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

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

Відкритий міжнародний університет розвитку людини “Україна”

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 3(38)/2021

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

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

м. Київ

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

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

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND LAW

SCIENTIFIC PROFESSIONAL JOURNAL

№ 3(38)/2021

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

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

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

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

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 17.8. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ "Видавничий дім "АртЕк".
04050, м. Київ, вул. Мельникова, буд. 63. Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою ДНУ ІІБП НАПрН України, протокол № 7 від 28.9.21 р.

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

Informative Law

Legal Informatics

Informative and National Safety

Recommended for publication by the IISL of the NALS of Ukraine, protocol № 7 dated 28.9.21.

Інформаційне право

УДК 342.4(328)

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

ПАРЛАМЕНТСЬКИЙ КОНТРОЛЬ У СФЕРАХ ДУХОВНОСТІ І КУЛЬТУРИ: БЕЗПЕКОВИЙ АСПЕКТ

Анотація. *В даній статті досліджується питання ефективності та якості здійснення парламентського контролю у сферах духовності і культури, як аспект забезпечення національної безпеки в сучасних умовах ведення гібридної агресії Російської Федерації проти України. Зазначено, що парламентський контроль в Україні є вкрай недостатнім та доволі суперечливим, що не дає змоги поки що стверджувати про усталеність парламентського контролю як такого, про його належне наукове осмислення та правове закріплення в сучасних умовах, особливо в умовах ведення гібридної агресії Російської Федерації проти України. Констатовано, що соціальні зміни, зумовлені глобалізаційними процесами, впливають на стан забезпечення національної безпеки у таких сферах, як культура і духовність. Нині зазначене питання вивчено недостатньо, а тому потребує подальшої розробки. Зазначено, що у сфері культури певні позитивні зміни щодо здійснення державного (парламентського) контролю в останні роки досягнуто. Однак, у сфері духовності (духовної культури) та в пов'язаній з нею релігійній сфері, внаслідок здійснюваних Російською Федерацією ідеологічних диверсій та інформаційних спецоперацій, в Україні фактично породжена духовна криза, вирішення якої є невідкладним завданням державної влади. Парламентський контроль у зазначених сферах, який має здійснюватися через призму національної безпеки, фактично відсутній. Напрацьовано ряд пропозицій, які доцільно впровадити у процес здійснення парламентського контролю за згаданими сферами.*

Ключові слова: *духовна криза; духовні цінності, духовність, експансія, культура, парламентський контроль, світогляд.*

Summary. *This article examines the issue of the effectiveness and quality of the implementation of parliamentary control in the spheres of spirituality and culture, as an aspect of ensuring national security in the modern conditions of the hybrid aggression of the Russian Federation against Ukraine. It is noted that parliamentary control in Ukraine is extremely insufficient and rather contradictory, which does not yet allow to talk about the stability of parliamentary control as such, about its proper scientific understanding and legal consolidation in modern conditions, especially in the context of the hybrid aggression of the Russian Federation against Ukraine. It was stated that social changes caused by globalization processes affect the state of ensuring national security in such spheres as culture and spirituality. Currently, this issue has not been studied enough, and therefore needs further development. It was noted that in the field of culture, certain positive changes in the implementation of state (parliamentary) control have been achieved in recent years. However, in the sphere of spirituality (spiritual culture) and in the related religious sphere, as a result of the ideological sabotage and special informational operations carried out by the Russian Federation, a spiritual crisis has actually been generated in Ukraine, the resolution of which is an urgent task of the state power. Parliamentary control in these areas, which should be carried out through the prism of national security, is virtually absent. A number of proposals have been worked out, which are advisable to be introduced into the process of exercising parliamentary control over the aforementioned spheres.*

Keywords: *spiritual crisis, spiritual values, spirituality, expansion, culture, parliamentary control, worldview, values.*

Аннотация. *В данной статье рассматривается вопрос эффективности и качества осуществления парламентского контроля в сферах духовности и культуры, как аспект обеспечения национальной безопасности в современных условиях ведения гибридной агрессии Российской Федерации против Украины. Отмечено, что парламентский контроль в Украине является крайне недостаточным и довольно противоречивым, что не позволяет пока говорить о устойчивость парламентского контроля как такового, о его надлежащем научном осмыслении и правовом закреплении в современных условиях, особенно в условиях ведения гибридной агрессии Российской Федерации против Украины. Констатировано, что социальные изменения, обусловленные глобализационными процессами, влияют на состояние обеспечения национальной безопасности в таких сферах, как культура и духовность. Сейчас данный вопрос изучен недостаточно, а потому нуждается в дальнейшей разработке. Отмечено, что в сфере культуры определенные позитивные изменения по осуществлению государственного (парламентского) контроля в последние годы достигнуты. Однако, в сфере духовности (духовной культуры) и в связанной с ней религиозной сфере, в результате осуществляемых Российской Федерацией идеологической диверсии и информационных спецопераций, в Украине фактически порожден духовный кризис, разрешение которого является неотложной задачей государственной власти. Парламентский контроль в указанных сферах, который должен осуществляться через призму национальной безопасности, фактически отсутствует. Наработано ряд предложений, которые целесообразно внедрить в процесс осуществления парламентского контроля над упомянутыми сферами.*

Ключевые слова: *духовный кризис, духовные ценности, духовность, экспансия, культура, парламентский контроль, мировоззрение, ценности.*

Постановка проблеми. Демократичне врядування неможливе без функціонування принципів прозорості та підзвітності. Головна роль у забезпеченні зазначеного покладається на парламент. Контрольні повноваження парламенту є однією з найважливіших сфер його діяльності. Як показує практика, парламентський контроль може бути найбільш ефективним лише тоді, коли парламент має доступ до різноманітних джерел інформації.

Ключову роль у процесі здійснення парламентського контролю відіграють парламентські комітети, а також тимчасові спеціальні та слідчі комісії, які мають його здійснювати фактично в усіх сферах життєдіяльності. В цілому парламентський контроль є дієвим механізмом розвитку демократичної, правової, соціальної держави та громадянського суспільства. Саме від повноти реалізації Верховною Радою України своїх контрольних повноважень, системності, ефективності і всебічності здійснювання нею парламентського контролю залежить урегульованість функціонування суспільних відносин у державі, вирішення завдань, які стоять перед державою. Зазначене є нині вкрай важливим в умовах здійснення гібридної агресії Російської Федерації проти України, тому питання здійснення парламентського контрою набуло надзвичайної гостроти саме у сфері національної безпеки.

Розробкою проблем парламентаризму з позицій досягнень світової теорії та практики займались такі вітчизняні вчені, як: О. Андрійко, А. Георгіца, В. Журавський, О. Копиленко, М. Козюбра, А. Колодій, В. Копєйчиков, Л. Кривенко, М. Мироненко, В. Опришко, В. Погорілко, В. Селиванов, Ю. Тодика, В. Шаповал, Ю. Шемшученко та ін.

За період незалежності в Україні були захищені дисертаційні дослідження, зокрема, Ю. Барабашем, О. Майданник, які безпосередньо стосувались проблем реалізації на теренах України парламентського контролю.

Однак, щодо окресленої проблеми, присвяченим питанням духовності і культури через призму національної безпеки в умовах гібридного конфлікту, наукових праць поки що не вистачає.

Метою статті є визначення та оцінка ефективності здійснення парламентського контролю у сферах духовності і культури в умовах гібридної агресії Російської Федерації, розкрити його недоліки і прогалини та напрацювати пропозиції щодо шляхів і механізмів підвищення його ефективності.

Виклад основного матеріалу. Як зазначено в наукових дослідженнях, принцип народовладдя як універсальна політико-правова ідея сучасного конституціоналізму є невід'ємною складовою системи загальновизнаних конституційних цінностей, що у своїй сукупності становлять засади демократичного конституційного ладу України. Адже демократія – це і є, насамперед, здійснення влади безпосередньо народом чи від його імені та в його інтересах спеціально уповноваженими на це органами публічної влади [1].

Саме народний суверенітет є необхідною передумовою правового обмеження держави, оскільки народ через демократичні процедури легітимації влади наділяє її частиною відповідні державні органи, за допомогою конституції формує державу, владні структури, делегує їм відповідні повноваження, тим самим добровільно обмежуючи свій суверенітет і водночас встановлюючи межі втручання держави у суспільне життя [2].

Демократія передбачає встановлення підконтрольності держави, її органів, народу, що логічно тягне за собою виникнення правового обов'язку держави діяти щодо суспільства, кожного його члена тільки в межах права [3, с. 389]. Зазначене органічно вплітає в категорію "правозаконність" ознаку взаємної відповідальності держави і громадянина, оскільки, з одного боку, держава відповідальна за свою представницьку діяльність перед верховним суб'єктом влади, а разом з тим і кожним його членом [4, с. 24].

Водночас необхідно зазначити, що ефективне функціонування будь-якого органу державної влади неможливе без налагодження дієвої системи контролю за виконанням прийнятих ним рішень, адже сама ефективність будь-якого рішення залежить від здійснення належного контролю за ним. Тому "контроль у сфері управління має як самостійне значення, так і є елементом, частиною інших функцій управління, засобом перевірки забезпечення виконання функцій управління, здійснюваним на заключних етапах процесу" [5, с. 18]. Важливість такого контролю підкреслюється в діяльності окремих державних органів зокрема структурним виокремленням контрольної функції у самостійну, відносно незалежну від реалізації інших функцій відповідного органу функцію, хоч і системно пов'язану з ними.

Саме тому, нині, в теорії та у практиці парламентаризму опрацьовані та конституційно закріплені різноманітні концепції здійснення парламентського контролю за виконанням законів, а також за діяльністю виконавчої влади загалом. Такий підхід є апробованим на практиці. Він видається правильним і підтверджується наявним зарубіжним досвідом функціонування парламентських інституцій. Зазначене стосується й українського парламентаризму, оскільки він увібрав у себе як згадані концепції парламентського контролю, так і їх реалізацію у практиці державотворення у сучасній Україні [6, с. 2]. Відповідно до зазначеного в положеннях частини другої статті 1 Закону України [7], Регламентом Верховної Ради України встановлюється порядок здійснення її контрольних функцій. Особливості здійснення контрольних функцій у сферах національної безпеки і оборони визначаються Законом України "Про національну безпеку України" [8].

Невід'ємним елементом, напрямком чи формою такого контролю є контроль з боку не лише самого парламенту як цілісного органу державної влади, але й його здійснення з боку створених у його структурі робочих органів – парламентських комітетів. Саме відповідно до положень статті 14 Закону України [9] комітети Верховної Ради України здійснюють свою контрольну функцію.

Водночас, досвід парламентського контролю, з огляду на історичну ретроспективу, є в Україні вкрай недостатнім та доволі суперечливим. Це не дає змоги поки що стверджувати про усталеність парламентського контролю як такого, про його належне наукове осмислення та правове закріплення в сучасних умовах, особливо в умовах ведення гібридної агресії Російської Федерації проти України. Як зазначають дослідники, практика функціонування парламентських комітетів в Україні вказує на те, що контрольна функція, на жаль, все ще не стала повноцінною та щоденною формою комітетської діяльності порівняно, скажімо, із законопроектною роботою комітетів Верховної Ради України. Підтвердженням зазначеного є те, що передбачене відповідно ст.ст. 6 і 53 законів України [8; 10] створення комітету Верховної Ради України, до предмета відання якого віднесено питання забезпечення контрольних функцій Верховної Ради України за діяльністю органів спеціального призначення з правоохоронними функціями, правоохоронних органів спеціального призначення та розвідувальних органів, до цього часу не вирішено, хоча відповідний законопроект, внесений до Верховної Ради України у 8-му її скликанні і перереєстрований у 9-му її скликанні [11] лежить без руху.

Тут доречно нагадати, що характерною ознакою демократичної держави є наявність системи органів, які здійснюють контрольні функції у сфері діяльності спеціальних служб, тобто, державні органи, які відповідно до національного законодавства призначені здійснювати розвідувальну та контррозвідувальну діяльність, а також інші спеціальні функції з метою забезпечення національної безпеки держави. Важливу роль у цій системі, незалежно від форми державного правління, відіграють законодавчі органи. Наявність дієвого парламентського контролю гарантує функціонування спеціальних служб у межах чинного законодавства і є запобіжником порушення ними конституційних прав і свобод людини та громадянина. У демократичних країнах парламентський контроль є продуктом певного історичного розвитку та національної політичної культури.

Демократичне суспільство потребує чітко регламентованого запобіжника перед існуючою спокусою для влади використати спецслужби у вузько партійних чи внутрішньополітичних, або навіть особистих інтересах. Головну роль у демократичній системі стримувань та противаг має відігравати парламентський контроль. Здатність парламенту та суспільства в цілому контролювати спеціальні служби є лакмусовим папірцем для перевірки на справжність демократії та верховенства права. Зарубіжні країни мають суттєвий досвід здійснення згаданого контролю, який слугує хорошим прикладом для українських парламентарів, було б лише у них бажання врегулювати дане питання. А тому нехтувати реалізацією парламентського контролю з боку комітетів того ж таки парламенту неправильно. Адже це врешті може мати небезпечні наслідки для розвитку парламентаризму в цілому [6]. Крім того, такий контроль, будучи рутинною, повсякденною формою роботи парламентських комітетів, повинен слугувати цілям забезпечення прозорості і відкритості парламенту України загалом, підвищення ефективності його діяльності тощо. Захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз в нинішніх умовах гібридної агресії має перебувати під постійним контролем як самого народу, так і створених ним державних органів.

Нині у світі відбуваються великі соціальні зміни, зумовлені глобалізаційними процесами, однак вплив глобалізації на стан забезпечення національної безпеки у таких сферах як культура і духовність вивчений недостатньо і потребує подальшої розробки. Адже духовність – це внутрішній світ людини, осередок її інтелектуальних і емоційно-вольових сил у єдності свідомості, самосвідомості, світогляду і волі. Духовність

об'єктивує свої цінності в ідеях, принципах, нормах, еталонах, діях позитивної чи негативної соціальної орієнтації, які формуються шляхом сприйняття та оцінки навколишніх явищ. Духовність – це втілення в світоглядних орієнтаціях людини сподівань, прагнень, ідеалів, духу народу, нації, що визначає спрямованість особистісних потреб, бажань і зумовлює настанову на відповідний життєвий вибір. Це осмислення людиною гуманістичного сенсу мети людської життєдіяльності.

Як зазначають дослідники, в структурі духовності доцільно розрізнювати дух і душу. Поняття "дух" прийнято пов'язувати з діяльністю свідомості. Дух завжди діяльний, активний, повний творчої енергії. Саме завдяки діяльності духу людина сприймає і оцінює світ насамперед в ідеях різного світоглядного характеру: філософсько-гуманістичних, морально-етичних, екологічних, релігійних та інших. Проте дух є цілісність в структурі особистості, яка робить її тим, що вона є.

На відміну від духу "душа" – це скоріше психологічний феномен. Вона відображає життя за допомогою почуттів, емоційних морально-психологічних станів, які виникають у зв'язку з оцінкою людиною тих чи інших явищ зовнішнього або внутрішнього світу. Тому душа може страждати, боліти, хвилюватись, радіти і таке інше [12].

У свою чергу, культура – сукупність матеріальних і духовних цінностей, створених людством протягом його історії. Усі ми належимо до тієї чи іншої культури. Культура – це поєднання людських знань, переконань і норм поведінки, які ми переймаємо, а потім передаємо майбутнім поколінням. Культура – ключовий фактор соціалізації, який регулює різні сфери взаємодії людей – від повсякденного спілкування до функціонування глобальної економіки. Тому культурі притаманна різноманітність її ролей у суспільстві.

Поняття культури є дуже багатозначним. Сьогодні існують десятки, якщо не сотні визначень культури. Зазвичай під нею розуміють рівень духовного (точніше, душевно-духовного) розвитку народу чи суспільства. Досягнення у мові, релігії, моралі, філософії, науці, мистецтві, системі освіти й виховання; власне, сукупність цих видів людської діяльності і звуть культурою. Іноді в поняття культури включають також право, державний лад, громадський устрій, етикет, суспільні звичаї і форми спілкування, а також економіку, промисловість, техніку, господарство. Однак все це, хоч воно також відбиває рівень духовного розвитку, доцільніше віднести до поняття цивілізації і, таким чином, розрізнити культуру від цивілізації [13].

Західні культурологи, незважаючи на різне розуміння ними суті культури, вбачають у ній примат духовного над матеріальним. Вони розуміють культуру як сукупність духовних символів, форму розумової діяльності, систему знаків, комунікацію, інтелектуальний аспект штучного середовища тощо.

Зазначимо, що духовна культура насамперед охоплює сферу духовного виробництва – це сукупність форм суспільної свідомості, способів створення і використання духовних цінностей, форм комунікації людей. Будь-яка абсолютизація чи недооцінка матеріальної або духовної сторони культури збіднює її як надзвичайно багатогранне, цілісне явище. Поняття духовної культури включає всі галузі духовної сфери; показує соціально-політичні процеси, що відбуваються в суспільстві. Елементами духовної культури є: звичаї, норми, цінності, знання, інформація, значення.

Духовна культура визнається як різноманітний досвід життєдіяльності соціальних суб'єктів, що включає в себе найсуттєвіші результати суспільного досвіду народів щодо освоєння суспільного буття, соціуму в цілому, багатогранних духовних цінностей. Такий досвід має загальний, універсальний характер. Це також такий спосіб свідомої організації особистістю своєї індивідуальної сенсожиттєвої діяльності в сфері духовного і матеріального виробництва, який забезпечує їй всебічну самореалізацію, самоздійснення

її сутнісних сил, різноманітних життєпроявів. Духовна культура як елемент духовного життя, суспільних, духовних відносин включає в себе певну систему цінностей, знань, переконань, світоглядних орієнтацій, норм, традицій в органічній єдності з соціальною гуманістично значимою діяльністю людей щодо освоєння, творення буття. До неї відносять продукти духовної діяльності людини, які існують переважно в ідеальному вигляді: поняття, уявлення, вірування, почуття і переживання, доступні свідомості і розумінню всіх людей. Духовна культура створює особливий світ цінностей, формує і задовольняє наші інтелектуальні та емоційні потреби. Духовна культура – це продукт суспільного розвитку, її основне призначення полягає у продукуванні свідомості.

Зазначимо, що культура виступає єдиним механізмом передачі соціального досвіду від покоління до покоління, від епохи до епохи, від однієї країни до іншої. Адже, крім культури, суспільство не має інакших способів передачі досвіду, нагромадженого попередниками. Саме через це культуру не випадково вважають соціальною пам'яттю людства, а розрив культурних зв'язки між поколіннями призводить до її втрати (феномен "манкуртизму") з усіма негативними наслідками [13].

І культура, і духовність відповідним чином співвідносяться з релігією. Вони мають спільні витоки і корені, які лежать у людській практиці. По мірі ускладнення суспільного організму, його матеріальної і духовної культури більш вагомими стають і самі релігійні системи, утворюючи своєрідну підсистему цінностей.

Відповідно, це надзвичайно важливі складові національної безпеки для України, особливо в нинішніх умовах. Саме внаслідок негативного ідеологічного впливу Російської Федерації на свідомість, духовність та культуру українських громадян насамперед прикордонних регіонів України, і не тільки їх, Україна має ряд конфліктних у військовому відношенні ситуацій на своїй території (окупований Крим, частково окуповані Донецька та Луганська області), а також конфліктні ситуації, що склалися у суспільстві в духовній та культурній сферах. Мова йде про гарантоване застосування та використання державної мови в усіх сферах життєдіяльності, використання та застосування свого національного культурного надбання в ЗМІ та в телекомунікаційних системах, а також про напрацювання та забезпечення у громадян в умовах нової системи духовних цінностей домінування принципу соціальної відповідальності за свою діяльність, справи і вчинки, що має мінімізувати підґрунтя для виникнення соціальних конфліктів на етнічному, культурному і релігійному ґрунті.

Як зазначають непоодинокі науковці, для подолання духовної кризи в нових соціально-історичних умовах потрібна радикальна перебудова свідомості і поведінки людей, формування нової шкали духовних цінностей, напрацювання відповідної державної політики, стратегій і державних програм, упередження від впливу на громадян радикальних і інших шкідливих для людського світогляду та духовності ідеологічних штампів та спеціальних програм окремих держав (на зразок "руського міра" Російської Федерації чи ісламського радикалізму), що в зрештою призводить до виникнення відповідної напруги у суспільстві, і навіть – до глибоких криз у гуманітарній та інших сферах життєдіяльності. Можливо припустити, що в новій системі духовних цінностей домінуючим буде принцип соціальної відповідальності за свою діяльність, справи і вчинки. Це – об'єктивна необхідність, веління нашого часу. Адже діяльність і поведінка, не підкріплені відповідальністю перед суспільством, здатні перетворити духовно нерозвинену особистість на людину-робота, який опікується лише собою і руйнує все навкруги.

В сучасній системі духовних цінностей глобальна відповідальність за життя на землі має мати пріоритети перед свободою, яка вже давно перетворилась на свавілля, на діяльність без контролю, кордонів і обмежень. Гідне місце мають посісти принципи

контролю і самоконтролю, установка на поведінку свідомо самоорганізованої, самоконтрольованої і саморегульованої людини. Саме людина, як член соціуму яка інтегрована в різні соціальні структури шляхом міжособистісних відносин, які регулюються і правом, і нормами моралі, цінностями духовної культури має домінувати в сучасному житті. Тому життя без моралі, духовності може призвести лише до соціальної дезорганізації та руйнації, що можна побачити в сучасному глобалізованому світі. Сформувати духовність у людини, це значить виховувати її в дусі істинного гуманізму, всеосяжно і ґрунтовно, з врахуванням духовних основ особи (ними є творчість, буття, свобода і відповідальність, сенс буття, любов), а також сучасного стану природничих і суспільних наук, рівня розвитку економіки та культури, літератури і мистецтва, соціальних і політичних відносин у світі і в нашій країні. Цей процес пов'язаний з перебудовою суспільства на засадах демократії, справедливості і чесності [14].

Для українського суспільства, яке формується в сучасних умовах як розвинуте, інформаційне суспільство, соціально направлене і освічене в правовому відношенні, згадані вище принципи вкрай важливі для свого становлення як цивілізованого суспільства. Саме суспільство, розвиваючись, має контролювати безпосередньо чи опосередковано, у взаємодії з органами державної влади, згадані процеси, корегувати та усувати відповідні негативи, що супроводжують його розвиток. Мова йде, насамперед, про представницькі органи країни, і парламент – в першу чергу. Це питання є важливим з точки зору забезпечення національної безпеки.

Сьогодні тема духовності означується як тяга до вершин культури. Дуже вдало висловився П'єр де Шарден, який сказав: "Ми не людські істоти, які мають духовний досвід, а духовні істоти, що мають людський досвід". Затхла атмосфера бездуховності просякає всі сфери нашої життєдіяльності і від того нам так дискомфортно і з іншими, і з самими собою.

Науково-технічний прогрес направив людину на те, що тимчасове. А. Ейнштейн сказав: "Я боюсь, що обов'язково прийде час, коли технічне замінить просте людське спілкування і світ отримає покоління ідіотів". Криза культури виникає в тих випадках, коли мораль тікає з-під ніг, коли розривається зв'язок з віковічними цінностями. Звичайно, для нас є важливим і лікування, і дах над головою, і їжа, але і в цьому самому мають потребу і тварини. Якщо ми занедбуємо те, що піднімає нас над тлінним світом, то рано чи пізно опиняємось у безвиході. Так було в часи занепаду античного світу, так є і в нашу днину [15].

Нині подібне відбувається в Україні, коли такі історично надбані цінності, як повага до старшого покоління, спадкоємність поколінь, вивчення, врахування і примноження історичного досвіду, стали для певних політичних кіл, насамперед які знаходяться у державній владі, своєрідним анахронізмом, пережитком минулого. Зазначене лише не сприяє консолідації українського суспільства перед викликами, що постали перед країною, а й призводить до його розшарування як в соціальному, культурному, духовному, мовному тощо сенсі, створює загрози відповідного характеру, що направлені на підрив подальшого існування держави.

Аналіз національного законодавства свідчить, що зазначеним категоріям в гуманітарній сфері державною владою приділено недостатньо уваги. Якщо в останні роки у питаннях культури, мови та освіти відбулися певні позитивні зміни – їм державна влада почала приділяти належну увагу, приймаючи ті, чи інші нормативно-правові акти та державні програми, що регулюють вирішення даного питання, то у питаннях духовності, духовної культури ситуація склалася протилежною, вона – негативна. Основна проблема – це розмитість в сучасних умовах історично напрацьованих моральних цінностей.

