того світового порядку, який склався після Другої світової війни"* [10].

Сьогодні беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх здобутків нашої держави на цьому шляху слід вважати надання у червні 2020 року Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти т.зв. секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв'язку, управління військами, конкретних родів військ тощо). Крім того, EOP дає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО [11]. До цього такий статус мали лише п'ять країн, зокрема Грузія, а також країни-члени ЄС Швеція та Фінляндія.

Варто зауважити, що на теперішньому етапі розвитку України стан її національної безпеки, насамперед, залежить від ефективності результатів процесу інформатизації та прогресу у впровадженні ІКТ у військовій сфері.

У сучасних умовах проникнення глобалізації в усі сторони суспільного життя забезпечення кібербезпеки вимагає від дослідників виконання завдання наукового осмислення та здійснення наукового аналізу проблем, що тісно пов'язані з гарантуванням кібербезпеки, як найважливішого компонента міжнародної та національної безпеки. Однак, на жаль, слід констатувати: нині майже всі підходи, що покликані забезпечити кібербезпеку України, орієнтовані на військово-політичні процеси. Безумовно, це пріоритетний напрям у забезпеченні національної безпеки. Та попри це, вони мають також акцентувати увагу на таких проблемах, як регіональна політична нестабільність, незаконний обіг наркотиків, злочинність, захист інформаційних прав людини тощо. Та й імідж держави залишається ще одним проблемним аспектом, що прямо залежить від її інформаційної політики. Нерідко нас сприймають як зручний полігон кіберзлочинності. Отже, глобалізація кіберпростору породила таке явище, як всеосяжний взаємообмін інформацією на загальносвітовому рівні.

В експертному середовищі останнім часом дедалі голосніше лунає така думка: щоб успішно втілювати в життя державну інформаційно-іміджеву політику, Україні слід створити інформаційну систему, яка б формувала та затверджувала позитивний образ нашої країни в російсько- та англомовному медіапросторах [12; 13]. У контексті зазначеного вище усе ж варто додати, що нині проблемі забезпечення кібернетичної безпеки приділяється достатня увага як на державному, так і на приватному рівнях. У зв'язку з проникненням технічних засобів обробки і передачі даних практично в усі сфери людської діяльності особливої актуальності набуває протидія кіберзагрозам.

Уже цілком очевидно, що інформаційна сфера є самостійною галуззю національної безпеки, де необхідно гарантувати охорону інформаційних ресурсів, механізми їхнього створення, застосування та поширення, комунікаційну інфраструктуру, реалізацію прав на інформацію держави, суспільства і громадян тощо.

На сучасному етапі перед Україною постало завдання здійснення переходу до якісно нового рівня управління шляхом забезпечення всіх учасників інформаційних правовідносин достовірною, своєчасною та повною інформацією. Це можливо виконати лише завдяки послідовному реформуванню інформаційного впровадження в системі органів державної влади й управління та правильній реалізації інформаційної політики. Інформаційна політика – це здатність і можливість суб'єктів політики впливати на свідомість та психіку людей, їхню діяльність і поведінку за допомогою інформації в інтересах держави та громадянського суспільства [14]. Нині вже ні в кого не викликає сумнівів той факт, що доступність і якість інформаційних ресурсів багато в чому визначають рівень розвитку країни, її статус у світовому співтоваристві і, безперечно, стануть базовим показником статусу в перші десятиліття XXI ст. Зважаючи на це, стратегічними напрямами національної політики забезпечення кібербезпеки мають бути:

– захист національних інформаційних інтересів, забезпечення кібербезпеки, захист від інформаційних експансій, кіберзагроз та інших недружніх акцій, їхнє усунення;

– створення, розвиток і забезпечення безпеки національних інформаційних ресурсів;

– входження у світове інформаційне співтовариство.

Продовжуючи аналіз, варто додати, що стан формування інформаційних ресурсів в Україні нині, на жаль, перебуває на низькому рівні. Однією з найважливіших умов розвитку єдиного кіберпростору України є всеохопна (домашня) комп'ютеризація, що дозволила б розширити кіберпростір і відкрити широкий доступ до інформаційних ресурсів, готуючи ґрунт для діалогу влади із населенням. Заслуговує на увагу те, що в Україні поступово формується ринок інформаційно-комунікаційних технологій, продуктів і послуг, зростає мережа абонентів відкритих світових мереж, збільшується кількість персональних комп'ютерів. Прискореними темпами здійснюється забезпечення населення мобільними засобами зв'язку, розширюються національна мережа зв'язку та супутникова мережа. Триває інформатизація органів державної влади, галузей економіки, банківської сфери, зв'язку, транспорту, освіти та культури тощо.

Іншим важливим аспектом внутрішнього чиннику забезпечення кібербезпеки є теоретичне осмислення та практична реалізація на рівні законодавчого забезпечення національних інтересів України в кіберсфері. Попри те, що поняття національного інтересу в різних дослідників інтерпретується неоднозначно, усе ж проглядається розуміння загальної концепції щодо нього. Концепція національного інтересу це також і концепція ідеологічна, ціннісна та суб'єктно-абстрактна. Його визначення (національного інтересу) залежить не тільки від усвідомлення та сприйняття реальної дійсності суб'єктом, що формує національний інтерес, а й від світоглядних аспектів, ціннісних орієнтирів, особистісних характеристик суб'єкта і рівня амбіційності впливу на нього з боку груп інтересів.

Висновки.

Вивчення й аналіз забезпечення кібербезпеки, насправді, охоплює різні вияви інформації та інформування, а також є необхідним для розвитку інформаційної сфери. Під джерелами загроз кібербезпеці розуміють, зокрема, загострення міжнародної конкуренції за володіння інформаційно-технічними ресурсами, прагнення потенційних супротивників до ущемлення інтересів України у світовому кіберпросторі, витіснення її

із зовнішнього та внутрішнього ринків тощо. Цілком очевидно, що в кібернетичній сфері національні інтереси і національна безпека України будуються на основі стратегічних і поточних завдань зовнішньої та внутрішньої політики держави щодо забезпечення кібербезпеки. Їх слід узгодити із цілями забезпечення кібербезпеки України.

У кібернетичній сфері можна виокремити чотири основні складові національних інтересів України:

– *Перша складова* національних інтересів України забезпечує дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни.

– *Другий компонент* національних інтересів України в кібернетичній сфері передбачає інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів.

– *Третя складова* національних інтересів України в кібернетичній сфері забезпечує застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів.

– *Четвертий компонент* національних інтересів України в кібернетичній сфері передбачає захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України. Іншими словами, четверта складова зазначає, що в разі несанкціонованого доступу до інформаційних систем, що містять персональні дані громадян, можуть бути порушені їхні конституційні права.

Отже, досліджуючи національні інтереси України в кібернетичній сфері, необхідно наголосити, що особливість національних інтересів полягає в тому, щоб створити в українського народу захисні механізми, які б унеможливлювали будь-які спроби зсередини і ззовні використовувати національне різноманіття в недружніх цілях національного розколу з далекосяжними намірами.

З огляду на все це національна політика в галузі забезпечення кібербезпеки має будуватися з урахуванням необхідності захисту життєво важливих інтересів людини, суспільства та держави, дотримання їх балансу, поступового розширення можливостей та неухильного дотримання основоположних прав та свобод. Представники державної влади зобов'язані надавати всебічну допомогу в захисті національних й актуальних для держави життєво важливих інтересів в кібернетичній сфері.

Зважаючи на це, та з метою вироблення концептуальних підходів до забезпечення кібербезпеки, підготовки проектів постанов і розпоряджень з питань кібербезпеки та захисту інформації, організації і проведення експертизи проектів галузевих нормативних документів з кібербезпеки, а також надання пропозицій щодо виконання вимог нормативних актів з кібербезпеки тощо, було б доцільно створити спеціальний аналітичний Центр з кібернетичної політики при РНБО України.

Використана література

1. Сегеда О.О. Цифрова дипломатія України як елемент нової публічної дипломатії. *ПОЛІТИКУС*. Вип 3. 2020. С. 139-147.

2. Global Risks 2012 Seventh Edition. Insight Report. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

3. Ткачук Т.Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України "Київський політехнічний інститут". Політологія. Соціологія. Право*. 2017. № 1 – 2. С. 242-246.

4. Харченко С.О. Наукові підходи до класифікації загроз інформаційній безпеці. Серія: *Державне управління*. 2019 р. № 2 (66). С. 191-197.

5. Носач А.В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України. *Право і суспільство*. 2019. № 3. С. 50-56.

6. Стрельбицький М.П., Благодарний А.М. Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти. *Information Security of the Person, Society and State*. 2019. № 1 (25). С. 37-45.

7. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года). URL: https://zakon.rada.gov.ua/laws/show/998_163#Text

8. Jeffrey A. Hart The Digital Opportunities Task Force: The G8's Effort to Bridge the Global Digital Divide. 26 p. URL: https://www.researchgate.net/publication/228852360_The_Digital_Opportun ities_Task_Force_The_G8's_Effort_to_Bridge_the_Global_Digital_Divide

9. Coronavirus underscores urgency to bridge digital divide. DW. URL: https://www.dw.com/en/coronavirus-underscores-urgency-to-bridge-digital-divide/a-53070723

10. Урочисте засідання, присвячене 20-ій річниці підписання Хартії про особливе партнерство між Україною та Організацією Північно-Атлантичного договору. – (Прес-служба Апарату Верховної Ради України). URL: https://www.rada.gov.ua/preview/anons_acred/146596.html

11. 12 червня 2020 року Україна отримала статус члена Програми розширених можливостей НАТО (NATO's Enhanced Opportunities Program – EOP). Урядовий портал: URL: https://www.kmu.gov.ua/news/ukrayina-otrimala-status-chlena-programi-rozshirenih-mozhlivostej-nato

12. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* № 2(25)/2018. С. 73-85.

13. Баровська А.В. Понятійно-категоріальний апарат інформаційної сфери: правовий аспект. – (Аналітична записка). Національний інститут стратегічних досліджень. URL: http://old2.niss.gov.ua/articles/532

14. Литвин Н.А. Наукові підходи щодо визначення поняття державної інформаційної політики в Україні. *Наука і правоохорона*. 2019. № 1(43). С. 253-261.

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

УДК 355.402

КРАВЧЕНКО Р.М., *кандидат юридичних наук.*
ORCID: https://orcid.org/0000-0003-1008-1708.

УДОСКОНАЛЕННЯ ПРАВОВИХ ОСНОВ КОНТРРОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Анотація. *Комплексний підхід щодо реформування Служби безпеки України зумовлює необхідність підготовки змін до нормативно-правових актів. У статті на підставі проведеного аналізу інституційних спроможностей органів військової контррозвідки Служби безпеки України запропоновано зміни та доповнення до чинного законодавства, які розширюють правове підґрунтя для виконання завдань контррозвідувального забезпечення Збройних Сил України. Пропозиції до вдосконалення правової регламентації діяльності органів військової контррозвідки Служби безпеки України унормовують організаційні, соціальні, кадрові, матеріально-технічні та інші питання їх функціонування.*

Ключові слова: *реформування Служби безпеки України, органи військової контррозвідки, , зміни та доповнення в нормативно-правові акти, контррозвідувальне забезпечення військових формувань.*

Summary. *A comprehensive approach to reforming the Security Service of Ukraine necessitates the preparation of amendments to regulations. The article, based on the analysis of the institutional capabilities of the military counterintelligence of the Security Service of Ukraine, proposes changes and additions to current legislation that expand the legal basis for counterintelligence support of the Armed Forces of Ukraine. Proposals to improve the legal regulation of the activities of military counterintelligence of the Security Service of Ukraine regulate organizational, social, personnel, logistical and other issues of it`s functioning.*

Keywords: *reforming the Security Service of Ukraine, military counterintelligence, changes and additions to regulations, counterintelligence support of military formations.*

Аннотация. *Комплексный подход к реформированию Службы безопасности Украины обуславливает необходимость подготовки изменений в нормативно-правовые акты. В статье на основании проведенного анализа институциональных возможностей органов военной контрразведки Службы безопасности Украины, предложены изменения и дополнения в действующее законодательство, которые расширяют правовую основу для выполнения задач контрразведывательного обеспечения Вооруженных Сил Украины. Предложения к совершенствованию правовой регламентации деятельности органов военной контрразведки Службы безопасности Украины упорядочивают организационные, социальные, кадровые, материально-технические и другие вопросы их функционирования.*

Ключевые слова: *реформирование Службы безопасности Украины, органы военной контрразведки, изменения и дополнения в нормативно-правовые акты, контрразведывательное обеспечение воинских формирований.*

Постановка проблеми. Реформування Служби безпеки України визначено одним з пріоритетів комплексного реформування Української держави відповідно до ключових стратегічних і програмних документів – Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, Стратегії сталого розвитку “Україна-2020”, схваленої Указом Президента України від 12 січня 2015 року № 5/2015, Концепції розвитку сектору безпеки і оборони України, затвердженої Указом Президента України від 14 березня 2016 року № 92/2016, Річних національних програм під егідою Комісії Україна – НАТО.

Досягнення очікуваного результату передбачається, зокрема, шляхом зміни правових, організаційних та інших засад функціонування Служби безпеки України з урахуванням сучасного досвіду провідних держав світу, демократичних перетворень у суспільстві, інтеграційного курсу України в європейський і євроатлантичний економічний, політичний та безпековий простір [1]. Посилення можливостей СБУ щодо забезпечення державної безпеки у військовій сфері потребує удосконалення правових основ, які б охоплювали своїм впливом суспільні відносини, що виникають у сфері контррозвідувального забезпечення Збройних Сил України.

Результати аналізу наукових публікацій. Проблемам удосконалення законодавчих та організаційно-правових засад діяльності Служби безпеки України присвячено значну кількість напрацювань вітчизняних науковців. Шилін М.О. досліджував аспекти реформування законодавства про Службу безпеки України [2]. Пилипчуком В.Г. розглядалися актуальні питання реформування і розвитку сектору безпеки України, на прикладі Служби безпеки України були проаналізовані організаційно-правові та історичні аспекти, позитивні напрацювання і проблеми розробки концептуальних засад реформування [3]. Кудіновим С.С. досліджувалися правові основи діяльності СБ України із забезпечення антитерористичної безпеки, визначені важливість вказаного виду діяльності для протидії тероризму, а також кроки для оптимізації протидії терористичній діяльності [4]. Пропозиції з удосконалення чинного законодавства щодо реалізації СБУ своїх повноважень у сфері захисту критичної інфраструктури розроблялися С. Телеником [5].

Водночас питання удосконалення законодавчих та організаційно-правових засад контррозвідувального забезпечення Збройних Сил України комплексно не досліджувалися, хоча для ефективної реалізації повноважень органів ВКР СБУ необхідним є закріплення у нормативних юридичних актах прав та обов'язків військової контррозвідки, а також інших учасників суспільних відносин, що виникають у цій сфері, яке наразі є недостатнім. Утім, забезпечення оптимального регулювання суспільних відносин неможливе без досконалої за формою та змістом нормативної бази [6].

Метою статті є формулювання пропозицій до змін та доповнень нормативно-правових документів з метою удосконалення правової регламентації діяльності органів військової контррозвідки Служби безпеки України (далі – ВКР СБУ), що здійснюють контррозвідувальне забезпечення Збройних Сил України.

Виклад основного матеріалу. Реформування Служби безпеки України, як складової сектору безпеки і оборони, визначено керівництвом нашої держави стратегічним завданням, що потребує вжиття активних та рішучих заходів [7].

У пояснювальній записці до проекту Закону України "Про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України" Головою СБУ Бакановим І.Г., зокрема, зазначено, що законопроектом пропонується впровадити правове підґрунтя для виконання СБ України своїх завдань шляхом зміни правових, організаційних та інших засад функціонування Служби безпеки України з урахуванням сучасного досвіду діяльності спецслужб держав – членів ЄС та держав – членів НАТО [8].

Відновлення вертикально інтегрованої структури військової контррозвідки, яку приведено у відповідність до побудови Збройних Сил і Міністерства оборони України, створення Департаменту військової контррозвідки, як окремого підрозділу у складі Центрального управління СБУ, значно підвищує координованість роботи з контррозвідувального забезпечення військових формувань [9].

Проте, попри зазначені позитивні зміни, подальшими кроками до підвищення ефективності діяльності органів ВКР СБУ має бути забезпечення оптимального правового регулювання суспільних відносин, що виникають в ході контррозвідувального забезпечення Збройних Сил України.

Досліджуючи сукупність обов'язків та прав органів ВКР СБУ, як основу їх правового статусу, нами було визначено коло повноважень, які вимагають додаткового унормування. З огляду на раніш зроблені висновки, автором пропонуються наступні зміни та доповнення до чинних нормативних актів, які можуть розширити правові підстави для реалізації завдань і функцій щодо контррозвідувального забезпечення Збройних Сил України.

Так, вважаємо за доцільне до Закону України "Про Службу безпеки України" внести доповнення наступного змісту:

- органи військової контррозвідки створюються для контррозвідувального забезпечення Збройних Сил України і Державної прикордонної служби України та інших військових формувань, дислокованих на території України, а також їх підрозділів, що направляються до інших держав з метою виконання бойових, миротворчих або гуманітарних завдань;

- чисельний склад органів військової контррозвідки, їх дислокація визначаються Головою Служби безпеки України, виходячи з умов дислокації військ (сил). Гранична чисельність військовослужбовців і працівників органів військової контррозвідки СБ України не може перевищувати 1 відсотка загальної чисельності Збройних Сил України;

- підрозділи військової контррозвідки розташовуються в межах відповідних військових гарнізонів. У разі потреби з метою організації їх діяльності їм виділяються необхідні приміщення з фондів Міністерства оборони України;

- забезпечення підрозділів військової контррозвідки СБУ охороною, транспортом та засобами зв'язку (у тому числі спеціальними), засобами індивідуального захисту, вогнепальною зброєю, іншим необхідним майном, а військовослужбовців цих підрозділів – обмундируванням, здійснюється Міністерством оборони України;

- в умовах особливого періоду, запровадження надзвичайного, воєнного стану або проведення антитерористичної операції із залученням з'єднань, військових частин та підрозділів Збройних Сил України, Національної гвардії України, Державної прикордонної служби України, інших військових формувань, місцем постійної дислокації яких є територія в межах військового гарнізону, особовий склад органів військової контррозвідки СБУ відряджається до районів розташування цих з'єднань, військових частин (підрозділів) на період виконання цими з'єднаннями, військовими частинами та підрозділами завдань за призначенням;

- військовослужбовці органів військової контррозвідки СБУ забезпечуються жилою площею за рахунок Міністерства оборони України за місцем проходження служби;

- при здійсненні контррозвідувальної діяльності співробітники органів військової контррозвідки СБУ мають право безперешкодно за посвідченням, що підтверджує посаду, входити на територію та у приміщення військових частин і штабів незалежно від встановленого в них режиму, витребувати від військових частин рішення, розпорядження, інструкції, накази та інші акти і документи, мати доступ до відповідних інформаційних баз даних; вносити у межах своєї компетенції військовому командуванню, органам військового управління, подання щодо усунення порушень закону, причин і умов, що їм сприяють; брати участь в організаційних заходах, які проводяться військовим командуванням, органами військового управління;

- військове командування та органи військового управління Збройних Сил України та інших військових формувань, утворених відповідно до законів України, а також інші органи державної влади та органи місцевого самоврядування, військовослужбовці та громадяни зобов'язані сприяти органам військової контррозвідки СБУ у виконанні ними своїх завдань;

- в окремих випадках до виконання завдань контррозвідувальної діяльності можуть тимчасово залучатися військовослужбовці Збройних Сил України. Безпосереднє керівництво під час виконання цих завдань покладається на відповідну посадову особу органів військової контррозвідки СБУ.

Закон України "Про Статут внутрішньої служби Збройних Сил України" доцільно доповнити положенням що командир (начальник) зобов'язаний повідомляти органи військової контррозвідки Служби безпеки України відому йому або підлеглим військовослужбовцям інформацію щодо фактів або ознак, розвідувальної, терористичної, антиконституційної, іншої підривної діяльності, а тому числі пов'язаної з несанкціонованим доступом до автоматизованих систем і комп'ютерних мереж, у відношенні власних або відомих контактів з особами, які можуть бути причетними до іноземних спецслужб та терористичних організацій.