Як сказав невідомий поет, – “все заплуталось у хаосі визначень і понять, таких як: гендерність, спотворення інституту сім’ї, секулярності, гедонізму, нових медичних технологій (клонування, генна інженерія, євгеніка), дехто навіть пропонує вивести новий вид людини шляхом більш досконалого схрещування”.

В контексті зазначеного вище, гострим для українського суспільства залишається невирішене теологічне (церковне) питання. Мова йде про релігійне протистояння в Україні, від вирішення якого державна влада фактично самоусунулася. Як зазначалося вище, національне законодавство не містить правових норм, які б врегульовували дану проблему. А парламентський контроль за згаданою проблемою з метою її вирішення, взагалі відсутній.

Спричинений діями Російської православної церкви церковний розкол в Україні, який фактично започаткований в інтересах імперської ідеології “руського міру” Російської Федерації, а також бажанням цієї церкви домінувати в православному світі, поставив саму Україну на грань розколу за релігійною ознакою.

Незважаючи на фактичне відокремлення церкви від держави, представники російської церкви в Україні (УПЦ) активно провадять політичну діяльність, балотуючись та обираючись до органів місцевого самоврядування різного рівня. При цьому, представники даної церкви: зайняли фактично антидержавницьку (проросійську) позицію щодо свого відношення до агресії на Сході України, окремі представники якої беруть активну участь у бойових діях та освячують злочинні дії сепаратистів; не сприймають українських воїнів та добровольців у питанні церковного освячення (благословення) воїнів на священну боротьбу з ворогом; не сприймають і не визнають Православну церкву України, яка зайняла активну патріотичну позицію у наданні духовної допомоги українським воїнам; вважають українську мову Богом неугодною для церковного служіння; пропагандують серед віруючих своїх громад фактично ідеологічні штампи “руського міру” тощо. Тим самим ця церква є фактично колабораціоністською силою в Україні, іноземним агентом, 5-ю колоною в Україні і, незважаючи на законодавчі вимоги про зміну своєї назви, оскільки не є самостійною релігійною структурою, ігнорує ці вимоги.

Даний негатив доповнюється існуючим до цього часу в Україні розколом в суспільстві за мовною та частково за етнічною ознакою, що теж є наслідком рукотворної діяльності, насамперед, державної влади Російської Федерації та її спецслужб, про що свідчать безліч невідворотних фактів.

Зазначені факти своєрідної “беззубості” державної влади щодо недопущення факту відкритого функціонування в Україні фактичного союзника її ворога свідчить про штучне створення руками самої державної влади передумов для виникнення загроз національній безпеці внутрішнього характеру.

Зазначимо, що ні Закон України “Про національну безпеку” [8], ні Стратегія національної безпеки [16], ні інші акти у сфері національної безпеки не містять положення, якими б регулювалося питання виховання, впровадження та захисту духовних цінностей, духовної культури у процесі становлення особистості громадянина України. Так само і в предметах розгляду питань у комітетах Верховної Ради України, і насамперед Комітету з питань національної безпеки, оборони та розвідки [17], відсутній такий предмет парламентського контролю, як загальний стан, а також стан здійснення заходів щодо напрацювання, забезпечення і захисту духовності та духовної культури громадян України. Історично склалося так, що саме релігія поширювала духовні практики, однак духовність не обов’язково релігійна. Духовність, як правило, пов’язана з традиційною моральністю.

Зазначене є особливо важливим для України, оскільки ціннісна орієнтація громадян слугує своєрідним критерієм, фільтром у визначенні ставлення людини до матеріальних та духовних цінностей, системи установок, відстоювання принципів і переконань. Вона передбачає позитивне чи негативне значення об'єктів навколишнього світу для індивідууму чи суспільства і визначається не їхніми властивостями як такими, а їх місцем та наявністю в людській життєдіяльності інтересів і потреб, соціальних відносин, критеріями і способами оцінки цього значення, виражених в моральних принципах і нормах, ідеалах, установках і цілях. Саме на цих принципах має здійснюватися виховання молодого покоління, покоління майбутнього України, оскільки сучасне покоління громадян не є в ціннісному відношенні однорідно-орієнтованим в нинішніх умовах щодо майбутнього молодої держави.

Саме нині є необхідність формування нових ціннісних орієнтацій, нових ціннісних ідеалів, ціннісного світогляду людини-громадянина, яка буде жити і працювати в XXI столітті в Україні – незалежній європейській державі, де цільові та ціннісні орієнтації сполучатимуть творчість, нові оригінальні ідеї з народними традиціями та культурою. Тому задамося питанням: Чи може людина жити без духовності? Звичайно може, але з великими труднощами, в стані деградації та з ризиком самознищення. Тому людина, що не здатна вибудовувати свою життєву перспективу, мотивувати себе щодо осмислених норм, переосмислювати притаманні їй мотивації та створювати собі нові мотивації, втрачає сенс життя, втрачає позитивні мотивації власного розвитку. Така ситуація в житті людини називається ***духовною кризою.*** Саме зазначене постійно нав'язує українському суспільству нинішній ворог України – Російська Федерація, так само як окремі принципи бездуховності приходять до нас із Заходу (втрата поваги до традиційних сімейних цінностей, аморальність тощо).

З огляду на зазначене, саме духовність, духовна культура українського народу в цілому і громадянина – зокрема, має бути захищена державною владою, розвиватися і збагачуватися, насамперед, в середовищі молодого покоління. Без зазначеного нівелюються національні цінності українського народу, які український народ зумів через віки свого приниження і гноблення зберегти і розвити. Тому, нині вкрай актуальним є вислів: "Народ, який вміє тільки запозичувати чужі фундаментальні еталони, зразки, норми та чужі фундаментальні системи мотивацій, не може ніколи бути вільним. Рано чи пізно він або завойовується, або погоджується на добровільне рабство, або зникає".

Сьогодні ми є не лише свідками, але й учасниками кризи моральності і правосвідомості, соціальної нестабільності, політичної дезорієнтації та дестабілізації молоді. Важливим чинником цієї кризи є крах тоталітарної системи, яка формувала у всіх єдину систему цінностей та орієнтацій. Сучасні цінності – актуально ідеологічна проблема, проблема формування світогляду, що виступає інтегративною основою діяльності, як окремого індивіду, так і будь-якої соціальної групи, колективу, нації. Це також нова проблема, що має проростати і кристалізуватися заново, причому вибір світоглядних позицій, а отже і цінностей покладається на індивід, як суб'єкта життєдіяльності. Це звичайно проблема загальної значущості, бо процес державотворення в Україні висуває на передній план такі спільні для всіх ідеологічні цінності, як патріотизм та громадянськість, та їх відображення у свідомості, світогляді та поведінці [18].

Україна, здобувши політичний суверенітет, так і не спромоглася здобути духовний суверенітет. Причому духовний суверенітет з точки зору перспектив країни є визначальним. Якщо країна має духовний суверенітет, зберігає та відтворює власний духовний простір – навіть втрати економічного чи політичного суверенітету їй не страшні, бо з часом ці суверенітети відтворяться.

Націю визначає духовна спільнота, яка має духовний суверенітет, за будь-яких умов зберігає та відтворює духовний простір, доброзичливо ставиться до духовних людей та забезпечує духовність усіх сфер життя в процесі перетворень фундаментального рівня. Якщо це не так, то маємо не націю, а співжиття громадян, хата яких скраю, і вони в будь-який момент готові або інтегруватися цілою країною куди завгодно – в Європу чи в Росію, – або емігрувати поодинці самостійно [19]. Тому на порозі XXI століття громадянська позиція особистості має формуватися не тільки на основі національної культури та духовності, а й на більш широких географічних перспективах, з урахуванням плюралізму, віросповідань (конфесій), систем ідей та прагнення до універсалізації. Якщо сформувати у людини чітко виражене усвідомлення своєї належності до певної держави, до нації, то вона буде свідомим громадянином та патріотом, в противному разі доведеться констатувати її манкуртизм. Кожному українському громадянину треба постійно пам'ятати про національну честь, якої ніхто не може позбавити, але яку можна втратити і заплямувати лише самому. Позбавляючись комплексу приниженості, меншовартості, він зберігає і національну честь, і власну гідність.

В контексті зазначеного важливого значення набуває процес виховання і розвиток почуття громадянського обов'язку і закріплення його відчуття у кожного громадянина України. Громадянин має усвідомлювати свою багатобічну залежність від держави, інтеріоризацію (перенесення в себе, усвідомлення) тих завдань, які поставила перед ним держава і які він повинен реалізувати в своїй діяльності, включаючи і захист держави від зовнішньої агресії. Вимоги українського суспільства в даний момент ґрунтуються на нагальній необхідності розбудови самостійної держави і захист її від зовнішнього ворога. Зазначене можна реалізувати через прояв своєї громадянської мужності, тобто здатності відстоювати державно-суспільні цілі, діяти рішуче, доцільно та активно за складних екстремальних ситуацій. Як зазначає американська дослідниця П. Уайт: "Якщо ми зацікавлені у формуванні громадянської мужності, вважаю за потрібне зосередитися на вихованні людей, які люблять свободу і справедливість, піклуються про благополуччя інших і знають як плекати і захищати ці цінності в повсякденному житті демократичного суспільства" [18].

Зазначені слова є вкрай актуальними для нинішньої України в цілому та для державної влади зокрема. Законодавство та парламентський контроль у згаданій сфері мають значну прогалину, що, у свою чергу, породжує певну пасивність органів виконавчої влади держави, не сприяє виправленню ситуації, що склалася в гуманітарній сфері та дозволяє ворогові реалізовувати свої завдання на території України, завдаючи певних збитків її національній безпеці.

Висновки.

Підсумовуючи вище викладене, можна констатувати наступне.

Парламентський контроль в гуманітарній сфері в контексті забезпечення національної безпеки в нинішніх умовах потребує невідкладного законодавчого врегулювання та практичного вдосконалення.

Зусилля державної влади в гуманітарній сфері та парламентський контроль в ній мають бути направлені на:

– напрацювання у громадян патріотичної самосвідомості, громадянської відповідальності і мужності, суспільної ініціативності і активності, готовності трудитися для розквіту Батьківщини, захищати її, підносити її міжнародний авторитет;

– виховання у громадян поваги до Конституції, законів Української держави, сформування потреби в їх дотриманні, прояву високої правосвідомості;

– виховання поваги до батьків, до свого родоводу, до традицій та історії рідного народу, усвідомлення своєї належності до нього, як його представника, спадкоємця і наступника;

– розв'язання проблеми релігійного розколу та правового врегулювання функціонування філіалу Російської церкви в Україні;

– вироблення у громадян гуманності, шанобливого ставлення до культури, традицій, звичаїв інших народностей, які населяють Україну, високої культури міжнаціонального спілкування (толерантність та полікультурність) тощо.

Ці та інші якості та риси мають формуватися в процесі засвоєння духовних надбань рідного народу, цілеспрямованого національного виховання, як системи ідей, поглядів, переконань, традицій, звичаїв та інших форм соціальної практики Українського народу, а також спрямованої на організацію життєдіяльності підростаючих поколінь, виховання їх в дусі природно-історичного розвитку матеріальної і духовної культури нації.

Використана література

1. Веніславський Ф. Ідея народовладдя в теорії та практиці українського державотворення (соціально-правова цінність ідеї народовладдя). *Вісник Конституційного Суду України.* 2011. № 3. С. 48-56.

2. Мацюк А. Громадянське суспільство – соціальна основа держави, влади і демократії. *Українське право*. 1995. № 1(2). С. 29-34.

3. Загальна теорія держави і права: підручник / Цвік М.В., Ткаченко В.Д., Богачова Л.Л. та ін.; за ред. М.В. Цвіка, В.Д. Ткаченка, О.В. Петришина. Харків: Право, 2002. 432 с.

4. Шипілов Л. М. Народовладдя як основа демократичної держави: монографія. Харків: Видавництво "ФІНН", 2009. 216 с.

5. Андрійко О.Ф. Організаційно-правові проблеми державного контролю у сфері виконавчої влади: автореф. дис. ...док. юрид. наук: спец. 12.00.07. Київ, 1999. 42 с.

6. Контрольні повноваження комітетів Верховної Ради України: правове регулювання та проблеми реалізації. *Часопис Парламент.* 2015. № 1. 52 с.

7. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI. URL: https://zakon.rada.gov.ua/ laws/show/1861-17#Text (дата звернення: 12.03.2021).

8. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.03.2021).

9. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР. URL: https://zakon.rada.gov.ua/laws/ show/116/95-%D0%B2%D1%80#Text (дата звернення: 12.03.2021).

10. Про розвідку: Закон України від 17.09.20 р. № 912-IX. URL: https://zakon.rada.gov.ua/ laws/show/912-20#Text (дата звернення: 12.03.2021).

11. Про парламентський контроль за дотриманням вимог Конституції та законів України щодо забезпечення національної безпеки в діяльності спеціальних служб та правоохоронних органів: проект закону України від 29.08.19 р. № 1204. URL: http://w1.c1.rada.gov.ua/pls//web proc4_1?pf3511=66508 (дата звернення: 12.03.2021).

12. Проблема духовності з соціально-історичної точки зору. URL: https://ru.osvita.ua/vnz/ reports/culture/30425 (дата звернення: 17.03.2021).

13. Багатозначність поняття культури. URL: https://ru.osvita.ua/vnz/reports/culture/10204 (дата звернення: 17.03.2021).

14. Липка О. Проблема формування духовності особи в сучасному українському суспільстві. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/20417/02_Lupka.pdf?Sequence=1 (дата звернення: 19.03.2021).

15. Про проблеми духовності у сучасному світі. URL: http://www.logos-kiev.org/publ/pro_problemi_dukhovnosti_u_suchasnomu_sviti/1-1-0-12 (дата звернення: 19.03.2021).

16. 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. *Офіційний вісник Президента України.* 2020. № 19. С. 26. Ст. 926.

17. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев’ятого скликання: Постанова Верховної Ради України від 29.08.19 р. № 19-IX. URL: https://zakon.rada.gov.ua/laws/show/19-20#Text (дата звернення: 24.03.2021).

18. Формування майбутніх громадян України. Моральні якості вчителів. URL: https://ru.osvita.ua/vnz/reports/psychology/9938 (дата звернення: 25.03.2021).

19. Дацюк С. Що таке духовність та навіщо вона потрібна? URL: https://www.pravda.com.ua/articles/2009/06/16/4026929 (дата звернення: 24.03.2021).

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

УДК 342.951

МАЛЯРЕНКО В.І., науковий співробітник**,** Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org /0000-0002-3433-3474.

КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ БОРОТЬБИ З ФЕЙКАМИ ТА ДЕЗІНФОРМАЦІЄЮ

Анотація. *Розглянуто поняття та види фейків. Визначено засади та способи виявлення фейків та дезінформації на прикладах країн ЄС. Проаналізовано досвід окремих держав ЄС у сфері протидії фейкам та дезінформації. Узагальнено практику деяких держав світу щодо криміналізації поширення недостовірної інформації та фейків. Запропоновано заходи щодо боротьби з фейками та дезінформацією. Визначено шляхи удосконалення протидії фейкам у вітчизняному медіа просторі.*

Ключові слова: *загроза, пропаганда, дезінформація, засоби масової інформації, фейки, аккаунт, протиправний контент, національна безпека, деструктивна діяльність, гібридна війна.*

Summary. *The concepts and types of fakes are considered. The principles and methods of detecting fakes and misinformation on the examples of EU countries are determined. The experience of some EU countries in the field of counterfeiting and misinformation is analyzed. The practice of some countries of the world to criminalize the dissemination of unreliable information and fakes is summarized. Measures to combat fakes and misinformation are proposed. The directions of the improvements of countering fakes in the domestic media space have been identified.*

Keywords: *threat, propaganda, misinformation, mass media, fakes, account, illegal content, national security, destructive activity, hybrid war.*

Аннотация. *Рассмотрены понятие и виды фейков. Определены основы и способы обнаружения фейков и дезинформации на примерах стран ЕС. Проанализирован опыт отдельных стран ЕС в сфере противодействия фейкам и дезинформации. Обобщена практика отдельных стран мира в отношении криминализации распространения недостоверной информации и фейков. Предложены мероприятия по борьбе с фейками и дезинформацией. Определены направления усовершенствования противодействия фейкам в отечественном информационном пространстве.*

Ключевые слова: *угроза, пропаганда, дезинформация, средства массовой информации, фейк, аккаунт, противоправный контент, национальная безопасность, деструктивная деятельность, гибридная война.*

Постановка проблеми. В сучасних умовах машина російської пропаганди шаленими темпами поширюється навколо світу. Останнім часом спостерігаються значні зусилля боку закордонних, у т.ч. структур РФ, для дискредитації діючої в Україні влади. З цією метою поширюється тенденційна і неправдива інформація за допомогою широкого спектру засобів інформаційного впливу. Сприяють поширенню негативної інформації та збору натовпів новітні засоби комунікації, насамперед соціальні мережі Інтернет. Активно поширюється деструктивна інформація фейкового характеру, спрямована на інспірування екстремістських дій, поєднаних з розпалюванням національної чи расової ворожнечі, поширення проявів ксенофобії, расизму та антисемітизму, що може стати причиною масових заворушень, вчинення злочинів проти основ національної безпеки держави і спричинити шкоду міжнародному авторитету будь-якої країни світу. Дезінформація сьогодні поширюється в “індустріальних масштабах”, і значний внесок в

це робить Росія. Тактика дезінформації постійно урізноманітнюється. Невипадково держава-агресор на постійній основі здійснює через свої або лояльні до РФ інформаційні ресурси заходи з дискредитації діяльності органів державної влади, а також проведення антиукраїнських інформаційних акцій. За таких умов висвітлення кращих практик зарубіжного досвіду у сфері боротьби з фейками та дезінформацією є актуальним та своєчасним в сучасних умовах.

Результати аналізу наукових публікацій. Окремі аспекти запобігання поширенню деструктивної інформації, пропаганди, дезінформації та маніпулювання свідомістю людини досліджували у своїх наукових працях: Б. Андрушків [1] В. Гурковський [2], М. Гребенюк [3], І. Кост [4], Р. Черниш [5], В. Брижко [6] та інші фахівці. Проте останні здобутки зарубіжного досвіду у площині законодавчого забезпечення протидії фейкам та дезінформації, які активно поширює держава-агресор, ці науковці не розглядали, що зумовлює актуальність цієї публікації.

Метою статті є висвітлення кращих сучасних зарубіжних практик запобігання поширенню фейків та дезінформації в умовах масштабних гібридних загроз російського походження.

Виклад основного матеріалу. Термін "фейк" (англ. – *fake*) має багато значень. Досить часто фейком називають недостовірну або неправдиву інформацію чи інформацію, яка не відповідає дійсності. Фейк – це підробка, фальшивка, яка поширюється спільно для того, щоб дезорієнтувати та дезінформувати аудиторію. Загалом термін "фейкові новини" зарубіжні законодавства тлумачать як повністю або частково вигадану інформацію про суспільні події, явища, інформацію про певних публічних осіб, яка подається у засобах масової інформації (далі – ЗМІ) під виглядом справжніх журналістських матеріалів.

Головна мета фейкових повідомлень як інструментарію інформаційної війни – посіяти сумніви й переконати аудиторію в правдивості поданої інформації.

Завдання поширення фейку полягає у тому, щоб: дезінформувати цільову аудиторію; пропагувати власне бачення, політику чи позицію; викликати агресію; похитнути позицію та переконання певного індивідуума та змусити його засумніватися; посіяти паніку та панічні настрої, невпевненість у завтрашньому дні; змінити уставлену думку аудиторії; спонукати до певної дії, активності; зацікавити аудиторію або переконати її за допомогою вигаданих фактів; залякати аудиторію тощо.

За методом поширення розрізняють масмедійні фейки (які створюють спеціально для ЗМІ і через них поширюються) і мережеві чутки (коли поширюють чиюсь вигадку через соціальні мережі).

За формою фейкова інформація може бути фотофейком, відеофейком і фейковим журналістським матеріалом.

Фейкову інформацію у соціальних мережах можна умовно поділити на декілька типів, залежно від їхнього завдання: фейки, які сіють паніку серед людей; фейки, які розпалюють міжнаціональну (расову, релігійну чи соціальну) ворожнечу, ксенофобію; фейки, які поширюють хибні думки, для того, щоб заплутати аудиторію; фейки, які маніпулюють свідомістю; фейки, які рекламують когось або щось; фейки, які приносять прибутки від їхнього поширення (жовта преса); фейки, які заплямують чиюсь репутацію; фейки, які мають розважальних характер.

Чисельні приклади маніпуляції фактами, дезінформація та фейки, які поширюються усіма можливими способами та засобами, хакерські атаки та сайти органів державної влади і втручання в електронні виборчі системи стали предметом обговорення не лише світових ЗМІ, а також й політичного керівництва США та ЄС.

Таким чином, західні суспільства почали не тільки викривати пропагандистські вкидання та фейки з боку РФ, а й визнали необхідність визначення правових засад протидії деструктивному впливу держави-агресора й почали створювати відповідні інституції та ухвалювати відповідні законодавчі ініціативи. Поширення чуток та неправдивої інформації на широкий загал у сучасному світі стало не лише буденністю, а й загрозливою реальністю, яка може заподіяти серйозну шкоду різним інтересам суспільства, людини та держави. Російська Федерація активно розвиває свої спроможності в цьому напрямку. В Європі вже неодноразово заявляли, що Кремль займається маніпуляціями, диверсіями й проводить різні операції в інформаційній площині для того, щоб дестабілізувати ситуацію в ЄС та США.

В ЄС з метою виявлення фейків та дезінформації, координації зусиль для її викриття була утворена структура "East StratCom Task Force". Цей інструмент допоміг краще зрозуміти тактику і техніку державних і недержавних гравців в сфері дезінформації і починати діяти проактивно.

Слід вказати, що країни Балтії визнані світовою спільнотою лідерами серед країн ЄС у сфері боротьби зі спробами втручання в їхню внутрішню політику та кампаніями з дезінформації, розгорнутими РФ. Ці країни постійно стикаються з кремлівською пропагандою і були вимушені їй протистояти. Однією з таких країн є Литва, чия ситуація на інформаційному полі дуже схожа з тією, що склалась у нашій державі. Росія за допомогою так званих "активних засобів" намагається похитнути державність Литви та скомпрометувати будь-які прояви протистояння їй. Кремлівські пропагандисти відхрещуються як від окупації Литви, так й окупації інших держав Балтії.

Серед визначальних чинників, які дозволили країнам Балтії, стати прикладом для інших держав, є розробка низки стратегічних документів (на рівні урядів), планів боротьби з поширенням фейків та дезінформації, а також масштабне фінансування протидії російській пропаганді та розповсюдженню фейкових новин. Так, наприклад, через підконтрольні Росії ЗМІ поширювалася тенденційна інформація про поширення актів антисемітизму та ксенофобії в Литві. Там такі матеріали ніхто всерйоз не сприйняв. Проте коли вони продублювались в медіа інших країн, зокрема в ізраїльській пресі, Литва відчула на собі потужний тиск.

У звіті з національної кібербезпеки, опублікованому Міністерством оборони Литви за 2020 рік, основним джерелом дезінформації у країні визнані ЗМІ, які "контрольовані кремлівським режимом". Зокрема вказується на зростання складних проросійських кібератак. Йдеться не лише про технологічний рівень, а й про особливості поширювального контенту. Подібний контент формує імідж Литви як ненадійної та ворожої держави, розпалює національну ненависть та ворожнечу. При цьому автори не соромляться поширювати фальсифікації, маніпулювати перекрученими фактами, спотворювати зміст заяв чи коментарів публічних осіб, можливостями здійснення відеомонтажу та виготовленням продукції "під прикриттям" інших осіб та установ. З метою протидії такому тиску новинні медіа Литви об'єднуються, намагаючись спільно протистояти російським фейкам. Адже суть цих фейків полягає в тому, що навиворіт перекручується зміст того, що ти бачиш і з чим здійснюється боротьба. Стратегія великої брехні працює, оскільки під час війни, пандемії, кризи брехня стає ефективною, а на цьому фоні системна робота зі спростування дезінформації – заходи постфактум, які не вирішують проблему, що склалася.

На жаль, на розвінчування фейків потрібно набагато більше часу, ніж на їх створення. Шалена швидкість, з якою неправдива інформація поширюється в світі, вражає. Розвиток Інтернету тільки сприяє її активному поширенню, хоча структура та

принципи відпрацьовані ще десятиріччя тому. Наразі створення фейків є питанням не стільки технологій, хоча можна підробити й фото і навіть відео, скільки своєрідним видом творчості. Фейки сьогодні найсерйозніша загроза для сучасних журналістів, якій вони мають протистояти. Маючи швидкий доступ до великого обсягу інформації, громадяни Литви її практично не аналізують. Більш того, динамічно зростає кількість людей, які нівелюють значення інформаційних ресурсів. Кожного року в Литві з'являється новий телеканал, який має свій сайт та транслює інформацію у вигідному йому ракурсі.

У Франції в листопаді 2018 року Національна Асамблея ухвалила Закон у сфері боротьби з інформаційними маніпуляціями, який наділяє національний регулятор широкими повноваженнями щодо припинення поширення каналами або соціальними мережами дезінформації без рішення суду у випадку, коли є підозра, що вони впливають на свідомість суспільства. Під дію цього Закону також підпали російські пропагандистські канали, які транслюються на території Франції. Національний регулятор (Вища аудіовізуальна рада Франції) під час виборчої кампанії зможе призупиняти і навіть відкликати ліцензії мовників, що зазнають іноземного впливу, якщо регулятор вважатиме, що це ЗМІ поширює фейкову інформацію. Інтернет-платформи та соціальні мережі протягом виборчої кампанії будуть змушені розкривати особи рекламодавців і суми сплачених ними коштів за поширення контенту. Передбачено прискорену процедуру розгляду в суді питань про припинення вірусного поширення неправдивих новин у період виборчої кампанії.

26 вересня 2018 року у Німеччині опубліковано Кодекс практик протидії дезінформації в мережі Інтернет. Цей Кодекс являє собою перелік зобов'язань, які платформи та асоціації, що представляють рекламодавців та рекламну галузь, добровільно застосовують для боротьби з дезінформацією та пропагандою.

У грудні 2018 року Великобританія та Польща домовилися про створення спільного підрозділу для протидії російській дезінформації, проведення щорічних консультацій з метою мінімізації ворожої діяльності Москви у медіа сфері. У Великобританії Парламентський комітет розробив та схвалив Закон з протидії фейкам.

В Італії теж планується вирішувати проблему поширення фейкової інформації в соцмережах.

В державах-членах ЄС розпочали активно розроблятися саме правові механізми протидії поширенню фейкової інформації [5, с. 126]. Вже більшість держав-членів ЄС переймаються питаннями законодавчого регулювання відповідальності за дифамацію у медіа. Типовими законодавчими механізмами боротьби з фейками та дезінформацією вважаються: проведення моніторингу соціальних медіа; залучення громадських організацій для викриття фейків; інформування про виявлену фейкову інформацію; притягнення до відповідальності осіб, які виготовили або поширювали таку інформацію; підвищення рівня медіаграмотності усіх категорій населення тощо.

Аналіз законодавства ЄС щодо боротьби з фейками надає змогу констатувати, що посилення такої боротьби в інформаційній сфері та протидія поширенню деструктивної та недостовірної інформації залишаються прерогативою цивільного законодавства – мова не йде про "криміналізацію" поширення фейків. У той же час Європейська Комісія запровадила жорсткі санкції проти суб'єктів, які поширюють дезінформацію, а також наполягатиме на більш жорсткому механізмі нагляду за онлайн-платформами. Підставами для цього стала доповідь оперативної групи зі стратегічних комунікацій EastStratCom, що відстежує дезінформацію з боку Росії. Група виявила понад 500 випадків прокремлівської дезінформації щодо CoVID-19 за рік і понад 10 тисяч

прикладів прокремлівської дезінформації з моменту початку моніторингу в 2015 році. У 2021 році під санкції потрапили РФ та КНР через поширення фейків.

Одночасно з вказаним, є країни які запровадили кримінальну відповідальність за поширення недостовірної інформації та фейків. Так, у Малайзії діє Закон про протидію фейковим новинам, яким передбачається покарання у виді позбавлення волі на строк до шести років і $123 тис. штрафу за поширення і створення новин, інформації, даних або доповідей, помилкових повністю або частково. Цей Закон поширюється не тільки на фізичних осіб, а також й на провайдерів. При цьому під дію Закону також підпадають не тільки громадяни, а й публікації, які створюються в інших країнах за участю малайзійців. Правозастосовна практика містить приклади притягнення до кримінальної відповідальності громадян, які через Інтернет критикували процес виборів у країні.

Парламент Сінгапуру схвалив Закон, спрямований на боротьбу з фейковими новинами. Законом передбачено кримінальну відповідальність за умисне поширення фейкової інформації у вигляді позбавлення волі строком на 10 років і накладання штрафу у розмірі до 1 млн. сінгапурських доларів. Також відповідно до Закону державні органи можуть зажадати внесення винною особою правок або видалення контенту. Крім того, органам державної влади надається право блокувати сайти, які поширюють недостовірну суспільно значиму інформацію.

Кримінальний кодекс Казахстану було доповнено статтею 274 “Поширення завідомо неправдивої інформації”, яка передбачає санкцію позбавлення волі до 7 років. Під істотною шкодою розуміється: порушення конституційних прав та свобод людини й громадянина, порушення штатної роботи організацій та установ, державних органів, провокування зриву важливих військових заходів, боєздатності військових частин тощо. Обтяжуючими обставинами є: поширення подібної інформації групою осіб або з використанням службового становища, що спричинило великі збитки, або з використанням мережі Інтернет чи ЗМІ. При цьому наслідки не є обов’язковою ознакою даного складу злочину.

В Єгипті діє Закон, який надає владі цієї країни право блокувати аккаунти в соціальних мережах та притягувати до відповідальності журналістів за поширення фейкових новин. Відповідно до цього законодавчого акта користувачі соціальних мереж, які мають понад 5 тис. передплатників, уважаються окремими ЗМІ і можуть піддаватися кримінальному переслідуванню за поширення неправдивих новин, фейків, підбурювання до протестних настроїв та іншої протиправної поведінки. Контролювати дотримання вимог закону і проводити оцінку контенту має парламент Єгипту.

У тоталітарних країнах світу регулювання соціальних мереж і боротьба з фейками – дуже “тонке” питання, яке може бути розцінено як обмеження свободи слова та розправу з політичними опонентами.

Висновки.

У світі існує два підходи до сфери відповідальності за поширення фейкової інформації. Перший (європейський) передбачає цивільно-правове врегулювання відповідальності за дифамацію у медіа та відповідальність за поширення фейків. Другий – кримінальне переслідування за поширення такої деструктивної інформації як приватних осіб, так і ЗМІ.

Загальновідомим є той факт, що будь-яка, навіть позитивна фейкова інформація в результаті має негативний вплив та є загрозливим явищем у медіа просторі. За таких умов, РФ активно використовує пропаганду та фейки як провідний інструмент своєї зовнішньої політики з метою негативного та деструктивного впливу на політику інших країн світу.

Взагалі дезінформація визначається різноманітними фейками, які поширюються державою-агресором з метою повалення конституційного ладу в Україні. Як вважаємо, для України позитивним аспектом є те, що внаслідок заборони російських джерел дезінформації – соцмереж, Інтернет-серверів, телеканалів – рівень довіри до російського ТБ серед українців зменшився.

Сьогодні дуже складно протидіяти кремлівської пропаганді та дезінформації внаслідок засиль проросійських лобі у різних сферах інформаційної життєдіяльності, зокрема у державах-членах ЄС. Разом з цим у провідних державах світу здійснюються подальші пошуки нормативних механізмів протидії фейкам, дифамації у соціальних медіа.

Що стосується боротьби з поширенням дезінформації, необхідно чітко розрізняти різні типи феномену фейкових новин: політичну пропаганду, журналістські помилки, сатиру, вигадані новини з метою економічної вигоди. Проте універсальних рецептів боротьби з фейками досі не існує. Загальновизнаним залишається орієнтація на то, що еталоном захисту від деструктивної пропаганди та маніпуляції свідомістю людини є передусім міцність демократичних традицій кожного суспільства.

Одним з можливих варіантів протидії цьому явищу може бути блокування таких фейків. Водночас, щоб застосовувати такий серйозний важіль, необхідно науково дослідити та розробити критерії визначення дезінформаційного впливу.

У 2021 році Міністерство культури та інформаційної політики України визначило два ключові пріоритети своєї роботи у сфері інформаційної політики та безпеки: посилення протидії дезінформації та проект з медіаграмотності. Навчання та просвіта користувачів на предмет того, як дезінформація працює, на що фейки спрямовані, яким чином відбувається маніпуляція – це є значно важливіше, ніж безпосереднє спростування конкретних фейків. З точки зору медіаграмотності важливі питання полягають у тому, яким чином розуміти роль медіа, як вони працюють, чому медіа можуть говорити неправду з поширенням цієї інформації на різні цільові аудиторії.

Україні доцільно на системній основі впроваджувати комплекс заходів з попередження негативної діяльності окремих закордонних інформаційних структур, медійних та навколо медійних організацій, провайдерів програмних послуг (РФ, Республіка Польща, Угорщина, Румунія), які намагаються сформувати механізми впливу на суспільно-політичну ситуацію в Україні шляхом створення позицій в інформаційному просторі держави, використання вітчизняних ЗМІ, мережі Інтернет, видавничо-поліграфічної та рекламної галузей, власних інформаційних можливостей для здійснення антиукраїнських інформаційних акцій, інспірування в середовищі національних меншин автономістських та сепаратистських настроїв, поширення деструктивної інформації в інтересах іноземних держав. Також необхідним є своєчасне виявлення, недопущення та припинення, у т.ч. шляхом проведення заходів профілактичного характеру, підготовки та поширення у вітчизняних ЗМІ, друкованих виданнях, мережі Інтернет (видання, соціальні мережі, блогосфера) інформаційних матеріалів, поліграфічної продукції із закликами до вчинення терористичних актів, насильницької зміни чи повалення конституційного ладу, захоплення державної влади, порушення територіальної цілісності, а також закликів, які розпалюють національну, расову чи релігійну ворожнечу, пропагують ідеї расизму, ксенофобії та екстремізму або інші протиправні діяння.

З метою нівелювання факторів негативного інформаційного впливу на формування суспільної думки і масової свідомості доцільно впроваджувати заходи з попередження та мінімізації наслідків вірогідних деструктивних процесів у державі, спричинених негативною інформаційною діяльністю окремих представників вітчизняних навколо

медійних громадських організацій, мас-медійних структур, журналістських професійних спілок та рухів, запобігання їх впливу на розвиток суспільно-політичної, соціально-економічної, етноконфесійної ситуації в державі, особливо напередодні та під час проведення в Україні суспільно важливих заходів, одним з найбільш важливих з яких є святкування 30-річчя незалежності України.

Використана література

1. Андрушків Б., Кирич Н., Погайдак О., Гагалюк О. Культосвітня компонента в сфері управління як засіб попередження вульгаризму у взаємовідносинах та поширення фейків в ЗМІ або важелі посилення економічної безпеки в державі. *Вісник економічної науки України*. 2019. № 2 (37). С. 214-222.

2. Гурковський В. Механізми використання дезінформації в умовах російської гібридної агресії. *Освіта регіону.* URL: http://social-science.com.ua/article/1393.

3. Гребенюк М.В., Леонов Б.Д. Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС. *Правова інформатика*. № 2(29)/2019. С. 82-89.

4. Кост І. Російська пропаганда в Україні як інформаційна складова конфлікту. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3332/3010

5. Черниш Р. Правовий досвід країн європейського союзу у сфері протидії поширенню фейкової інформації. *Підприємництво, господарство і право*. 2019. № 10. С. 123-128.

6. Брижко В.М. Маніпулювання свідомістю (в кн.: “е-боротьба в інформаційних війнах та інформаційне право”: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. С. 41-82).

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

УДК 342.951

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

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ ПРОТИДІЇ РОСІЙСЬКІЙ ІНФОРМАЦІЙНІЙ ЕКСПАНСІЇ ТА ПРОПАГАНДІ В СУЧАСНОМУ СВІТІ

Анотація. *Розглянуто гібридні інформаційні загрози, які поширює РФ в сучасних умовах. Визначено масштаби деструктивної діяльності та дезінформації з боку РФ.Узагальнено механізми поширення російської пропаганди та дезінформації. Визначено сучасні інституційні засади протидії російським фейкам та пропаганді. Окреслено засади функціонування центрів протидії російській пропаганді та дезінформації у США та деяких країнах ЄС. Визначено компетенцію та повноваження українського Центру протидії пропаганді та дезінформації. Деталізовано шляхи удосконалення діяльності вітчизняного Центру протидії пропаганді та дезінформації в умовах російської інформаційної агресії проти України.*

Ключові слова: *державна інформаційна політика, пропаганда, дезінформація, засоби масової інформації, фейки, національна безпека, деструктивна діяльність, гібридні загрози.*

Summary. *The hybrid information threats distributed by the Russian Federation in modern conditions are considered. The scale of destructive activity and misinformation on the part of the Russian Federation is determined. The mechanisms of spreading Russian propaganda and misinformation are generalized. Modern institutional principles of counteraction to Russian fakes and propaganda are determined. The principles of functioning of the centers of counteraction to the Russian propaganda and disinformation in the USA and some EU countries are outlined. The competence and powers of the Ukraine`s Center for Countering Propaganda and Disinformation have been determined. The directions of improvements of the activities of the domestic Center for Combating Propaganda and Disinformation in the context of Russian information aggression against Ukraine are detailed.*

Keywords: *state information policy, propaganda, misinformation, mass media, fake, national security, destructive activity, hybrid threats.*

Аннотация. *Рассмотрены гибридные информационные угрозы, которые распространяет РФ в современных условиях. Определены масштабы деструктивной деятельности и дезинформации со стороны РФ. Обобщены механизмы распространения российской пропаганды и дезинформации. Определены современные институциональные основы противодействия российским фейкам и пропаганде. Обозначены основы функционирования центров противодействия российской пропаганде и дезинформации в США и отельных странах ЕС. Определено компетенцию и полномочия украинского Центра противодействия пропаганде и дезинформации. Детализированы направления усовершенствования деятельности отечественного Центра противодействия пропаганде и дезинформации в условиях российской информационной агрессии против Украины.*

Ключевые слова: *государственная информационная политика, пропаганда, дезинформация, средства массовой информации, фейк, национальная безопасность, деструктивная деятельность, гибридные угрозы.*

Постановка проблеми. Держава-агресор вже 8-ий рік поспіль продовжує активно здійснювати інформаційну агресію по відношенню до України, спрямовану як на дестабілізацію внутрішньополітичної й соціальної ситуації, так на приниження міжнародного іміджу в світі, зокрема, на двосторонні та багатосторонні відносини

з провідними державами-партнерами. В умовах тривалої військової агресії РФ одну з найбільших загроз національній безпеці для України становить антиукраїнська пропагандистська інформаційна експансія, спрямована на непряме втручання у внутрішні справи нашої держави, шляхом інформаційного впливу на громадську думку, в першу чергу, проросійськи орієнтованого населення АР Крим та Південно-східної частини країни. На даний час ситуація в національній інформаційній сфері достатньо складна, що, серед іншого, пов'язане як з значним інформаційним впливом російських медіа на населення, так і з технічними проблемами мовлення українських електронних засобів масової інформації в окремих регіонах нашої держави та у світі, в цілому. Зокрема, систематично проводяться РФ аналогії ситуації в державі, починаючи з кінця існування УРСР та протягом всього періоду її незалежності із сьогоднішньою суспільно-політичною ситуацією в Україні, акцентуючи увагу на наявності економічної кризи, роздільності етнічних народів, суспільній некерованості, необхідності зміни державного устрою, наголошується на можливих негативних наслідках виходу нашої країни з СНД, проблемах національних меншин і внутрішньо переміщених осіб, зростання протестних настроїв громадян, падіння соціального рівня життя тощо. Однією з основних тем, які поширюють проросійські інформаційні ресурси, є проблема т.зв. націоналізму – фашизму. Зокрема, продовжується акцентування уваги глядачів й читачів на, нібито, використанні українською владою націоналістичних організацій для тиску на політичних опонентів, збільшенні проявів антисемітизму на території України, утисків прав національних меншин з боку української влади та учасників націоналістичних рухів, утисків прав російськомовного населення України.

Також з метою демонстрації т.зв. реальної ситуації в Україні, оприлюднюються матеріали інтерв'ювання підконтрольних представників єврейських, румунських, польських, угорських, вірменських, проросійських й інших громадських структур, які "підтверджують утиски своїх прав й свобод". Водночас, слід відзначити, що матеріали щодо "радикалізації української держави й активізації розвитку фашистсько-націоналістичних рухів в Україні" продовжують оприлюднюватися через підконтрольні РФ інформаційні ресурси у США, Польщі, Угорщині та інших країнах Європи. В ефірі підконтрольних РФ інформаційних ресурсів систематично оприлюднюються матеріали, які демонструють зубожіння українського населення на фоні збагачення та фінансового благополуччя бізнес-структур олігархів. Однією з тем, яку постійно поширює РФ через підконтрольні медіа-ресурси, є популяризація ідей автономізму, зокрема, посилення фінансової та політичної незалежності регіонів України від столиці у ручному режимі тощо. Таким чином, в умовах поточної зовнішньополітичної та внутрішньої ситуації в Україні, військової агресії з боку РФ надзвичайно важливе значення має ситуація в інформаційному просторі нашої держави.

За таких умов можна констатувати те, що з метою відновлення свого впливу в Україні Російська Федерація, продовжуючи гібридну війну, системно застосовує для цього політичні, економічні, інформаційно-психологічні важелі та засоби. Деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює соціальну ворожнечу, провокує конфлікти, підриває суспільну єдність. Відсутність цілісної державної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози. Тобто масштаби російської пропаганди та дезінформації постійно збільшуються, набираючи обертів, що потребує розробки інституційних та організаційно-правових механізмів запобігання таким деструктивним проявам.

Результати аналізу наукових публікацій. Механізми запобігання поширенню РФ деструктивної інформації, пропаганди та дезінформації досліджували у своїх наукових працях: В. Гурковський [1], М. Гребенюк [2], У. Коруц [3], І. Кост [4], І. Малик [5] та інші фахівці. Проте висвітлення останніх здобутків щодо інституційного забезпечення заходів протидії російській інформаційній пропаганді та фейкам, які поширює держава-агресор, вказані науковці не розглядали, що посилює актуальність цього наукового дослідження.

Метою статті є висвітлення як вітчизняних, так і зарубіжних здобутків щодо інституційного забезпечення заходів протидії російській інформаційній експансії та пропаганді у сучасному світі в умовах глобального геополітичного протиборства.

Виклад основного матеріалу. У сучасному світі інформаційний простір став місцем справжніх баталій за думки, переконання і настрої громадян. Події останніх років переконливо свідчать, що в арсеналі російської гібридної війни саме пропаганда і дезінформація належать до головної рушійної сили. В сучасних умовах кремлівська машина пропаганди та дезінформації працює на нових технологічних платформах і продовжує динамічно зростати як в РФ, так і на міжнародному рівні. Іншими словами, це є нова форма боротьби на інформаційному просторі XXI століття. РФ, виходячи із власних амбіцій, прагне послабити ті країни (у т.ч. Україну), які вважає своїми супротивниками, обрушуючи на цільову аудиторію потоки брехні, намагаючись підірвати віру громадськості в сумлінне державне управління, безпеку і оборону, незалежні засоби масової інформації тощо. За таких умов, кожна держава світу переймається питаннями методологічного та інституційного забезпечення протидії таким спробам.

Розглядаючи гібридні загрози інформаційній безпеці нашої держави з точки зору геополітичних спрямувань суміжних з Україною держав, насамперед РФ, необхідно відзначити вкрай негативну тенденцію до збільшення інформаційних матеріалів із відвертою антиукраїнською спрямованістю та упередженим висвітленням фактично усіх внутрішніх і зовнішніх процесів, які відбуваються як в Україні, так і на міжнародній арені за участю нашої держави. Фіксується намагання шляхом пропаганди створити власне ідеологічне та психологічне підґрунтя в російськомовному середовищі України, що є необхідною передумовою для реалізації своїх зовнішньополітичних намірів для повернення України у т.зв. “російську зону впливу”.

В сучасних умовах залишається високий рівень зовнішніх загроз вітчизняному інформаційному простору України, викликаних активною інформаційно-пропагандистською експансією РФ. Ведення РФ інформаційної війни одночасно з прямою військовою агресією є важливим елементом гібридної війни проти України. Таким чином, здійснюються спроби через інформаційну сферу впливати на процеси в нашій державі, підривати авторитет легітимної української влади з метою деморалізації суспільства та посилення протестних настроїв. Викликає занепокоєння той факт, що останнім часом значно активізувалася діяльність інформаційних структур РФ, яка спрямована на підтримку проросійської орієнтації частини населення України, сепаратистських настроїв в окремих регіонах держави, лобіювання інтересів невизнаних “ДНР” та “ЛНР”.

Антиукраїнська інформаційна кампанія реалізується російською стороною за низкою напрямів, зміст яких передбачає: популяризація ідей федеративного державного устрою України як альтернативи розпаду держави; забезпечення безперервного потоку маніпулятивної інформації щодо подій в Україні, на її окупованих територіях, та в світі; стимулювання антивоєнних настроїв та рухів; провокування автономістських настроїв на Закарпатті, Буковині, Бессарабії, Слобожанщині, Галичині, регіональних громадських

рухів під відповідними гаслами; внесення розколу в середовище українських правлячих кіл, у т.ч. шляхом публікації провокаційних матеріалів, критики центральних органів влади, які "ігнорують інтереси регіонів", компрометації громадсько-політичних діячів, інспірування масових протестів; створення в Україні підконтрольних РФ громадських структур під прикриттям представництв європейських організацій для проведення активної роботи в інформаційно-аналітичній сфері в геополітичних інтересах РФ.

Безпосередньо в РФ реалізація антиукраїнських акцій здійснюється, передусім, через використання соціальних мереж та підконтрольних телевізійних ЗМІ (телеканали "ОРТ", "LifeNews", "НТВ" та ін.), які поширюють інформацію тенденційного характеру. Діяльність закордонних неурядових структур і їх представництв в Україні, які підтримують РФ, спрямовується на: здобування та поширення інформації для дискредитації органів державної влади; погіршення іміджу країни на міжнародній арені; формування громадської думки в інтересах іноземних держав. За таких умов, актуальним для будь-якої країни світу є запровадження комплексу заходів з метою адекватного реагування на відповідні виклики та формування власної наступальної інформаційної політики.

В той же час, у поточному році очікується розширення мережі контактерів з числа проросійськи налаштованих політичних експертів та громадських діячів, які б коментували події в Україні в інтересах пропаганди держави-агресора, створюючи необхідну картинку для споживачів – глядачів телеканалів та читачів інформаційних ресурсів. Загалом при проведенні відповідної деструктивної діяльності Російської Федерації проти України будуть й надалі використовуватись як реальні проблеми, перш за все, в соціальній та економічній галузі, так і політичні кризові ситуації, в т.ч. у контексті повного знецінення національної валюти, вичерпання нашою державою власних валютних й інших фінансових резервів, небажання міжнародних структур надавати кошти у необхідних обсягах через незадовільний стан реалізації державних реформ, зокрема, владних інститутів й антикорупційної системи тощо. Продовжуватимуть здійснюватись інформаційні заходи з акцентування уваги глядачів та читачів на необхідності відновлення торгівельно-економічних й інших зв'язків з Росією, як єдиним "надійним партнером, який зацікавлений у добробуті українського населення" тощо.

Актуальним засобом впливу на формування громадської думки залишаються друковані засоби масової інформації. Зокрема, вони активно використовуються на території, підконтрольній сепаратистам "ДНР" та "ЛНР". До найбільш популярних належать наступні газети: "Новороссия" (друкується у типографії "Новый мир", головний редактор – Д. Корецький); "Вестник Новороссии"; "Новороссийский курьер"; "Республика" (офіційний друкований орган "ЛНР"); "XXI век" і "Жизнь Луганска" (видаються за підтримки "військової комендатури ЛНР"); "Народная газета" (використовується для легітимізації керівництва "ДНР"); "Народный фронт Новоросии" (створена за підтримки громадського руху "Новоросия", лідер − П. Губарев); "Свободный Донбасс" (створена за підтримки військових кореспондентів при штабі "ДНР"). У зв'язку із викладеним слід очікувати, що діяльність підконтрольних РФ закордонних неурядових структур та їх представництв в Україні, надалі спрямовуватиметься на здобування інформації для дискредитації органів державної влади, погіршення іміджу країни на міжнародній арені, формування громадської думки в інтересах іноземних держав. Враховуючи спектр наявних викликів та загроз, які динамічно поширює держава-агресор, світова спільнота переймається питаннями інституційного забезпечення заходів з метою протидії російській деструктивній діяльності у глобальному медіа-просторі, мінімізації гібридних загроз інформаційного характеру.