У Законі України "Про Дисциплінарний статут Збройних Сил України" визначити, що у разі, якщо військовослужбовець виявив факти або ознаки розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України, він повинен доповісти про це безпосередньому командирові (начальникові), а також може надіслати письмову заяву старшому командирові (начальникові) або до органу військового управління, органу військової контррозвідки Служби безпеки України.

Ввести до Указу Президента України від 10.12.08 р. № 1153/2008 "Про Положення про проходження громадянами України військової служби у Збройних Силах України" юридичну норму, згідно з якою органи військової контррозвідки Служби безпеки України можуть надавати обов'язкові для розгляду пропозиції щодо доцільності перебування військовослужбовців у резерві кандидатів для призначення на посади миротворчого персоналу, до багатонаціональних органів військового управління та дипломатичних представництв України.

У наказі Міністерства оборони України від 21.11.17 р. № 608 "Про затвердження Порядку проведення службового розслідування у Збройних Силах України" доцільно додатково визначити, що службове розслідування може призначатися у разі зникнення або дезертирства військовослужбовців та працівників, які протягом останнього року мали доступ до цілком таємної чи службової інформації в сфері оборони, перебували в підрозділах спеціального призначення; порушення вимог режиму секретності; несанкціонованого доступу до електронно-обчислювальних машин та автоматизованих систем передачі інформації; вчинення чи спроб вчинення самогубства військовослужбовцями та працівниками Збройних сил, які мали доступ до таємної чи службової інформації. До участі у проведенні вказаних службових розслідувань залучаються співробітники органів військової контррозвідки Служби безпеки України.

Доповнити зміст наказу Міністерства оборони України від 29.11.18 р. № 604 "Про затвердження Інструкції з надання доповідей і донесень про події, кримінальні правопорушення, військові адміністративні правопорушення та адміністративні правопорушення, пов'язані з корупцією, порушення військової дисципліни та їх облік у Міністерстві оборони України, Збройних Силах України та Державній спеціальній службі транспорту" нормою, згідно з якою про факти або ознаки розвідувальних,

терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України командири (начальники) військових частин доповідають своїм безпосереднім командирам (начальникам), інформують органи військової контррозвідки Служби безпеки України.

У наказі Міністерства оборони України від 14.04.15 р. № 164 "Про затвердження Інструкції з організації та проведення психофізіологічного дослідження персоналу із застосуванням поліграфа у Міністерстві оборони України та Збройних Силах України" унормувати, що перевірка з використанням поліграфа застосовується при вирішенні питання про оформлення допуску до державної таємниці військовослужбовцям, працівникам Збройних Сил, державним службовцям або кандидатам на посаду в Міноборони та Збройні Сили. Дослідження проводиться з метою отримання умовної та орієнтувальної інформації про наявність таких обставин, у тому числі у минулому: перебування на агентурному зв'язку в спецслужбі іншої держави; сприяння діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом; наявність громадянства іншої держави або документа, виданого уповноваженими органами іншої держави, про те, що суб'єкт дослідження набуде її громадянства, якщо вийде з громадянства України; розголошення відомостей, які є конфіденційною, таємною або службовою інформацією; приховані мотиви вступу на службу до ЗС України. Уповноважені співробітники органів військової контррозвідки Служби безпеки України мають право доступу до інформації про факт, процедуру та результати дослідження, при цьому забезпечують її конфіденційність.

У наказі Міністерства оборони України від 22.02.16 р. № 95 "Про затвердження Концепції підготовки Збройних Сил України" регламентувати, що підготовка ЗС України включає в себе контррозвідувальну підготовку тобто цілеспрямований та організований процес послідовних заходів навчання та виховання всіх категорій військовослужбовців ЗС України, спрямований на формування у них потрібного рівня знань, у відношенні загроз іноземної розвідувальної, терористичної та іншої протиправної діяльності, а також порядку інформування про неї органів військової контррозвідки Служби безпеки України. Планують, організовують, проводять та контролюють заходи контррозвідувальної підготовки у ЗС України органи військової контррозвідки Служби безпеки України.

В Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України, затвердженій наказом Міністерства оборони України від 14.06.13 р. № 401, додатково передбачити, що органи військової контррозвідки Служби безпеки України можуть проводити правове інформування визначених категорій військовослужбовців з метою доведення і роз'яснення законодавства України, що стосується протидії протиправній діяльності спеціальних служб іноземних держав, окремих організацій, груп та осіб, що створюють загрози національній безпеці України.

До Бойового статуту механізованих і танкових військ Сухопутних військ Збройних сил України, затвердженого наказом командувача Сухопутних військ Збройних Сил України від 25.05.16 р. № 238, внести наступні доповнення:

- співробітники органів військової контррозвідки Служби безпеки України можуть проводити допити полонених і перебіжчиків, вивчення захоплених у противника документів, зразків озброєння та військової техніки ;

- для підготовки та ведення інформаційної боротьби у бригаді створюється нештатна група інформаційної боротьби у такому складі: помічник начальника оперативного відділення – начальник групи інформаційної боротьби, начальник РЕБ, офіцер відділення виховної роботи, офіцер психологічних операцій із складу центру (загону) інформаційно-психологічних операцій, співробітник органів військової контррозвідки Служби безпеки України.

Наказ Міністра оборони України від 05.05.99 р. № 142 "Про введення в дію Концепції морально-психологічного забезпечення підготовки та ведення операцій (бойових дій) Збройних Сил України" доповнити нормою, згідно з якою під час планування та організації заходів морально-психологічного забезпечення структурні підрозділи морально-психологічного забезпечення на усіх рівнях військового управління підтримують постійну взаємодію з органами військової контррозвідки Служби безпеки України.

Наказ Міністра оборони України від 29.06.10 р. № 336 "Про затвердження Положення про організацію військово-соціологічних, соціально-психологічних та психологічних досліджень у Збройних Силах України" доповнити положенням, що результати моніторингу морально-психологічного стану особового складу у з'єднаннях, військових частинах, підрозділах, військових навчальних закладах, установах та організаціях, аналізу суспільно-політичної обстановки в районах дислокації військ (сил) та її впливу на морально-психологічний стан особового складу, прогноз динаміки його можливих змін можуть надаватися до органів військової контррозвідки Служби безпеки України за їх запитом.

Закріпити у наказі Міністерства оборони Україні від 02.04.19 р. № 145 "Про затвердження Порядку організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками" обов'язок підрозділів координації контролю в Міністерстві оборони та Збройних Силах України інформувати органи військової контррозвідки Служби безпеки України про ідентифіковані ризики інформаційної безпеки, пов'язані із впливом на інформаційні системи, наслідком яких є порушення конфіденційності, цілісності, автентичності або доступності інформаційних ресурсів.

Внести зміни до наказу Міністерства оборони України від 04.05.18 р. № 196 "Про затвердження Порядку організації в Міністерстві оборони України та Збройних Силах України прийому та супроводження іноземних інспекційних груп під час виконання міжнародних договорів і угод у сфері контролю над звичайними озброєннями". Зокрема, останній абзац додатку 2 "Склад оперативної групи під час проведення інспекції за вимогою в межах зазначеного району за ДЗЗСЄ" викласти в такій редакції: до складу оперативної групи залучаються (за згодою) представники Міністерства внутрішніх справ України, Національної гвардії України, Національної поліції України, Державної прикордонної служби України, Державної служби спеціального зв'язку та захисту інформації України, Департаменту військової контррозвідки Служби безпеки України, Державного космічного агентства України, Державного концерну "Укроборонпром".

У наказі Міністерства оборони України від 05.06.19 р. № 284 "Про затвердження Положення про організацію будівництва об'єктів у Міністерстві оборони України та Збройних Силах України" додатково передбачити, що виконавці функцій замовника будівництва об'єктів ЗС України погоджують з органами військової контррозвідки Служби безпеки України списки працівників суб'єктів господарювання, які будуть залучені до нового будівництва, реконструкції, технічного переоснащення, реставрації чи капітального ремонту об'єктів спеціального призначення.

Внести до наказу Міністерства оборони України від 19.12.17 р. № 665 "Про здійснення міжнародного співробітництва Міністерством оборони України та Збройними Силами України" наступні доповнення:

- органи міжнародного співробітництва про прийняті рішення щодо проведення заходів міжнародного співробітництва на території України, відрядження за кордон особового складу для участі в заходах міжнародного співробітництва, а також верифікаційної діяльності за міжнародними договорами та угодами в галузі контролю над озброєнням завчасно інформують органи військової контррозвідки Служби безпеки України;

- органи міжнародного співробітництва про результати проведення заходів міжнародного співробітництва у встановленому порядку інформують органи військової контррозвідки Служби безпеки України;

- військовослужбовці (працівники) Збройних Сил України, які направляються у службові відрядження за кордон, після повернення з відряджень проходять опитування органами військової контррозвідки Служби безпеки України.

У наказі Міністерства оборони України від 17.11.16 р. № 610 "Про затвердження Положення про середньострокове та короткострокове оборонне планування в Міністерстві оборони України і Збройних Силах України" передбачити обов'язок начальника Головного управління оборонного та мобілізаційного планування – заступника начальника Генерального штабу Збройних Сил України щорічно надавати до органів військової контррозвідки Служби безпеки України Орієнтовний план утримання та розвитку Збройних Сил України на відповідний рік в обсязі, необхідному для виконання завдань контррозвідувальної діяльності.

До наказу Міністерства оборони України від 18.01.16 р. № 23 "Про затвердження Інструкції з підготовки та застосування національних контингентів, національного персоналу в міжнародних операціях з підтримання миру і безпеки" внести доповнення, що контррозвідувальне забезпечення національних контингентів, національного персоналу під час участі в міжнародних операціях здійснюється органами військової контррозвідки Служби безпеки України.

Будь-яка діяльність, у тому числі й діяльність з удосконалення законодавства, здійснюється у певний спосіб, тобто за допомогою використання певних прийомів, методів, з дотриманням певного порядку дій (певних процедур) [10]. Удосконалення законодавства – це діяльність суб'єктів правотворчості по зміні стану чинного законодавства, яка здійснюється за допомогою використання відповідних правових засобів та правотворчої техніки; результатом такої діяльності є належна якість законодавства, а метою – ефективність законодавства. Відтак, на наш погляд, перелік запропонованих змін та доповнень до законодавства не є вичерпним, зокрема, також існує потреба у вдосконаленні підзаконних нормативних актів, що видаються в межах компетенції Службою безпеки України.

Висновки.

У роботі визначено обов'язки та права органів ВКР СБУ, а також коло повноважень, які вимагають додаткового унормування. Пропонується ряд вищезазначених змін та доповнень до чинних нормативних актів, які можуть розширити правові підстави для реалізації завдань і функцій контррозвідувального забезпечення Збройних Сил України. Вважаємо, що упровадження запропонованих заходів з удосконалення законодавства у сфері контррозвідувального забезпечення Збройних Сил України сприятиме практичному вирішенню проблем, пов'язаних з забезпеченням належної якості та ефективності контррозвідувальної діяльності.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 04.03.16 р. "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.16 р. № 92/2016. *Урядовий кур'єр*. 2016. № 52.

2. Шилін М.О. Щодо реформування законодавства про Службу безпеки України: матеріали постійного діючого наукового-практичного семінару *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення*, м. Харків, 27 трав. 2016 р. С. 199-202. Харків: Право, 2016. Вип. 7. URL: http://dspace.nlu.edu.ua/bitstream/123456789/10665/1/SB_seminar_27_05_2016.pdf

3. Пилипчук В.Г. Досвід реформування і розвитку сектору безпеки України (кінець XX – початок XXI ст.). *Стратегічні пріоритети*. 2013. № 3. С. 115-121. URL: http://nbuv.gov.ua/UJRN/spa_2013_3_17

4. Кудінов С.С. Шляхи удосконалення правового регулювання забезпечення Службою безпеки України антитерористичної безпеки. *Підприємництво, господарство і право*. 2019. № 2. URL: http://pgp-journal.kiev.ua/archive/2019/2/45.pdf

5. Теленик С. Служба безпеки України як суб'єкт державної системи захисту критичної інфраструктури. *Право України*. 2019. № 3. С. 260-286.

6. Основні напрями розвитку кримінального права та шляхи вдосконалення законодавства України про кримінальну відповідальність: матеріали міжнар. наук.-практ. конф., м. Харків, 11–12 жовт. 2012 р. / редкол.: В.Я. Тацій (голов. ред.), В.І. Борисов (заст. голов. ред.) та ін. Харків: Право, 2012. 632 с. С. 6.

7. Урядування та реформування національних служб безпеки та розвідки: кращі міжнародні практики: матеріали третьої міжнародної конференції, м. Київ, 24 трав. 2016 р., URL: https://ukrainesecuritysector.com/wp-content/uploads/2017/07/2017-Conference-3-UKR.pdf

8. Про внесення змін до Закону України "Про Службу безпеки України": пояснювальна записка до проекту закону України щодо удосконалення організаційно-правових засад діяльності Служби безпеки України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

9. Про внесення змін до Указів Президента України від 27 грудня 2005 року № 1860 та від 5 травня 2020 року № 166: Указ Президента України від 13.10.20 р. № 431/2020. *Урядовий кур'єр.* 2020. № 201.

10. Риндюк В.І. Удосконалення законодавства як правотворча діяльність. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2015. Вип. 34(1). С. 40-43. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2015_34(1)__11

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

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

УДК 342.97

КОСІЛОВА О.І., *кандидат політичних наук, доцент,* науковий співробітник Інституту права Київського національного університету імені Тараса Шевченка.
ORCID: https://orcid.org/0000-0002-5574-3771.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КОНСТИТУЦІЙНИХ ПРАВ І СВОБОД: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

Аннотація. *У статті аналізуються сутність та зміст правового забезпечення прав та свобод громадян, визначаються провідні тенденції правового забезпечення та адміністративно-правового забезпечення зокрема. Аналізується зміст категорії "забезпечення" прав і свобод, досліджується механізм правового забезпечення та адміністративно-правового забезпечення як його підвид; досліджується структура механізму правового забезпечення. Визначаються суб'єкти та об'єкти адміністративно-правових відносин, специфіка адміністративно-правового забезпечення у контексті сучасного реформування галузі адміністративного права.*

Ключові слова: *права і свободи, забезпечення прав і свобод, адміністративно-правове забезпечення, механізм адміністративно-правового забезпечення прав, адміністративно-правові відносини.*

Summary. *The article analyzes the essence and content of legal support of the rights and freedoms of citizens, identifies the leading trends in legal support and administrative and legal support in particular. The content of the category "provision" of rights and freedoms is analyzed, the mechanism of legal provision and administrative and legal provision as its component is investigated; the structure of the mechanism of legal provision is explored. The subjects and objects of administrative and legal relations, the specifics of administrative and legal support in the context of modern reform of the field of administrative law are determined.*

Keywords: *rights and freedoms, ensuring rights and freedoms, administrative and legal support, the mechanism of administrative and legal support of rights, administrative and legal relations.*

Аннотация. *В статье анализируются сущность и содержание правового обеспечения прав и свобод граждан, определяются ведущие тенденции правового обеспечения и административно-правового обеспечения в частности. Анализируется содержание категории "обеспечение" прав и свобод, исследуется механизм правового обеспечения и административно-правового обеспечения как его подвид; исследуется структура механизма правового обеспечения. Определяются субъекты и объекты административно-правовых отношений, специфика административно-правового обеспечения в контексте современного реформирования отрасли административного права.*

Ключевые слова: *права и свободы, обеспечения прав и свобод, административно-правовое обеспечение, механизм административно-правового обеспечения прав, административно-правовые отношения.*

Постановка проблеми. Правове забезпечення прав і свобод людини і громадянина у сучасних умовах набуває особливого значення та є актуальною суспільно-значущою проблемою як для України, так і багатьох сучасних держав. Його зміст обумовлюється

складнощами щодо забезпечення закріплених у Конституції держави прав і свобод людини й громадянина та в низькому рівні їх захисту. У зв'язку з цим, проблема правового забезпечення прав і свобод особи та гарантованості їх реалізації потребує всебічного комплексного наукового дослідження, зокрема аналізу механізму забезпечення прав і свобод в адміністративному праві. Оскільки захист прав людини – це не другорядне, побічне завдання перетворень, що відбуваються в українському суспільстві, – це основна мета, яка повинна створити гідні умови життя кожному, гарантувати свободу та забезпечити фундаментальні права [1, с. 210]. Тим більше, що в Україні проблематика адміністративно-правового захисту прав і свобод людини та громадянина на дисертаційному й монографічному рівнях є малодослідженою та потребує здійснення подальшого наукового аналізу.

Результати аналізу наукових публікацій. Забезпечення прав і свобод людини і громадянина є предметом дослідження фахівців різних галузей права, цим питанням займаються низка науковців з різних галузей юридичної науки. Забезпеченню конституційних прав і свобод людини та громадянина у своїх працях приділяли увагу О.П. Васильченко, В.О. Демиденко, Є.Ю. Захаров, Н.Н. Крестовская, О.І. Наливайко, А.Ю. Олійник, В.В. Пацкан, П.М. Рабинович, А.А. Романова, М.В. Савчин., О.Ф. Скакун, Ю.М. Тодика, М.В. Цвік та інші. Різні аспекти адміністративно-правового забезпечення прав і свобод людини та громадянина досліджували такі вчені, як В.Б. Авер'янов, О.Ф. Андрійко, О.М. Бандурка, Ю.П. Битяк, С.Т. Гончарук, О.М. Гумін, І.О. Ієрусалімова, В.К. Колпаков, О.П. Костюшко, Г.В. Конюх, Є.Є. Колесников Є.Є., Л.О. Мамчур, Я.В. Лазур, Р.С. Мельник, Є.В. Пряхін, І.М. Шопіна та інші.

Метою статті є визначення змісту поняття "забезпечення прав і свобод", а також структури, специфіки адміністративно-правового забезпечення прав і свобод.

Виклад основного матеріалу. Розпочати наше дослідження пропонуємо з термінологічного аналізу категорії "забезпечення" у правовій науці. Слід зазначити, що існуючі визначення поняття "забезпечення" прав і свобод людини та громадянина є численними. Вітчизняні науковці по-різному тлумачать зміст поняття "забезпечення" прав і свобод, також по-різному визначають їх складові. У зв'язку з цим у науковій юридичні літературі можемо констатувати використання різного його термінологічного значення, як-то: "забезпечення", "реалізація", "здійснення", "гарантування" [1, с. 210].

Незважаючи на існуюче різноманіття наукових підходів до визначення сутності терміну "забезпечення" прав і свобод, їх можна об'єднати у дві основні групи. На думку одних авторів, це стадія реалізації прав людини. Згідно з цією точкою зору забезпечення виконує допоміжну роль по відношенню до реалізації. Проте такий підхід не отримав широкої наукової підтримки. Прибічники іншого підходу тлумачать забезпечення прав людини більш широко, як систему їх гарантування. Так, під забезпеченням прав і свобод розуміється система загальних (політичних, економічних, духовних та ін.) і спеціально юридичних засобів та інститутів, спрямованих на створення умов для реалізації прав людини, а також забезпечення їх всебічної охорони та захисту від порушень [2, с. 456].

Зокрема, О.Ф. Скакун зазначає, що термін "забезпечення" має досить широке значення і трактується як надання чогось кимось у достатній кількості, створення усіх необхідних умов для здійснення чого-небудь; гарантувати щось; захищати, охороняти когось, що-небудь [3, с. 273].

А.А. Романова вважає, що система забезпечення прав і свобод людини та громадянина складається з чотирьох підсистемних елементів, а саме: інституційне забезпечення, правове забезпечення, організаційне забезпечення, ресурсне забезпечення [4, С. 600].

Я. Троян зазначає, що категорія “захист прав і свобод людини” в основному використовується у вузькому значенні, тобто необхідність в останньому виникає у разі загрози або реального зазіхання на них або в результаті їх порушення. Захист прав і свобод особи за своїм змістом спрямовані на регламентацію порядку дій суб’єктів права з метою недопущення порушення гарантованих прав, максимального усунення можливостей такого порушення або порядку відновлення порушених прав шляхом закріплення відповідних прав, повноважень цих суб’єктів та органів [1, с. 211].

А.Ю. Олійник вважає, що забезпечення конституційних свобод в Україні – це створення сприятливих умов для їх здійснення, охорона, захист суб'єктивних свобод від правопорушення, відновлення порушеного права компетентними державними органами чи органами місцевого самоврядування, їх посадовими або службовими особами та об’єднаннями громадян здійснення матеріальних чи процесуальних юридичних засобів [5, с. 47].

П.М. Рабинович визначає складові елементи державної діяльності у сфері забезпечення прав і свобод: “сприяння для здійснення прав і свобод людини...; охорона прав і свобод людини...; захист прав і свобод людини (відновлення порушення правомірного стану, притягнення порушників до відповідальності)” [6, с. 45].

На думку В.С. Бігуна, забезпечити права людини означає створити умови, за яких права людини поважаються та визнаються, як державою, так і особою, та ефективно реалізуються, за потреби захищаються за допомогою права. Це, зокрема, передбачає трансформацію основоположних прав людини в юридичні права та обов’язки суб’єктів права, коли певні можливості людини, які визначаються як основоположні права, будуть гарантовані державою через їх визначення як загальнообов’язкових правил поведінки, а держава та інші суб’єкти матимуть обов’язок їх дотримуватися, гарантувати [7].

О.Є. Костюченко, характеризує ключові ознаки правового забезпечення шляхом виключення його складових. Зокрема, він зазначає: “якщо виключити норми права, які утворюють правові умови реалізації прав і свобод, то відповідно забезпечення втратить нормативність й перестане бути правовим; у разі виключення засобів реалізації прав і свобод закріплені норми права втратять свою дієвість; відсутність гарантій нівелює обов’язок держави створити умови користування правами і свободами; виключення охорони унеможливлює попередження порушень прав і свобод; відсутність захисту зробить неможливим відновлення порушених прав. Виключення з необхідних ознак безперервної діяльності суб’єктів права загалом робить неможливим весь процес забезпечення, починаючи від створення правових умов реалізації прав і свобод і завершуючи охороною цих прав і свобод, а у крайньому випадку і захистом порушених прав... Таким чином, правове забезпечення – це безперервна діяльність суб’єктів права, в межах їх компетенції, зі створення правових умов, усіма правовими засобами щодо закріплення, реалізації, гарантування, охорони та захисту прав і свобод осіб та їх груп” [8, с. 15].

Погоджуючись з таким підходом до правового забезпечення, проаналізуємо його похідне поняття – “адміністративно-правове забезпечення”. Так, “адміністративно-правове забезпечення” як галузеве поняття переважно не розкривається у наукових працях. Дослідження з адміністративного права взагалі не містять визначення цього поняття, залишаючи його для домислу читача і обмежуючись лише розкриттям змісту однієї або декількох ознак адміністративно-правового забезпечення. Адміністративно-правове забезпечення в загальному вигляді являє собою систему правових приписів, що визначає і характеризує систему організаційних засад певного роду діяльності [9, с.76].

В.Б. Авер'янов наголошує, що своєрідність "адміністративно-правового забезпечення" полягає у тому, що адміністративне право за своїм глибинним призначенням має визначатися як "право забезпечення і захисту прав людини". У цьому – сутність усієї трансформації теорії і практики українського адміністративного права на сучасному етапі [10, с. 67].

І.М. Шопіна зазначає, що адміністративно-правове забезпечення, це система адміністративно-правових засобів та способів, і процедур їх легалізації, що здійснюється з метою створення умов для всебічної реалізації прав, свобод та інтересів людини, громадянського суспільства, суб'єктів підприємницької діяльності, а також інших суб'єктів адміністративно-правових відносин [11, с. 142].

На думку О.М. Гуміна, Є.В. Пряхіна, адміністративно-правове забезпечення варто розглядати у широкому та вузькому розумінні. У широкому розумінні адміністративно-правове забезпечення – це упорядкування суспільних відносин уповноваженими на те державою органами, їх юридичне закріплення за допомогою правових норм, охорона, реалізація і розвиток. Вузьке визначення адміністративно-правового забезпечення буде змінюватися залежно від того, про які суспільні відносини буде вестися мова. До основних елементів адміністративно-правового забезпечення слід віднести: 1) об'єкт адміністративно-правового забезпечення; 2) суб'єкт адміністративно-правового забезпечення; 3) норми права (норми адміністративного права); 4) адміністративно-правові відносини та їх зміст; 5) гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення [12, с. 46].

І.О. Ієрусалімова вважає, що адміністративно-правове забезпечення прав і свобод людини та громадянина представляє собою повноту регулювання за допомогою норм адміністративного права суспільних відносин, що виникають для та в процесі їхньої реалізації, а також надання за допомогою цих норм відповідних гарантій, які разом з іншими правовими та неправовими гарантіями створюють стійку систему можливостей користування правовими цінностями в державі [13, с. 84].

Таким чином, більшість дослідників визначає адміністративно-правове забезпечення як один з галузевих елементів правового забезпечення, що має подібну структуру, засоби та форми їх забезпечення.

Поділяємо думку Є.Є. Колесникова, що для реалізації закріплених прав, свобод та законних інтересів людини держава потребує налагодження правового механізму забезпечення прав і свобод людини, який являє собою систему засобів, спрямованих на створення та підтримання існування умов поваги до всіх основних прав, свобод та законних інтересів людини, що є втіленням гідності людини як члена суспільства [14, с. 523].

Як відомо, механізми визначають як внутрішню будову, систему чого-небудь, сукупність станів і процесів, з яких складається певне фізичне, хімічне та інше явище [15]. Тоді як під механізмом правового забезпечення прав і свобод слід розуміти функціонуючу як єдине ціле систему правових засобів, за допомогою яких здійснюється правове регулювання суспільних відносин. До елементів механізму правового регулювання віднесено: норми права; юридичний факт (підстави для переходу абстрактних правових норм в конкретні права і обов'язки учасників суспільних відносин); акти безпосередньої реалізації права (фактична поведінка суб'єктів права щодо здійснення своїх прав і обов'язків); акти застосування права (забезпечують реалізацію права) [16, с. 354].

Водночас, у правовій науці представлені й інші погляди на сутність та складові елементи механізму забезпечення прав і свобод.

Зокрема, О.І. Наливайко механізм забезпечення прав і свобод людини визначає як діяльність органів держави і місцевого самоврядування, громадських об'єднань і громадян із створення умов (гарантій) для правомірної та неухильної їх реалізації і захисту [17, с. 22].

Я.В. Лазур зазначає, що механізм забезпечення прав і свобод громадян у державному управлінні має багато спільних ознак із механізмом правового регулювання, механізмом реалізації та забезпечення конституційних прав, свобод і обов'язків громадян. Механізм забезпечення прав і свобод громадян у сфері державного управління дослідник визначає як процес діяльності органів державного управління щодо створення належних умов реалізації, охорони та захисту прав і свобод громадян від протиправних дій, шляхом виконання матеріальних і процесуальних юридичних засобів та способів [18, с. 393]. Дослідник пропонує виділити наступні елементи механізму забезпечення прав і свобод громадян: а) норма права; б) правовідносини; в) принципи прав і свобод громадян; г) стадії їх забезпечення; д) гарантії здійснення прав і свобод громадян; е) юридичні факти; є) акти застосування норм права [18, с. 395].

С.Т. Гончарук дещо по іншому визначає сутність механізму адміністративно-правового забезпечення через регулювання. На його думку – це система адміністративно-правових засобів (елементів), за допомогою яких здійснюють правове регулювання (упорядкування) суспільних відносин у сфері державного управління. Структуру механізму адміністративно-правового регулювання становлять адміністративно-правові норми, акти тлумачення й акти реалізації адміністративно-правових норм, адміністративно-правові відносини [19, с. 23].

Таким чином, ключовим об'єктом адміністративно-правового регулювання забезпечення прав і свобод людини та громадянина є адміністративно-правові відносини, що виникають між суб'єктами з приводу реалізації, охорони, захисту та відновлення їхніх порушених прав і свобод. Відносини органів публічної адміністрації та громадян як суб'єктів адміністративно-правових відносин є частиною адміністративно-правових відносин і мають основні ознаки цих відносин. При цьому в літературі зазначається, що адміністративно-правовий режим відносин органів виконавчої влади і людини повинен виходити зі становища останньої як такого суб'єкта, перед яким органи виконавчої влади відповідальні за свою діяльність, і ґрунтуватися на беззаперечному визнанні пріоритету прав людини, її законних інтересів, правомірності її вимог та очікувань від діяльності державних органів, їх посадових осіб [20, с. 36].

Суб'єкти цих відносин мають різний правовий статус і завдання. Органи публічної адміністрації у відносинах з громадянами діють у межах своєї компетенції, а громадяни – своїх прав. Кожен із суб'єктів в адміністративно-правових відносинах, що виникають між громадянином і органом публічної адміністрації, наділені відповідними правами й обов'язками, які кожна зі сторін має право реалізувати та повинна дотримуватися і виконувати стосовно одна одної.

Адміністративно-правові відносини між органами публічної адміністрації та громадянами відзначаються різноманітністю і певними особливостями. У літературі існують різні підходи до їхнього поділу. Зокрема, йдеться про поділ адміністративно-правових відносин на типи в межах предмета адміністративного права. Виокремлюються такі відносини адміністративних зобов'язань, як публічносервісні, вертикальні, горизонтальні, реординаційні [21, с. 50-51; 22, с. 136-138].

Суб'єктами адміністративно-правових відносин із забезпечення прав і свобод людини та громадянина, з одного боку, є органи публічного управління – органи виконавчої влади, Президент України, Уповноважений Верховної Ради з прав людини,

правоохоронні органи, а з іншого – фізичні особи, навчальні заклади, підприємства, інші державні органи, установи й організації, діяльність яких пов'язана із забезпеченням прав і свобод людини та громадянина щодо їх реалізації, охорони, поновлення тощо. Органи виконавчої влади мають право породжувати адміністративні правовідносини в односторонньому порядку, керуючись інтересами держави й завданнями, що стоять перед ними [23, с. 165].

Погоджуючись з вказаним переліком, вважаємо за необхідне доповнити визначений перелік суб'єктів інститутами громадянського суспільства та органами місцевого самоврядування, які займають чільне місце у забезпеченні прав і свобод громадян.

Незалежно від виду адміністративно-правових відносин, поділяємо думку О.Ф. Андрійко, шо у відносинах органів публічної адміністрації (як і всіх органів державної влади) з громадянами центральне місце повинно належати принципу взаємної поваги інтересів особи і держави, що має сприяти функціонуванню збалансованої системи взаємних прав та обов'язків органів публічної адміністрації і громадян. При цьому, з одного боку, громадянин зобов'язаний виконувати вимоги владних приписів відповідних державних органів, а з другого – держава та її органи мають забезпечувати і гарантувати свободу громадян за умови, що свобода одних не порушує права та законні інтереси інших. Принцип взаємної поваги інтересів громадянина й органів публічної адміністрації визначається закономірностями взаємовідносин між громадянами та державою [24, с. 23].

Висновки.

Сприяння утвердженню пріоритету прав і свобод людини і громадянина, ефективній реалізації обумовлених цими правами та свободами правомірних інтересів громадян є найважливішим завданням адміністративно-правового регулювання у сфері виконавчої влади, існуючий стан якого потребує значної уваги в інтересах його дальшого покращення. Основними чинниками забезпечення прав і свобод громадян є юридичні гарантії та соціальні умови. До системи юридичних гарантій прав і свобод громадян належать нормативно-правові та інституційно-організаційні засоби їх забезпечення.

Демократичні реформи, які здійснюються у нашій державі призводять до поступового зростання ролі людини та громадянського суспільства, у змісті та спрямованості упорядкування суспільних відносин органами публічного адміністрування. У зв'язку з цим роль адміністративно-правового забезпечення, як основного виду діяльності сервісної держави поступово зростатиме, натомість провідна роль адміністративно-правового регулювання втрачатиметься.

Серед вітчизняних науковців не має єдиної позиції щодо змісту правового забезпечення прав і свобод людини і громадянина. Узагальнюючи проаналізовані наукові позиції можемо зробити висновок, що *під правовим забезпеченням прав і свобод розуміють систему їх гарантування, створення сприятливих умов для їх здійснення, охорона, захист суб'єктивних свобод від правопорушення, регламентацію порядку дій суб'єктів права з метою недопущення порушення гарантованих прав, усунення можливостей такого порушення або порядку відновлення порушених прав шляхом закріплення відповідних прав, повноважень цих суб'єктів та органів.*

Таким чином, можна визначити наступні підсистемі елементи системи забезпечення прав і свобод людини та громадянина: інституційне забезпечення, правове (нормативне) забезпечення, організаційне забезпечення, ресурсне забезпечення; та

елементи державної діяльності, що включають: сприяння, охорону, захист (відновлення правомірного стану, притягнення порушників до відповідальності).

Тоді як під механізмом правового забезпечення слід розуміти систему правових засобів, за допомогою яких здійснюється правове регулювання суспільних відносин, до елементів якої віднесено: норми права; юридичний факт (підстави для переходу абстрактних правових норм в конкретні права і обов‘язки учасників суспільних відносин); акти безпосередньої реалізації права (фактична поведінка суб’єктів права щодо здійснення своїх прав і обов’язків); акти застосування права (забезпечують реалізацію права).

Забезпечення прав і свобод людини та громадянина передбачає комплекс суспільних відносин, які виникають з метою реалізації, охорони, захисту та відновлення порушених прав і свобод. Важливе місце в цій системі посідають адміністративно-правові відносини, оскільки обов’язок держави забезпечити права та свободи і створити сприятливі умови для їх реалізації людиною, який походить з пріоритету прав і свобод людини та громадянина в державі, наділяє органи публічного управління (зокрема правоохоронні органи як органи виконавчої влади) владно-розпорядчими функціями задля реалізації прав і свобод людини та громадянина, що передбачають адміністративно-правові норми.

Поділяємо думку В.Б. Авер’янова, що адміністративне право за своїм глибинним призначенням має визначатися як “право забезпечення і захисту прав людини”. Адміністративно-правове забезпечення складає систему адміністративно-правових засобів та способів, і процедур їх легалізації, що здійснюється з метою створення умов для всебічної реалізації прав, свобод та інтересів людини, громадянського суспільства, суб’єктів підприємницької діяльності, а також інших суб’єктів адміністративно-правових відносин. Узагальнюючи правові позиції вітчизняних науковців, можемо визначити наступні основні елементи адміністративно-правового забезпечення: 1) об’єкт адміністративно-правового забезпечення; 2) суб’єкт адміністративно-правового забезпечення; 3) норми права (норми адміністративного права); 4) адміністративно-правові відносини та їх зміст; 5) гарантії, заходи, засоби, форми та методи адміністративно-правового забезпечення.

Використана література

1. Троян Я. Інститут забезпечення конституційних прав і свобод: поняття, основні ознаки. *Підприємництво, господарство і право*. 2018. № 6. С. 210-215. URL: http://pgp-journal.kiev.ua/archive/2018/6/39.pdf (дата звернення: 02.12.2020).

2. Цвік М.В., Петришин О.В., Авраменко Л.В. Загальна теорія держави та права: підручник для студентів юридичних вищих навч. закладів ; за ред. д-ра юрид. наук, проф., акад. НАПрН України М.В. Цвіка, д-ра юрид. наук, проф., акад. НАПрН України О.В. Петришина. Харків: Право, 2011. 584 с.

3. Скакун О.Ф. Теорія права і держави: підручник. 2-ге вид. Київ: Алерта; ЦУЛ, 2011. 520 с.

4. Романова А.А. Система забезпечення прав і свобод людини та громадянина в Україні. *Форум права*. 2012. № 2. С. 599-602. URL: http://nbuv.gov.ua/UJRN/FP_index (дата звернення: 20.11.20).

5. Олійник А.Ю. Конституційно-правовий механізм забезпечення основних свобод людини і громадянина в Україні: монографія. Київ: Алерта, КНТ, Центр навчальної літератури, 2008. 153 с.

6. Рабинович П.М. Права людини і громадянина у Конституції України (до інтерпретації вихідних конституційних положень). Харків: Вид-во “Право”, 1997. 154 с.

7. Бігун В.С. Судове право розуміння у механізмі забезпечення прав людини. URL: http://bihun.in.ua/jushits/jurhit/article/632 (дата звернення: 20.11.20).

8. Костюченко О.Є. Визначення поняття "правове забезпечення". *Науковий вісник Національного університету державної податкової служби України*. 2015. № 1 (68). С. 11-16.

9. Мамчур Л.О. Адміністративно-правові засади взаємодії правоохоронних органів України з публічними інституціями: дис. …канд. юрид. наук: 12.00.07. Київ. 2019. 220 с.

10. Авер'янов В.Б. Доктринальні засади сучасного розвитку і реформування українського адміністративного права. Київ: Вид. дім "Ін Юре", 2002. С. 60-73.

11. Шопіна І.М. Феномен адміністративно-правового забезпечення в адміністративному праві України. *Наука і правоохорона.* 2018. № 4. С. 143-144. URL: http://naukaipravoohorona.com/journal/ukr/2018_4.pdf (дата звернення: 19.11.20).

12. Гумін О.М., Пряхін Є.В. Адміністративно-правове забезпечення: поняття та структура. *Наше право.* 2014. № 4. С. 46-50. URL: file:///C:/Users/User/Downloads/Nashp_2014_4_9.pdf (дата звернення: 18.11.20).

13. Ієрусалімова І.О. Механізм адміністративно-правового забезпечення прав і свобод людини та громадянина: дис. …канд. юрид. наук: 12.00.07. Київ. 2006. 205 с.

14. Колесников Є.Є. Поняття та особливості адміністративно-правового забезпечення захисту прав споживачів. *Форум права.* 2011. № 2. С. 432-438.

15. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т. Бусол. Київ-Ірпінь: ВТФ "Перун", 2003.1440 с.

16. Крестовская Н.Н., Матвеева Л.Г. Теория государства и права: элементарный курс. Харьков: Одиссей, 2007. 384 с.

17. Наливайко О.І. Правовий захист людини як предмет дослідження загальної теорії права: зб. наук. праць *Держава і право: Юридичні і політичні науки.* 2001. Вип. 12. С. 18-24.

18. Лазур Я.В. Поняття, сутність та елементи адміністративно-правового механізму забезпечення прав і свобод громадян у державному управлінні. *Форум права*. 2009. № 3. С. 392-398.

19. Гончарук С.Т. Адміністративне право України. Загальна та особлива частини: навч. посіб. Київ: Нац. акад. внутр. справ, 2000. 240 с.

20. Авер'янов В.Б. Державне управління: проблеми адміністративно-правової теорії та практики. Київ: Факт, 2003. 384 с.

21. Колпаков В.К. Адміністративно-правові відносини: на шляху до сучасної концепції: зб. наук. праць VI Міжнар. наук.-практ. конф. *Адміністративне право України: стан і перспективи розвитку*ю Київ: Ін-т держави і права ім. В.М. Корецького НАН України, 2011. 470 с.

22. Авер'янов В.Б. Нова доктрина українського адміністративного права: концептуальні позиції. *Право України*. 2006. № 5. С. 11-12.

23. Костюшко О.П. Забезпечення адміністративно-правових гарантій прав і свобод людини та громадянина. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 2 (14). С. 162-177.

24. Андрійко О.Ф. Адміністративно-правове забезпечення прав і свобод громадян в Україні: теорія і практика. *Альманах права*. 2017. Вип. 8. С. 23-26.

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

УДК 342.951

УХАНОВА Н.С., старший науковий співробітник НДІ інформатики і права НАПрН України.
ORCID: https://orcid.org/0000-0002-2366-5166.