Так, наприклад, в США у 2018 році було утворено Центр глобальної взаємодії для боротьби з російською інформаційною кампанією за такими напрямками як: залучення передових технологій з метою своєчасного виявлення іноземних кампаній з дезінформації; аналіз іноземної аудиторії, найбільш схильної до дезінформації; розвиток партнерських відносин з ключовими фігурами на місцевому рівні з метою розробки контенту для найбільш вразливої від фейків аудиторії тощо. Загалом в ЄС також існує Центр протидії дезінформації, створений ще у 2015 році. У фокусі його уваги на першому плані – російська пропаганда та фейки. Невипадково 25 квітня 2018 року ПАРЄ ухвалила резолюцію про протидію російській пропаганді на рівні ЄС, згідно з якою державам-членам Ради Європи рекомендується створити власні органи (observatories) для відстеження фактів поширення дезінформації і фейків російського походження.

З початку 2017 року офіційно розпочав свою діяльність Центр протидії тероризму та гібридним загрозам при Міністерстві внутрішніх справ Чеської Республіки. Його створенню передували перегляд стратегічних підходів НАТО щодо реагування на нетрадиційні способи ведення війни, а також схвалення Єврокомісією стратегії боротьби з гібридними загрозами та сприяння стійкості ЄС, яка стала доповненням програми розширення співробітництва з Північноатлантичним альянсом. У рамках реалізації стратегії було заплановано створення загальноєвропейського центру для збору та аналізу інформації щодо гібридних загроз. Основною метою діяльності Центру є розвінчування міфів і дезінформації з боку Російської Федерації. Частково цей центр провадить публічну освітню роботу, тобто, має публічні акаунти в соцмережах, де описуються ворожі наративи, приклади дезінформації. Також там є фахівці, які аналізують хто і яким чином, через які вебсайти, через які ЗМІ, через яких людей розповсюджує інформацію. Центр тісно співпрацює зі спецслужбами й іншими правоохоронними органами.

У Фінляндії з 2017 року розпочав роботу Центр по боротьбі з гібридними загрозами. Серед гібридних загроз засновники центру виділяють, серед іншого, поширення неправдивої інформації, атаки проти інформаційних систем, а також інші види атак за допомогою сучасних технологій.

У Польщі – державі, яка є членом ЄС та НАТО, у 2017 році було утворено неурядову організацію, яка займається питаннями виявлення та протидії російській пропаганді – фундація Центр аналізу пропаганди та дезінформації. Ця структура є першою такого роду інституцією у Польщі, діяльність якої спрямована на системний аналіз та ідентифікацію загроз інформаційного характеру у польському інформаційному просторі. Також у Міністерстві закордонних справ Польщі є команда експертів, які здійснюють боротьбу з історичними дезінформаціями з боку РФ.

За прикладом Польщі, Україна створила державну структуру аналогічного формату. На виконання положень Стратегії національної безпеки України [6] з урахуванням загроз інформаційній безпеці та масштабів агресивної інформаційної експансійної політики РФ проти України, політичне керівництво вчасно прийняло рішення щодо необхідності утворення Центру протидії дезінформації, який інституційно був створений рішенням РНБО України від 11 березня 2021 року, яке було введене в дію Указом Президента України від 19 березня 2021 року [7]. Цим Указом [8] було затверджено положення про Центр протидії дезінформації, який відповідно до його засад його функціонування є робочим органом Ради національної безпеки і оборони України. До його основних ключових завдань належить: здійснення заходів з протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері; посилення та забезпечення інформаційної безпеки держави; виявлення та протидії

дезінформації; протидія пропаганді, деструктивним інформаційним впливам і кампаніям; запобігання спробам маніпулювання громадською думкою тощо.

Як вважає Президент України, у майбутньому Центр має стати міжнародним хабом протидії дезінформації та пропаганді в усьому світі. Створення такого хабу має допомогти зосередити зусилля із залученням наших західних партнерів, досвіду спеціалістів з країн, які є нашими союзниками. Це дозволило би ефективно відпрацьовувати ті маніпуляції і фейки, які поширює держава-агресор. Україна не може діяти симетрично Кремлю і створювати армію ботів, які будуть готувати і розповсюджувати певні меседжі з деструктивним пропагандистським контентом.

Висновки.

Росія є та залишається основним джерелом дезінформації у світі. Ціла низка досліджень вказує, що більшість дезінформацій, пропагандистських кампаній проводяться саме з боку РФ. Звичайно, це все почалося після агресії проти України у 2014 році. Власне, тільки після цієї агресії центри з протидії дезінформації й почали на постійній основі створюватися у державах ЄС та США. Такі центри займаються висвітленням того, що є фейками і що є дезінформацією. Як у світових, так і національних масштабах, для України РФ виступає першою загрозою, у тому числі й в інформаційному просторі. Російська пропаганда дуже добре продумана і цілеспрямована. Щоб вистояти, потрібно запровадити свої методи боротьби, насамперед розповідати, яку небезпеку для демократичного світу сьогодні становить агресивна експансійна політика і пропаганда Росії. На цьому фоні, як вважаємо, в Україні зберігається високий рівень іноземної присутності в структурі вітчизняних ЗМІ, тенденційність спроб РФ впливати на внутрішні та зовнішньополітичні процеси в нашій державі. Зазначене вимагає розробки ефективних механізмів протидії загрозам, які спричиняють шкоду державним інтересам в інформаційній сфері. Крім того, аналіз оприлюднених матеріалів свідчить про активізацію поширення тенденційної та дискредитуючої інформації щодо діяльності офіційної влади України.

За таких умов вважаємо за доцільне адекватно реагувати на відповідні виклики та формування Україною власної наступальної інформаційної політики, у тому числі й в медіа-просторі закордонних держав з використанням потужностей й можливостей, кадрового потенціалу новоствореного Центру протидії дезінформації як робочого органу РНБО України. Також доцільно посилити контроль за діяльністю закордонних інформаційних структур та їх функціонерів, в першу чергу РФ. На постійній основі слід вживати дієвих заходів щодо: недопущення з їх боку здійснення антиукраїнської інформаційної діяльності; проведення інформаційних акцій через використання підконтрольних ЗМІ та вітчизняних журналістів; прискорення реалізації заходів, спрямованих на виявлення, попередження та припинення використання іноземними організаціями та їх функціонерами, радикально налаштованими представниками вітчизняних мас-медійних кіл на шкоду безпеці України; блокування поширення в ЗМІ та вітчизняному інтернет-просторі деструктивних матеріалів, що містять заклики до посягань на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни тощо.

Використана література

1. Гурковський В. Механізми використання дезінформації в умовах російської гібридної агресії. *Освіта регіону.* URL: http://social-science.com.ua/article/1393

2. Гребенюк М.В., Леонов Б.Д. Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС. *Правова інформатика*. № 2(29)/2019. С. 82-89.

3. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. *Підприємництво, господарство і право*. 2020. № 8. С. 334-339.

4. Кост І. Російська пропаганда в Україні як інформаційна складова конфлікту. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3332/3010

5. Малик І. Механізми протидії негативним впливам інформаційної пропаганди. *Humanitarian vision*. 2015. Vol. 1. Num. 2. С. 47-54. URL: http://nbuv.gov.ua/UJRN/hv_2015_1_2_10

6. 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. URL: https://www.president.gov.ua/documents/3922020-35037

7. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації" від 19.03.21 р. № 106. URL: https://www.president.gov.ua/documents/1062021-37421

8. Питання Центру протидії дезінформації: Указ Президента України від 07.05.21 р. № 187. URL: https://www.president.gov.ua/documents/1872021-38841

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

УДК 340.15(477)

МАНЬГОРА В.В., *кандидат юридичних наук, доцент,* доцент кафедри права Вінницького Національного аграрного університету.
ORCID: https://orcid.org/0000-0003-3812-3797.

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ УКРАЇНИ ПІД ВПЛИВОМ МІЖНАРОДНОГО ПРАВА

Анотація. *В статті досліджуються особливості реформування правової системи України під впливом міжнародного права. Визначено основні засоби зближення національних правових систем. Охарактеризовано основні напрями впливу міжнародного права на національні правові системи, такі як: зближення національних правових систем, уніфікація права, гармонізація права, діяльність міжнародних організацій, створення модельних законів. Визначено основні засоби зближення національних правових систем. Розроблено пропозиції щодо реформування правової системи України під впливом міжнародного права.*

Ключові слова: *національна правова система, міжнародне право, уніфікація права, гармонізація права, міжнародні організації, модельні закони.*

Summary. *The article examines the features of reforming the legal system of Ukraine under the influence of the international law. The main means of convergence of the national legal systems are identified. The main directions of influence of the international law on national legal systems are described, such as: convergence of the national legal systems, unification of law, harmonization of law, activity of international organizations, creation of model laws. The main means of convergence of the national legal systems are identified. Proposals for reforming the legal system of Ukraine under the influence of international law have been developed.*

Keywords: *national legal system, international law, unification of law, harmonization of law, international organizations, model laws.*

Аннотация. *В статье исследуются особенности реформирования правовой системы Украины под влиянием международного права. Определены основные средства сближения национальных правовых систем. Охарактеризованы основные направления влияния международного права на национальные правовые системы, такие как: сближение национальных правовых систем, унификация права, гармонизация права, деятельность международных организаций, создание модельных законов. Определены основные средства сближения национальных правовых систем. Разработаны предложения по реформированию правовой системы Украины под влиянием международного права.*

Ключевые слова: *национальная правовая система, международное право, унификация права, гармонизация права, международные организации, модельные законы.*

Постановка проблеми. Сьогодні яскраво виражені світові тенденції глобалізації економіки, культури, політичної і правової сфер життя, які ведуть до взаємодії, взаємовпливу національних правових систем. Від якості і напрямів розвитку міжнародного права залежать національні правові системи, якість демократії, розвиток громадянського суспільства. Взаємодія правових систем під впливом міжнародного права має різні форми, але схожість значно збільшується, цьому сприяє рецепція цілих національних систем, в тому числі як вимушена, так і більш м'яка трансплантація (перенесення). Великий вплив на сучасний розвиток справляють нові технічні можливості – засоби транспорту, зв'язку, інформації. Посилення інтеграційних процесів у всіх сферах, зокрема в правовій, стало визначальною тенденцією сучасного життя.

Результати аналізу наукових публікацій. Проблему реформування правової системи України під впливом міжнародного права досліджували М.В. Буроменський, Г.К. Дмітрієва, Є.В. Житарєв, О.М. Іваненко, І.І. Лукащук, Н.М. Оніщенко, Є.Д. Стрельцова, В.Ю. Цюкало та інші. Є.Д. Стрельцовою у 2020 р. було захищено докторську дисертацію: "Теорія і практика уніфікації міжнародного права в умовах глобалізації (міжнародний та національно-правовий аспекти)". У дисертації вперше у вітчизняній науці міжнародного права обгрунтовано концепцію уніфікації міжнародного права як універсального механізму його сучасного розвитку та з'ясовано впливи міжнародно-правової уніфікації на українське законодавство.

Метою статті є визначення основних напрямків реформування правової системи України в сучасних умовах.

Виклад основного матеріалу. В сучасному праві визнано примат міжнародного права над національним правом країн. Ставлення України до питання про співвідношення національного та міжнародного права вперше було сформульоване в Декларації про державний суверенітет України 1990 р., де був проголошений "пріоритет загальновизнаних норм міжнародного права перед нормами внутрішньодержавного права" (ст. X) [1]. У Законі України "Про дію міжнародних договорів на території України" [2], а пізніше в Законі України "Про міжнародні договори України" ця норма Декларації була доповнена: "…укладені і належним чином ратифіковані Україною міжнародні договори становлять невід'ємну частину національного законодавства України і застосовуються у порядку, передбаченому для норм національного законодавства" [3]. Конституція України у ст. 9 закріпила: "Чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України. Укладання міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України" [4].

Особливості застосування в Україні суб'єктами внутрішнього права норм міжнародного права встановлені Конституцією та законами України. В Україні визнаються частиною національного законодавства норми міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. Це насамперед договори, ратифіковані Верховною Радою України.

За період незалежності Верховна Рада України ратифікувала, прийняла або дала згоду на приєднання до більш ніж 1000 міжнародних договорів. Зазначені договори стосуються питань політики, економіки, фінансів, отримання міжнародних позик і кредитів, захисту прав та свобод людини і громадянина, діяльності України в рамках міждержавних організацій, направлення контингентів Збройних Сил України до інших країн, допуску збройних сил іноземних держав на територію України тощо [5, с. 140].

Основними напрямами впливу міжнародного права на національні правові системи є: зближення національних правових систем, уніфікація права, гармонізація права, діяльність міжнародних організацій, створення модельних законів.

Процес зближення національних правових систем передбачає:

- розробку загальної політики державно-правового розвитку;
- здійснення заходів з метою подолання відмінностей;
- прийняття засобів з метою вироблення загальних, спільних юридичних правил зближення законодавств, коли визначається загальний курс держав в даній сфері, напрямки, етапи зближення, способи зближення.

Зближення правових систем відбувається не тільки між правовими системами однієї сім'ї, а між різними правовими сім'ями. Прецедентне право має вплив на правову систему України, після того як Україна вступила до Ради Європи 9 листопада 1999 року,

і громадяни України отримали право звертатися до Європейського суду з прав людини, який виносить прецеденти по скаргах.

23 лютого 2006 року був прийнятий Закон України "Про виконання рішень та застосування практики Європейського суду з прав людини", який гарантував, що рішення Суду є обов'язковим для виконання Україною. За даними Європейського суду з прав людини у 2019 році Україна входить в трійку лідерів за кількістю звернень. Частіше, ніж громадяни нашої країни, до Європейського суду з прав людини скарги подавали тільки громадяни Туреччини і Росії. Проти України подано 8833 скарги. Всього, з 1959 року проти України прийнято 1413 рішень. З них 572 стосуються права на справедливий суд, 429 – тривалості проваджень, 379 – права на свободу і безпеку і 358 – захисту власності [6].

Деякі рішення Європейського суду з прав людини спонукали Україну змінити національне законодавство та вдосконалити діяльність державних органів.

На думку Голови Комітету з міжнародного права Національної асоціації адвокатів України В. Власюка, "виконувати рішення – це не тільки виплачувати гроші заявнику. Це ще й вносити зміни до законодавства, а також спроби поміняти так звану адміністративну практику – правила функціонування держорганів. На жаль, іноді держава "копає сама собі яму", як у випадку зі справою "Юрій Іванов проти України", коли в результаті відверто популістської політики уряду були порушені Конвенційні гарантії пенсіонерів. Рішення уряду дозволило заощадити невеликі гроші тактично, але стратегічно призвело до тисяч задоволених скарг, в кожній з яких ЄСПЛ не тільки зобов'язав перерахувати пенсію скаржнику, але і виплатити йому компенсацію в розмірі 2 – 3 тисяч Євро" [6].

Вступ до Ради Європи в 1999 році також змусив Україну накласти мораторій на виконання смертних вироків і сприяв реформуванню кримінального права. 5 квітня 2001 року було прийнято Кримінальний кодекс України.

Зближення правових систем передбачає гармонізацію права. Гармонізація – це створення норм, адаптованих до національної правової системи, які нічим не відрізняються від інших норм національного права і застосовуються в загальному порядку. Гармонізація національних правових систем передбачає певну адаптацію національних законодавств до загальних міжнародних стандартів. Другий розділ "Права, свободи та обов`язки людини та громадянина" Конституції України від 28 червня 1996 року містить всі основні положення "Загальної декларації прав людини" від 10 грудня 1948 року, "Міжнародного пакту про громадянські та політичні права" від 16 грудня 1966 року, "Міжнародного пакту про економічні, соціальні та громадянські права" від 16 грудня 1966 року, "Конвенції про захист прав людини і основоположних свобод" від 4 листопада 1950 року.

В доктрині широко поширеною є думка, що уніфікація це створення (або введення в дію) в національному законодавстві уніфікованих норм, як з використанням міжнародно-правових засобів, так і в односторонньому порядку [7, с. 102].

Уніфіковані норми створюються з метою регулювання суспільних відносин в тих випадках коли не співпадають національні законодавства. Уніфікація спрямована на полегшення міжнародно-правового співробітництва.

В другій половині XIX століття з'явилися перші спроби уніфікації права, які були викликані практичними потребами, зокрема розвитком торгівлі та міжнародних відносин.

Останнім часом зростає роль нового виду правових актів, які сприяють правовій уніфікації – модельних (рекомендаційних) законодавчих актів. Модельний закон це законодавчий акт рекомендаційного характеру, який є орієнтиром для розвитку та зближення національних законодавчих актів. Модельні закони є містком між нормами міжнародного права і національного права.

Модельний закон – це акт, який приймається або міжнародною організацією, або вищим законодавчим органом федеративної держави. Лисенко С. вважає, що в принципі такий закон не можна назвати законом у повному сенсі цього слова. Даний акт носить рекомендований характер і приймається він з метою уніфікації законодавства різних держав, які входять до міжнародної організації або суб'єктів федерації. Разом з тим, якщо модельний закон включає в себе базові принципи, то він повинен включатися до національного законодавства. Національні закони, які включають у себе основні положення модельного закону, повинні прийматися беззаперечно, але в окремих випадках вони також носять індивідуальний характер, тобто при їх прийнятті враховують національні особливості [8, с. 172].

Модельні закони поділяються на види які:

- приймаються законодавчим органом федерації для її суб'єктів;
- міждержавними об'єднаннями держав для держав-членів;
- міжнародними організаціями в якості правового зразка;
- розробляються вченими-юристами та спеціалістами і носять доктринальний характер [9, с. 172].

Розвиток законодавства федерацій на сучасному етапі спрямований на гармонізацію правових норм. В США до модельних законів відносяться передусім акти запропоновані Комісією з уніфікації права штатів, які потім приймаються законодавчими органами штатів [10, с. 84]. Вироблення Модельного кримінального кодексу (англ. – *Model Penal Code*) США проводилося Американським інститутом права з початку 30-х років минулого століття. Протягом 1962 – 1985 років нові кримінальні кодекси були прийняті в 34 штатах. Ще 8 штатів не отримали нові кодекси в результаті саботажу з боку легіслатур, які загальмували розгляд та прийняття проектів з різних причин. Втім, реальність дещо відрізнялася від сподівань співробітників Американського інституту права, адже правила новації Кодексу "втілювалися у життя" частково, так як жодна з легіслатур не прийняла Модельний кодекс в цілому використовувався як основа для розробки власних проектів кримінальних кодексів [11, с. 110-111].

В США були розроблені проекти модельних кодексів та законів таких як Модельний торговий Кодекс, Єдиний закон про арбітраж, Єдиний закон про охорону дитинства, Модельний закон про забезпечення угод, Уніфікований закон про організацію системи відставки державних службовців, Уніфікований закон про повторне використання землі з закинутими об'єктами промислової забудови та багато інших [12, с. 301].

Модельні закони приймалися в рамках Організації Об'єднаних Націй, Ради Європи, Європейського Союзу, Співдружності Незалежних Держав, Союзу африканських держав, Організації Американських держав, Асоціації держав Південно-східної Азії та інших міжнародних організацій.

З метою підтримки реформування та оновлення законодавства держав з арбітражної процедури, з тим щоб врахувати особливі риси та потреби міжнародного комерційного арбітражу, Комісією ООН з права міжнародної торгівлі (ЮНСІТРАЛ) розробила Типовий закон ЮНСІТРАЛ про міжнародний торговий арбітраж, схвалений Генеральною Асамблеєю ООН 11 грудня 1985 р. Його було рекомендовано державам як зразок для відповідних національних законів. Цим скористалися Австралія, Бахрейн, Бермудські Острови, Болгарія, Угорщина, Німеччина, Гватемала, Зімбабве, Єгипет, Індія, Іран, Канада, Кенія, Кіпр, Литва, Мальта, Мексика, Нігерія, Нова Зеландія, Оман, Перу, Російська Федерація, Сінгапур, Спеціальний адміністративний район Гонконг, Туніс, Україна, Шрі-Ланка, в рамках Об'єднаного Королівства Великобританії і Північної Ірландії: Шотландія, і в рамках Сполучених Штатів Америки – в Каліфорнії, Коннектикуті, Орегоні і Техасі.

24 лютого 1994 р. було прийнято Закон України "Про міжнародний комерційний арбітраж" [13]. Закон відображає досягнутий у всесвітньому масштабі консенсус щодо ключових аспектів практики міжнародного арбітражу, прийнятої у багатьох державах світу, які представляють усі регіони і володіють різними правовими та економічними системами.

Прикладом розробки науковцями модельного закону є "Базовий міжнародний податковий кодекс", який у 1992 році був розроблений в Гарвардському університеті. Даний кодекс був рекомендований державам як модельний закон і запропоновано на його основі формувати податкове законодавство [8, с. 173].

Загалом модельні закони найчастіше пропонуються для матеріального права, але вони не є рідкістю у процесуальному праві. Наприклад, у 1858 – 1859 рр. у Пруссії, Австрії обговорювали питання створення загальнонімецького Торгового кодексу.

Прикладом інтеграційних процесів у процесуальній правовій сфері є діяльність Ібероамериканського інституту цивільного процесуального права, створеного в 1957 р. Основна мета цього Інституту – уніфікація цивільного процесуального права в іспано- і португаломовних країнах. Одним із результатів його діяльності була розробка і прийняття в 1988 р. Модельного цивільного процесуального кодексу. У різному ступені ідеї Модельного кодексу були сприйняті в Уругваї, Коста-Риці, Колумбії, Перу, Мексиці, Аргентині, Португалії, Бразилії, Болівії, Венесуелі [14, с. 207]. Також в рамках Ібероамериканського інституту цивільного процесуального права схвалено ще тексти наступних модельних кодексів:

- Модельний кодекс з розгляду колективних (групових) позовів;
- Модельний кодекс судової етики;
- Модельний кримінальний кодекс [15, с. 55].

Влітку 1992 року створено проект модельного Цивільного кодексу для країн Латинської Америки в рамках Організації Американських держав.

Зближення правових систем передбачає певну адаптацію національних законодавств до загальновизнаних міжнародних стандартів. Це питання для країни, які намагаються вступити в загальноєвропейські структури, до Європейського Союзу.

16 вересня 2014 р. Верховна Рада України та Європейський Парламент синхронно ратифікували Угоду про асоціацію між Україною та ЄС. Почалася міжнародна договірно-правова уніфікація законодавства, в основі якої лежать акти ЄС, на які посилається Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27червня 2014 р. як на міжнародно-правову підставу адаптації, гармонізації та уніфікації українського законодавства з правом ЄС, однак вона значно більш масштабна за інші уніфікаційні заходи, в яких Україна бере участь [16, с. 30-31].

Для держав, які планують вступати до Європейського Союзу існує спеціальний збірник законів (*aquis communitaire*), тобто збірник принципів чи модельних законів, які кандидати повинні прийняти, інакше вони не можуть розраховувати на безпеку у складі співтовариства [8, с. 174].

Висновки.

Сучасна правова система реформується під впливом змін в міжнародному праві. За сучасного періоду розвитку системи національного права європейський вибір України став одночасно й рухом до стандартів реальної демократії, інформаційного, соціально-орієнтованого суспільства та ринкового господарства, що базуються на принципах верховенства права й забезпечення прав та свобод людини і громадянина. Система національного права наразі перебуває на стадії наближення та адаптації до системи права ЄС. На цій стадії важливою умовою є гармонізація законодавства з

правом ЄС та вироблення концептуальних положень щодо формування механізму взаємодії систем права ЄС та України і закріплення їх на законодавчому рівні, що дозволить належно сформувати адаптаційний механізм систем права України та ЄС.

Використана література

1. Про державний суверенітет України: Декларація Верховної Ради УРСР від 16.07.90 р. № 55-XII. URL: https://zakon.rada.gov.ua/go/55-12 (дата звернення: 04.06.2021).

2. Про дію міжнародних договорів на території України: Закон України від 10.12.91 р. № 1953-XII. URL: https://zakon.rada.gov.ua/go/1953-12 (дата звернення: 04.06.2021).

3. Про міжнародні договори України: Закон України від 29.06.04 р. № 1906-IV. URL: https://zakon.rada.gov.ua/go/1906-15 (дата звернення: 04.06.2021).

4. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 04.06.2021).

5. Цюкало В. Питання імплементації міжнародно-правових норм у правову систему України. *Слово національної школи суддів України.* 2013. С. 139-159.

6. Власюк В. Кількість скарг проти України до ЄСПЛ свідчить про неефективну роботу держорганів. URL: https://unba.org.ua/news/5141-kil-kist-skarg-proti-ukraini-do-espl-svidchit-pro-ne efektivnu-robotu-derzhorganiv-vitalij-vlasyuk.html (дата звернення: 04.06.2021).

7. Швакин С.В. Международно-правовая унификация норм права в процессе конвергенции национальных правовых систем: сб. материалов VII Международной научно-практической конференции *Законность и правопорядок в современном обществе,* г. Новосибирск, 2011 р. Новосибирск: Издательство "СИБПРИНТ", 2011. С. 101-106.