ІНФОРМАЦІЙНА КУЛЬТУРА ОСОБИСТОСТІ: СУТНІСТЬ І ЗМІСТ

Анотація. *Статтю присвячено дослідженню сутності та ознак інформаційної культури особистості і з'ясуванню її ролі у сфері правового регулювання суспільних відносин у державі. Методологія дослідження феномену інформаційної культури особистості базується на положеннях загальнонаукового діалектичного методу наукового пізнання. Крім того, для повного та ґрунтовного розкриття теми статті використані формально-юридичний та формально-логічний методи. Обґрунтовано, що найголовнішим чином на розвиток такої культури у сучасний період впливають внутрішні чинники (зокрема додержання принципів законності, верховенства права і захист прав людини) та зовнішні загрози безпеці людини та громадянина всередині держави. Доведено, що інформаційну культуру у вузькому сенсі можна трактувати як оптимальні способи обміну даними, інформацією та подання їх зацікавленому споживачу для вирішення теоретичних і практичних завдань, а також як механізми вдосконалення системи навчання, підготовки людини до ефективного використання інформаційних засобів та інформації. До основних елементів інформаційної культури належать наступні: а) комунікативний (культура спілкування); б) лексичний (культура письма і оформлення ділової документації, мовна культура); в) інтелектуальний (культура науково-дослідної і розумової діяльності); г) інформаційно-правовий; світоглядний та моральний. Всі вказані елементи інформаційної культури особистості взаємопов'язані і взаємозумовлені. Зроблено висновок, що на сучасному етапі розвитку інформаційного суспільства особливої актуальності набула тематика захисту персональних даних, яка вийшла на новий рівень. Аргументується, що в майбутньому перспективним механізмом захисту персональних даних в інформаційній сфері буде використання технологій Blockchain, що дозволить забезпечити надійну синхронізацію і безпеку даних, унеможливить їх зміну в результаті зовнішнього втручання. Запропоновано інформаційну культуру особистості трактувати як відображення комплексу матеріально-інтелектуальних цінностей людини, що дозволяють ефективно застосовувати різноманітні способи роботи з інформацією, в тому числі бути учасником інформаційних правовідносин. У подальшому перспективним дослідженням у сфері інформаційної культури особистості стане розробка структури цієї категорії та її взаємозв'язок з іншими правовими категоріями галузі інформаційного права. Особливо важливе питання, що потребуватиме правового врегулювання, стане сфера і технології застосування штучного інтелекту як феномену, який не лише допоможе здійснити квантовий стрибок у сфері медицини, науки, освіти, а й несе собою великі ризики у сфері безпеки.*

Ключові слова: *інформація, інформаційна культура, інформаційне суспільство, інформаційна безпека, гібридна війна, пандемія.*

Summary. *The article deals with the study of the essence and features of the information culture of an individual and clarification of its role in the field of legal regulation of public relations in the state. The methodology of research of the phenomenon of personal information culture is based on provisions of the general scientific dialectical method of scientific knowledge. Besides, formal legal and formal logical methods were applied for full and thorough coverage of the topic of this article. It is substantiated that the development of such a culture in the modern period is mainly influenced by internal factors (including observance of the principle of legality, the rule of law, and protection of human rights), and external threats to human and civil security within the state. It is proved that information culture in the narrow sense can be interpreted as the best ways to exchange data, information and present them to interested*

consumers to solve theoretical and practical problems, as well as mechanisms to improve the learning system, prepare people for effective use of information. The main elements of information culture include the following: a) communicative (communication culture); b) lexical (culture of preparing and issuing business documentation, language culture); c) intellectual (culture of research and mental activity); d) information and legal; worldview and moral. All these elements of the personal information culture are interconnected and interdependent. It is concluded that the topic of personal data protection, which has reached a new level, has become especially relevant at the present stage of development of the information society. It is argued that a promising mechanism for personal data protection in the information sphere will be the use of Blockchain technologies, which will ensure reliable synchronization and security of data, prevent them from changing as a result of external interference. It is proposed to interpret the information culture of an individual as a reflection of a set of material and intellectual values of man, which allow to effectively apply various methods of working with information, including being a participant in information relations. A promising study in the field of information culture of an individual will be the development of the structure of this category and its relationship with other legal categories of information law. A particularly important issue that will require legal regulation will be the field and technology of using artificial intelligence as a phenomenon that will not only help to make a quantum leap in medicine, science, education, but also carries great security risks.

Key words: *information, information culture, information society, information security, hybrid war, pandemic.*

Аннотация. *Статья посвящена исследованию сущности и признаков информационной культуры личности и выяснению ее роли в сфере правового регулирования общественного отношения в государстве. Методология исследования феномена информационной культуры личности базируется на положениях общенаучного диалектического метода научного познания. Кроме того, для полного и основательного раскрытия темы статьи использованы формально-юридический и формально-логический методы. Обосновано, что главным образом на развитие такой культуры в современный период влияют внутренние факторы (в частности соблюдение принципов законности, верховенства права и защита прав человека) и внешние угрозы безопасности человека и гражданина внутри государства. Доказано, что информационную культуру в узком смысле можно трактовать как оптимальные способы обмена данными, информацией и представление их заинтересованному потребителю для решения теоретических и практических задач, а также как механизмы усовершенствования системы обучения, подготовки человека к эффективному использованию информационных средств и информации. К основным элементам информационной культуры принадлежат следующие: а) коммуникативный (культура общение); б) лексический (культура письма и оформление деловой документации, языковая культура); в) интеллектуальный (культура научно-исследовательской и умственной деятельности); г) информационно-правовой; мировоззренческий та моральный. Все указанные элементы информационной культуры личности взаимосвязаны и взаимообусловлены. Сделан вывод о том, что на современном этапе развития информационного общества особую актуальность приобрела тематика защиты персональных данных, которая вышла на новый уровень. Аргументируется, что в будущем перспективным механизмом защиты персональных данных в информационной сфере будет использование технологий Blockchain, что позволит обеспечить надежную синхронизацию и безопасность данных, сделает невозможным их изменение в результате внешнего вмешательства. Предложено информационную культуру личности трактовать как отображение комплекса материально-интеллектуальных ценностей человека, которые позволяют эффективно применять разные образы работы с информацией, в том числе быть участником информационного правоотношения. В дальнейшем перспективным исследованием в сфере информационной культуры личности станет разработка структуры этой категории и ее взаимосвязь с другими правовыми категориями области информационного права. Особенно важным вопросом, который будет нуждаться в правовом урегулировании, станет сфера и технологии применения искусственного интеллекта как феномена, который не только*

поможет осуществить квантовый прыжок в сфере медицины, науки, образования, а и несет собой большие риски в сфере безопасности.

Ключевые слова: *информация, информационная культура, информационное общество, информационная безопасность, гибридная война, пандемия.*

Постановка проблеми. Діяльність переважної більшості населення держав (до 90 %), що вступили в стадію інформаційного суспільства, завдяки засобам інформатики і сучасним інформаційним технологіям, буде так чи інакше пов'язана з інформацією. Інформаційне суспільство дозволяє вирішувати глобальні проблеми сучасної цивілізації, наявність яких є серйозною перешкодою для переходу до сталого розвитку в планетарному масштабі [9, с. 75]. На думку вчених, стратегічними напрямами формування сучасного інформаційного суспільства в Україні виступають: по-перше, повсюдне використання інформаційно-комунікаційних технологій задля вдосконалення системи державного управління, а також відносин між державою й громадянами, створення електронних форм спілкування між державними органами і фізичними та юридичними особами; по-друге зростання ролі місцевого самоврядування у створенні сучасного інформаційно-комунікаційного середовища в Україні [5, с. 16].

Комплексне дослідження інформаційних правовідносин провів Д.Ю. Шпенов. Інформаційні правовідносини науковець визначає як урегульовані правом та охоронювані державою суспільні відносини, що виникають у процесі виробництва, збирання, отримання, зберігання, перетворення, пошуку, передачі, поширення, споживання та захисту інформації, а також функціонування інформаційної інфраструктури. При цьому учасники зазначених відносин виступають носіями інформаційних прав і обов'язків. На думку вченого, такі відносини виникають, розвиваються і припиняються в інформаційній сфері при самостійному обігу інформації, при створенні й застосуванні автоматизованих інформаційних технологій, засобів і механізмів інформаційної безпеки [15]. На переконання І.В. Арістової, дуже важливим є питання прийняття Верховною Радою України рішення щодо розробки Інформаційного кодексу України. Адже, на думку дослідниці, єдиний інформаційний простір України торкається всіх сфер діяльності в суспільстві, охоплює всі регіони та території країни [5, с. 190]. Інформаційні відносини, що виникають та реалізуються, виступають загальним об'єктом нової комплексної галузі інформаційного права, норми якої регулюють суспільні відносини в інформаційній сфері. Тому питання про формування інформаційної культури особистості є своєчасним і набуває дедалі більшої актуальності.

Результати аналізу наукових публікацій. Теоретичною базою для підготовки статті послужило компаративне дослідження українського законодавства про інформацію з метою пошуку істотних ознак інформаційної культури як правового явища. Оскільки понятійно-категоріальний апарат даної проблематики характеризується поліваріантністю тлумачення необхідних для формування авторських дефініцій, у цій роботі стало необхідним також звернення до робіт зарубіжних вчених. Так, теоретичним підґрунтям статті послужили праці таких провідних вітчизняних і зарубіжних дослідників, як: І. Арістова, С. Валянський, О. Дзьобань, М. Кучерявенко, С. Матузак, С. Ожегов, А. Рац, С. Смичок, А. Федоров, Н. Шведова, Д. Шпенов та ін. Дослідження феномену інформаційної культури особистості перебуває в полі зору переважно науковців-культурологів, політологів і філософів та майже не здійснювалося з правової точки зору на доктринальному рівні, а тому є вчасним і актуальним.

Метою статті є з'ясування сутності та ознак інформаційної культури особистості та визначення її ролі у сфері правового регулювання суспільних відносин у державі.

Виклад основного матеріалу. У Стратегії розвитку інформаційного суспільства в Україні, схваленої розпорядженням Кабінету Міністрів України від 15.05.13 р. № 386-р зазначається, що загальносвітовою тенденцією є трансформація індустріального суспільства у постіндустріальне, що відбувається в умовах посилення глобалізаційних процесів, розширення сфери послуг і нематеріального виробництва у результаті науково-технічного прогресу, у тому числі масштабного, глибинного та динамічного проникнення інформаційно-комунікаційних технологій в усі сфери життєдіяльності особи, суспільства, суб'єктів господарювання й держави [13]. Аналіз даного нормативно-правового акта свідчить, що становлення інформаційної сфери в Україні ще триває, існує безліч проблем, що гальмують розвиток інформаційного суспільства в державі. Ще й досі не сформована повноцінна нормативно-правова база в інформаційній сфері. Крім того, слід говорити про те, що суспільна свідомість також зазнає впливу, який і чинить інформація як новий об'єкт правового регулювання. Зокрема можна говорити про об'єктивні обставини, які тим чи іншим чином вплинули в тому числі на формування інформаційної культури особистості в Україні. Найголовнішим чином на розвиток такої культури впливають внутрішні чинники (зокрема додержання принципів законності, верховенства права і захист прав людини і громадянина як головної цінності) та зовнішні загрози безпеці людини та громадянина всередині держави.

Події, що відбувалися в Україні, пов'язані з політичною кризою та військовими діями, продемонстрували слабкі місця в інформаційній і правовій сфері. Згідно з дослідженням Transparency International 2013 року, Україна була третьою за корумпованістю державою в Європі після Білорусі та Росії. Ті події, що трапилися в державі у подальшому, окупація Криму та регіонів Східної України, лише погіршили ситуацію [3] та вивели на поверхню ті проблеми, що стосуються такого нового виду міждержавних конфліктів, як гібридна війна, що поєднує не лише бойові дії, а й інформаційну атаку як на громадян держави, так і на державу в цілому. У цей період на етапі розвитку і формування інформаційної культури питання надійності, достовірності та безпеки інформації з доступних джерел становить серйозну задачу. Це пов'язано частково з ефектом, який часто називають "туман війни", тобто відсутністю тактичної інформації про події, що відбуваються. Отже критичний аналіз інформаційних ресурсів має вирішальне значення. На думку експертів, моніторинг регулярних звітів у режимі реального часу через соціальні мережі надавав докладні відомості про повсякденне життя на територіях, на які поширюються бойові дії, які було б неможливо отримати від іншого джерела. Серед інших цінних джерел інформації також називають публічну інформацію Місії спостерігачів ОБСЄ. До того ж, виявилися дуже корисними аналітичні та програмні документи, написані незалежними сторонніми експертами [2, с. 76]. Тобто на формування і "кристалізацію" інформаційної культури особистості, поряд зі свідомістю, напряму впливають зовнішні чинники.

Для більш глибокого розуміння сутності інформаційної культури особистості слід проаналізувати визначення утворюючих її елементів. Так, термін "культура" у словниковій літературі трактується як сукупність виробничих, громадських і духовних досягнень людей [1]. Крім того у словникових джерелах категорія "культура інформаційна" (*information culture*) визначається як сукупність матеріальних та інтелектуальних цінностей в області інформації, а також історично певна система їх відтворення та функціонування в соціумі. По відношенню до аудиторії інформаційна культура може виступати системою рівнів розвитку особистості людини, здатного сприймати, аналізувати, оцінювати інформацію, засвоювати нові знання у цій галузі. Аналогами такого терміну є також категорії "відео культура" (*video culture*),

кінематографічна культура (*film culture*), медіакультура (*media culture*) [12, с. 23].

Культура особистості, в тому числі інформаційна, має тісний зв'язок з феноменом свідомості людини, в основі якої лежить буденна свідомість. Остання часто і цілком справедливо ототожнюється з так званим здоровим глуздом, тобто здатністю бачити речі такими, як вони є. Але на відміну від свідомості наукової, яка теж досліджує світ на предмет істинності, відповідності суб'єктивної інформації об'єктивному стану справ, буденна свідомість принципово емпірична і не концептуальна. База фактів сприймається повсякденною свідомістю суб'єктивно, тобто психічна за формою інформація проходить лише початкову, донаукову обробку свідомості. На думку вчених, момент зіставлення, узагальнення і класифікації інформації в сукупності становить операційну базу аналітизму, дозволяє повсякденну свідомість вельми успішно пристосовувати до оточуючого світу, насамперед, практично діяльнісного, прагматичного, а не ідеологічного пристосування [14, с. 50]. Це означає, що формування інформаційної культури особистості починається фактично з її буденної свідомості та має декілька етапів розвитку, який проходить крізь призму аналізу інформації, яка оточує людину і якою вона користується. У даному випадку мова йде про фізичну особу, яка потенційно може бути учасником інформаційних правовідносин.

Інформаційну культуру в економічному словнику трактують як знання і навички ефективного користування інформацією, що передбачає різнобічне вміння пошуку необхідної інформації та її використання [4]. У сучасний період інформаційне суспільство не випадково називають "навчальним суспільством", суспільством, що еволюціонує в суспільство знань. Підставою для цього виступають принципові зміни в сфері виробництва споживання інформації та знань:

1) перетворення інформації і знань на провідну перетворюючу силу суспільства, усвідомлення інформаційних ресурсів як стратегічних ресурсів суспільства;

2) становлення ринкової економіки, економіки знань, в основі якої лежить глобальна інформатизація, стрімкий розвиток інформаційно-комунікаційних технологій;

3) постійне зростання обсягів інформаційних потоків в поєднанні з їх динамічністю, мінливістю, обумовлених скороченням циклу поновлення як виробничих, так і соціальних технологій, який став випереджати темпи зміни поколінь;

4) розуміння необхідності безперервної освіти і здатності до перекваліфікації як невід'ємної частини збереження соціального статусу особистості;

5) залежність долі кожної людини від здатності своєчасно знаходити, отримувати, адекватно сприймати і продуктивно використовувати нову інформацію [16, с. 76, 77].

Основними факторами, що визначили виникнення феномена інформаційної культури, були: перехід інформації в розряд найважливіших універсальних категорій суспільного розвитку; зростання обсягів інформації, інформатизація суспільства, розвиток інформаційної техніки і технологій; становлення інформаційного суспільства, тобто "…людські спільноти – перш за все, інформаційні системи, будь-яка дія, подія, твір є результат отримання, обробки і виробництва інформації" [7, с. 13]. Цим визначається особлива важливість інформаційної культури і необхідність всебічного вивчення цього явища. Важливим є і той факт, що в інформаційному суспільстві різко зростає необхідність постійного оновлення знань, підвищення кваліфікації, освоєння нових видів діяльності, створення нових культурних цінностей [6, с. 12; 13].

Інформаційну культуру у вузькому сенсі можна трактувати як найбільш оптимальні способи обміну даними, інформацією та подання їх зацікавленому споживачу для вирішення теоретичних і практичних завдань, а також як механізми вдосконалення системи навчання, підготовки людини до ефективного використання

інформаційних засобів та інформації. До основних елементів інформаційної культури належать наступні: а) комунікативний (культура спілкування); б) лексичний (культури письма і оформлення ділової документації, мовна культура); в) інтелектуальний (культура науково-дослідної і розумової діяльності); г) інформаційно-правовий; світоглядний та моральний. Всі вказані елементи інформаційної культури особистості взаємопов'язані і взаємозумовлені [8].

Визначальну роль для дослідження феномена інформаційної культури як правового явища має інформаційно-правовий елемент. Для прикладу, з метою посилення ролі інформаційної культури на світовому рівні ООН було розроблено Конвенцію про використання електронних повідомлень в міжнародних договорах [10]. Ця концепція у подальшому сприятиме вдосконаленню інформаційних відносин, у тому числі у сфері укладання та виконання угод між суб'єктами правовідносин.

На сучасному етапі розвитку інформаційного суспільства особливої актуальності набула тематика захисту персональних даних, яка вийшла на новий рівень. Особливої значимості ця тема набула в умовах загальносвітової пандемії коронавірусу COVID-19 і стосується у тому числі й персональних даних про пацієнтів.

Уявляється, що в майбутньому перспективним механізмом забезпечення захисту інформації в інформаційних правовідносинах буде використання технологій Blockchain, що дозволить забезпечити надійну синхронізацію і безпеку даних, унеможливить їх зміну в результаті зовнішнього втручання. Категорія "Blockchain" означає програмно-комп'ютерний алгоритм децентралізованого публічного або приватного реєстру або бази даних, функціонування якої забезпечується шляхом взаємодії через Інтернет тимчасової мережі або будь-яким іншим способом, який гарантує належний криптографічний захист всіх записів, транзакцій, проведених з використанням новітніх технологій. Blockchain являє собою багатофункціональну і багаторівневу інформаційну технологію, призначення якої проявляється в обліку і передачі різної інформації. Якщо розглядати Blockchain як систему обліку інформації, що становить медичну таємницю, то ця технологія заснована на криптографічно захищеному, хронологічно сталому обліку транзакцій, під яким слід розуміти фіксацію всіх переходів одиниць обліку Blockchain між користувачами такої мережі. Отже, Blockchain виконує функцію обліку даних. Така одиниця обліку має такі обов'язкові ознаки, як стандартизованість і незмінність [11, с. 8, 43]. З правової точки зору дана технологія дозволить забезпечити високий рівень захисту даних, що в цілому сприятиме розвитку децентралізованої системи обліку будь-якої інформації, що виступає об'єктом правового регулювання у правовідносинах між суб'єктами.

Кібербезпека стала головним пріоритетом для урядів держав усього світу, бізнесу і громадян. Цифрова безпека стає синонімом національної безпеки. Нове інформаційне суспільство слід розглядати як ключовий позитивний елемент, який розширює можливості громадян, розвиває бізнес і допомагає побудувати відкрите, інноваційне, безпечне та стійке суспільство.

Висновки.

Сучасна парадигма інформаційного суспільства вказує на важливість взаємозв'язку культурного та соціального вимірів розвитку інформаційних технологій. Реалізація технологій інформаційного суспільства в різноманітних соціально-культурних середовищах також повинна бути соціально та культурно прийнятною та максимально демократичною. Це означає, що основні моделі правового регулювання відносин в інформаційній сфері повинні бути чітко визначені та адаптовані між собою. Особливо це актуалізується в умовах пандемії та закриття кордонів, внаслідок чого майже всі

сфери суспільного життя були імплементовані в інформаційну сферу, включаючи такі сфери, як освіта, наука, спорт, культурне просвітництво, міждержавне спілкування тощо. Мова йде про перспективи подальшого розвитку електронного врядування, посилення культурних зв'язків на глобальному рівні, "стирання" кордонів між державами та світової глобалізації.

Аналіз наукових підходів та інформаційної нормативної бази дозволяє виділити основні ознаки інформаційної культури особистості як феномену у сфері інформаційного права, а саме: а) виступає вираженням правової свідомості особистості; б) залежить від зовнішніх джерел інформації; в) є наслідком формування інформаційного суспільства; г) виступає одним із індикаторів правової свідомості особистості. На цій підставі інформаційну культуру особистості можна трактувати як відображення комплексу матеріально-інтелектуальних цінностей людини, що дозволяють ефективно застосовувати різноманітні способи роботи з інформацією, в тому числі бути учасником інформаційних правовідносин. У подальшому перспективним дослідженням у сфері інформаційної культури особистості стане розробка структури цієї категорії та її взаємозв'язок з іншими правовими категоріями галузі інформаційного права.

Особливо важливим питанням, що потребуватиме правового врегулювання, стане сфера і технології застосування штучного інтелекту як феномену, що у даний час реалізується або у формі програмного пакету (віртуальна платформа, чат-боти, програми тощо, які не мають матеріальної оболонки), або ж програмно (робот, дрон тощо) в якості інструмента для конкретних цілей, закладених у рамках інформаційних правовідносин, що виникають між суб'єктами – як фізичними так і юридичними особами. Застосування штучного інтелекту не лише допоможе здійснити квантовий стрибок у сфері медицини науки, освіти, а й несе за собою великі ризики у сфері безпеки. Прояв інформаційної культури особистості в процесі використання технологій штучного інтелекту має бути заснований на принципах поваги до людської гідності, гуманізму, суворому додержанні прав і свобод людини і громадянина.

Використана література

1. Andras Racz Russia's Hybrid war in Ukraine. Breaking the Enemy's to Resist, Fla Report (2016), 43. URL: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf (Last accessed: 25.01.2021).

2. Matuszak, S. The Oligarchic Democracy: The Influence of Business Groups on Ukrainian Politics, OSW Studies № 42, Centre for Eastern Studies, 2012, Warsaw. URL: https://www.osw.waw.pl/sites/default/files/prace_42_en.pdf, accessed 5 March 2015 (Last accessed: 25.01.2021).

3. Transparency International, Corruption Perceptions Index (2013). URL: http://cpi.transparency. org/cpi2013/results (Last accessed: 25.01.2021).

4. Андреев А.Н. Культурология. Личность и культура. Минск: Дизайн ПРО, 1998. 160 с.

5. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти: монография; за заг. ред. О.М. Бандурки. Харків: Ун-т внутріш. справ, 2000. 368 с.

6. Валянский С.И., Калюжный Д.С. Другая история науки. Москва: ИМФРА-М., 2002. С. 13.

7. Гендина Н.И., Колкова Н.И., Стародубова Г.А., Уленко Ю.В. Формирование информационной культуры личности: теоретическое обоснование и моделирование содержания учебной дисциплины. Москва: Межрегиональный центр библиотечного сотрудничества. 2006. 512 с.

8. Горелова В.Е. Информационная культура и её роль в формировании личности: автореф. дис. …канд. культурологи: 24.00.01. Киров, 2008. 17 с.

9. Дзьобань О.П. Філософія інформаційних комунікацій: монографія. Харків: Майдан, 2012. 224 с.

10. О использовании электронных сообщений в международных договорах: Конвенция Организации Объединенных Наций. Комиссия ООН по праву международной торговки. Нью-Йорк, 2007. 101 с.

11. Кудь А., Кучерявенко М., Смичок Є. Цифрові активи та їх правове регулювання у світлі розвитку технології блокчейн: моногр. Харків: Право, 2019. 216 с.

12. Ожегов С.И., Шведова Н.Ю. Словарь русского языка. URL: http://cyberlan.com.ua/wp-content/uploads/2015/07/Tolkovij-slovarj-russkogo-yazika.pdf (дата звернення: 25.01.2021).

13. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.13 р. № 386-р. URL: http://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80 (дата звернення: 25.01.2021).

14. Федоров А.В. Словарь терминов по медиаобразованию, медиапедагогике, медиаграмотности, медиакомпетентности. Москва: МОО “Информация для всех”, 2014. 64 с.

15. Шпенов Д.Ю. Інформаційні правовідносини: автореф. дис. …канд. юрид. наук: 12.00.07. Київ, 2012. 19 с.

16. Экономический электронный словарь. URL: http://slovariki.org/ekonomiceskij-slovar/14962 (дата звернення: 25.01.2021).

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

УДК 349.2:351.74

ІРХА Ю.Б., *кандидат юридичних наук*, науковий співробітник
НДІ інформатики і права НАПрН України.
ORCID: https://orcid.org/0000-0002-6442-0974.

ЗАХИСТ ТРУДОВИХ ПРАВ ОСІБ РЯДОВОГО І НАЧАЛЬНИЦЬКОГО СКЛАДУ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ, ЗВІЛЬНЕНИХ ЗІ СЛУЖБИ ЧЕРЕЗ СКОРОЧЕННЯ ШТАТІВ ВНАСЛІДОК ЛІКВІДАЦІЇ МІЛІЦІЇ

Анотація. *У статті досліджуються окремі проблеми захисту трудових прав осіб рядового і начальницького складу органів внутрішніх справ України, звільнених зі служби через скорочення штатів внаслідок ліквідації міліції. Стверджується, що на працівників міліції поширюються гарантії трудових прав, які визначені у Кодексі законів про працю України і не врегульовані нормами спеціальних законів України. Доводиться, що вивільнені працівники міліції в обов'язковому порядку мали бути ознайомлені з переліком вакансій в органах та підрозділах Національної поліції України. Перебуваючи на службі особи, особи рядового та начальницького складу ОВС України мали легітимні очікування щодо довгострокої реалізації свого права на працю у правоохоронному органі, а також на стабільність та захищеність свого юридичного та соціально-економічного становища. Зроблено висновок про недотримання державою конституційного принципу верховенства права при реформуванні органів внутрішніх справ України.*

Ключові слова: *верховенство права, право на працю, гарантії трудових прав, ліквідація міліції, працівники міліції, звільнення зі служби через скорочення штатів.*

Summary. *The article deals with some problems of protection of labor rights of privates and officers of the internal affairs bodies of Ukraine dismissed from service due to downsizing as a result of the liquidation of the militia. It is alleged that militia officers are guaranteed labor rights, which are defined in the Labor Code of Ukraine and are not regulated by special laws of Ukraine. It is proved that the released militia officers should be given lists of vacancies in organs and units of the National Police of Ukraine. While serving, privates and officers of the militia of Ukraine had legitimate expectations for the long-term realization of their right to work in law enforcement, as well as for the stability and protection of their legal and socio-economic status. It is concluded that the state fails to comply with the constitutional principle of the rule of law in reforming the internal affairs bodies of Ukraine.*

Keywords: *rule of law, right to work, guarantees of labor rights, liquidation elimination of militia, militia workers, dismissals from service on staff reduction.*

Аннотация. *В статье исследуются отдельные проблемы защиты трудовых прав лиц рядового и начальствующего состава органов внутренних дел Украины, уволенных со службы по сокращению штатов в результате ликвидации милиции. Утверждается, что на работников милиции распространяются гарантии трудовых прав, определенных в Кодексе законов о труде Украины и не урегулированы нормами специальных законов Украины. Доказывается, что высвобожденные работники милиции в обязательном порядке должны были быть ознакомлены с перечнем вакансий в органах и подразделениях Национальной полиции Украины. Находясь на службе лица рядового и начальствующего состава ОВД Украины имели законные ожидания на долгосрочную реализацию своего права на труд в правоохранительном органе, а также на стабильность и защищенность своего юридического и социально-экономического положения. Сделан вывод о несоблюдении государством конституционного принципа верховенства права при реформировании органов внутренних дел Украины.*

Ключевые слова: *верховенство права, право на труд, гарантии трудовых прав, ликвидация милиции, работники милиции, увольнения со службы по сокращению штатов.*

Постановка проблеми. Проведення інституційних реформ в Україні доволі часто відбувається в умовах суспільно-політичної нестабільності та низьких темпів соціально-економічного зростання. Довгоочікувані реформаторські пропозиції, як правило, знаходять підтримку в парламенті та суспільстві, однак їх швидка реалізація на практиці досить часто призводить до порушення прав, свобод та законних інтересів громадян в Україні. Безсистемність, низький рівень нормопроектувальної техніки, а також відсутність належних фінансових, матеріальних, технічних та кадрових ресурсів для подальшої довгострокової підтримки та розвитку розроблених реформ, нівелюють більшість раціональних ініціатив. У результаті заявлені благі цілі та завдання започаткованих реформ не приносять суттєвої користі ані суспільству, ані державі. Більше того, в окремих випадках такі реформи погіршують ситуацію, адже нове ще не значить краще. Від незавершених та/або неякісних реформ в державному секторі насамперед страждають співробітники органів державної влади, державних підприємств, установ, організацій, які першими відчувають на собі всі недоліки від реалізації задумів реформаторів, а також негативну реакцію громадськості.

У зв'язку із запитом суспільства на реформування органів внутрішніх справ України (далі – ОВС України) у 2015 році ухвалено Закон України "Про Національну поліцію" від 02.07.15 р. № 580-VIII (далі – Закон № 580), який дав поштовх до оновлення усієї системи правоохоронних органів у державі. Внаслідок утворення Національної поліції України як центрального органу виконавчої влади діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, було ліквідовано міліцію як державний озброєний орган виконавчої влади.

Реалізація положень Закону № 580 хоч і стала правовою підставою для утворення Національної поліції України та набору працівників до її органів та підрозділів, однак на практиці це призвело до порушення трудових прав багатьох осіб рядового і начальницького складу ОВС України, які були звільненні зі служби через скорочення штатів.

Результати аналізу наукових публікацій. Захист трудових прав осіб рядового і начальницького складу ОВС України є предметом наукових розробок багатьох українських вчених. Цією проблематикою займалися, зокрема, Д.М. Величко, В.С. Венедіктов, В.Я. Гоц, М.І. Іншин, В.Ю. Кікінчук, М.М. Клемпарський, А.В. Кудрявцев, І.В. Огієнко, О.В. Лавріненко, Л.В. Могілевський, П.Д. Проскуряков, І.В. Шульженко, В.І. Щербина, Т.П. Яценко.

Незважаючи на розробленість питання захисту трудових прав працівників ОВС України, у вітчизняній доктрині не повною мірою висвітлено питання захисту їх прав при звільненні зі служби через скорочення штатів внаслідок ліквідації міліції, що і стало предметом цього наукового пошуку.

Метою статті є визначення та оцінка теоретичних та практичних проблем, які виникли при звільнення осіб рядового і начальницького складу ОВС України зі служби внаслідок ліквідації міліції, а також надання рекомендацій щодо захисту та відновлення їх трудових прав.

Виклад основного матеріалу. Згідно Конституції України кожен має право на працю, що включає можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується; держава створює умови для повного здійснення громадянами права на працю, гарантує рівні можливості у виборі професії та роду трудової діяльності, реалізовує програми професійно-технічного навчання, підготовки і перепідготовки кадрів відповідно до суспільних потреб; громадянам гарантується захист від незаконного звільнення (частини перша, друга, шоста статті 43 Конституції України).

У своїх рішеннях Конституційний Суд України зазначив, що:

– зміст права на працю полягає у можливості кожної особи заробляти собі на життя працею, яку вона вільно обирає або на яку вільно погоджується (стаття 43 Конституції України). Це право забезпечується обов'язком держави створювати громадянам умови для повного його здійснення, гарантувати рівні можливості у виборі професії та роду трудової діяльності, реалізовувати програми професійно-технічного навчання, підготовки і перепідготовки кадрів відповідно до суспільних потреб. Однак це конституційне право громадянина не може пов'язуватись лише з певною формою трудового договору, який укладається громадянином відповідно до його волевиявлення (абзац третій пункту 4 мотивувальної частини Рішення від 09.07.98 р. № 12-рп/1998);

– свобода праці передбачає можливість особи займатися чи не займатися працею, а якщо займатися, то вільно її обирати, забезпечення кожному можливості без дискримінації вступати у трудові відносини для реалізації своїх здібностей. За своєю природою право на працю є невідчужуваним і по суті означає забезпечення саме рівних можливостей кожному для його реалізації. Реалізація права громадянина на працю здійснюється шляхом укладення ним трудового договору і виконання кола обов'язків за своєю спеціальністю, кваліфікацією або посадою, яка передбачається структурою і штатним розписом підприємства, установи чи організації (абзаци другий, третій підпункту 4.1 пункту 4 мотивувальної частини Рішення від 07.07.04 р. № 14-рп/2004);

– конституційне право громадян на працю означає можливість кожного заробляти собі на життя працею, вільно вибирати професію чи спеціальність відповідно до своїх здібностей і бажань, реалізовувати свої бажання щодо зайняття працею за трудовим договором (контрактом) на підприємстві, в установі, організації незалежно від форм власності або самостійно забезпечувати себе роботою (абзац другий підпункту 3.1 пункту 3 мотивувальної частини Рішення від 16.10.07 р. № 8-рп/2007);

– право заробляти собі на життя є невід'ємним від права на саме життя, оскільки останнє є реальним лише тоді, коли матеріально забезпечене. Право на працю закладено у самій людській природі. Його має кожна людина, воно є невідчужуваним, тому самій особі належить виключне право розпоряджатися своїми здібностями до праці. Визначене статтею 43 Конституції України право на працю Конституційний Суд України розглядає як природну потребу людини своїми фізичними і розумовими здібностями забезпечувати своє життя. Це право передбачає як можливість самостійно займатися трудовою діяльністю (індивідуально-трудова діяльність, фермерство тощо), так і можливість працювати за трудовим договором чи контрактом (абзаци другий, третій підпункту 6.1.1 пункту 6 мотивувальної частини Рішення від 29.01.08 р. № 2-рп/2008).

У процесі реалізації конституційного права на працю особа вступає у триваючі правовідносини із роботодавцем, який зобов'язаний неухильно додержуватися законодавства про працю, у тому числі під час припинення трудового договору з найманим працівником.

За твердженнями В. Венедіктова, під припиненням трудового договору необхідно розуміти родове поняття, яке об'єднує всі підстави розірвання трудових зв'язків: як за ініціативою працівника, власника чи уповноваженого ним органу, третіх осіб, так і у зв'язку з вибуттям працівника зі спискового складу підприємства, у зв'язку з його смертю [1, с. 106]. На переконання С. Глазько, припинення трудового договору є припиненням трудових правовідносин за волевиявленням працівника, роботодавця, вимогою третіх осіб, які не є сторонами трудового договору, або за наявності визначених у законодавстві життєвих обставин [2, с. 17]. В. Шишлюк вважає, що припинення

трудового договору – це закінчення дії трудових правовідносин за угодою (згодою) сторін, волевиявленням сторін чи третіх осіб, які не є їх стороною, а також з підстав, що не залежать від волі сторін, у порядку, визначеному законодавством [3, с. 14].

У своєму дисертаційному дослідженні Е. Бабенко виокремлює індивідуальне та колективне припинення трудових відносин. Під індивідуальним припиненням трудових правовідносин, науковець пропонує розуміти звільнення найманого працівника з роботи роботодавцем, з котрим цей працівник перебуває у відповідних відносинах, здійснюване за умов і з підстав, із дотриманням усіх гарантій, передбачених законодавством України про працю, а також належним чином документально оформлене.

Водночас, колективне припинення трудових правовідносин (вивільнення працівників) Е. Бабенко розглядає як окремий вид припинення трудових правовідносин, який об'єктивується у сукупності соціально-виробничих і правових відносин, що виникають, тривають і припиняються у результаті реалізації роботодавцем права (у випадку ліквідації юридичної особи-роботодавця – обов'язку) на одночасне розірвання трудового договору з усіма чи значною кількістю найманих працівників на підставі норм чинного законодавства, за наявності спеціальних фактичних обставин об'єктивної дійсності, що обумовлюють нагальну потребу щодо реалізації роботодавцем цього права (обов'язку), та відповідно до спеціального порядку вивільнення працівників [4, с. 359, 362].

У теорії трудового права визначено, що трудовий договір припиняється тільки за наявності підстав для його припинення. Підставою припинення договору є юридичний факт або сукупність юридичних фактів, закріплених у законі та необхідних для припинення трудового договору. Вони поділяються на два види:

– дії (життєві ситуації, що відбуваються за волею людей; вольові акти їх поведінки) сторін трудового договору або осіб, які не є його сторонами;

– події (життєві обставини, настання яких не залежить від волі та свідомості людей: закінчення строку трудового договору; смерть працівника або роботодавця – фізичної особи тощо).

Підстави припинення трудового договору закріплено у Кодексу законів про працю України (далі – Кодекс). Залежно від того, хто є ініціатором припинення трудового договору, підстави поділяються на такі групи: 1) припинення трудового договору за спільною (взаємною) ініціативою сторін трудового договору (наприклад, угода сторін, закінчення строку); 2) розірвання трудового договору з ініціативи працівника (статті 38, 39 Кодексу); 3) розірвання трудового договору з ініціативи роботодавця (статті 40, 41 Кодексу); 4) розірвання трудового договору з ініціативи осіб, які не є його стороною (третіх осіб) (пункти 3,7 статті 36, стаття 45 Кодексу) [5].

У Кодексі визначені загальні підстави припинення трудового договору, водночас, керуючись приписами його статті 7, у інших законах України для окремих категорій працівників можуть встановлюватися додаткові (особливі) підстави для такого припинення з огляду на специфіку їх роботи. Такий підхід був застосований до працівників міліції, і продовжує діяти щодо суддів, прокурорів, державних службовців, військовослужбовців, поліцейських тощо.

Ліквідація міліції зумовила колективне припинення трудових відносин з особами рядового і начальницького складу ОВС України. Значна частина цих осіб була звільнена зі служби через скорочення штатів. Незважаючи на бажання окремих осіб реалізувати своє конституційне право на працю у новоутвореному правоохоронному органі, держава не вжила достатніх організаційно-правових заходів щодо працевлаштування вивільнених працівників міліції до органів та підрозділів Національної поліції України.

Зазначене було обумовлено твердженнями про те, що на осіб рядового і начальницького складу ОВС України не поширюються гарантії трудових прав, визначених у Кодексі, а також що Національна поліція України не є правонаступником міліції.

На нашу думку, такий підхід не відповідає позитивним обов'язкам держави, які визначені Конституцією України.

Опрацювання Закону України "Про міліцію" та Положення дає підстави стверджувати про наявність деяких прогалин у правовому регулюванні окремих питань реалізації та захисту трудових прав працівниками міліції у процесі проходження ними служби. У зазначених актах була відсутня пряма вказівка на можливість застосування положень Кодексу до правовідносин, які ними не врегульовано, що зумовило порушення трудових прав осіб рядового і начальницького складу ОВС України при звільненні зі служби внаслідок ліквідації міліції.

На переконання Т. Яценко, під юридичними гарантіями припинення службово-трудових відносин працівників ОВС України необхідно розуміти передбачену нормативно-правовими актами діяльність сторін трудового договору (контракту), яка сприяє безперешкодному здійсненню юридичних можливостей і досягненню найбільш ефективних соціально значущих результатів на даній стадії правовідношення. За твердженнями дослідника загальні гарантії припинення трудових відносин з працівниками суспільного виробництва, передбачені Кодексом та іншими нормативно-правовими актами стосовно припинення службово-трудових відносин осіб рядового та начальницького складу ОВС України мають з необхідністю доповнюватися спеціальними гарантіями, що містяться у нормах як законодавства про державну службу, так і положеннях відомчого нормативно-правового забезпечення [6, с. 55, 56].

У теорії права загальновизнано, що при розбіжності між положеннями загального і спеціального нормативно-правового акту, перевага надається спеціальному, якщо він не скасований виданим пізніше загальним актом. Норми спеціального законодавства є пріоритетними та підлягають першочерговому застосуванню. При цьому у разі відсутності у загальному або спеціальному законодавстві норм, які регулюють певні суспільні відносини, (наявність прогалини у законодавстві), допускається застосування аналогії закону чи аналогії права для врегулювання відповідних відносин.

Відповідно до статті 8 Цивільного кодексу України якщо цивільні відносини не врегульовані цим Кодексом, іншими актами цивільного законодавства або договором, вони регулюються тими правовими нормами цього Кодексу, інших актів цивільного законодавства, що регулюють подібні за змістом цивільні відносини (аналогія закону); у разі неможливості використати аналогію закону для регулювання цивільних відносин вони регулюються відповідно до загальних засад цивільного законодавства (аналогія права).