8. Лисенко С. Принцип моделювання в законодавчому процесі Європейського Союзу та можливість використання зазначеного принципу в українському законодавстві у сфері інформаційної безпеки. *Право.ua*. 2015. С. 172- 175.

9. Колодій А.М. Використання розроблених у СНД модельних законів як засіб вдосконалення законодавства України. З*аконодавство України та міжнародне право (проблеми гармонізації).* Київ: Ін-т законодавства ВР України, 1998. Вип. 4. С. 72-77.

10. Данилов И.И. История развития модельного законодательства в США. *Российский юридический журнал.* 2016. № 3. С. 84-89.

11. Полянський Є.Ю. Щодо питання генезису кримінального права США: матеріали Міжнар. наук.-практ. конф., присвяченої 250-річчю трактату Чезаре Беккаріа, *Про злочини та покарання: еволюція кримінально-правової доктрини*, м. Одеса, 13 черв. 2014 р. / редкол.: С.В. Ківалов (голов. ред.), В.О. Туляков (заст. голов ред.), Є.Л. Стрельцов (заст. голов ред.), Д.О. Балобанова; МОН України, НУ ОЮА, ПРЦ НАПрН України, Одес. відділ. ГО "Всеукр. асоц. кримін. права". Одеса: Юрид. л-ра, 2014.С. 105-111.

12. Житарєв Є.В. Еволюція модельного законодавства та його адаптація до сучасних умов. *Форум права*. 2013. № 1. С. 300-305. URL.: http://archive.nbuv.gov.ua/e-journals/FP/2013-1/13gevdcu.pdf (дата звернення: 04.06.2021).

13. Про міжнародний комерційний арбітраж: Закон України від 24.02.94 р. № 4002-XII. URL: https://zakon.rada.gov.ua/go/4002-12 (дата звернення: 04.06.2021).

14. Биля-Сабадаш І. Право країн Латинської Америки серед правових систем сучасності. *Вісник Академії правових наук України*. 2009. № 3. С. 199-208.

15. Ермакова Е.П. Принципы судопроизводства по гражданским делам в конституциях стран Латинской Америки. *Бизнес в законе.* 2011. № 3. С. 55-59.

16. Стрельцова Є.Д. Теорія і практика уніфікації міжнародного права в умовах глобалізації (міжнародний та національно-правовий аспекти): автореф. дис. ...д-ра юрид. наук: 12.00.11. Одеса, 2020. 42 с.

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

УДК: 37.015.3

БЕЛАНЮК М.В., *кандидат юридичних наук, старший дослідник*,
учений секретар ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-3083-1732.
УХАНОВА Н.С., старший науковий співробітник ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-2366-5166.

ІНФОРМАЦІЙНА КУЛЬТУРА ОСОБИСТОСТІ: СУТНІСТЬ ПОНЯТТЯ

Анотація. *У статті на основі широкого кола джерел здійснена спроба розкрити сутність поняття "інформаційна культура особистості". Досліджено та узагальнено погляди вітчизняних і зарубіжних вчених, що стосуються сутності поняття "інформаційна культура особистості" та запропоновано авторське його визначення.*

Ключові слова*: культура, інформація, особистість, інформаційна культура особистості.*

Summary. *The article, based on a wide range of sources, attempts to reveal the essence of the concept of "information culture of the individual". Authors investigate and generalize the views of domestic and foreign scientists concerning the essence of the concept of "information culture of the individual" and propose the author's definition of the studied concept.*

Keywords: *culture, information, individual, information culture of an individual.*

Аннотация. *В статье на основе широкого круга источников осуществлена попытка раскрыть сущность понятия "информационная культура личности". Исследованы и обобщены взгляды отечественных и зарубежных ученых, касающиеся сущности понятия "информационная культура личности" и предложено авторское его видение.*

Ключевые слова: *культура, информация, личность, информационная культура личности.*

Постановка проблеми. Вперше за всю історію людства інформація і знання зайняли домінуючу позицію по відношенню до таких найважливіших категорій, як матерія і енергія. Пріоритет інформації у порівнянні з іншими благами і цінностями, набуття інформаційними ресурсами статусу стратегічних, визначається також і тим, що в будь-якій сфері діяльності, включаючи економічну, політичну, соціальну, перевагами володіють ті, хто володіє повнотою доступу до інформації та відповідними засобами її отримання, обробки, поширення і зберігання. Саме тому сучасний період розвитку людства правомірно пов'язують з розвитком інформаційного суспільства, рівень якого залежить не тільки від кількості і якості збереженої інформації та її доступності, а й від уміння нею користуватися у повсякденному житті.

Істотний вплив на суспільну поведінку людини, на розвиток економічної і політичної системи, на функціонування практично всіх соціальних інститутів здійснюють нова система цінностей і новітні пізнавальні й практичні пріоритети, зумовлені трансформацією культури, виникненням нових культурних практик, зміною інформаційного простору сучасного соціуму.

Більшість дослідників переконані, що інформаційний ресурс, який є продуктом інтелектуальної діяльності суспільства, разом з фінансовими, трудовими та іншими ресурсами здатний вирішити глобальні проблеми людства.

Набуття знань про інформаційне середовище, законів його функціонування, вміння орієнтуватися в інформаційних потоках, інакше кажучи формування інформаційної культури як всього суспільства, так і кожного його члена є надзвичайно актуальним.

Результати аналізу наукових публікацій. Роботи вчених щодо поняття інформаційної культури доводять, що періодизацію розвитку цього феномену можна розділити на три періоди: перший – 70-80-ті роки, другий – 80-90-ті роки, третій – від 90-х років до сьогодення. Поняття інформаційної культури вперше увів в науковий обіг у 1988 р. Воробйов Г. у праці "Твоя информационная культура", проте не надаючи трактування самого терміну [1]. Починаючи з середини XX століття і до нашого часу питання інформації, комп'ютеризації, інформаційної культури та інформаційної компетентності є об'єктом дослідження багатьох українських та зарубіжних вчених, зокрема, Анісімова С., Бєлякова К., Воронкової В., Гадзало А., Галети Я., Джинчарадзе Н., Дзьобаня О., Калініної Л., Нєгодяєва А., Партико З., Прудникової О., Ровенського В., Уйомова А., Сопілко І., Степанова В. та ін. Проблемам інформаційного права та інформаційної безпеки людини присвячені роботи Брижка В., Золотар О., Фурашева В., Пилипчука В. та ін.

Однак, незважаючи на значну кількість публікацій, проблема трактування сутності поняття "інформаційна культура особистості" залишається не вирішеною.

Метою статті є узагальнення поглядів вітчизняних і зарубіжних вчених щодо сутності поняття "інформаційна культура особистості" та пропозиції щодо авторського визначення цього поняття.

Виклад основних положень. Інформація завжди була найважливішою, невід'ємною складовою частиною життя людини. На думку дослідників, в сучасній цивілізованій демократичній державі до основоположних прав людини належить право на інформацію, адже саме завдяки йому особистість має можливість задовольнити свої фундаментальні потреби [2, с. 11].

Однак до середини XX століття зазначена категорія не була предметом пильної громадської уваги і аналізу з точки зору її впливу на особистість і державу. Принципово новий рівень ставлення людства до інформації з'явився після Другої світової війни, коли економічне лідерство стало усвідомлено ототожнюватися з наукомісткою продукцією, глибокими знаннями, вмінням швидко нарощувати професійний потенціал за рахунок вмілої обробки інформації. Якщо раніше в виробничій діяльності людства вирішальна роль відводилась речовим і енергетичним ресурсам, то в наш час головним ресурсом суспільства стала інформація.

Для того, щоб забезпечити адекватне застосування понятійного апарату у нашому науковому дослідженні, перш за все слід уточнити сутність понять "культура", "інформація", "особистість", "інформаційна культура".

Згідно досліджень О. Прудникової, на сьогоднішній день існує понад тисяча тлумачень поняття "культура" в різних галузях знань [3, с. 12].

Найбільш повно, на нашу думку, поняття "культура" представлено П. Герчанівською у словнику культурологічних термінів, де подано 7 дефініцій поняття. Термін культура походить від латинського слова *cultura*, що означає обробіток, виховання, освіта, розвиток, шанування та в контексті нашого дослідження може бути розтлумачене як "світ символічних позначень явищ і понять, сконструйований людьми з метою фіксації й трансляції соціально значимої інформації, знань, уявлень, досвіду, ідей та ін." [4, с. 96].

Згідно трактування словника української мови, культуру слід розуміти як сукупність матеріальних і духовних цінностей, створених людством протягом його історії [5 , с. 394]. Схожу трактовку надають і укладачі психологічного словника, де поняття культура розглядається як сукупність досягнень і високий рівень розвитку людства в суспільному виробництві, розумовому і духовному відношеннях [6, с. 150].

З точки зору правової науки поняття "культура" розуміється як сукупність матеріального і духовного надбання певної людської спільноти (етносу, нації),

нагромадженого, закріпленого і збагаченого протягом тривалого періоду, що передається від покоління до покоління, включає всі види мистецтва, культурну спадщину, культурні цінності, науку, освіту та відображає рівень розвитку цієї спільноти [7].

Поняття "культура" розмежовує природний світ і світ соціальний, створений людиною в результаті праці. Громадянин стає членом суспільства в міру засвоєння знань, мови, цінностей, норм, звичаїв, традицій свого народу, своєї соціальної групи і всього людства. Культура – це засіб вираження творчості, формування індивідуальної самобутності та зміцнення відчуття себе в суспільстві. Культурний досвід – це можливості для дозвілля, розваг, навчання й обміну досвідом з іншими. Аналіз можна було б продовжувати, однак вже зазначене надає можливість зробити висновок, що культура, як соціальне явище, здійснює важливі функції, які полягають в трансляції соціального досвіду, збережені соціальної інформації та соціалізації, і саме культура робить людину особистістю.

Найбільш вагомі дослідження щодо визначення терміну "особистість" знаходимо в царині психології, проте, за словами Смирнова С., жодне визначення не надає вичерпної інформації та не фіксує найбільш суттєві особливості такого складного і багатопланового утворення як особистість [8, с. 85].

Наведемо тлумачення терміну "особистість" у різних галузях знань:

- у психології: 1) особлива якість, що здобувається індивідом у суспільстві, у сукупності відносин, суспільних за своєю природою, у які індивід залучається [9, с. 385]; 2) феномен суспільного розвитку, специфічне утворення, індивід, соціокультурна форма існування психіки [6, с. 195]; 3) індивідуальна форма існування і розвитку соціальних зв'язків і відносин [10, с. 4].

- культурології: 1) поняття, що інтегрує властивості людини як *Homo sapiens*, як творця й носія культури, а також як соціальної істоти; 2) стала система соціально значущих рис, що характеризують індивіда як члена суспільства або спільності [4, с. 138].

- у філософії: 1) суб'єкт суспільних відносин, носій свідомості та системи суспільно значущих якостей [11, с. 457-458]; 2) індивідуальний носій суспільних відносин і функцій, суб'єкт пізнання та перетворення світу, прав і обов'язків, етичних, естетичних та всіх інших соціальних норм [11, с. 357].

Таким чином, в роботах більшості дослідників поняття "особистість" використовується для позначення особливостей, якостей, станів індивіда, обумовлених його діяльністю і комунікацією з іншими людьми.

З позиції права особистість – це суб'єкт права, волі. Її відмінною рисою є прагнення до власної і повага до чужої незалежності. Саме з образом людини як особистості корелюється право.

Поняття особистості має яскраво виражений міждисциплінарний характер і широко вживається у правовій науці, хоча і не містить дефініції самого поняття у законах, але часто зустрічається у Кримінально-процесуальному кодексі України , наприклад: "повага честі і гідності особистості" учасників кримінального судочинства (ст. 9 КПК України) , "адміністративне правопорушення з урахуванням особистості винного" (п. 2 ст. 4**.**1 КПК України). Вираз "особистість винного" вживається в кримінальному законі і в контексті з умовним засудженням (ч. 2 ст. 73 КК України). Цілий розділ (VII) Особливої частини КК України присвячений "злочинам проти особистості". В процесі судочинства встановлюються "особистість підсудного", "дані, що стосуються його особи" (ч. 1 ст. 265 КПК України) і т. д. Також широко використовується термін "особа" в цивільному праві, особливо коли справа стосується захисту честі і гідності особистості громадянина у

випадках заподіяння йому неправомірними діями моральної шкоди, моральних страждань з урахуванням його індивідуальних особливостей (ст. 150-152, 1099-1101 ЦК України).

З моменту народження про людину можна говорити лише як про індивіда – представника виду *Homo sapiens*, який має зумовлені природою особливості, властивий йому генотип. В подальшому, в силу існуючих у суспільстві відносин розвиваються її індивідуальні особливості. Таким чином, відбувається поступовий процес її соціалізації, формування її особистості. Тобто, людина не народжується особистістю, а стає нею. З цієї точки зору у порівнянні з поняттям "індивід" поняття "особистість" – з'являється значно пізніше народження людини, а формування особистості залежить від соціуму, в якому вона знаходиться.

Отже, особистість – це людина зі своїми унікальними поглядами та переконаннями, індивідуальність, єдність соціально-психологічних якостей у міжособистісних, суспільних відносинах, яка свідомо бере участь у різних видах діяльності, розуміє свої дії і здатна керувати ними. Саме в цьому розумінні поняття "особистість" використовується в праві.

Перейдемо до аналізу терміну "інформація", який є латинським за походженням (*informatio* – "відомості, роз'яснення"), теж неоднозначно трактується в науковій літературі. Культурологи під цим терміном розуміють "відомості, дані, повідомлення, що передаються за допомогою сигналів, знаків і є об'єктом зберігання, переробки та передачі" [6, с. 80].

У Великому енциклопедичному юридичному словнику поняття "інформація" розглядається як документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві й державі та навколишньому природному середовищі [12, с. 338].

Аналізуючи термін "інформація", вважаємо за необхідне надати його тлумачення в галузі кібернетики, де воно є одним з найзагальніших понять і тлумачиться як певні відомості, сукупність якихось даних, знань тощо [3, с. 338].

В роботах науковців термін "інформація" трактується як: 1) повідомлення про події, що відбуваються як у зовнішньому, по відношенню до системи, середовищі так і в самій системі [13]; 2) будь-яке повідомлення або передача відомостей про будь-що, що заздалегідь не було "відоме" [14, с. 8].

Проведене дослідження щодо тлумачення поняття доводить, що інформація займає вагоме місце в житті людини, адже еволюція нашого суспільства та виникнення державних інституцій завжди були пов'язані з накопиченням, поширенням та обробкою відповідної інформації.

Як вже зазначалось раніше, XXI сторіччя завдяки величезному технологічному прогресу та глобалізаційним процесам створило новий тип суспільства – інформаційний. У зв'язку з тим сформувався новий тип людини – "людини інформаційної" [15]. Під впливом технологічної бази й інформаційно-технологічних можливостей змінюються не лише самосвідомість особистості, а й її біологічне і соціальне існування. На думку дослідників, зараз як ніколи слід враховувати кожне з діалектично взаємопов'язаних начал людини – фізичне, психічне й соціальне для повного її розвитку в умовах інформаційного суспільства, Багато суперечностей викликає питання про те, які саме зміни для суспільства принесе інформатизація, проте майже всі дослідники впевнені, що особливу роль у сучасному світі й становленні нової людини відіграє інформаційна культура [16].

Інформаційна культура є частиною загальної культури, адже вони мають певні спільні риси. Крім того, інформаційна культура виступає як неодмінний і продуктивний

чинник засвоєння людиною культурної реальності та культурного потенціалу. На думку І. Негодаєва, сфера інформаційної культури набагато ширша за сферу комп'ютеризації або інформаційної техніки і охоплює процеси наукової діяльності, освіти, управління природними і соціальними процесами, сферу побуту, дозвілля [17].

Антонченко М.О. розглядає інформаційну культуру як особливий соціальний механізм трансляції значущої інформації, тобто як спосіб діяльності, що спрямований на накопичення, збереження та передачу ідей, знань і матеріально-духовних цінностей. Інформаційну культуру людини вона визначає як *"системне утворення особистості, яке інтегрує знання про основні методи інформаційних технологій, уміння використовувати наявну інформацію для вирішення прикладних завдань, навички використання персонального комп'ютера і технологій зв'язку, здібності представити інформацію в зрозумілій для усіх формі, орієнтуватися на розширенні та поновленні знань"*. При цьому робиться висновок, що задача освіти сьогодні – створити простір для розвитку інформаційної культури особистості, яка сприяє формуванню самостійного мислення, відчуттю нового, умінню відслідковувати зміни та реагувати на них, умінню приймати рішення в складних нестандартних ситуаціях, що можливо лише за умов повного інформування людини. При такому підході у того, хто навчається повинна складатися свідома мотивація на постійне розширення професійного та загальнокультурного кругозору, а також уявлення про відкритість системи знань, які набуваються у закладах освіти, переконання у тому, що основу міцності та надійності знань дає лише безперервний процес пошуку та споживання інформації, її критична обробка протягом усього життя [18].

Кудренко О. інформаційну культуру розуміє як досягнутий рівень організації інформаційних процесів, ступінь задоволення потреб людини в інформаційному спілкуванні, рівень ефективності створення, збору, збереження, обробки, передачі та використання інформації, що забезпечує цілісне бачення світу, можливість його моделювання, передбачення результатів прийнятих людиною рішень [19].

Дуже важливою у контексті нашого дослідження вважаємо позицію Прудникової О., яка здійснила ґрунтовне дослідження сутності інформаційної культури з філософської точки зору. Дослідниця переконана, що інформаційна культура має включати наступні вміння: адекватно формалізувати знання; інтерпретувати формалізовані дані та використовувати нові інформаційні технології у своїй життєдіяльності; ефективно використовувати сучасну комп'ютерну техніку та інформаційні технології, що сприяють формуванню парадигми інформаційної людини. На думку науковця, інформаційна культура має виступати стрижнем світоглядної культури та поєднувати в собі культуру мислення й мовлення, культуру комунікацій, культуру організації праці, культуру роботи з інформацією у всіх її виявах [3].

В сфері комп'ютеризації та інформаційної техніки, в термін "інформаційна культура" вкладають не лише вміння одержувати, накопичувати, шукати, збирати й передавати інформацію за допомогою ЕОМ, використовуючи бази даних і різні інформаційні системи, а й уміння висловлювати свої думки та ідеї в літературній, графічній і художній формах із використанням ЕОМ, уміння спілкуватися та співпрацювати з іншими людьми [9, с. 26].

На думку культурологів, у широкому аспекті поняття "інформаційна культура" слід розглядати як сукупність усіх цінностей в інформаційній сфері, створених людством протягом різних етапів історичного розвитку (поява писемності; впровадження комп'ютерних технологій тощо); у вузькому – як оптимальні засоби маніпулювання знаками, даними, інформацією та подання їх зацікавленому споживачеві для вирішення теоретичних і практичних завдань [20, с. 129].

В галузі економіки інформаційна культура розглядається як невід'ємна складова загальної культури, як правова норма професійної діяльності, яка впливає на правила поведінки, мотивацію особистості, комунікабельність, спілкування в інформаційному суспільстві. Її основними компонентами вважаються: культура організації подання інформації; культура сприймання та користування інформацією; культура використання нових інформаційних технологій тощо [21].

Дотримуються схожої думки щодо тлумачення досліджуваного поняття дослідники Бєляков К., Онопрієнко С. та Шопіна І., вважають інформаційну культуру інтегральною цілісністю, що включає світоглядні, ціннісні, когнітивні, комунікативні та інструментальні компоненти життєдіяльності людини, соціальних груп та держави, які у сукупності спрямовані на формування інформаційного суспільства, виступають орієнтиром розвитку інформаційного законодавства і знаходять свій прояв в інформаційній діяльності [2].

На думку дослідника Степанова В., під інформаційною культурою слід розуміти здатність суспільства ефективно використовувати наявні інформаційні ресурси і засоби інформаційних комунікацій, застосовуючи для цих цілей передові досягнення в галузі розвитку засобів інформатизації та інформаційно-комунікаційних технологій [13].

Погоджуючись з думкою Галета Я., вважаємо, що інформаційна культура є не лише показником загальної культури в її соціотехнічному аспекті, а й важливою характеристикою професійної компетентності сучасного фахівця, оскільки від рівня його володіння навичками працювати з інформаційно-комунікаційними технологіями та інформаційно-аналітичними уміннями залежать успішність професійної діяльності, розвиток креативного мислення, здатність моделювати робочі процеси і явища, здійснювати комунікацію [22, с. 25].

Отже, спільною рисою для розглянутих вище підходів тлумачення поняття інформаційної культури є те, що вона розглядається як складова загальної культури, а також тісно пов'язана з розвитком певної сфери професійної активності особистості.

Якщо ж говорити про інформаційну культуру особистості, то значні дослідження цього феномену були проведені Семенюк Н. Дослідниця переконана, що інформаційна культура особистості є умовою успішної адаптації людини до життя.

У новій освітній глобальній філософії серйозна увага приділяється інформаційній підготовці особистості, адже інформація має принципово важливе значення як для тих, хто вчить, так і для тих, хто навчається. Суть такої підготовки в тому, щоб навчити не лише прийомам раціональної роботи з книгою, алгоритмам інформаційного пошуку, ліквідації комп'ютерної неграмотності, освоєнню гіпертекстових, мультимедійних та інших інформаційно-комунікаційних технологій, а й сформувати інформаційну компетентність, яка включає вміння шукати, вилучати та критично аналізувати інформацію, вміння самостійно добувати і виробляти нові знання.

Наявність інформаційної компетентності дозволяє сформувати інформаційний світогляд, який являє собою систему узагальнених поглядів на інформацію, інформаційні ресурси, інформаційні системи, інформаційні технології, інформатизацію, інформаційне суспільство та місце людини в ньому, на ставлення людей до навколишнього інформаційного середовища, а також обумовлені цими поглядами їх переконання, ідеали, принципи пізнання і діяльності [15].

Важливим також є внесок Джинчарадзе Н., яка досить детально працювала над вивченням феномену інформаційної культури особистості. Вона вважає, що інформаційна культура особистості складається з таких багатоаспектних та взаємопов'язаних елементів як: інформаційний потенціал, світогляд та менталітет, інформаційно-орієнтаційна діяльність, мікро- та макро інфомодель, інфопотреба та інші" [23].

Таким чином, одні дослідники розглядають інформаційну культуру під кутом її впливу на суспільство, інші – на особистість, що дає можливість зробити висновок про те, що розвинена суспільна інформаційна культура впливає на розвиток кожної особистості та навпаки – сформованість інформаційної культури суб'єктів соціуму відбивається на інформаційній культурі суспільства.

Узагальнюючи думки вчених, до ознак інформаційної культури особистості можна віднести: здатність використовувати у своїй діяльності технічні інформаційні пристрої та програмні продукти; знати особливості інформаційних потоків у своїй професійній діяльності, вміти адекватно формулювати свою потребу в інформації, орієнтуватися у великому обсязі інформації; вміти ефективно шукати, відбирати необхідну інформацію, аналізувати та критично оцінювати; мати навички коректного інформаційного спілкування, вміти створювати якісно нову інформацію, ідентифікувати і попереджати можливі види інформаційних небезпек (дезінформацію, інформаційний тероризм, фейк) та ін. Невід'ємною частиною інформаційної культури є освоєння нових інформаційних технологій та вміння їх застосовувати для автоматизації рутинних та неординарних операцій, що вимагають нетрадиційного творчого підходу.

Отже, щодо трактування поняття "інформаційна культура особистості", можна констатувати, що її слід розглядати *як частину базисної культури особистості, що характеризує інформаційну сферу життєдіяльності людини і включає: сукупність знань, умінь і навичок роботи з інформаційними джерелами; наявність творчого підходу в сфері інформаційної діяльності, що дозволяє ефективно працювати при пошуку, передачі, отриманні інформації; вміння на цій базі генерувати якісно нову інформацію.*

Говорячи про інформаційну культуру, не можна не порушити питання інформаційної свободи, а саме: законність поширення інформації засобами масової інформації, мережею Інтернет, узгодженість термінології в інформаційному законодавстві тощо [24].

Під впливом інформатизації відбувається соціально-економічна трансформація, саме тому виникає необхідність державного функціонально-регуляторного управління в інформаційній сфері завдяки науково обґрунтованим поглядам на багатогранну роль інформаційного права та потребам систематизації юридичних норм в умовах становлення інформаційного суспільства в Україні.