Згідно положень пункту 9 статті 10 Цивільного процесуального кодексу України "якщо спірні відносини не врегульовані законом, суд застосовує закон, що регулює подібні за змістом відносини (аналогія закону), а за відсутності такого – суд виходить із загальних засад законодавства (аналогія права)". За приписами пункту 6 Кодексу адміністративного судочинства України "у разі відсутності закону, що регулює відповідні правовідносини, суд застосовує закон, що регулює подібні правовідносини (аналогія закону), а за відсутності такого закону суд виходить із конституційних принципів і загальних засад права (аналогія права)".

Суд Справедливості Європейського Союзу у рішенні у справі "Yvonne van Duyn v. Home Office" зазначив, що принцип правової визначеності означає, що зацікавлені особи повинні мати змогу покладатись на зобов'язання, взяті державою, навіть якщо

такі зобов'язання містяться в законодавчому акті, який загалом не має автоматичної прямої дії (пункт 13) [7].

На нашу думку, після прийняття на службу до міліції особа була учасником не тільки державно-службових, але й трудових правовідносин. У зв'язку з цим особи рядового і начальницького складу ОВС України є носіями прав та обов'язків, які визначені як Конституцією України та законами України, що регулювали діяльність та порядок проходження служби працівниками міліції, так і законами що регулюють реалізацію та захист трудових прав громадян.

Оскільки правовідносини щодо проходження служби працівниками міліції регулюються нормами спеціального законодавства, то вважаємо, що положення трудового законодавства підлягають застосуванню у випадках, якщо нормами спеціального законодавства не врегульовано спірні правовідносини або коли про це йдеться у спеціальному законі. У такий спосіб забезпечується рівність прав та принцип недискримінації у трудових відносинах. Зазначене узгоджується із судовою практикою, зокрема Конституційного Суду України (Рішення від 07.05.02 р. № 8-рп/2002) та Верховного Суду (постанови від 01.03.18 р. у справі № 806/1551/17; від 05.08.20 р. у справі № 826/20350/16).

Враховуючи теоретичні засади співвідношення загального та спеціального правового регулювання, ми вважаємо, що внаслідок ліквідації міліції особи могли бути звільнені з ОВС України виключно з дотриманням тих гарантій їх трудових прав, які визначені у Кодексі та не врегульовані нормами спеціальних законів України.

Правове регулювання припинення службово-трудових правовідносин з особами рядового і начальницького складу ОВС України здійснювалося відповідно до положень Кодексу з урахуванням вимог спеціальних норм, які були визначені у Законі України "Про міліцію" від 20.12.90 р. № 565–XII та конкретизовані у Положенні про проходження служби рядовим і начальницьким складом органів внутрішніх справ України, затвердженого Постановою Кабінету Міністрів УРСР від 29.07.91 р. № 114 (далі – Положення).

За твердженнями Т. Яценко службово-трудові відносини органів, служб та підрозділів внутрішніх справ з працівниками ОВС України виступають як нормативно урегульований двосторонній зв'язок. Кожна з сторін має кореспондуючі одна одній права та обов'язки, належне виконання та захист яких здійснюється комплексами юридичних гарантій, які містяться в нормах матеріального і процесуального характеру. Порушення будь-якої правової можливості, перешкода її здійснення припускає обов'язкове притягнення винних посадових осіб до службово-трудової відповідальності [6, с. 54, 55].

На переконання І. Огієнко, службово-трудовим правовідносинам осіб рядового і начальницького складу ОВС України був притаманний ряд особливостей, обумовлених специфікою здійснюваної службової діяльності від імені держави, і спрямованої на здійснення завдань і функцій держави, яка впливає на об'єктивну необхідність встановлення певних обмежень і заборон, додаткових гарантій трудової діяльності, специфічного регулювання робочого часу і часу відпочинку. При цьому, основи правового статусу працівників міліції як суб'єктів трудового права, визначалися саме законодавством про працю та мали ряд особливостей, які були необхідними для збереження балансу у правовому положенні працівника ОВС України порівняно з працівниками інших сфер [8, с. 376].

Звільнення зі служби осіб рядового і начальницького складу ОВС України, як зазначає Ю. Кікінчук, могло здійснюватися лише на підставах, передбачених законом,

під якими розуміють такі життєві обставини, що законодавчо визначаються як юридичні факти для припинення служби. Сама по собі наявність зазначеної в законі підстави не припиняє службових (трудових) відносин, необхідним є певний юридичний акт – дія відповідної особи (наказ керівника, рапорт працівника), що відображає волю (ініціативу) сторін щодо припинення служби [9, с. 198].

Ми підтримуємо твердження І. Шульженко, що специфіка умов праці (служби) в ОВС України визначала критерії диференціації правового регулювання припинення трудових правовідносин з працівниками міліції. До таких критеріїв відносилися: по-перше, додаткові підстави припинення трудових правовідносин порівняно з Кодексом; по-друге, особлива процедура звільнення з ОВС України; по-третє, надання додаткових правових гарантій і пільг для працівників ОВС України, передбачених спеціальним законодавством про проходження служби, які компенсують специфіку умов праці в ОВС України [10].

Відповідно до абзацу першого пункту 10 розділу XI "Прикінцеві та перехідні положення" Закону № 580 "працівники міліції, які відмовилися від проходження служби в поліції та/або не прийняті на службу до поліції в тримісячний термін з моменту попередження про наступне вивільнення, звільняються зі служби в органах внутрішніх справ через скорочення штатів".

У своєму дослідженні М. Іншин наголошує, що правовий механізм регулювання процесу скорочення штату співробітників системи МВС України складається як з матеріальних і процесуальних норм, так і з правил загального, спеціального і локального (відомчого) характеру. Науковець вважає, що вивільнення працівників органів внутрішніх справ – це сукупність певних економічних, соціально-службових, правових відносин, що викликані економічними та організаційно-службовими чинниками і пов'язані з скороченням штату працівників системи органів Міністерства внутрішніх справ України з метою підвищення ефективності їх служби та праці [11, с. 11, 12].

О. Лавріненко аргументовано стверджує про відсутність у законодавстві України поняття "скорочення штату працівників", що зумовлює певні труднощі у правозастосуванні. На його переконання, до основних ознак поняття "скорочення штату" слід віднести таке:

а) воно є одним із правових наслідків "змін в організації виробництва і праці" (пункт 1 частини першої статті 40 Кодексу);

б) зазначене скорочення проводиться з ініціативи роботодавця та за певною процедурою (Глава III-А Кодексу);

в) його мета полягає в поліпшенні роботи підприємства, установи, організації та забезпеченні його найбільш кваліфікованими кадрами. Це поняття слід відрізняти від суміжного – "скорочення чисельності" працівників, адже, якщо скорочення чисельності може відбуватись й без усунення відповідних посад, то скорочення штату, як правило, зумовлює зменшення чисельності працівників [12, с. 110].

Дострокове звільнення працівників міліції з ОВС України здійснювалося в порядку, передбаченому Положенням, за приписами якого особи рядового, молодшого середнього, старшого і вищого начальницького складу, звільняються зі служби в запас (з постановкою на військовий облік) через скорочення штатів – при відсутності можливості подальшого використання на службі (абзац десятий пункту 8, підпункт "з" пункту 63, підпункт "г" пункту 64).

У разі звільнення працівника ОВС України через скорочення штатів, йому передбачалося надання можливості присвоєння чергового спеціального звання до підполковника міліції включно (за наявності у нього вислуги 20 та більше років

(у пільговому обчисленні); отримання у році звільнення, за їхнім бажанням, чергової відпустки; збереження за ним та членами його сім'ї права на медичне обслуговування та санаторно-курортне лікування в медичних закладах, санаторіях і будинках відпочинку системи МВС України (за наявності у нього вислуги 20 та більше років (у пільговому обчисленні) (пункти 19, 35, 56 Положення).

Крім того, згідно з Постановою Кабінету Міністрів України від 17.07.92 р. № 393 "Про порядок обчислення вислуги років, призначення та виплати пенсій і грошової допомоги особам офіцерського складу, прапорщикам, мічманам, військовослужбовцям надстрокової служби та військової служби за контрактом, особам начальницького і рядового складу органів внутрішніх справ та членам їхніх сімей" особи, звільнені з ОВС України через скорочення штатів, мали право на виплату:

– одноразової грошової допомоги в розмірі 50 відсотків місячного грошового забезпечення за кожний повний календарний рік служби (за наявності вислуги 10 років) (пункт 10);

– щомісячної грошової допомоги у розмірі окладу за військовим (спеціальним) званням протягом року після звільнення (у разі звільнення без права на пенсію) (пункт 11).

Припинення трудового договору є правомірним за одночасної наявності таких умов: 1) передбаченої законодавством підстави припинення трудового договору; 2) дотримання порядку звільнення; 3) юридичного факту припинення трудового договору (наказу чи розпорядження роботодавця, заяви працівника, відповідного документа особи, уповноваженої вимагати розірвання договору) [5].

Д. Величко звертає увагу на те, що важливу роль у процесі звільнення працівника за скороченням чисельності або штату відіграє сам порядок або процедура звільнення, недотримання яких часто є підставою для визнання звільнення незаконним [13, с. 9].

У Законі № 580 визначено, що:

– "працівники міліції, які виявили бажання проходити службу в поліції, за умови відповідності вимогам до поліцейських, визначеним цим Законом, упродовж трьох місяців з дня опублікування цього Закону можуть бути прийняті на службу до поліції шляхом видання наказів про призначення за їх згодою чи проходження конкурсу на посади, що заміщуються поліцейськими, у будь-якому органі (закладі, установі) поліції. Посади, що пропонуються особам, зазначеним у цьому пункті, можуть бути рівнозначними, вищими або нижчими щодо посад, які ці особи обіймали під час проходження служби в міліції" (пункт 9 розділу XI "Прикінцеві та перехідні положення");

– "працівники міліції, які відмовилися від проходження служби в поліції та/або не прийняті на службу до поліції в тримісячний термін з моменту попередження про наступне вивільнення, звільняються зі служби в органах внутрішніх справ через скорочення штатів. Указані в цьому пункті особи можуть бути звільнені зі служби в органах внутрішніх справ до настання зазначеного в цьому пункті терміну на підставах, визначених Положенням про проходження служби рядовим та начальницьким складом органів внутрішніх справ" (пункт 10 розділу XI "Прикінцеві та перехідні положення");

– "перебування працівників міліції на лікарняному чи у відпустці не є перешкодою для їх звільнення зі служби в органах внутрішніх справ відповідно до "Прикінцевих та перехідних положень" цього Закону (пункт 11 розділу XI "Прикінцеві та перехідні положення").

Водночас, у Законі № 580 немає положень про те, що Національна поліція України є правонаступником міліції, що зумовило відсутність в новоствореному

правоохоронному органі обов'язку з працевлаштування вивільнених осіб рядового і начальницького складу ОВС України шляхом надання їм переліку вакансій в його органах та підрозділах.

Відповідно до частини першої статті 104 Цивільного кодексу України юридична особа припиняється в результаті реорганізації (злиття, приєднання, поділу, перетворення) або ліквідації. У разі реорганізації юридичних осіб майно, права та обов'язки переходять до правонаступників.

У Кодексі зазначено, що зміна підпорядкованості підприємства, установи, організації не припиняє дії трудового договору; у разі зміни власника підприємства, а також у разі його реорганізації (злиття, приєднання, поділу, виділення, перетворення) дія трудового договору працівника продовжується. Припинення трудового договору з ініціативи власника або уповноваженого ним органу можливе лише у разі скорочення чисельності або штату працівників (частини третя, четверта статті 36).

Згідно із Законом України "Про загальну структуру і чисельність Міністерства внутрішніх справ України" від 10.01.02 р. № 2925-III зі змінами за рахунок Державного бюджету України утримувалося 152000 працівників ОВС України, з яких чисельність осіб рядового і начальницького складу не може перевищувати величину, визначену із розрахунку 300 осіб на 100000 населення (стаття 2), а за Законом № 580 загальна чисельність поліції, що утримується за рахунок коштів Державного бюджету України, до 1 січня 2018 року не може перевищувати 140 тисяч осіб (частина п'ята статті 13).

Звертаємо увагу на те, що Верховний Суд України сформулював юридичну позицію, згідно з якою ліквідація юридичної особи публічного права має місце у випадку, якщо в розпорядчому акті органу державної влади або органу місцевого самоврядування наведено обґрунтування доцільності відмови держави від виконання завдань та функцій такої відмови. У разі ж покладення виконання завдань і функцій ліквідованого органу на інший орган, мова йде фактично про реорганізацію. Таким чином, встановлена законодавством можливість ліквідації державної установи (організації) з одночасним створенням іншої, яка буде виконувати повноваження (завдання) особи, що ліквідується, не виключає, а включає зобов'язання роботодавця (держави) по працевлаштуванню працівників ліквідованої установи (постанови від 04.03.14 р. у справі № 21-8а14; від 27.05.14 р. у справі № 21-108а14; від 28.10.14 р. у справі № 21-484а14).

Зазначеної позиції дотримується і Верховний Суд при розгляді спорів щодо незаконного звільнення з органів державної влади (постанови від 23.04.20 р. у справі № 822/880/16; від 30.04.20 р. у справі № 821/813/16).

Крім того, Верховний Суд вказав, що надання згоди працівником міліції на призначення на посаду в органі поліції, неможливе без його обізнаності із переліком усіх наявних вакантних посад в даному органі. Тобто, наданню згоди повинна була передувати пропозиція щодо призначення на відповідну посаду, а саме – ініціатива керівництва, оскільки згода особи, по своїй суті, є відповіддю на цю ініціативу, а наслідком такої згоди є призначення особи на посаду у відповідності до узгодженої пропозиції. Отже, особа, попереджена про звільнення внаслідок скорочення штатів, у цьому випадку не має можливості виявити ініціативу, і своє волевиявлення здійснює шляхом згоди на ініціативу керівництва. Така ініціатива є обов'язковою, оскільки без неї не може бути встановлено наявність чи відсутність можливості подальшого використання особи на службі відповідно до підпункту "г" пункту 64 Положення. Лише у разі, якщо особа відмовилася від усіх пропозицій щодо зайняття посад і не подала заяви (рапорту) про участь у конкурсі на зайняття посад, виникають підстави для

застосування пункту розділу XI “Прикінцеві та перехідні положення” Закону № 580 і звільнення особи за скороченням штатів (постанова від 14.11.19 р. у справі № 16/4671/15).

Порівняльний аналіз законодавства свідчить, що Національна поліція України виконує завдання, які раніше виконувала міліція, зокрема: протидія злочинності; забезпечення публічної безпеки і порядку; охорона прав і свобод людини, а також інтересів суспільства і держави. Оскільки органи та підрозділи Національної поліції України створені на базі раніше існуючих органів та підрозділів системи МВС України з майже однаковою чисельністю особового складу, а поліцейські виконують функції, які раніше виконували працівники міліції, то існують достатні підстави стверджувати, що Законом № 580 міліція була реорганізована в Національну поліцію України, яка є її фактичним правонаступником.

Україну проголошено правовою державою, в якій визнається і діє принцип верховенства права (стаття 1, частина перша статті 8 Основного Закону України).

За юридичною позицією Конституційного Суду України складовими принципу верховенства права є, зокрема, правова передбачуваність та правова визначеність, які необхідні для того, щоб учасники відповідних правовідносин мали можливість завбачати наслідки своїх дій і бути впевненими у своїх законних очікуваннях, що набуте ними на підставі чинного законодавства право, його зміст та обсяг буде ними реалізовано (абзац третій пункту 4 мотивувальної частини Рішення Конституційного Суду України від 11.10.05 р. № 8-рп/2005).

Крім того, Конституційний Суд України вказав, що у контексті статті 8 Конституції України юридична визначеність забезпечує адаптацію суб’єкта правозастосування до нормативних умов правової дійсності та його впевненість у своєму правовому становищі, а також захист від свавільного втручання з боку держави. Кожна особа влаштовує своє життя з усвідомленням того, що правове регулювання вимагає стабільності й органи державної влади не можуть свавільно вносити зміни, які порушують засадничі принципи права. Отже, очікування індивіда у зв’язку зі зміною законодавчого регулювання є правомірними, якщо вони є розумними та існує можливість заподіяння шкоди від порушення таких очікувань (абзац четвертий підпункту 4.1 пункту 4, абзац шостий підпункту 4.2 пункту 4 мотивувальної частини Рішення від 20.06.19 р. № 6-р/2019).

Враховуючи наведене, є очевидним, що перебуваючи на службі особи рядового та начальницького складу ОВС України мали легітимні очікування на довгострокову реалізацію свого права на працю у правоохоронному органі, а також на стабільність та захищеність свого юридичного та соціально-економічного становища.

На наше переконання, звільнивши працівників міліції через скорочення штатів без надання конкретних пропозицій щодо подальшого працевлаштування до Національної поліції України, держава фактично усунулася від виконання конституційного обов’язку щодо утвердження та захисту прав і свобод цих осіб, в частині здійснення ними гарантованого Основним Законом України права на працю та на захист від незаконного звільнення.

Висновки.

Проведене дослідження дозволяє зробити висновок про те, що у процесі виконання вимог пунктів 8 – 11 розділу XI “Прикінцеві та перехідні положення” Закону № 580 щодо осіб рядового та начальницького складу ОВС України мали бути здійснені заходи щодо їх працевлаштування до органів та підрозділів Національної поліції України.

Працівникам міліції в обов'язковому порядку мали бути доведені переліки вакансій в органах та підрозділах Національної поліції України, на які вони можуть претендувати з огляду на їх спеціальність, кваліфікацію, досвід роботи, рівень фізичної підготовки, стан здоров'я, спеціальне звання, вислугу років та займану посаду в ОВС України на момент набрання чинності Законом № 580.

Лише після ознайомлення із цим переліком особа могла сформувати власну волю щодо подальшої реалізації її конституційного права на працю, ініціювавши її прийняття на службу до органів та підрозділів Національної поліції України або звільнення з ОВС України у зв'язку з скороченням штату чи з інших підстав, визначених у Положенні.

З огляду на наведене, є підстави стверджувати про недотримання державою конституційного принципу верховенства права при реформуванні ОВС України, а також про порушення нею трудових прав окремих осіб рядового і начальницького складу ОВС України при їх звільненні зі служби через скорочення штатів. Тому вбачається наявність перспектив у розгляді судових справ щодо захисту та поновлення трудових прав зазначених осіб.

Використана література

1. Венедиктов В.С. Трудовое право Украины. Харків: Консум, 2004. 302 с.

2. Глазько С.М. Правове регулювання припинення трудового договору: теоретичний аспект: автореф. дис. …канд. юрид. наук: 12.00.05. Харків, 2005. 19 с.

3. Шишлюк В.Р. Припинення трудового договору за законодавством України і Польщі: автореф. дис. …канд. юрид. наук: 12.00.05. Одеса, 2017. 20 с.

4. Бабенко Е.В. Доктрина захисту трудових прав працівників при припиненні трудових правовідносин: дис. …д-ра. юрид. наук: 12.00.05. Київ, 2019. 423 с.

5. Поняття та класифікація підстав припинення трудового договору. URL: https://pidru4niki.com/1329051143363/pravo/pripinennya_trudovogo_dogovoru (дата звернення: 25.12.2020).

6. Яценко Т.П. Деякі питання щодо забезпечення механізму захисту службово-трудових прав працівників ОВС України. *Наше право*. 2009. № 1. Ч. 2. С. 53-56.

7. Рішення Суду справедливості Європейського Союзу від 4 грудня 1974 року у справі "Yvonne Van Duyn v. Home Office". URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61974CJ0041&from=EN (дата звернення: 25.12.2020).

8. Огієнко І.В. Особливості припинення службово-трудових правовідносин працівників органів внутрішніх справ за загальними підставами, визначеними Кодексом законів про працю України. *Форум права*. 2008. № 2. С. 376-380.

9. Кікінчук В.Ю. Процедура звільнення зі служби в органах внутрішніх справ. *Право і Безпека*. 2010. № 3. С. 197-202.