Дослідники переконані, що зараз як ніколи є потреба в прийнятті більш ефективного Інформаційного кодексу України з систематизованим законодавством, врегульованими інститутами інформаційного права, процедурами та механізмами розподілу адміністративних та технічних функцій щодо інформаційного забезпечення [15; 25; 26].

Крім того, зазначена проблема набула глобального характеру, адже держави не можуть самостійно боротися в повній мірі із тими негативними викликами, які пов'язані з розширенням світової мережі та поширенням кіберзлочинності з одного боку, і потребами у посиленні захисту прав людини, її приватності та персональних даних, захисту авторського права тощо, з іншого.

Кардинальним вирішенням цієї проблеми має стати налагодження системи обміну інформацією щодо питань кібербезпеки в питаннях протидії та попередженню вчиненню злочинів в мережі, що посягають на права і свободи людини і громадянина із залученням можливостей держави, суспільства, бізнесу та громадян [27].

Висновки.

У результаті проведеного аналізу наукових джерел виявлено, що проблема трактування терміну "інформаційна культура особистості" ускладнена багатозначністю цього поняття через його міждисциплінарність. Його можна розуміти як феномен; як

частину особистісного знання, загальної культури людини; як рівень розвитку знань, умінь, навичок; як область знань, що досліджує деякі проблеми; як навчальну дисципліну.

У науковій та навчальній літературі публікується безліч поглядів, часом абсолютно протилежних. Однозначного і всеосяжного визначення цього поняття дослідники не дають. Вивчивши літературні джерела вітчизняних і зарубіжних авторів, і узагальнивши існуючі визначення "інформаційної культури", ми виявили, що даний термін розглядається вченими з позицій різних наукових підходів, має різні сутнісні ознаки і не має однозначного тлумачення. Найбільш розробленим аспектом при дослідженні проблеми інформаційної культури є її розгляд на рівні особистості.

У нашому розумінні інформаційна культура особистості являє сукупність інформаційного світогляду і системи знань і умінь, що забезпечують цілеспрямовану самостійну діяльність по оптимальному задоволенню індивідуальних інформаційних потреб з використанням як традиційних, так і нових інформаційних технологій, де пріоритетними є загальнолюдські духовні цінності.

Подальші перспективи наукових досліджень вбачаємо у більш детальному вивченні засобів формування інформаційної культури особистості. Для вирішення цієї проблеми необхідно застосувати комплексний підхід щодо скоординованості робіт соціальних інститутів, діяльність яких спрямована на формування гармонійно розвиненої особистості з високим рівнем інформаційної культури.

Використана література

1. Воробьев Г.Г. Твоя информационная культура. Москва: Молодая Гвардия, 1988. 306 с.

2. Бєляков К.І., Онопрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір: монографія / за заг. ред. К.І. Бєлякова. Київ: КВІЦ, 2018. 168 с.

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

4. Герчанівська П.Е. Культурологія: термінологічний словник. Київ: Національна академія керівних кадрів культури і мистецтв, 2015. 439 с.

5. Словник української мови: в 11 тт. / за ред. І.К. Білодіда. – (АН УРСР. Інститут мовознавства). Київ: Наукова думка, 1970 – 1980. Т. 4. С. 394.

6. Психологічний словник / авт.-уклад. В.В. Синявський, О.П. Сергєєнкова; ред. Н.А. Побірченко. Київ: Науковий світ, 2007. 274 с.

7. Про культуру: Закон України від 14.12.10 р. № 2778-VI. URL: https://zakon.rada.gov.ua/laws/show/2778-17#Text

8. Смирнов С.Д. Педагогика и психология высшего образования: от деятельности к личности: учеб. пособие для студ. высш. учеб. заведений. 3-е изд., стер. Москва: Издательский центр "Академия", 2007. 400с.

9. Леонтьев А.Н. Избранные психологические произведения: в 2-х т. / под ред. В.В. Давыдова и др. Москва: Педагогика, 1983. Т. 1. 392 с.

10. Анцыферова Л.И. К психологи личности как развивающейся системы. *Психология формирования и развития личности*. Москва: Наука, 1981. С. 3-19.

11. Степанов В.Ю. Інформаційна культура сучасного інформаційного суспільства : зб. наук. пр. *Вісник Харк. держ. акад. культури*. 2009. Вип. 27. С. 91-97.

12. Великий енциклопедичний юридичний словник / за ред. акад. НАН України Ю.С. Шемшученка. Київ: ТОВ "Юридична думка", 2007. 992 с.

13. Семенюк Н. Необхідність інформаційного супроводу освіти впродовж життя : зб. наук. пр. *Гілея*. Київ: ВІР УАН, 2013. Вип. 78 (11). С. 294-297.

14. Анисимов С.Ф. Человек и машина. Москва, 1959. 56 с.

15. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 446 с.

16. Ровенский В., Уемов А., Уемова Е. Машина и мысль. Москва, 1960. 69 с.

17. Негодаев И.А. Информатизация культуры: монография. Ростов-на-Дону: ЗАО "Книга", 2003. 320 с.

18. Антонченко М.О. Інформаційна культура як складова загальнолюдської культури URL: https://fi.npu.edu.ua/files/Zbirnik_KOSN/2/25.pdf

19. Кудренко О. Проблеми формування інформаційної культури майбутніх офіцерів: матер. V Міжнародної наукової конференції ХНУПС ім. І.Кожедуба, м. Харьків, 21-22 трав. 2020 р. Харьків, 2020. С. 11.

20. Українська людина в європейському світі: виміри ідентичності: навч. посібник / кол. авт. / за ред. д-ра екон. наук, проф. Т.С. Смовженко, д-ра філос. наук, проф. З.Е. Скринник. Київ: УБС НБУ, 2015. 609 с.

21. Гадзало А.Я. Інформаційна культура як важлива складова людського капіталу. URL: http://www.rusnauka.com/23_WP_2009/Economics/50415.doc.htm

22. Галета Я. Інформаційна культура в професійній підготовці майбутнього педагога. *Рідна школа*. 2011. № 11. С. 25.

23. Джингчарадзе Н.Г. Інформаційна культура особи: формування та тенденції розвитку (соціально-філософський аналіз): дис. ...д-ра філос.наук: 09.00.03. Київ: Київський ун-т ім. Т. Шевченка, 1997. 452 с.

24. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення: аналітична записка. URL: http://www.niss. gov.ua/ articles/1189

25. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – НДІІП НАПрН України. Київ: Видавничий дім "АртЕК", 2020. 288 с.

26. Пилипчук В. Г., Дзьобань О.П. Проблема агресії і насильства: світоглядно-інформаційний вимір. *Освіта регіону*. 2012. № 2. 244 с.

27. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник*. 2017. № 3(44). С.61-69.

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

УДК 355.45:343.1

КОВАЛЬОВ К.Є., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1243-3973.

ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ

Анотація. *Стаття присвячена питанням обігу інформації з обмеженим доступом. Досліджуються проблеми, пов'язані з обігом інформації з обмеженим доступом в Україні, та аналізується міжнародний досвід у сфері захисту інформаційних ресурсів.*

Ключові слова: *державна таємниця, інформація з обмеженим доступом, міжнародний досвід, інформаційна безпека, законодавство.*

Summary. *The article is devoted to the circulation of restricted information. The problems related to the circulation of restricted information in Ukraine are studied, and the international experience in the field of information resources protection is analyzed.*

Keywords: *state secret, restricted information, international experience, information security, legislation.*

Аннотация. *Статья посвящена вопросам циркуляции информации с ограниченным доступом. Исследуются проблемы, связанные с оборотом информации с ограниченным доступом в Украине, а также анализируется международный опыт в области защиты информационных ресурсов.*

Ключевые слова: *государственная тайна, информация с ограниченным доступом, международный опыт, информационная безопасность, законодательство.*

Постановка проблеми. Аналіз наукових та практичних матеріалів, а також нормативно-правових актів стосовно інформації з обмеженнями у доступі та інтелектуальної власності, як її похідної і контррозвідувального забезпечення їх охорони та захисту (протидії конкурентній розвідці, або промисловому шпигунству – отримання недоступної інформації про економічну діяльність конкурентів) є актуальною і полягає у необхідності забезпечення захисту інформаційних ресурсів з обмеженим доступом.

Для вирішення вказаного завдання, контррозвідувальним підрозділам (умовне найменування, яке нами приймається для скорочення терміна і під яким розуміються органи з протидії промисловому шпигунству та конкурентної розвідки), необхідно мати повний перелік інформаційних ресурсів, які мають грифи обмеження і лише на їх основі визначати систему відповідних заходів з їх забезпечення.

При цьому важливим є те, що за радянського періоду та в останнє десятиріччя 20 століття в Україні державою забезпечувався ефективний захист лише таємної інформації, котра завжди була її власністю.

На нашу думку, необхідно більш детально розглянути та обґрунтувати вирішення зазначеної проблеми.

Результати аналізу наукових публікацій. Дослідженням проблем захисту інформації з обмеженим доступом займалися такі вчені, як: О.Є. Архіпова, О.Ф. Бантишева, Р.В. Корсун, Б.Д. Леонов [1], В.М. Лопатін, В.В. Макаренка, І.М. Мейдич, А.С. Пашкова, А.В. Савченка, М.І. Хавронюк, О.В. Шамсутдінова, В.М. Шлапаченка та ін.

Проте, як вважаємо, в сучасних умовах захист інформації з обмеженим доступом потребує удосконалення. Тому є необхідність дослідити проблему захисту інформації з обмеженим доступом контррозвідувальними органами.

Метою статті є удосконалення захисту інформації з обмеженим доступом на підставі аналізу нормативно-правових актів з охорони інформації з обмеженнями у доступі, зокрема у сфері інтелектуальної власності.

Виклад основного матеріалу. Слід зазначити, що безпека будь-якої соціальної одиниці (держави, організації, підприємства) в першу чергу залежить від здатності державного механізму забезпечити керованість економічних перетворень, політичного і суспільного будівництва та багатьох інших факторів. Але, в першу чергу, державний механізм повинен чітко визначити і передбачати внутрішні та зовнішні загрози, які виникають, чи в найближчому майбутньому можуть виникнути на шляху його розвитку. Лише за першої умови додатково може виникнути необхідність додаткової охорони та захисту такого роду інформаційних масивів.

Однією з найбільш важливих складових діяльності із забезпечення безпеки держави, суспільства та особи є розвідувальна діяльність спецслужб, яка здійснюється безперервно. Практика діяльності СБ України свідчить про те, що "масштаб збитків, які несе Україна внаслідок тільки іноземного шпигунства, не піддається оцінці. Є всі підстави остерігатися, що цей чинник може стати діючим на довгий термін". Як би не відрізнялися точки зору на суть розвідувальної діяльності, а саме на характеристику її основних структурних елементів – мету і об'єкт. Головна мета розвідувальної діяльності – це отримання інформації з обмеженим доступом про сторону, у відношенні якої ведеться розвідка, і саме яку ми маємо всі підстави називати розвідувальною інформацією. Головним завданням, сутністю розвідувальної діяльності є здобування саме "закритої" інформації. Адже використання спеціальних, досить дорогих у матеріальному плані сил та засобів ведення розвідки для здобування інформації, яка слабко охороняється, або недостатньо захищена, є занадто дорогою забаганкою. Не потребує великих зусиль обґрунтування відповіді на питання "а хто ж протидіє розвідці?". Звичайно ж контррозвідка. Тобто спеціалізована структура, головним завданням якої є не допустити витік інформації, на яку ведеться полювання конкурентами. Розвідувальні органи іноземних держав завжди цікавила, цікавить і буде цікавити "секретна" інформація загального характеру про: політичний потенціал України; плани реалізації політичної стратегії; пріоритетні інтереси в сфері політичних відносин; зовнішньоекономічні зв'язки; економічні систему й потенціал України; плани з реалізації економічної стратегії; військовий потенціал України; зовнішні військово-політичні відносини і військово-стратегічні позиції; військово-стратегічні плани вищого військового командування та інші [2].

Перерахована інформація, у залежності від її призначення зосереджується за зазначеними сферами діяльності держави на наступних об'єктах:

- *у політичній сфері:* державні органи; органи управління зовнішньополітичною діяльністю; органи державної безпеки; органи, що здійснюють адміністративно-політичні функції в країні (у тому числі органи правопорядку); суспільно-політичні організації, і насамперед організації, що здійснюють міжнародні зв'язки; міжурядові політичні організації;
- *в економічній сфері:* державні органи, що здійснюють планування і керівництво економікою й окремими її галузями; державні установи, що планують і здійснюють зовнішні економічні зв'язки; міжурядові організації у сфері економічних відносин; головні підприємства промисловості, транспорту і зв'язку; наукові установи, що ведуть дослідження в галузі економіки тощо;

- *у військовій сфері:* центральні управління Міністерства оборони України, Генеральний штаб, штаби видів збройних сил, стратегічних угруповань військ, об'єднань, з'єднань і частин; об'єднані військові організації; військові частини, оснащені новими видами зброї і бойової техніки, арсенали і склади їх зберігання; установи, що займаються науково-дослідними і дослідно-конструкторськими роботами в сфері озброєння і військової техніки, іспитові полігони; засоби закритого оперативного зв'язку Міністерства оборони; підрозділи, що займаються стратегічними військовими перевезеннями тощо;

- *у науково-технічній сфері:* державні органи планування і координації наукових робіт; Академія наук України, науково-дослідні інститути, що ведуть роботу на важливих напрямках розвитку науки і техніки.

Зазначені відомості секретного змісту викладені у Зводі відомостей, що становлять державну таємницю [3].

Загальну систему завдань контррозвідки в найбільш загальному вигляді можна визначити як виявлення, попередження і припинення розвідувальної діяльності, що проводиться у виді агентурної і технічної розвідки, а також розвідки з використанням легальних можливостей, спрямованої на одержання секретних відомостей, у політичній, економічній, військовій і науково-технічній сферах діяльності України, що знаходяться на фізичних об'єктах зазначених сфер; виявлення, попередження і припинення розвіддіяльності, яка проводиться, в основному, у виді агентурної розвідки, спрямованої на одержання секретної інформації від секретоносіїв, та – технічної розвідки, спрямованої на одержання інформації з каналів зв'язку.

Таким чином, одним із найбільш пріоритетних видів діяльності контррозвідки – це протидія агентурній розвідці, тому що її діяльність спрямована на здобування інформації про стратегічні плани держави, її органів, організацій і окремих осіб у реальному часі, що можуть дати також інші види розвідки, а особливо на перспективу. Це підтверджується розвитком подій у сучасному світі [4 – 13].

Отже, нами підтверджується актуальність захисту "таємниць" контррозвідкою, котра, в сучасних умовах забезпечується комплексом, а не системою заходів на державному рівні.

Цікавими з цього приводу є висновки ряду фахівців стосовно призначення органів контррозвідки закордонних країн у системі захисту засекреченої інформації й діяльності: "Захист секретної інформації й діяльності, витік або розголошення яких може завдати шкоди національній безпеці, покладено на міністерства, відомства й організації, які несуть повну відповідальність за схоронність науково-дослідних і дослідно-конструкторських розробок, передових технологій, зразків пріоритетної промислової продукції, як у цивільній, так і військовій сферах.

У США, зокрема, це завдання покладене на Міністерство юстиції й Управління по нагляду за забезпеченням безпеки інформації. У ФРН відповідальність за організацію й забезпечення режиму таємності на підприємствах і в науково-дослідних установах покладена на Міністерство економіки.

Завдання контррозвідувальних органів закордонних країн із захисту засекреченої інформації й діяльності від витоку або несанкціонованого розголошення визначається: розробкою загальних рекомендацій із забезпечення таємності діяльності відомчих служб безпеки; перевіркою осіб з метою оформлення допуску до секретної інформації й виробництв; організацією підбору, підготовки й навчання співробітників служб безпеки промислових підприємств і державних установ; співробітництвом з адміністрацією й службами безпеки відомств, корпорацій і фірм по запобіганню витоку промислових і інших секретів; перевіркою ефективності задіяних систем забезпечення безпеки інформації й діяльності від витоку або несанкціонованого розголошення; наданням допомоги в

проведенні технічних заходів, спрямованих на забезпечення безпеки секретної інформації й матеріалів; інформуванням адміністрації відомчих служб безпеки, громадськості про форми й методи роботи спеціальних служб; обміном інформацією із зацікавленими організаціями з питань поліпшення захисту секретів і підготовки пропозицій в органи виконавчої влади для прийняття управлінських рішень; розслідуванням випадків розголошення або витоків засекреченої інформації або діяльності, що призведе до збитків інтересам національної безпеки".

Достатньо важливим елементом у протидії розвідувальним спрямуванням виступає сфера так званого військово-технічного співробітництва, яка включає до свого складу обмін та торгівлю військовими технологіями та технологіями подвійного використання.

Таким чином, у сучасному процесі розвитку міжнародного науково-технічного співробітництва із промислово розвиненими країнами питання, пов'язані з купівлею-продажем технології, що включає передачу знань, науково-технічного, комерційного й управлінського досвіду ("ноу-хау"), набувають особливої актуальності і вимагають комплексного врегулювання, насамперед на національному рівні.

У зв'язку з переходом до ринкової економіки в Україні прийнято пакет важливих законів (про власність, підприємництво, інвестиції, валютне регулювання, банківську діяльність, спільні підприємства тощо). На цьому фоні також необхідно налагодити ефективний захист майнових інтересів власників "ноу-хау" не тільки в процесі співробітництва із закордонними країнами, але й в Україні.

Промислово розвиненими країнами, зокрема ФРН, США, Великобританією, Канадою, Японією та Швейцарією, накопичений великий законодавчий досвід у регламентуванні відносин в області захисту комерційної таємниці. Тому вивчення й аналіз форм правового забезпечення майнових інтересів власників торговельних секретів, "ноу-хау" в цих країнах дозволяє більш цілеспрямовано й продуктивно підійти до моделювання спеціального законодавства, відсутнього на даний час в Україні. У США діє спеціальне законодавство, що поєднує правила поведінки зацікавлених осіб в галузі використання торговельних або ділових секретів. У Великобританії та США для рішення спорів сторін залучаються прецедентні судові й адміністративні рішення. У ФРН (країна з кодифікованим правом) відносини регулюються правилами, включеними в закони, що ставляться до різних законодавчих галузей [14, с. 18-48].

У сучасних умовах Україна потребує удосконалення заходів із взаємодії зазначених органів щодо координації їх зусиль у сфері економічних секретів, а також у формуванні системи комплексного захисту державної й комерційної таємниці. Вона має 4 групи об'єктів: особливо важливі оборонні об'єкти з державною формою матеріальної й інтелектуальної власності, на яких зосереджують державні секрети; оборонні об'єкти, що підлягають конверсії; підприємства недержавного сектора, на яких розміщуються оборонні замовлення; недержавні підприємства із приватною формою власності, на яких охороняються відомості, що становлять комерційну таємницю (інтелектуальну власність підприємства).

Участь контррозвідки як спецслужби в захисті комерційної таємниці на таких підприємствах у випадку протиправних зазіхань на цінну конфіденційну інформацію з боку іноземних розвідок і промислових шпигунів повинна ефективно регулюватися нормативно-правовими актами на відміну від сучасності [15, с. 49-50].

З цього приводу показовим є аналіз сучасного стану нормативно-правового закріплення захисту інформації та інтелектуальної власності у нормах державних та недержавних структур України на основі якого можливе удосконалення їх нормативно-правового регулювання за визначеними вище напрямками.

Визначений Декларацією про незалежність, Конституцією та Законом України "Про основи національної безпеки України" курс на відродження української державності, побудови соціальної та демократичної держави покладає на СБ України забезпечення політичної, економічної, науково-технологічної, соціальної, воєнної, інформаційної та екологічної безпеки. Вказане акцентується рішеннями СБ України, що закріплені в низці основних, базових нормативних документів.

Тому визначення завдань контррозвідки із забезпечення інформаційної безпеки держави та захисту інтелектуальної власності в Україні в межах своєї компетенції у сучасних умовах набули крайньої актуальності.

Досить актуальною для України на цей час визначається проблема захисту власного інформаційного простору та національних інформаційних ресурсів.

Однак, як і в попередні роки повторюються помилки, що були закладені раніше, але визначається необхідність сприяння державних органів керівникам відповідних структур у охороні державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави.

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287 [16], зазначається, що одним із пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС. Водночас, ст. 7 Закону України "Про основи національної безпеки України" [17], визначено загрози національній безпеці України в інформаційній сфері, однією з яких є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю.

Сучасний стан правової регламентації захисту інформації з обмеженим доступом в Україні визначається прийняттям останнім часом Законів України "Про інформацію", "Про доступ інформації" та "Про державну таємницю".

Схематично поділ інформації за режимом доступу відповідно до цих законів включає в себе три такі категорії: конфіденційна, таємна і службова інформація.

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

Таємною є інформація з обмеженим доступом, яка має вищий, порівняно з іншими категоріями утаємниченої інформації, ступінь захисту, оскільки її розголошення однозначно спричинить завдання шкоди певній особі, суспільству, державі. До таємної інформації належить державна таємниця, професійні таємниці (адвокатська, лікарська тощо), таємниця слідства та інші види таємної інформації, які визначені спеціальними законами.

Службова інформація запроваджена як нова категорія інформації з обмеженим доступом, згідно ст. 9 Закону України "Про доступ до публічної інформації". До такої інформації належать відомості:

---

[*] *Прим. від ред.* Згідно чинного Державного стандарту України "Технічний захист інформації. Терміни та визначення" від 1997 р. (ДСТУ 3396.2-97): *"**конфіденційна інформація** – це відомості, які знаходяться у **володінні, користуванні або розпорядженні** окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов"* (див. [19]). Тобто мова йде про тріаду повноважень права власності окремих осіб. При цьому, будь-який Державний стандарт України є нормативно-правовим, законодавчим актом.

1) що містяться в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Документам, що містять службову інформацію, присвоюється гриф "для службового користування". Доступ до таких документів надається відповідно до ч. 2 ст. 6 Закону України "Про доступ до публічної інформації".

Головною метою діяльності СБ України визначаються організація та забезпечення захисту інтересів України і її громадян від розвідувально-підривної діяльності спецслужб іноземних держав, організацій, груп та окремих осіб, сприяння вищим органам влади України в реалізації курсу держави на зміцнення її оборонного та економічного потенціалу.

До основних, пріоритетних завдань контррозвідки у захисті національних інтересів традиційно відноситься захист науково-технологічного потенціалу України; захист інтелектуального та наукового потенціалу від витоку за межі України (висококваліфікованих фахівців оборонного комплексу); захист від несанкціонованої передачі за кордон інформації, що становить державну таємницю, та конфіденційної інформації, яка є власністю держави, і витік якої може завдати шкоди інтересам України.

Виходячи з викладеного, цілком обґрунтованим є висновок, що захист інформаційної сфери України є пріоритетним для СБ України, тобто захист національного інформаційного простору є одним із пріоритетних національних інтересів України, як і проведення наукових досліджень, підготовка навчально-методичних видань стосовно оперативних та законодавчих засад захисту держави в інформаційній сфері, з питань забезпечення ефективних і оптимальних шляхів його організації.

Основними напрямами діяльності СБ України у сфері захисту економічного, науково-технічного та оборонно-промислового потенціалу України, традиційно вважається здійснення заходів щодо протидії спрямуванням спецслужб іноземних держав до пріоритетних науково-технічних програм та розробок у сфері створення новітніх систем і зразків озброєння та військової техніки, недопущення фактів витоку інформації, яка становить державну таємницю та передбачену законом конфіденційну інформацію; здійснення заходів з нейтралізації загроз національній безпеці в інформаційній сфері.

Невід'ємною складовою економічної безпеки є надійність захисту державної таємниці та службової інформації.

Однією з головних загроз економічній безпеці держави є можлива втрата технологічної незалежності України, наукових шкіл, надбань та пріоритетів внаслідок комерціалізації і переорієнтації вітчизняних наукових центрів на іноземного замовника, витоку перспективних технологій і інтелектуальної власності тощо.

Захист економічного, науково-технічного і оборонно-промислового потенціалу держави забезпечується: захистом державної таємниці, пріоритетних оборонно-промислових та науково-технічних розробок, сприянням збереженню науково-технічного потенціалу держави, сприянням у порядку, передбаченому чинним законодавством, підприємствам, установам, організаціям у збереженні комерційної та іншої визначеної законом таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України, організацією і проведенням на цій основі заходів щодо виявлення спрямувань та

обмеженням доступу спецслужб, організацій та окремих представників іноземних держав до них тощо.

Аналіз стану реалізації положень щодо діяльності СБ України за період з проголошення незалежності до теперішнього часу засвідчив, що потреба у концептуальній оцінці адекватності роботи контррозвідки загрозам державній безпеці в інформаційній сфері вимагає вжиття невідкладних заходів організаційного та оперативного характеру з метою створення єдиного механізму, який дозволяв би цілеспрямовано впливати на них специфічними засобами.