10. Шульженко І.В. Вплив специфічних умов праці в органах внутрішніх справ на диференціацію правового регулювання припинення трудових правовідносин з працівниками ОВС України. *Підприємництво, господарство і право*. 2010. № 7. С. 125-128. URL: http://elibrary.donnuet.edu.ua/966/1/Shulzhenko_2_Vpliv%20spec.%20umov%20praci.pdf (дата звернення: 25.12.2020).

11. Іншин М.І. Управління та правове регулювання вивільнення працівників органів внутрішніх справ: автореф. дис. …канд. юрид. наук: 12.00.07. Харків, 1998. 18 с.

12. Лавріненко О.В. Звільнення працівників ОВС зі служби за скороченням штатів: теоретико-правовий аналіз чинного законодавства та напрями його вдосконалення. *Право і Безпека*. 2006. Т. 5. № 4. С. 108-115.

13. ВеличкоД.М. Правовий аналіз звільнення працівників за скороченням штату: історичні аспекти і проблемні питання. *Право та державне управління*. 2013. № 4 (13). С. 4-10.

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

УДК 340.15 (477)

МАНЬГОРА Т.В., *кандидат юридичних наук,* доцент кафедри права
Вінницького Національного аграрного університету.
ORCID: https://orcid.org/0000-0002-7010-8768.

ДОСЛІДЖЕННЯ ІСТОРІЇ КОДИФІКАЦІЇ УКРАЇНСЬКОГО ПРАВА А. ЯКОВЛІВИМ

Анотація. *Розглянуто дослідження історії кодифікації українського права, зокрема "Українського кодексу 1743 року "Права, по которым судится малороссийский народ" А. Яковлівим.*

Ключові слова: *"Права, по которым судится малороссийский народ", А. Яковлів, кодифікація українського права.*

Summary. *Considered study the history of Ukrainian law codification, including "Ukrainian Code 1743 "The Laws that the Nation of Little Russia is Judged" A. Yakovliv.*

Keywords: *"The Laws that the Nation of Little Russia is Judged" (1743), A. Yakovliv, Ukrainian law codification.*

Аннотация. *Рассмотрены исследования истории кодификации украинского права, в частности "Украинский кодекса 1743 "Права, по которым судится малороссийский народ" А. Яковлива.*

Ключевые слова: *"Права, по которым судится малороссийский народ", А. Яковлив, кодификация украинского права.*

Постановка проблеми. Андрій Іванович Яковлів – відомий український політичний діяч, учений-правознавець, історик українського права, член Української Центральної Ради (УЦР), директор канцелярії УНР, дипломат, ректор Українського Вільного Університету (УВУ), фундатор багатьох еміграційних українських осередків, автор численних праць з історії держави і права, звичаєвого, конституційного, цивільного, торгового, процесуального, порівняльного, морського, річкового права. А. Яковлів займався дослідженням історії кодифікації українського права, зокрема "Українського кодексу 1743 року "Права, по которым судится малороссийский народ". Його дослідження з даної проблеми мають важливе значення для розвитку юридичної науки і потребують вивчення в умовах реформування та створення нових кодифікаційних актів.

Результати аналізу наукових публікацій. Дослідженню кодифікації українського права у працях А. Яковліва присвячені праці К. Вислобокова, Т. Гошко, А. Петрика.

Метою статті є оцінка аналізу кодексу "Права, за якими судиться малоросійський народ" (1743) А. Яковлівим.

Виклад основного матеріалу. В 1939 р. вийшла друком стаття А. Яковліва "До історії кодифікації українського права XVIII в.", в якій автор торкається причин, що вплинули на те, що Кодекс 1743 р. не дістав офіційної санкції. В 1940 р. А. Яковлів виступив в Українському Історико-Філологічному Товаристві в Празі з доповіддю "Чому кодекс "Права по которим судится малоросійський народъ" не був затверджений". Пізніше в 1942 р. німецькою мовою вийшла праця "Das Deutsche Recht in der Ukrainian" [6], яка містила в собі детальний огляд джерел магдебурзького права в

Україні, які в більшості були також і джерелами для Кодексу 1743 р. Крім того, цілий розділ VII присвячено історії Кодексу, його джерелам, викладові його змісту, впливам німецького права та оцінці Кодексу, як пам'ятника українського права XVIII ст. [6].

У 1944 р. було опубліковано статтю "Нові джерела кодексу ""рава по которым судится малороссийский народ" [4], в якій дослідник подає виклад про джерела, які Кодифікаційна Комісія використовувала додатково до основних джерел, зазначених в царських указах. А. Яковлів характеризує такі джерела: "Хелмське право" в польській редакції П. Кушевича, "Енхірідіон" І. Церазина, "Оборона сирот і вдов" та "Ужинання дібр, жоні від мужа тестаментом записаних" Б. Ґроїцького, повний переклад на латинську мову саксонського Кодексу "Sachsenspiegel" та магдебурзького "Jus Municipale magdeburgensis" та праці німецького криміналіста Бенедикта Карпцова "Processus juris", "Definitiones Forenses", "Practica rerum criminalicum"" [5, с. 14]. Стосовно "Хелмінського права", А. Яковлів виправив помилку Комісії щодо авторства використовуваного нею списку, довівши, що належить він перу не П. Щербича, а польського правника П. Кушевича [2, с. 368].

А. Яковлів спирався на видані О. Кістяківським тексти та літературу, не маючи можливості в умовах еміграції залучити широке коло архівних матеріалів. Дослідник також використав доступні йому польські, латинські і німецькі джерела XVI–XVII ст., що були разом з Литовським статутом покладені в основу Кодексу [1, с. 10-11].

Над проблемою А. Яковлів продовжував працювати і в повоєнний час, намагався, попри всілякі перешкоди і негаразди, видати монографію. В 1949 р. окремим томом Записок НТШ "Український кодекс 1743 року "Права, по которым судится малороссійскій народъ" таки побачив світ.

Що ж до роботи А. Яковліва над даною проблематикою, то Т. Гошко відмітила її етапність. Першим кроком стала постановка проблеми, чому проект кодексу "Прав, по которым судится малороссийский народ" не був офіційно затверджений [2, с. 365]. В першому розділі А. Яковлів дає короткий огляд літератури, аналізує праці О. Кістяківського, І. Теличенка, Є. Слабченка, М. Василенка, О. Малиновського, М. Товстоліса, М. Чубатого, з даної проблеми.

А. Яковлів вказує причини, чому Кодекс 1743 р. не дістав офіційної санкції. На його думку, це сталося з двох причин: через навмисне недбайливе відношення російського уряду та через опозицію певного кола українських патріотів, що працювали в Комісії, а пізніше охопила українські правлячі кола, проти зміни Литовського Статуту, як "фундаментального права", "новим правом", де в чому відмінним, а також, через недовіри до царського уряду та до його наказу запровадити в Україні нові закони [5, с. 14].

Після закінчення кодексу силами українських правників ніхто з українського боку не рекламував його затвердження, а коли кодекс було повернуто Сенатом, для перегляду, то старшинська рада відмовилась його переглядати, та просила залишити непорушним по давньому Литовський Статут і правові книги магдебурзького права. Таким чином, кодекс не здобув затвердження не тому, що про нього "навмисно забув Сенат", а тому, що його відкинув гетьманський уряд за погодженням зі Старшинською Радою з мотивів національно-політичного характеру. Внаслідок цього Статут і магдебурзьке право залишалось як основне джерело права й після скасування автономії України й системи статутових судів. На початку XIX ст. Литовський статут став єдиним джерелом права, замінивши собою правні книги Магдебурзького права в магістратських судах, і був чинним в Україні включно до 1842 р., коли був замінений російським Зводом Законів. Причому, деякі норми Литовського Статуту, що стосувалися родинного й спадкового права, були реципровані X-м томом російського Зводу Законів (Цивільний

кодекс), як партикулярне право для населення Чернігівської та Полтавської губерній (приблизно територія колишньої Гетьманщини) і були діючим законом аж до введення в Україні радянського Цивільного кодексу [3, с. 77-78].

В своїй монографії "Український кодекс 1743 року "Права, по которым судится малороссийский народ" А. Яковлів здійснює аналіз досліджень з даної проблеми, встановлює обставини створення кодексу та розглядає його джерела, також аналізує його зміст та подає зразки тексту договору (54 додатки). Виклад змісту Кодексу вчений розглядає за такою системою: 1) ввідний закон до Кодексу, 2) державне право, 3) адміністративне право, 4) цивільне право, 5) карне право, 6) судовий устрій та процесуальне право [5, с. 111]. Присвячує свою працю творцям Кодексу – 49 членам Кодифікаційної Комісії, видатним правникам XVIII ст. [5, с. 5], імена яких подає в окремому додатку [5, с. 182].

Основними джерелами Кодексу 1743 р., на думку А. Яковліва були: Литовський статут, "Саксонське зерцало", магдебурзьке право.

"Статут великого княжества Литовського", або коротко – "Литовський Статут" – це кодекс законів, що були чинними в Литовській потім Литовсько-Польській державі. Вперше був складений та набрав законної сили 1529 р., так званий "Старий Статут", що був чинний до 1566 р., коли був ухвалений новий, другий Статут, що називався "Волинським", бо був призначений, між іншим, для вжитку на Волині. Третій Статут затверджено 1587 р. і він набрав обов'язкової сили 1588 р. на території Литовської держави, в тому числі і на українських землях, що після Люблінської унії 1569 р. були інкорпоровані Польщею. А. Яковлів підкреслює, що – "усі три редакції Статуту були написані на тодішній офіційній мові "руській", яка найближче стояла до тогочасної української літературної мови" [5, с. 36]. На думку професора українського права, виданням Литовського Статуту завершено попередній процес уніфікації різних правових систем давніх руських земель з національним литовським правом. Замість різноманітного місцевого права: Волинського, Київського тощо, вперше утворено загальне, "посполите" право для всіх частин Литовської держави. В цьому об'єднаному праві значну частину займали давні українські звичаєві норми, стверджені земськими привілеями, що ще в XII ст. були зафіксовані в "Руській Правді", та процесуальні звичаї українських народних (копних) судів [5, с. 37]. Тому, підкреслює А. Яковлів, Литовський Статут був такий близький до правосвідомості українського народу й був прийнятий в Україні, як "своє власне національне право" [5, с. 37].

Оцінюючи Литовський Статут, як основне джерело Кодексу "Права, по которым судится малороссийский народ", історик права звертає увагу на те, що на другу та третю редакції значний вплив мало іноземне право. В першу чергу, відмічає вплив польського права, особливо в редакції 1566 р., завдяки тому, що 1564 р. в Литві була введена польська система шляхетських судів (земських, гродських та підкоморських). Певний вплив польське право мало на норми карного права Статуту. В останній редакції Статуту простежуються впливи римського права, які були не безпосередні, а опосередковані через німецьке право та його глоси [5, с. 39].

Що ж стосується німецького права, то воно теж мало вплив на Статут, як безпосередньо так і опосередковано в цивільному праві і особливо – в карному праві. Запозиченню німецького права сприяли особи, що були покликані до комісії зі складання Статуту 1588 р., серед яких були знавці канонічного й міського магдебурзького права, як, наприклад, голова комісії – віленський єпископ Валеріян Протасевич, та видатний знавець магдебурзького права, королівський секретар і віленський війт, доктор обох прав Августин Ротунд-Мелетський [5, с. 39]. На думку

А. Яковліва, запозичення кодифікаторами Литовського Статуту норм німецького права, сприяло його впливу на норми Кодексу 1743 р. [5, с. 39].

Джерела німецького права, що їх використала Комісія при складанні Кодексу, дослідник поділяє на три групи: до першої належать джерела, що були названі в царських указах, як "права Магдебургскіе и Саксонскіе", які Комісія назвала "Зерцалом Саксонским", "…съ приложенными при немъ особливо артикулами правъ: Магдебургскаго или гражданскаго (то б то городського) и Хельминскаго" та "Порядок". До другої групи належать джерела, які Комісія використовувала й цитувала під текстом, але про них не згадала в своїх звітах та в передмові до Кодексу. До третьої групи належать джерела, які Комісія використовувала, але не подала з них цитат [5, с. 40].

А. Яковлів визначає, що джерела німецького права здійснювали вплив на Кодекс в трьох напрямках:

а) запозичення з німецького права надали нормам Кодексу абстрактного характеру, що цілком відповідало прагненням самої Кодифікаційної Комісії;

б) джерела німецького права сприяли збільшенню й поширенню законодавчого матеріалу, що містився в Литовському Статуті, але був уже недостатній для регулювання правового життя в Україні XVIII ст.; особливо це поширення помітне на нормах Кодексу, що стосується цивільного та, почасти, й карного права;

в) також доводиться відзначити негативний вплив німецького права на Кодекс, а саме – карного кодексу Карла V. На підставі цього джерела Комісія значно розширила матеріальну частину карного права, було збільшено кількість видів злочинів і посилено покарання за злочини, також було запозичено покарання, які не відповідали вже правосвідомості українського громадянства та внесено в Кодекс спосіб допиту "під муками" [5, с. 110].

Крім Литовського Статуту й німецького права, Кодифікаційна Комісія використовувала також і українські джерела.

До цієї групи джерел в першу чергу потрібно віднести українське звичаєве право. Комісія визнала за звичаєвим правом силу закону неписаного, яким суди мають керуватися при вирішені спорів у тих випадках, коли в писаному законі відсутні відповідні норми [5, с. 50].

На думку А. Яковліва, звичаєве право відігравало також немалу й своєрідну роль при складанні Кодексу. Як самостійне джерело, звичаєве право було використане Комісією, в переважній більшості, при складанні трьох глав Кодексу, але його роль і вплив позначилися на цілому Кодексі. Як джерело, українське звичаєве право було використане Комісією у формі неписаного народного права, або у формі постанов та розпоряджень органів автономної влади, або ж, у формі звичаїв та практики існуючих того часу адміністративних і судових установ української держави. Але основне значення українського звичаєвого права полягало в тому, зазначає дослідник Кодексу, що воно було використане кодифікаторами для зміни, пояснення й доповнення матеріалу, запозиченого з чужих джерел, а головне – для пристосування цього матеріалу до місцевих умов життя й побуту. Українське звичаєве право було для Комісії засобом, який вона використала для українізації запозичених іноземних законів, воно створило підґрунтя, на якому Комісія збудувала свою "Всезбірку прав, по яким судиться український народ" [5, с. 110].

Крім звичаєвого права, Комісія використовувала, як джерела до Кодексу:

а) гетьманське законодавство: гетьманські універсали, інструкції, розпорядження;

б) договори українських гетьманів з московськими царями, починаючи з договору Б. Хмельницького з 1654 р. [5, с. 51].

Нарешті, Комісія іноді користувалась і джерелами російського імперського законодавства. Так, на деяких нормах Кодексу помітно впливи: 1) російського законодавства доби Петра І (“Регламентъ Воинскый”, “Регламентъ Духовный”, “Судъ по формъ”); 2) законів та указів за цариці Анни Іванівни. Тільки ж цитат з цих джерел Комісія не подавала під текстом Кодексу [5, с. 51].

Отже, основним завданням Комісії, на думку А. Яковліва, було звести в один Кодекс: Литовський Статут, Саксонське земське (landrecht) та Магдебурзьке міське (Weichbildrecht) право тобто, погодити між собою три, але коли взяти до уваги певну спорідненість німецьких кодексів, то принаймні дві правові системи, що відрізнялися між собою з погляду часу, місця й обставин походження [5, с. 52].

Основними принципами, яких дотримувалася Комісія при кодифікації були: а) зміна системи Литовського Статуту; б) об’єднання законодавчого матеріалу за його змістом та внутрішнім юридичним зв’язком; в) включення в Кодекс нових, утворених Комісією норм на зміну і доповнення матеріалу з старих правних книг [5, с. 57].

Зміна системи Литовського Статуту пов’язана з тим, що зібраний новий матеріал не можна було вмістити в 14 розділах Статуту. Кодекс 1743 р. складався з 30 глав. В Литовському Статуті на першому місці стояли три розділи, що були присвячені державному праву: особі монарха, його прерогативам та охороні від порушення (I), обороні держави та обов’язкам військової служби (II), нарешті, правам та привілеям шляхетського стану (III). Кодифікаційна Комісія змінила цей порядок в той спосіб, що першу главу присвятила вступним постановам про межі чинності Кодексу з погляду території й людності [5, с. 57].

Андрій Іванович відзначає, що Комісія систематизувала зібраний матеріал на підставі вимог цивільного права, додержуючись пандектної системи: в главі X було вміщено норми шлюбного права, в главі XI – норми про опіку, в главах XIV–XVI вміщено норми облігаційного права, в главах XVII –XIX – норми речового права, нарешті, в окрему главу – XXVIII – виділили норми торговельного (власне ярмаркового) права [5, с. 59].

Також позитивні зміни відбулися в карному праві, вказує А. Яковлів, збільшено у Кодексі кількість норм, які містилися в 6 окремих главах, для порівняння – в Статуті 4 розділи. Оцінюючи систему викладу карного права в Кодексі, дослідник визначає, що виклад більш послідовний і детальний, ніж в Статуті, виклад норм точніший і ясніший [5, с. 59].

Здійснюючи загальний висновок про систему Кодексу, в порівнянні з системою в Литовському Статуті, А. Яковлів підсумовує, що “вона була більш модерною та задовольняла основним вимогам тодішньої науки і права, її можна було б визнати за досконалу, якби вона була послідовно проведена” [5, с. 59].

“Український кодекс 1743 року “Права, по которым судится малороссийский народ”, професор вважає найвидатнішою пам’яткою діючого права [5, с. 230]. Оцінюючи Кодекс А. Яковлів зазначає: “Повнотою і якістю змісту, способом викладу норм закону й абстрактних правних дефініцій та досконалою юридичною термінологією Кодекс далеко перевищував існуючі тоді підручні правні книги. Тому він значно був поширений в Україні, про що свідчить велика кількість списків, що дійшли до нас; по ньому вивчали українське право й використовували його як авторитетний та досконалий підручник-коментар до Литовського Статуту й Магдебурзького права. Для історії українського права й правних ідей Кодекс “Права по которым судится малороссийский народ” був і залишається надзвичайно цінним пам’ятником, який свідчить про те, що в Україні правні концепції на початку XVIII в. досягли високого ступеня розвитку, а

тодішні українські правники стояли нарівні з найвидатнішими європейськими правниками" [5, с. 79].

Висновки.

Отже, монографія А. Яковліва "Український кодекс 1743 року "Права, по которым судится малороссийский народ", має важливе значення в українській історико-правовій науці. Він продовжив працю попередніх дослідників Кодекса 1743 р., доповнив та поглибив знання про цей кодифікований акт. Праця А. Яковліва є зразком всебічного історико-правового дослідження.

Кодифікація окремих галузей українського права потребує більш детального вивчення попереднього правотворчого досвіду та історико-правових досліджень кодифікації українського права А. Яковлівим.

Використана література

1. Вислобоков К.А. "Права, за якими судиться малоросійський народ" (1743): джерелознавчий та кодикологічний аналіз: автореф. дис. …канд. іст. наук: 07.00.06 / Державний комітет архівів України, Український науково-дослідний інститут архівної справи та документознавства. Київ, 2004. 22 с.

2. Гошко Т. До історіографії німецького права в Україні. Україна в Центрально-Східній Європі / ред. кол.: В. Смолій (відп. ред.), В. Станіславський (заст. відп. ред.), Т. Чухліб (заст. відп. ред.), В. Кононенко (відп. секр.), В. Матях, Б. Черкас. НАН України. – (Інститут історії України; Український національний комітет з вивчення країн Центральної і Південно-Східної Європи). Вип. 12 – 13. Київ: Інститут історії України, 2013. С. 347-377.

3. Яковлів А. До історії кодифікації українського права XVIII в. Праці історико-філологічного товариства в Празі. Прага, 1939. Т. 2. С. 70-79.

4. Яковлів А. Нові джерела кодексу "Права по которым судится малороссийский народ". Праці Українського Історично-Філологічного Товариства в Празі. Прага, 1944. Т. 5. С. 71-77.

5. Яковлів А. Український кодекс 1743 року: "Права по которымъ судится малороссійский народ": його історія, джерела та систематичний виклад змісту. Записки Наукового товариства ім. Т.Г. Шевченка. Праці Історично-філософічної секції. Мюнхен: Заграва, 1949. 211 с.