Потребують врегулювання питання забезпечення оборонно-промислового комплексу, захисту конфіденційної інформації, що є власністю держави, надійного захисту відомостей, що становлять державну таємницю (своєчасне виявлення, попередження і припинення фактів витоку секретних відомостей та усунення причин, що створюють передумови до цього).

Все зазначене вище є вкрай важливим для подальшого удосконалення забезпечення охорони та захисту інформації з різними обмеженнями у доступі.

Отже, для удосконалення характеристик системи захисту інформаційної сфери України та її складової – системи захисту інтелектуальної власності необхідно систематизувати та упорядковувати за змістом. Це також підтверджується рядом проблем у забезпеченні охорони та захисту інформації з відповідними грифами.

Детальний аналіз положень доступних для загального доступу джерел, як наукового, так і нормативного змісту дає нам підстави говорити про необхідність забезпечення захисту контррозвідкою всього переліку “таємниць” (інформації з обмеженим доступом), а саме: “службової таємниці”, “комерційної таємниці”, “ноу-хау”, “банківської таємниці”, “інформації про громадян” (персональних даних), “адвокатської таємниці”, “професійної таємниці”, “нерозкритої інформації” тощо, інформація у яких не є державною таємницею.

Тобто на даному етапі гостро постало питання стосовно проблем оцінки захищеності секретної інформації.

З метою оцінки захищеності інформації необхідно оцінити комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню інформації та втратам її матеріальних носіїв. Відпрацьовані критерії захищеності інформації дозволять забезпечити законність та об’єктивність оцінки стану захищеності інформаційних ресурсів. Це дасть змогу отримати “орієнтири” для планування роботи із підвищення рівня захищеності інформації. А для цього потрібен механізм визначення стану захищеності інформації з обмеженим доступом на підприємствах та установах.

Безперечно, це сприятиме ефективному вирішенню проблем профілактики адміністративних порушень законодавства про державну та інші види таємниць. Тобто, основними причинами вчинення адміністративних порушень законодавства про державну таємницю є елементарне незнання секретоносіями норм чинного законодавства про державну таємницю, що зумовлюється відсутністю належної та доступної системи професійного навчання секретоносіїв [18, с. 152].

Кримінальний Кодекс України встановлює відповідальність за значну кількість злочинів, які порушують цілісність, достовірність, законну приналежність, конфіденційність та (або) доступність інформації.

Висновки.

З метою попередження адміністративних правопорушень у сфері охорони державної таємниці необхідно поліпшити фінансування витрат на здійснення діяльності, пов’язаної з державною таємницею; удосконалити регіональну систему підготовки та

перепідготовки працівників режимно-секретних органів; посилити вимоги до перевірки рівня знання секретоносіями законодавства про державну таємницю та правил секретного діловодства, а також збільшити суми штрафів, що накладаються за порушення законодавства про державну таємницю.

Значна кількість нормативних актів розглядає інформаційну безпеку в контексті більш загального поняття – національної безпеки (захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам).

Отже, чим активніше розвивається інформаційна сфера, тим більше політична, економічна, оборонна та інші складові національної безпеки будь-якої держави залежать від інформаційної безпеки, причому в ході розвитку технічного прогресу ця залежність дедалі більше зростатиме.

При цьому мова йде про необхідність забезпечення безпеки не лише інформації з обмеженим доступом, але й іншої інформації, оскільки в умовах інформаційного суспільства надається правова охорона інформації як об'єкта права власності, і має бути не лише відвернена загроза несанкціонованого доступу до інформації (порушення конфіденційності), але й загроза порушення її цілісності, достовірності та доступності інформації.

Використана література

1. Ковальов К.Є., Леонов Б.Д. Забезпечення охорони державної таємниці у сфері оперативно-розшукової діяльності за законодавством окремих держав: порівняльний аналіз. *Інформація і право*. № 1(20)/2017. С. 82-92.

2. Гордієнко С.Г. Феномен інформації та забезпечення її охорони і захисту при веденні бізнесу: курс лекцій. – (НТУУ "КПІ"). URL: http://ipp.kpi.ua/wp-content/uploads/2016/04/%D0%9A%D1%83%D1%80%D1%81-%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9-%D0%A4%D0%B5%D0%BD%D0%BE%D0%BC%D0%B5%D0%BD-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-docx (дата звернення: 08.05.2021).

3. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Служби безпеки України від 23.12.20 р. № 383.

4. ЦРУ меняет технику на агентов. URL: http://www.agentura.ru/dossier/usa/cia/gossreforms (дата звернення: 08.05.2021).

5. Андрій Євтушенко. Шпигуноманія-2. *Дзеркало тижня.* № 38 (463). – (4-10 жовтня 2003 року). URL: http://www.dt.ua/1000/1050/42776 (дата звернення: 09.05.2021).

6. Юлія Янчар. У США шпигуноманія. *Львівська газета.* № 166 (236). – (19 вересня 2007 року). URL: http://www.gazeta.lviv.ua/articles/2007/09/19/26355 (дата звернення: 09.05.2021).

7. Джемаль О., Сотников И., Тульский М., Маякова Е. Топ-8 ученых-шпионов. Кого и как можно обвинить в шпионаже. Тайный сбор информации сменили законные методы покупки секретных научных данных. URL: http://compromat.ru/main/nauka/shpieny.htm (дата звернення: 09.05.2021).

8. Использование легальных методов промышленного шпионажа в сетевой разведке. URL: http://www.warning.dp.ua/comp10.htm (дата звернення: 10.05.2021).

9. Лучшая российская шпионка за 30 лет. URL: http://inosmi.ru/europe/20101213/164884915.html (дата звернення: 10.05.2021).

10. Промышленный шпионаж – реальность в СНГ. URL: http://dere.com.ua/library/other/prom_spion.shtml (дата звернення: 10.05.2021).

11. Промышленный шпионаж или бизнес-разведка. *Goodwin.* – (08.15.2011). URL: http://z-filez.info/story/promyshlennyy-shpionazh-ili-biznes-razvedka (дата звернення: 11.05.2021).

12. Промышленный шпионаж, конкурентная разведка, бенч-маркетинг и этика цивилизованного бизнеса. URL: http://www.marketing-ua.com/articles.php?articleid=1499 (дата звернення: 11.05.2021).

13. Чехи запуганы байками о российских шпионах. URL: http://inosmi.ru/europe/20101226 /165208963.html (дата звернення: 12.05.2021).

14. Андрощук Г.А., Крайнев П.П. Правовое регулирование защиты коммерческой тайны за рубежом. *Экономическая безопасность, разведка и контрразведка*. 2002. № 1(1). С. 18-48.

15. Белая книга российских спецслужб. 2-е изд. перераб. Москва: Информ.-издат. агенство “Обозреватель”, 1996. С. 49-50.

16. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287/2015. *Офіційний вісник України*. 2015. № 43. С. 1353.

17. Про основи національної безпеки України: Закон України № 964-IV від 19.06.03 р. *Офіційний вісник України*. 2003. № 29. Ст. 1433.

18. Адміністративне право України: підручник для юридичних вузів і факультетів / Ю.П. Битяк, В.В. Богуцький, В.М. Паращук та ін. Харків: Право, 2001. 152 с.

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

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

Правова інформатика

УДК 002.6:004:340.1+316.329.8

БАРАНОВ О.А., *доктор юридичних наук, с.н.с.,* керівник Наукового центру цифрових трансформацій і права ДНУ ІІБП НАПрН України.

СОЦІАЛЬНА ТА ЦИФРОВА ТРАНСФОРМАЦІЇ: ДЖЕРЕЛО ПРАВОВИХ ПРОБЛЕМ

Анотація. *Аналізується природа виникнення, сутність, зміст та особливості здійснення соціальної та цифрової трансформації. Обґрунтовується в інтересах правової науки визначення дефініцій термінів "соціальна трансформація" та "цифрова трансформація". З'ясовуються джерела та зміст правових проблем, які можуть виникнути при формуванні правового забезпечення здійснення соціальної та цифрової трансформації у сучасному суспільстві. Наводяться приклади таких правових проблем.*

Ключові слова: *трансформація, соціальна трансформація, цифрова трансформація, інтернет речей, законодавство.*

Summary. *The nature of origin, essence, content and features of social and digital transformation are analyzed. The definition of the terms "social transformation" and "digital transformation" is substantiated in the interests of legal science. The sources and content of legal problems that may arise in the formation of legal support for social and digital transformation in modern society are clarified. Examples of such legal problems are given.*

Keywords: *transformation, social transformation, digital transformation, internet of things, legislation.*

Аннотация. *Анализируется природа возникновения, сущность, содержание и особенности осуществления социальной и цифровой трансформации. Обосновывается в интересах правовой науки определения дефиниций терминов "социальная трансформация" и "цифровая трансформация". Выясняются источники и содержание правовых проблем, которые могут возникнуть при формировании правового обеспечения осуществления социальной и цифровой трансформации в современном обществе. Приводятся примеры таких правовых проблем.*

Ключевые слова: *трансформация, социальная трансформация, цифровая трансформация, интернет вещей, законодательство.*

Постановка проблеми. В останній період розвитку людства (3 – 4 століття) відбулося неочікуване та зростаюче в історичному контексті розширення, поглиблення та ускладнення економічних, виробничих, культурних, освітніх та інших соціальних зв'язків як в межах окремих держав, так і між державами. Одночасно, природньо відбулося значне кількісне та якісне збільшення суб'єктів суспільних відносин, які беруть участь або мають відношення до певних процесів в у суспільстві.

В таких умовах, прийняття обґрунтованих рішень вимагало все більшого обсягу інформації та даних про соціальні процеси, внутрішні та зовнішні умови їх реалізації, а також різнобарвної інформації про суб'єкти, які є дотичними до них. На відміну від попередніх часів, в останні 1 – 1,5 століття помітно зросла актуальність проблеми забезпечення прийняття оптимальних (раціональних) рішень в умовах:

– наростання бар'єрів організаційного, правового, інтелектуального, фінансового, економічного та технологічного характеру щодо забезпечення збору та оброблення інформації (даних), достатньої як за обсягом, так і за якістю;

– різкого збільшення обсягів різноманітної та різнорідної інформації, яку людина має споживати протягом доби, тижня, місяця або року;

– надто швидкої динаміки змін у часі мети та змісту політичних, урядових, соціальних, економічних, технологічних, культурних, освітніх процесів як в окремих державах, так у всьому світовому співтоваристві;

– постійного суттєвого підвищення вимог щодо швидкості та якості прийняття рішень;

– наявності природньої обмеженості когнітивних можливостей людства щодо збору та оброблення значного масиву інформації, швидкості та якості прийняття рішень.

Саме наявність фундаментальної проблеми обмеженості когнітивних здібностей людства робить досить проблематичною своєчасну реакцію на зміни параметрів зовнішніх і внутрішніх факторів, що впливають на соціальні процеси, а це, в свою чергу, є причиною: погіршення якості соціального моделювання, різкого скорочення часового горизонту впевненого прогнозування, особливо в частині середньо- і довгострокових стратегій розвитку, неприпустимого зниження якості і швидкості прийняття рішень.

Саме зниження якості і швидкості прийняття рішень людством спричинило формування перед початком XXI століття системи загрозливих цивілізаційних викликів: нераціональне розселення людства на планеті; обмеження продовольчих та виснаження планетарних ресурсів; погіршення екології та зміна клімату; зниження стійкості екосистеми існування людства; надзвичайно високі темпи соціальних процесів тощо.

Стосовно вкрай бентежної оцінки планетарного стану цивілізації та зовсім не райдужного прогнозу майбутнього людства добре відома позиція багатьох інтелектуалів і міжнародних організацій. Концентрованим вираженням такої позиції є доповідь Римського клубу "Come On! Капіталізм, короткозорість, населення і руйнування планети" [1]. Концентрована думка доповіді зводиться до наступного: результати планетарної діяльності людства ведуть до краху світової економіки, тому необхідно переглянути напрямки і зміст взаємодії урядів, підприємств, фінансових систем, інноваторів та сімей з нашою планетою.

Історично відомо, що відповіддю на цивілізаційні виклики стає майже безперервне проведення чисельних різноманітних соціальних трансформацій (реформ) у різних сферах діяльності соціуму, які відбуваються на особистому, корпоративному, локальному, національному, регіональному та міжнародному рівнях, що має місце майже у всіх країнах світу. Однією з таких загальновідомих реформ стала цифрова трансформація (цифровізація), яка спрямована насамперед на вирішення фундаментальної когнітивної проблеми людства.

З врахуванням дискусій, які відбувались останні декілька десятків років за участі політиків, урядовців, науковців, топ-менеджерів різноманітних світових компаній, фахівців та експертів з різних галузей діяльності, зокрема, і юридичної, можна сформулювати майже консенсусне розуміння особливостей здійснення соціальної та цифрової трансформації:

по-перше, реалізація будь-якої масштабної соціальної трансформації потребує відповідного правового забезпечення, яке здебільшого має базуватись на оновленому законодавстві;

по-друге, ефективність здійснення соціальної трансформації значно підвищується за умови синхронного проведення цифрової трансформації відповідних соціальних процесів;

по-третє, здійснення цифрової трансформації має наслідком появу особливостей в реалізації суспільних відносин з огляду на застосування цифрових технологій, що, як правило, обумовлює необхідність вдосконалення законодавства;

по-четверте, ефективність здійснення цифрової трансформації потребує відповідної синхронної соціальної трансформації як результату реалізації обов'язкового реінжинірингу соціальних процесів з метою спрощення їх алгоритмізації та подальшої оптимізації застосування цифрових технологій, що в свою чергу також потребує відповідного правового забезпечення;

по-п'яте, суттєвий вплив на якість формування правового забезпечення, вдосконалення законодавства має розуміння сутності, змісту та особливостей здійснення соціальної трансформації та цифрової трансформації.

Таким чином, актуальними є питання визначення сутності, змісту та особливостей соціальної трансформації та цифрової трансформації, з'ясування правових проблем формування правового забезпечення їх здійснення.

Метою статті є визначення дефініцій термінів "соціальна трансформація" та "цифрова трансформація" в інтересах правової науки, з'ясування змісту правових проблем, які можуть мати місце при формуванні правового забезпечення здійснення соціальної та цифрової трансформації.

Виклад основного матеріалу. Світова спільнота довгі десятиліття очікує від науковців та практиків результати об'єктивного аналізу системного стану цивілізації та планети, виявлення достовірних причин появи планетарних викликів, надійного прогнозування майбутнього розвитку та, що є головним, обґрунтованих рекомендацій щодо подолання негативних наслідків перманентних кризових явищ та їх уникнення в подальшому.

Але сучасна наука зазнає певних труднощів у розробці інструментарію щодо створення моделей глобального, регіонального, національного чи локального розвитку, які б були релевантними реальним соціальним процесам. Недосконаліть моделей розвитку в повній мірі є характерною практично для всього спектру соціального життя суспільства: зовнішня політика, державне управління, економіка, правоохоронна система, військова сфера, сфера охорони здоров'я, освіти, культури тощо, що має суттєві негативні наслідки. Особливо це стосується економіки, яка є основою життєдіяльності людства. Так використання недосконалих економічних моделей в процесі стратегічного та середньострокового прогнозування та планування, зазвичай, призводить як до макроекономічних помилок, навіть планетарного масштабу, так і до мікроекономічних прорахунків.

Постійні "позапланові" світові, національні та галузеві економічні кризи, неефективні рецепти виходу з них є яскравим свідченням недосконалості методів, способів і механізмів моделювання та прийняття рішень як при складанні прогнозних моделей економічного розвитку, так і в процесі практичної реалізації цих моделей. У реальному житті корекція або зміна економічних моделей розвитку, як правило, відбувається лише після факту встановлення наявності кризи або в цілому в економіці, або в окремому її сегменті, тобто іншими словами, реакція на кризові явища практично завжди відбувається з запізненням.

Низка експертів справедливо вважає, що саме результати сучасної економічної діяльності людства стали негативним чинником, що реально загрожують перспективам цивілізації на Землі. Це зумовило появу безлічі конкуруючих теорій виходу людства з кризового економічного становища [2], практично в кожній з яких пропонуються певні моделі проведення соціальної трансформації. Тому ми є свідками того, що протягом останнього століття майже безперервно в різних країнах світу відбувається проведення всіляких реформ, трансформаційних перетворень в державі та суспільстві, але без явного довготермінового позитивного результату.

Таким чином, ми спостерігаємо дію “вічного двигуна” – суспільство рухається по замкнутому колу: помилка у прийняті рішень (криза) – індикація причини кризи – побудова нової соціальної моделі – перехід до нової моделі (реформа) функціонування суспільства – функціонування нової моделі – нова криза …і так далі. Для того, щоб перервати це коло, вкрай важливо відповісти на питання: чому в процесі цивілізаційного розвитку виникають кризи?

В якості системної причини кризових явищ в економіці, які відбуваються все частіше, можна назвати базову причину – це постійне зниження якості рішень щодо визначення джерел кризових явищ, мети і змісту реформ та плану їх проведення, процесу здійснення реформ та в процесі подальшої поточної економічної діяльності. Зниження якості прийняття рішень пов’язано з наступним:

– постійне зростання темпів протікання соціальних процесів у порівняні з минулим;

– труднощі щодо отримання великих обсягів інформації про зовнішні та внутрішні умови здійснення економічної діяльності та про велику кількість об’єктів і суб’єкті, яка є необхідною для забезпечення релевантного опису соціальних процесів і створення адекватних економічних моделей;

– необхідність приймати рішення для великої кількості соціальних процесів в режимі реального часу;

– наявності природньої обмеженості когнітивних здібностей людини в частині збору та обробленні великих обсягів інформації (даних) для прийняття рішень, адекватних сучасним цивілізаційним викликам та сучасному стану соціальних процесів, внутрішніх і зовнішніх впливів;

– прогресуюча обмеженість когнітивних, фізичних і біологічних можливостей людини щодо здійснення великої кількості сучасних та майбутніх видів соціальної діяльності.

Неминучість трансформаційних процесів. Світова цивілізація, окремі держави, як і будь-які інші динамічні системи (біологічні, технічні або соціальні), розвиваються в умовах безперервних *зовнішніх і внутрішніх впливів* різної природи і різних форм, час настання і параметри яких не завжди є відомими. Загальне філософське уявлення про сутність терміну ***“динамічна система”*** наступне – *це система, стан якої змінюються в часі під дією зовнішніх і внутрішніх сил* [3].

Стійкість, яка є найважливішою властивістю, означає збереження динамічною системою своєї базової структури і основних показників виконання функцій протягом певного часу в умовах зовнішніх і внутрішніх впливів. Динамічна система (далі – ДС), як будь-яка система, характеризується структурою та сукупністю складових її елементів, їх функціоналом, внутрішніми та зовнішніми зв’язками, а також внутрішніми та зовнішніми впливами. При цьому в сучасній науці і практиці поняття “динамічна система” охоплює системи практично будь-якої природи – фізичні, хімічні, біологічні, технічні, економічні, соціальні тощо. До *соціальних динамічних систем* доцільно віднести окремі держави та їх міжнародні союзи, юридичні осіби публічного і приватного права та їх об’єднання, які здійснюють діяльність в будь-якому сегменті соціальної активності, фізичних осіб та їх об’єднання.

Зовнішні та внутрішні впливи можуть мати як позитивний, так і негативний характер дії на функціонування ДС. Позитивні впливи – це ті, які сприяють досягненню мети функціонування ДС і, як мінімум, не погіршують якісні характеристики цього функціонування. А негативні впливи – це впливи, які призводять до істотного погіршення якісних показників функціонування ДС і, навіть, можуть привести до неможливості досягнення мети функціонування (до функціональної загибелі ДС) .

Відомо, що *самозбереження* – це прагнення якомога довше зберегти своє життя, прагнення убезпечити себе від чогось [4]. Отже, ***самозбереження динамічної системи*** – *це така властивість, завдяки якої забезпечується досягнення цілей функціонування ДС шляхом нейтралізації дії негативних впливів*.

Таким чином, базовою умовою існування, функціонування і розвитку ДС є наявність такої фундаментальної атрибутивної властивості як самозбереження. Відсутність у ДС властивості самозбереження в умовах мінливих зовнішніх і внутрішніх негативних впливів веде до стагнації системи внаслідок зниження рівня якості функціонування, іноді, до трагічно низького рівня, що веде до її загибелі.

Наявність властивості самозбереження забезпечується спеціальною підсистемою адаптації ДС, яка призначена для нейтралізації дії негативних впливів, що перешкоджають досягненню мети функціонування ДС. Нейтралізація дії негативних впливів відбувається в результаті певної реакції ДС, ініційованої підсистемою адаптації, що як мінімум дозволяє зберегти якісні характеристики функціонування ДС та як максимум – створити найбільш сприятливі умови для їх підвищення.

Спектр змісту реакції ДС (формування керуючих впливів, а для соціальних ДС – це прийняття рішень) як відгуку на активність підсистеми адаптації може бути дуже широким: від зміни деяких внутрішніх параметрів ДС, проведення певної її внутрішньої трансформації (перебудови) на рівні цілепокладання, на функціональному та/або структурному рівнях до залучення зовнішніх ресурсів.

Таким чином, саме властивість самозбереження, яка дозволяє мінімізувати дію негативних впливів за рахунок змін (перебудови, трансформації) ДС, лежить в основі всіх процесів еволюції та розвитку в живій природі та соціальному середовищі.

Необхідно зауважити, що в найкращому випадку для забезпечення ефективності самозбереження підсистема адаптації повинна встигнути ініціювати необхідну реакцію на певний параметр негативного впливу, а ДС – встигнути сформувати і виконати відповідний керуючий вплив (прийняти та реалізувати рішення) раніше, ніж відбудеться наступна зміна цього параметру негативного впливу. Але, реальні ДС і їх підсистеми адаптації не можуть виконати зазначену умову тому, що вони мають низку обмежень щодо ініціювання та реалізації своєчасної реакції на негативні впливи, серед яких основним є обмеження щодо швидкості формування і виконання керуючого впливу (прийняття рішень), а також: інформаційні, енергетичні, структурні, просторові, ресурсні, організаційні, управлінські та, навіть, інтелектуальні обмеження. Сказане буде справедливим до тих пір, поки підсистема адаптації не матиме функції прогнозування, яка дозволяє заздалегідь, до настання події, пов’язаної з негативними впливами, ініціювати необхідну реакцію.

Підсумовуючи, констатуємо наступне: у будь-якій ДС реалізація функції самозбереження як основи існування і розвитку відбувається в умовах наявності протиріччя між необхідністю своєчасно реагувати на негативні впливи та об’єктивним існуванням обмежень щодо забезпечення необхідної якості та швидкості такого реагування.

Одним з найбільш ефективних шляхів вирішення зазначеного вище протиріччя є здійснення трансформації (зміни, перетворення) ДС.

Сформулюємо для цього дослідження базову категорію: ***трансформація*** – *це зміна, перетворення, або корекція мети функціонування, структур та/або функцій динамічної системи, зокрема, методів, способів і механізмів реалізації цих функцій, для нейтралізації або сприяння дії зовнішніх і внутрішніх впливів на подальший розвиток цієї системи.*

При цьому будемо розуміти, що ***розвиток –*** *це процес закономірної зміни, переходу з одного стану в інший, більш досконалий; перехід від старого якісного стану до нового, від простого до складного, від нижчого до вищого* [5].

Отже, з метою забезпечення ефективності властивості самозбереження ДС та її підсистема адаптації повинні бути здатні виконувати такі завдання:

– ідентифікація впливів;

– спостереження і прогнозування розвитку впливів;

– аналіз дії позитивних та негативних впливів на показники функціонування ДС;

– синтез цільових, функціональних, структурних та інших "пропозицій" щодо трансформації ДС, зокрема, щодо зміни правил поведінки (вдосконалення або створення нового законодавства) для мінімізації наслідків негативних впливів;

– формування "пропозицій" щодо шляхів, методів, способів та засобів забезпечення трансформації ДС;

– аналіз дії позитивних та негативних впливів на показники функціонування трансформованої ДС;

– корекція (за необхідності) попередніх "пропозицій" щодо трансформації ДС.

Описаний алгоритм повністю відповідає теорії Н. Вінера щодо управління зі зворотним зв'язком [6]. Саме наявність "зворотного зв'язку" в ДС, тобто наявність інформації про результати реалізації прийнятих рішень, дозволяє формувати керуючий вплив не тільки в залежності від змін внутрішніх та зовнішніх впливів, але і в залежності від ефективності реакції ДС на попередній керуючий вплив. Більш того, стає можливим при формуванні керуючих впливів враховувати результати прогнозування майбутніх станів внутрішніх і зовнішніх впливів, можливих трансформацій ДС тощо. Трансформаційні процеси в ДС дозволяють адаптувати її функціонування відповідно до мінливих внутрішніх і зовнішніх умов (впливів).