6. Yakovliv A. Das Deutsche Recht in der Ukrainian. Munchen, 1942. 232 s.

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

До відома читачів

Утворення Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"

КАБІНЕТ МІНІСТРІВ УКРАЇНИ
РОЗПОРЯДЖЕННЯ
від 3 лютого 2021 р. № 85-р
Київ

Про утворення Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"

1. Погодитися з пропозицією Національної академії правових наук щодо утворення Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України", реорганізувавши шляхом перетворення Науково-дослідний інститут інформатики і права Національної академії правових наук.

2. Рекомендувати Національній академії правових наук у місячний строк затвердити статут Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України" та здійснити організаційні заходи щодо її матеріально-технічного і кадрового забезпечення.

3. Взяти до відома, що утворення Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України" здійснюється в межах загальної чисельності Науково-дослідного інституту інформатики і права Національної академії правових наук, що реорганізується, та видатків, передбачених Національній академії правових наук у державному бюджеті на відповідний рік.

Прем'єр-міністр України **Д. ШМИГАЛЬ**
Інд. 29

URL: //www.ippi.org.ua

* * * * * * * * * *

Щодо представника Національної академії правових наук України при Апараті Верховної Ради України

Відповідно до законів України "Про наукову і науково-технічну діяльність", "Про наукову і науково-технічну експертизу", "Про регламент Верховної Ради України", Постанови Верховної Ради України "Про заходи з реалізації рекомендацій щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України", а також Меморандуму про взаємодію Апарату Верховної Ради України і Національної академії правових наук України запроваджено (обрано, на громадських засадах) представника Національної академії правових наук України при Апараті Верховної Ради України, положення про якого за погодженням з Апаратом Верховної Ради України затверджено постановою Бюро президії Національної академії правових наук України від 29.12.2020 р. № 176/5.

Представник Національної академії правових наук України при Апараті Верховної Ради України – член Національної академії правових наук України, який забезпечує координацію наукових досліджень та організацію взаємодії наукових установ НАПрН України з підрозділами Апарату та комітетами Верховної Ради України з питань законотворчої діяльності.

Наукове і науково-методичне забезпечення діяльності Представника НАПрН України покладається на Апарат Президії та наукові установи НАПрН України, а науково-організаційне забезпечення – на НДІ інформатики і права НАПрН України (*від ред.* – Державну наукову установу "Інститут інформації, безпеки і права Національної академії правових наук України").

URL: //www.ippi.org.ua

* * * * * * * * * * *

НАУКОВІ ДОСЛІДЖЕННЯ НАУКОВО-ДОСЛІДНОГО ІНСТИТУТУ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ у 2020 р.

На виконання показників паспорта бюджетної програми 6581040 вченими НДІІП НАПрН України у 2020 р. виконувалися такі НДР:

- “Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері”: затверджено Постановою Президії НАПрУкраїни від 03.07.2017 р. № 103/4; реєстр УкрІНТЕІ від 20.12.2017 р. № 0117U007745;
- “Науково-методичне, правове та інформаційне забезпечення формування національної інтегрованої системи нормативно-правових актів в умовах децентралізації в Україні”: затверджено Постановою Президії НАПрУкраїни від 22.06.2015 р. № 91/5; реєстр УкрІНТЕІ від 01.01.2016 р. № 0115U004522;
- “Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні”: затверджено Постановою Президії НАПрУкраїни від 21.06.2016 р. № 97/7; реєстр УкрІНТЕІ від 27.10.2016 р. № 0116U007745;
- “Правове забезпечення застосування цифрових технологій в умовах трансформації суспільства”: затверджено Постановою Президії НАПрУкраїни від 15.06.2018 р. № 106/7; реєстр УкрІНТЕІ від 04.12.2019 р. № 0119U003166;
- “Теоретичні та інформаційно-правові засади забезпечення національної безпеки в умовах євроінтеграції України”: затверджено Постановою Президії НАПрУкраїни від 03.07.2017 р. № 103/4; реєстр УкрІНТЕІ від 20.12.2017 р. № 0117U007744.

В рамках досліджень опубліковано: 5 монографій, 1 словник, 4 наукових фахових журнали, 5 збірників наукових праць, 51 наукова стаття, у т.ч. 8 статей в наукових журналах, що індексуються в Scopus та Web of Science, 12 інформаційно-аналітичних дайджестів. Загалом, у звітному періоді співробітниками НДІІП НАПрН України було опубліковано 342 наукові роботи обсягом 11308 с.

НАУКОВІ ВИДАННЯ

Захист прав, приватності та безпеки людини в інформаційну епоху: монографія / авт. кол.: В.Г. Пилипчук, В.М. Брижко, І.М. Доронін, В.С. Батиргареєва, П.П. Богуцький, О.О. Золотар, О.Г. Радзієвська, А.В. Тарасюк, Т.Ю. Ткачук ; за заг. ред. академіка НАПрН України В.Г. Пилипчука. Київ-Одеса: “Фенікс”, 2020. 260 с. – ISBN 978-966-928-618-5.

Монографія присвячена актуальним теоретико-правовим та прикладним проблемам становлення інформаційної епохи, захисту інформаційних прав людини та безпеки її персональних даних відповідно до сучасних міжнародно-правових стандартів і стандартів Європейського Союзу, особливостей захисту інформаційної безпеки людини у зв’язку з цифровою трансформацією та введенням карантинно-обмежувальних заходів.

У сучасних техніко-технологічних та соціальних умовах життя людини та діяльності держави розвиток новітніх інформаційних технологій, штучного інтелекту, поширення інформаційно-комунікаційних систем і мереж сприяють новим поглядам на визначення подальших шляхів до ідеалів захисту прав людини, за умов збалансованості відносин (людина-держава), які дедалі більше визначають потреби у нормативно-правовому врегулюванні на принципово нових засадах, що може суттєво відрізнятися від нормативного упорядкування відносин, сформованих за часів аграрного та індустріального суспільства у XIX – XX століттях.

В роботі здійснено комплексний розгляд підходів та пропозиції до вирішення питань інформаційної приватності людини та безпеки персональних даних, проблем правового захисту конфіденційної інформації в контексті захисту приватності життя людини та публічності інформаційних (зокрема цифрових) комунікацій.

Видання розраховане на фахівців, експертів і вчених, науково-педагогічних працівників, аспірантів, докторантів і студентів вищих навчальних закладів, представників державних органів, а також державних і недержавних закладів, установ та організацій.

* * * * * * * * *

Консолідована система нормативно-правової інформації в умовах децентралізації державної влади в Україні – невід'ємна складова демократії: монографія / І.Ф. Корж, Д.В. Ланде, С.В. Лихоступ ; за заг. ред. І.Ф. Коржа. Київ: Видавничий дім "АртЕк", 2021. 417 с.

Монографія присвячена вирішенню проблем доступу громадян України до нормативно-правової інформації, реформуванню суспільних відносин у процесі децентралізації, як на центральному, так і муніципальному рівнях, дослідженню стану організаційно-правових основ осучаснення місцевого самоврядування, зокрема, щодо взаємодії публічних органів з громадянським суспільством, трансформації суспільних відносин у процесі утворення об'єднаних територіальних громад тощо.

В монографії, як основу інформаційного суспільства, розкрито механізми комунікації публічної влади з суспільством, обґрунтовано важливість вільного доступу громадян до правової інформації, включаючи публічну інформацію у формі відкритих даних, проаналізовано стан та напрями цифрової трансформації (цифровізації) України.

В роботі наведено та проаналізовано різні види інформаційних технологій інформування з правових питань, напрями консолідації нормативно-правової інформації в Україні. Робиться загальний висновок про те, що існує важлива потреба у створенні національної консолідованої системи нормативно-правових актів на базі веб-порталу Верховної Ради України.

* * * * * * * * *

Національна безпека: світоглядні та теоретико-методологічні засади: монографія ; за заг. ред. О.П. Дзьобаня. Харків: "Право", 2021. 776 с. ISBN 978-966-998-088-5.

Монографію присвячено комплексному міждисциплінарному дослідженню феномену національної безпеки в культурно-історичному, онтологічному, аксіологічному, структурно-функціональному та міжнародному вимірах. У виданні на системній основі поєднані різнорівневі методологічні підходи до дослідження основних аспектів національної безпеки. Сутність ключових категорій безпекової сфери досліджується крізь призму інтерсуб'єктивної філософської парадигми. Аналізуються стійкість і лабільність соціальної системи через дію базових констант і варіативних величин, розкривається філософська концепція місця й ролі системи забезпечення національної безпеки в сучасних умовах.

Монографія розрахована на науковців, викладачів, здобувачів наукових ступенів, студентів, державних службовців, усіх, хто цікавиться проблемами національної безпеки.

* * * * * * * * *

Національна безпека України в інформаційну епоху: правові аспекти: монографія / І.М. Доронін. Київ: Видавничий дім "АртЕк", 2020. 350 с.

У роботі здійснено дослідження проблематики правового виміру забезпечення національної безпеки України в сучасному світі. Розглянуто загальну еволюцію концепту "національна безпека" у вітчизняній правовій науці з акцентуванням уваги на його сприйнятті в інформаційну епоху. Досліджено передумови виникнення, процеси розвитку і трансформації національної безпеки України, становлення та систематизацію правових засад її забезпечення. Детально проаналізовано вплив фактору триваючої агресії проти нашої держави і еволюції інформаційного суспільства на стан забезпечення національної безпеки і трансформації відповідної системи її забезпечення. Ґрунтовно досліджено складний характер суспільних змін в інформаційну епоху, що зумовлюють зміни у парадигмі правового регулювання. На підставі аналізу висловлених у вітчизняній літературі точок зору щодо розподілу права на окремі галузі та їхнього взаємного зв'язку і систематизації, запропоновано розглядати "право національної безпеки", як галузь права, в умовах трансформації традиційних підходів до його систематизації.

Монографія стане у пригоді науковцям, викладачам права, а також юристам-практикам, працівникам державних органів та всім, хто цікавиться проблемами сучасної теорії права і забезпечення національної безпеки України.

* * * * * * * * *

Інформаційна війна: соціально-онтологічний та мілітарний аспекти: монографія / Р.В. Гула, О.П. Дзьобань, І.Г. Передерій, О.О. Павліченко, Г.О. Філь. Київ: "Каравела", 2020. 288 с.

Монографія розкриває особливості інформаційного протиборства у постмодерному суспільстві. Проаналізовано сучасні тенденції трансформації концепцій інформаційної війни у воєнній теорії. Розкрито особливості сучасних кіберзагроз. Висвітлені основні тенденції у військовому будівництві кібервійськ провідних держав світу. Запропоновано низку практичних рекомендацій для удосконалення системи національної безпеки в умовах інтенсифікації гібридних війн транснаціонального характеру.

* * * * * * * * *

Концептуальні засади права національної безпеки України: монографія / П.П. Богуцький. Київ-Одеса: "Фенікс", 2020. 376 с.

* * * * * * * * *

Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / А.В. Тарасюк. Київ: Видавничий дім "АртЕк", 2020. 415 с.

* * * * * * * * *

Електронні довірчі послуги: правовий аспект транскордонного використання: монографія / О.В. Костенко; за заг. ред. О.А. Баранова. Київ: Видавничий дім "АртЕк", 2020. 215 с.

* * * * * * * * *

ІНШІ НАУКОВІ ВИДАННЯ СПІВРОБІТНИКІВ ІНСТИТУТУ

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

Монографію присвячено дослідженню проблем інформаційного етапу розвитку суспільства, інформаційної безпеки української держави в духовно-ціннісному вимірі, з'ясуванню соціокультурних, екзистенційних та правових проблем сучасного суспільства на тлі глобалізації та інформатизації. Важливе місце приділено проблемам осмислення права в сучасних соціокультурних умовах. Особливість монографії – розгляд проблем у філософському, філософсько-правовому та державотворчому аспектах.

Для студентів, аспірантів, викладачів юридичних закладів вищої освіти, працівників органів державного управління та місцевого самоврядування.

* * * * * * * * *

Інформаційне право та інформаційне законодавство / В.М. Брижко, В.М. Фурашев. – 2-ге вид., доп. Харків: Видавництво "Право", 2021. 288 с. – ISBN 978-966-998-080-9.

Видання є науковою роботою, яка присвячена проблематиці стану, перспектив та системному впорядкуванні відносин в інформаційній сфері на основі узагальнення, впродовж 1998 – 2020 рр., філософсько-гуманітарних, науково-теоретичних та практичних знань про інформаційне право та інформаційне законодавство, як специфічні форми соціального буття.

Метою роботи є сприяння формуванню нової системи поглядів та підходів до методології застосування приписів інформаційного права та норм інформаційного законодавства, які безпосередньо пов'язані з приватністю, захистом, безпекою даних та інформаційних ресурсів в умовах поширення та розвитку електронно-інформаційних технологій та систем, в контексті цінності і соціальної значущості категорії "право" у впорядкуванні суспільних відносин.

Висновки та деякі пропозиції у роботі сформульовані на підставі результатів досліджень видатних учених у таких сферах знань філософії права як онтологія, аксіологія, антропологія, гносеологія, герменевтика й праксеологія, концептуальну основу яких завжди складали пошуки природи сутності та цінностей правових ідей у створенні умов реального захисту людини. При цьому особливістю інформаційно-комунікаційної сфери є те, що ідеалу в абсолютному інформаційному захисті, безпеці людини та гармонізації інформаційних відносин не досягнути ніколи, це – ілюзорна утопія. Але вектор спрямування історичних змін у соціальних, політичних та правових поглядах, появи нових юридичних принципів і намагань досягнути більшої чіткості норм (дефініцій) регуляції відносин це надає.

Видання може бути корисним при доповненні учбово-методичних програм і матеріалів дисциплін, пов'язаних з інформаційним правом і інформаційним законодавством України.

* * * * * * * * *

Демократичний цивільний контроль над сектором безпеки і оборони: теорія і практика: навчальний посібник / авт. кол.: В.А. Ященко, В.Г. Пилипчук, П.П. Богуцький, О.Д. Довгань, І.М. Доронін, О.В. Петришин; за заг. ред. В.Г. Пилипчука. Київ-Одеса: "Фенікс", 2020. 224 с.

У посібнику на основі узагальнення результатів фундаментальних і прикладних досліджень розглянуто теоретичні, правові та організаційні аспекти становлення і розвитку системи демократичного цивільного контролю над сектором безпеки і оборони в сучасних умовах, зокрема, питання сутності, змісту та організаційної моделі цивільного контролю і його демократичної природи. Висвітлено генезис формування і розвитку системи

демократичного цивільного контролю в Україні та відповідний досвід країн-членів ЄС і НАТО. Особлива увага приділяється аргументації соціальної і професійної необхідності демократичного цивільного контролю та механізмам його практичної реалізації.

Видання розраховане на експертів і вчених в галузі права національної безпеки та військового права, фахівців сектора безпеки і оборони, науково-педагогічний склад, аспірантів і докторантів, курсантів, студентів і слухачів профільних закладів вищої освіти.

* * * * * * * * *

Енциклопедія соціогуманітарної інформології / коорд. проекту та заг. ред. проф. К.І. Бєляков. Київ: Видавничий дім "Гельветика", 2020. Т. 1. 472 с.

Проект є науковим виданням у формі словника-довідника, в якому розкрито зміст основних доктринальних та нормативно-правових понять, термінів та словосполук, що використовуються в обігу наукових досліджень інформаційних процесів, явищ та відносин в соціальних та гуманітарних галузях наукових знань. Надано інформацію про органи та підрозділи виконавчої влади, а також наукові установи та видання (у тому числі закордонні), громадські об'єднання, що є суб'єктами інформатизації з відповідними коментарями провідних фахівців за напрямами. Викладено відомості про вітчизняних вчених, які займаються проблематикою наукового та організаційно-правового забезпечення процесу інформатизації держави, дослідженнями інформаційної сфери в цілому. Пропонується систематизований за галузями знань та спеціальностями перелік наукових розробок на рівні дисертаційних досліджень.

Розраховано на студентів, слухачів, аспірантів та викладачів як гуманітарних, так й технічних навчальних закладів, державних службовців і законотворців, а також усіх, хто цікавиться дослідженнями впливу інформаційних процесів на суспільне життя. Виданням може використовуватися у навчальному процесі.

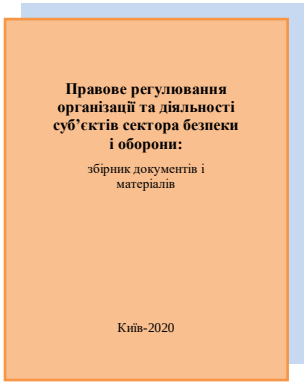
* * * * * * * * *

Державний гімн України: історико-правові аспекти: збірник документів і матеріалів / упоряд. Л.В. Заславська, В.С. Голубовська, С.О. Дорогих. Київ: Видавничий дім "АртЕк", 2020. 98 с.

Збірник документів і матеріалів знайомить читача з усіма законодавчими документами, що були прийняті та запропоновані, в якості проектів, з початку створення Гімну України на заміну Гімну Української РСР.

Видання розраховане на фахівців, експертів і вчених, представників органів влади та усіх, кому цікавий процес створення та застосування головного музичного твору України.

* * * * * * * * *



Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони: збірник документів і матеріалів / упоряд.: М.В. Беланюк, І.М. Доронін, О.В. Лебединська, О.Г. Радзієвська, В.Г. Пилипчук, О.В. Шамара, В.М. Фурашев. Київ: Видавничий дім "АртЕк", 2020. 756 с.

До збірника увійшли законодавчі акти, документи і матеріали, що регулюють організацію та діяльність суб'єктів сектора безпеки і оборони України та здійснення демократичного цивільного контролю, а також міжнародні правові акти з питань захисту прав і свобод людини та Рекомендації Парламентської Асамблеї Ради Європи щодо організації цивільного контролю над службами внутрішньої безпеки і воєнною організацією держави.

Видання розраховане на фахівців сектора безпеки і оборони, вчених в галузі права національної безпеки та військового права, науково-педагогічних працівників, студентів, курсантів, аспірантів і докторантів профільних закладів вищої освіти.

* * * * * * * * * * *

До відома авторів

"**ІНФОРМАЦІЯ І ПРАВО**" – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   – *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   – *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   – *відстань між рядками – 1 інтервал;*
   – *кількість матеріалу однієї статті – не більше 15 стор.*

Стаття має передбачати такі обов'язкові структурні елементи:

- УДК.
- Ім'я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.
- Назва статті (укр. та англ. мовами).
- Анотація та ключові слова (укр., англ. та рос. мовами).
- **Розв'язання проблеми,** шляхом наукового вирішення завдання:
  - **постановка проблеми** *(загальна характеристика);*
  - **результати аналізу наукових публікацій** – надаються відомості про стан вирішення проблеми та ПІБ авторів, з обов'язковим посиланням на їхні роботи (в […]), повний опис бібліографії яких вказується в підрозділі "Використана література"; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;
  - **формування мети** *(постановка завдання)* статті;
  - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
- **Висновки** за результатами розв'язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
- **Використана література.** Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання" або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.
- Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- ***Актуальність теми***.
- ***Новизна та обґрунтованість одержаних результатів***.
- ***Наукова (практична) цінність результатів***.
- ***Висновок про можливість відкритої публікації***.

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України "Про затвердження порядку формування переліку наукових фахових видань України" від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов'язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту**.

Реквізити для оплати робіт:
Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада Інституту не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
  Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за додержання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:

– відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
– внесення до статті змін редакційного змісту у зв'язку з обмеженням обсягу загального матеріалу.

* * * * * * * * * *

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(36)/2021

Засновники журналу:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІІП НАПрН України); - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини "Україна".
Видавець:	© НДІІП НАПрН України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики 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 – НДІІП НАПрН України; URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.

Founders of journal:	- Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine (SRIIL of the NALS of Ukraine); - Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine; - Open International University of Human Development "Ukraine"
Publisher:	© SRIIL of the NALS of Ukraine.
Address of release:	01032, Kyiv, Saksaganskogo str., 110-V. Scientific Rresearch Institute of Informatics and Law of the National Academy of Law 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 – Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine; URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.