Оскільки, наявність будь-яких впливів, зокрема, негативних на функціонування ДС є апріорною внаслідок досить високого рівня ентропії навколишньої екосистеми, то для ДС необхідною умовою розвитку є наявність можливості проведення трансформацій. Або, іншими словами, в реальних умовах не вбачається можливим функціонування та розвиток динамічних систем без можливості проведення трансформаційних процесів.

Соціальна трансформація. Останнім часом для позначення процесів змін, модернізації, вдосконалення або реформування широко використовується термін "соціальна трансформація", метою якої оголошують забезпечення підвищення ефективності функціонування суспільства або окремих його частин. Але, за суттю процеси соціальної трансформації здійснювались протягом всього життя людства.

Історично можна нарахувати декілька переломних моментів в цивілізаційному розвитку, які потребували фундаментальних та системних змін засад функціонування суспільства. Як правило, індикатором необхідності проведення змін у суспільстві було різке зниження ефективності його функціонування, що мало наслідком погіршення умов існування людей та якості їх життя як на планеті в цілому, так і в окремих регіонах або країнах.

Одним з панівних методів здійснення соціальної трансформації (фундаментальних та системних змін у розвитку суспільства) є техніко-економічний метод, базовим критерієм якого є ефективність функціонування суспільства. Історія свідчить, що техніко-економічні методи трансформації реалізуються за допомогою промислових (технологічних, науково-технологічних тощо) революцій, результати яких сприймаються людством як революційні зміни в продуктивних силах суспільства та в організації його діяльності в найширшому сенсі [7].

Аналізуючи умови виникнення та результатів доходимо до висновку, що промислова революція завжди була відповіддю на цивілізаційний виклик, обумовлений виникненням

системного протиріччя між необхідністю забезпечення самозбереження і розвитку цивілізації та наявністю цивілізаційних системних обмежень щодо нейтралізації дії негативних впливів, які загрожували самому існуванню цивілізації.

До сучасних цивілізаційних викликів можна віднести наступні: невисока якість стратегічного планування розвитку окремих галузей, країн і цивілізації в цілому; різке підвищення взаємозв'язку і взаємозумовленості об'єктів, суб'єктів, процесів і явищ як в локальному, так і в світовому вимірі через всепоглинаюче проникнення глобалізації; необхідність наявності великих обсягів інформації та врахування великої кількості об'єктів і суб'єктів для релевантного опису соціальних процесів і прийняття рішень; необхідність приймати рішення в режимі реального часу; обмеженість когнітивних здібностей людини для прийняття рішень адекватних сучасному стану соціальних процесів, внутрішніх і зовнішніх впливів; обмеженість фізичних і біологічних можливостей людини для реалізації великої кількості сучасних і майбутніх видів соціальної діяльності.

Якісно новим у цьому переліку викликів є те, що частина з них пов'язана з обмеженістю когнітивних можливостей людини та обмеженістю її можливостей як біологічної істоти. Саме ці обмеження є однією з основних причин низького рівня ефективності процесу прийняття рішень людиною. До розгляду сутності цього виклику та шляхів його подолання повернемося пізніше.

Здійснення промислово-технологічних революцій з метою подолання певних історичних цивілізаційних викликів закономірно мало наслідком трансформаційні перетворення суспільного устрою, що відбивалось у змінах законодавства, тобто іншими словами промислово-технологічні революції супроводжувались певними соціальними трансформаціями.

На основі запропонованої дефініції категорії "трансформація" сформулюємо наступне визначення: ***соціальна трансформація*** *– це зміна, перетворення або корекція цілей, структури і функцій суспільства, зокрема, методів, способів і механізмів реалізації цих функцій з метою нейтралізації цивілізаційних викликів, які є загрозою ефективності його подальшого розвитку.*

Цифрова трансформація. Відповіддю на сучасні цивілізаційні виклики стала четверта промислова (технологічна) революція, до основних досягнень якої слід віднести інформаційні комп'ютерні технології (далі – ІКТ), мережу Інтернет, Інтернет-технології, Індустрії 4.0, штучного інтелекту, робототехніки, Великих даних, Хмарних обчислень, генної інженерії, електронних комунікацій, нано- та біотехнології тощо. Спільне застосування цих технологічних досягнень створює надпотужний синергетичний вплив на підвищення ефективності будь-якої людської діяльності, є основою забезпечення великої економії ресурсів, значного поліпшення якості життя людей тощо [8].

Масштабність впровадження досягнень четвертої промислово-технологічної революції як правило вимагає проведення певної соціальної трансформації як в межах окремої країни або групи країн, так і в межах всієї цивілізації. Це пояснюється тим, що синергія цивілізаційного ефекту від застосування нових технологій збільшується в геометричній прогресії за умови їх масштабування на основі широкого використання інформаційних комп'ютерних технологій (цифрових технологій) [9; 10].

Як добре відомо, широке застосування ІКТ та Інтернет-технологій, яке почалося з середини 60-х років минулого століття, вже наприкінці 90-х років практично у всіх державах сприймається як базова умова підвищення ефективності в будь-якій сфері людської діяльності.

Свідчення великої уваги світового співтовариства до застосування ІКТ знайшло відображення у розвитку ідеї інформаційного суспільства, яку розділяли практично всі

країни. Особливу роль у розвитку інформаційного суспільства в планетарному масштабі відіграла Всесвітня зустріч на вищому рівні з питань інформаційного суспільства (ВЗІС, World Summit on the Information Society, WSIS), яка проходила в два етапи – в Женеві (2003) та в Тунісі (2005) [11]). В результаті роботи форуму були прийняті документі: "Декларація принципів. Побудова інформаційного суспільства – глобальне завдання в новому тисячолітті" [12], Женевський план дій [13], Туніське зобов'язання [14] та Туніська програма для інформаційного суспільства [15].

В подальшому Генеральний секретар ООН робить щорічну доповідь про прогрес, досягнутий у реалізації рішень WSIS на національному, регіональному та міжнародному рівнях, а також щодо напрямів подальшої діяльності, пов'язаної з цим. В доповіді за 2019 рік були зроблені такі основні висновки та пропозиції [16]:

– зростають темпи розвитку технологій – більшість сучасних технологій, продуктів і послуг були в зародковому стані на початку 21 століття, включаючи соціальні мережі і хмарні технології, великі масиви даних і Інтернет речей;

– сфера охоплення найбільших ІТ компаній поширюється на передові технології, які створюють умови для розвитку інформаційного суспільства, включаючи штучний інтелект, машинне навчання, робототехніку та квантові обчислення;

– кібербезпека стала однією з головних турбот урядів, ділових кіл і громадян;

– швидкі темпи технологічного розвитку приведуть до зміни сучасного розуміння інформаційного суспільства;

– "цифрова взаємозалежність" людей вимагає постійного аналізу тенденцій в галузі технології та використання ІКТ і нових підходів до їх впровадження та управління ними з метою отримання максимальної вигоди та зведення до мінімуму ризиків;

– необхідно вивчати перспективи, ставити нові і більш широкі цілі розширення використання можливостей ІКТ з метою розвитку різних областей від навколишнього середовища до торгівлі та запобігання конфліктам.

Крім пильної уваги до проблем впровадження та використання ІКТ в світовому масштабі з боку ООН, спостерігається такий же інтенсивний процес на рівні регіональних міжнародних організацій і регіональних об'єднань – Ради Європи, ОБСЄ, Європейського Союзу, Організації американських держав, Африканського Союзу, Ліги арабських держав і великої кількості окремих держав.

Таким чином, сучасне людство пов'язує позитивні очікування в своєму розвитку з широким використанням ІКТ, перш за все, з досягненнями Інтернет-технологій, Індустрії 4.0, штучного інтелекту, робототехніки, Великих даних, Хмарних обчислень, електронних комунікацій тощо.

З урахуванням, сучасного осмислення результатів і перспектив розвитку широкого використання ІКТ, вважаємо за доцільне зробити наступне визначення: ***інформаційне суспільство*** *– суспільство в якому вся сукупність суспільних відносин максимально реалізується на основі використання інформаційних комп'ютерних технологій з метою підвищення ефективності діяльності в різних сферах (політика, економіка, державне управління, військова справа, охорона здоров'я, освіта, культура, розваги, особисте життя тощо)* [17].

З середини 20-го століття в лексикон людства послідовно входили поняття комп'ютеризація, інформатизація, інформаційне суспільство, цифровізація, які за своєю суттю відображають один і той же процес – процес повсюдного застосування та використання надзвичайно цікавих можливостей ІКТ, які дозволяють значно підвищити ефективність діяльності в будь-якій сфері соціальної активності. Оскільки критична маса передбачуваних соціальних реформ базується на використанні ІКТ, то поряд з терміном

“соціальна трансформація” став активно використовуватися термін “цифрова трансформація”.

На основі раніше наданих визначень понять будемо вважати, що ***цифрова трансформація*** *– це соціальна трансформація, яка відбувається на основі максимального використання цифрових технологій таких як: ІКТ, мережа Інтернет, Інтернет-технології, Індустрії 4.0, штучного інтелекту, робототехніки, обробки Великих даних, Хмарних обчислень, електронних комунікацій та багатьох інших*.

Виходячи з аналізу дефініцій і внутрішньої сутності соціальної трансформації та цифрової трансформації, можна зробити висновок про їх діалектичний зв’язок як категорій змісту і форми. Зміст – це соціальна трансформація, яка полягає в зміні або перетворенні організації суспільного життя, іноді докорінному. Застосування цифрових технологій в процесі здійснення соціальної трансформації означає особливу форму її реалізації – цифрову трансформацію. При цьому можуть мати місце відомі наслідки діалектичного зв’язку категорій змісту і форми. Конкретний зміст соціальної трансформації обов’язково детермінує вибір форм (методів, способів, засобів і механізмів) цифрової трансформації. У свою чергу обов’язковість забезпечення певних умов реалізації конкретних форм цифрової трансформації може призвести до необхідності проведення відповідної соціальної трансформації, або корекції її змісту, якщо соціальна трансформація передбачала здійснення цифрової трансформації.

Отже, цифрова трансформація може здійснюватися або в рамках соціальної трансформації як базова умова забезпечення ефективності останньої, або може здійснюватися самостійно. Але в останньому варіанті обов’язковим етапом здійснення цифрової трансформації є реінжиніринг соціальних процесів сфери діяльності, яка підлягає цифровізації, що, здебільшого, має наслідком необхідність проведення певної соціальної трансформації.

Правові проблеми. Ми маємо зробити висновок про те, що у загальному випадку й соціальна трансформація, й цифрова трансформація можуть призводити до:

– зміни парадигми функціонування держави, соціуму і його окремих сегментів, регіонів та галузей економіки, бізнесу та інших сфер життєдіяльності людей;

– зміни змісту і складу окремих складових системи суспільних відносин, які охоплюються ними, а іноді, навіть до появи нових за змістом груп суспільних відносин;

– переходу до нових інноваційних моделей публічного управління, економічної, виробничої, освітянської, будь-якої творчої діяльності та багатьох інших соціальних процесів.

Такі переміни у соціальній структурі суспільних відносин мають наслідком певну корекцію або зміну відповідної соціальної моделі суспільства та одночасно будь-яких інших видів моделей соціуму (економічної, інформаційної, правової тощо). А це неминуче тягне за собою трансформацію (вдосконалення) правової системи суспільства.

Дійсно, як правило, застосування чинної правової моделі регулювання суспільних відносин до нової (трансформованої) соціальної моделі суспільства призводить до виникнення правових проблем. Крім загальновідомих причин виникнення правових проблем, необхідно враховувати ще й те, що застосування цифрових технологій, зазвичай, стає каталізатором появи нових за змістом суспільних відносин або появи особливостей в реалізації вже відомих суспільних відносин. Отже, соціальна або цифрова трансформації, оскільки вони є джерелом виникнення правових проблем, мають супроводжуватися відповідними змінами системи законодавства, які в свою чергу мають бути обґрунтовані відповідними науковими правовими дослідженнями.

Таким чином, до питання виникнення і вирішення правових проблем в сучасних умовах необхідно підходити з системних, інтегральних позицій вивчення місії, цілей, завдань і наслідків як соціальної трансформації, так і цифрової трансформації суспільства. А це означає, що аналіз можливих правових проблем та пошуки шляхів їх вирішення також бажано розпочинати із найбільш загальних, базових положень правової системи які є дотичними до тієї чи іншої сфери здійснення соціальної та цифрової трансформації.

В цілому, виявлення та вирішення правових проблем, що супроводжують процеси трансформації або які виникають внаслідок цих процесів, є надскладним системним завданням, що потребує інтеграції зусиль представників не лише різних галузей права, але й залучення науковців, експертів та фахівців, які представляють різноманітні сфери практичної суспільної діяльності та різноманітні галузі знань.

Задля ілюстрації останньої думки наведемо приклади деяких правових проблем, поява яких пов'язана із застосуванням різних цифрових технологій, в основному тих, що зазначені у визначенні поняття "цифрова трансформація".

І. Мережа Інтернет.

На сучасному етапі розвитку людства мережа Інтернет, як технологічний засіб телекомунікацій, забезпечує передачу інформації практично на всіх рівнях суспільної діяльності: на міжнародному, міждержавному, національному, регіональному, локальному, корпоративному та міжособистому тощо. Технологічно передача практично всієї інформації здійснюється у формі даних (цифрових даних) за допомогою різних телекомунікаційних систем: фіксованих мереж (проводові, оптоволоконні, квантові, радіорелейні тощо) та мобільних мереж (стільникові, супутникові тощо). Загальносвітова мережа Інтернет складається із безлічі взаємопов'язаних локальних автономних мереж різної національної юрисдикції. Але питання регулювання забезпечення сумісності їх технологічного функціонування та організації адресного (доменного) простору кінцевих технічних пристроїв, між якими здійснюється передавання даних вирішується на міжнародному рівні.

Правові проблеми функціонування та розвитку мережі Інтернет:

створення сприятливих правових умов для динамічного будівництва високошвидкісного доступу до мережі Інтернет, зокрема, з використання інших об'єктів інфраструктури;

формування правового забезпечення конкурентного середовища для діяльності інтернет-провайдерів, зокрема, на житлових об'єктах населених пунктів;

визначення правових гарантій недопущення дискримінації за будь-якими ознаками щодо доступу за необхідними показниками якості до мережі Інтернет;

удосконалення законодавства щодо захисту прав населення як споживачів високотехнологічних послуг Інтернет-провайдерів;

визначення правових умов, бажано міжнародних, забезпечення сталого, надійного, безпечного, безперервного функціонування мережі Інтернет на всіх рівнях соціального користування.

ІІ. Штучний інтелект та робототехніка [17 – 19].

З початку третього тисячоліття вибухово збільшився інтерес до технологій штучного інтелекту (далі – ШІ) завдяки: різкому збільшенню попиту на точність і швидкість прийняття рішень людиною; значному здешевленню апаратної частини технологій ШІ; багаторазовому зростанню можливостей ШІ в моделюванні (відтворенні) людських когнітивних функцій; реальній можливості збору та обробки великої кількості даних; наявності розвиненої інфраструктури Інтернету тощо.

Визнається, що роботи з ШІ матимуть великий вплив на суспільство і повсякденне життя людей, дозволяючи вирішувати безліч важливих соціальних проблем з мінімальним використанням необхідних ресурсів при максимальній ефективності, неминуче стаючи при цьому необхідним атрибутом суспільних відносин або у якості їх об'єкта, або у якості їх суб'єкта. Без сумніву, застосування роботів із ШІ при наданні послуг та проведенні робіт, зокрема, в автономному режим, тобто без участі людини, має надто широкі перспективи у будь-яких сферах соціальної активності.

Можливе виконання роботами із ШІ ролі суб'єкта суспільних відносин може призвести до виникнення великої кількості правових проблем [20], частина з яких в даний час навіть важко піддається ідентифікації. Зміст дискусій на цю тему свідчить про невизначеність юридичної наукової думки про можливі шляхи вирішення цих проблем в рамках традиційної системи права.

Реакцією на все це стало прийняття за останні 3 – 4 роки біля сорока державами національних стратегій розвитку та використання ШІ, в яких основна мета – це динамічний і системний розвиток ШІ як базової умови підвищення конкурентоспроможності країн.

Застосування ШІ, роботів із ШІ як інноваційної форми здійснення діяльності в багатьох сферах людської активності, що забезпечує взаємозв'язок з матеріальними або нематеріальними об'єктами за участю або без участі людини, вимагає проведення системних і комплексних правових досліджень в рамках конституційного, цивільного, інформаційного, кримінального, адміністративного та інших галузей права.

Для вирішення основних правових проблем функціонування та розвитку ШІ, роботів із ШІ можна визначити наступні завдання:

– розробити визначення дефініції правових термінів "штучний інтелект", "робот", "робот із штучним інтелектом" визначити характеристики, показники, критерії оцінки тощо для кожного їх класу та типу;

– запропонувати юридично значиму класифікацію ШІ, роботів із ШІ на певні типи чи класи з огляду на автономність та безпеку застосування;

– провести дослідження особливостей реалізації правовідносин, юридичних прав, обов'язків і відповідальності сторін у разі використання роботів із ШІ різних типів чи класів;

– описати і дослідити особливості здійснення суспільних відносин в конкретних сферах суспільної активності (наприклад, у виробництві, ритейлу, транспорті, охороні здоров'я тощо) в умовах застосування роботів із ШІ різних класів та типів;

– визначити правові засади регулювання суспільних відносин, пов'язаних з використанням ШІ, роботів із ШІ різних класів та типів;

– обґрунтувати визначення юридичного статусу ШІ, роботів із ШІ різних класів та типів, запропонувати систему правових вимог до оформлення та юридичної фіксації цього статусу;

– розробити критерії щодо визначення юрисдикції ШІ, роботів із ШІ для різних варіантів організації їх функціонування, наприклад, для випадку коли програмне забезпечення буде розміщуватися в хмарних транскордонних технологіях;

– дослідити можливості створення юридично значимих методів, способів і механізмів визначення та фіксації причин і мотивів "поведінки" ШІ, роботів із ШІ;

– розробити рекомендації щодо можливості юридичної фіксації дій роботів, забезпечення прозорості, поліпшення звітності та можливості перевірки діяльності роботів із ШІ різних класів та типів;

– запропонувати систему правових вимог щодо забезпечення достовірності індикації та фіксації подій або явищ в реальному світі, факт наявності яких стає причиною для здійснення певних дій сторін правовідносин за умови використання ШІ, роботів із ШІ;

– дослідити та обґрунтувати визначення юридичних ризиків та обмежень використання ШІ, роботів із ШІ різних класів та типів в певних сферах застосування;

– запропонувати правові механізми нагляду, встановлення відповідальності за порушення правових вимог, юридичних зобов'язань та відшкодування завданих збитків;

– розробити пропозиції щодо процесуальних особливостей розгляду в суді суперечок, пов'язаних з правовідносинами за умови використання ШІ, роботів із ШІ;

– провести оцінки впливу на майбутнє цивільне законодавство [20] створення в довгостроковій перспективі особливого юридичного статусу для автономних роботів із ШІ, а також провести аналогічні дослідження для інших галузей права.

ІІІ. Технології Інтернету речей (Internet of Things, IoT).

Технології IoT застосовуються сьогодні чи будуть застосовуватись у найближчому майбутньому практично у всіх можливих сферах суспільної активності [21]. Тому завдання ідентифікації правових проблем для різних сфер застосування технологій IoT є вкрай актуальним та надто складним. Складність пояснюються наступним:

– з огляду на надзвичайно високі темпи розвитку суспільства маємо проводити аналіз майбутніх суспільних відносин у сферах та сегментах людської діяльності, які ще не існують або тільки-тільки народжуються;

– правовий аналіз має проводиться на засадах міждисциплінарного дослідження із одночасним залученням юристів практиків та законотворців;

– юридичні дослідження щодо ідентифікації правових проблем застосування технологій IoT від самого початку мають базуватись на міжгалузевому підході;

– юристи, які залучаються до аналізу правового регулювання існуючих або майбутніх суспільних відносин, мають на експертному рівні мати знання принципів, засад та закономірностей функціонування відповідних предметних сфер та сегментів людської діяльності.

В якості прикладу наведемо перелік ідентифікації правових проблем для деяких предметних сфер застосування технологій IoT:

а) сфера охорони здоров'я:

– недосконале законодавче регулювання надання послуг е-медицини, зокрема, щодо їх надання в дистанційному режимі;

– не визначені межі та зміст конкретної юридичної відповідальності для медичного персоналу, операторів телекомунікацій, виробників обладнання та розробників програмного забезпечення медичних комп'ютерних систем та пристроїв;

– не визначено національний правовий режим допуску на ринок медичних послуг програмного забезпечення для мобільних засобів, засобів діагностики, засобів здійснення інвазійних маніпуляцій тощо, що керуються дистанційно, або функціонують автономно із застосуванням ШІ;

– не сформульовані законодавчі вимоги щодо прозорості інформування населення про всі особливості надання медичних послуг з використанням технологій IoT;

– недосконале законодавство щодо правового режиму збору інформації в системі охорони здоров'я, зокрема, збору та використання персональних даних пацієнта та правових умов дистанційного доступу до е-картки пацієнта;

б) сфера електронних комунікацій, зокрема мережа Інтернет, як технологічна основа IoT:

– скасування ліцензування діяльності та лібералізація ринку надання послуг, введення економічних санкцій до порушників законодавства;

– вдосконалення прозорих правових умов для забезпечення справедливої конкуренції для учасників ринку з різною економічною вагою;

– посилення захисту прав споживачів технологічно складних послуг електронних комунікацій;

– недосконаліть правових гарантій незалежності регуляторного органу у сфері електронних комунікацій;

– недосконаліть правового визначення повноважень центрального органу виконавчої влади в частині формування державної технічної політики у сфері електронних комунікацій та користування радіочастотним ресурсом;

– непослідовне правове закріплення принципу технологічної нейтральності користування радіочастотним ресурсом;

– відсутність ефективного правового регулювання режиму колективного та спільного користування радіочастотним ресурсом;

– відсутність правового регулювання можливості користуванням “білими” діапазонами (White Space) радіочастотного ресурсу;

– відсутність правового режиму створення вторинного ринку правом користування радіочастотним ресурсом (Spectrum trading).

Зазначене стосується також багатьох інших сфер соціальної діяльності таких як, наприклад: промисловість, сільське господарство, банківська діяльність, енергетика, медицина, освіта, публічне управління, ретейл, збройні сили, транспорт тощо.

Зрозуміло, що на порядку денному актуалізується питання вдосконалення (модернізації) правових моделей застосування різноманітних технологій IoT шляхом організації проведення міжгалузевих теоретико-методологічних досліджень у цивільному, інформаційному, морському, транспортному, авіаційному, медичному, кримінальному, адміністративному, сімейному законодавстві тощо.

Висновки.

1. Соціальні динамічні системи (світова цивілізація, окремі держави, суб’єкти публічного та приватного права, юридичні та фізичні особи, об’єднання людей) функціонують в умовах постійних зовнішніх і внутрішніх впливів різної природи і різних форм, що призводить як до позитивних, так і до негативних наслідків. Момент дії цих впливів та значення їх параметрів, як правило, є невідомими та випадковими.

2. Базовою атрибутивною властивістю соціальних динамічних систем є самозбереження, завдяки чому забезпечується стійкий процес розвитку та досягнення цілей функціонування шляхом нейтралізації дії негативних впливів.

3. З метою мінімізації наслідків негативних впливів на функціонування соціальних динамічних систем вдаються до проведення соціальної трансформації, або іншими словами до проведення змін, перетворень, або корекції мети функціонування, структури і функцій суспільства або окремих його складових, в тому числі, методів, способів і механізмів реалізації його функцій, для нейтралізації або сприяння дії зовнішніх і внутрішніх впливів на його подальший розвиток.

4. До початку XXI століття людство усвідомило наявність комплексу викликів, що створюють загрозу існуванню цивілізації. Тому для мінімізації негативних наслідків цих цивілізаційних викликів на міжнародному та національних рівнях реалізується безліч

проектів соціальної трансформації різного спрямування та масштабності. Левова частка цих проектів базується на широкому використанні інформаційно-комп'ютерних технологій (цифрових технологій).

5. Процес широкого використання цифрових технологій, особливо під час здійснення соціальних трансформацій, отримав назву цифрових трансформацій.

Цифрова трансформація проводиться з метою нейтралізації цивілізаційних викликів та відбувається на основі максимального використання цифрових технологій таких як: ІКТ, мережа Інтернет, Інтернет-технології, Інтернет речей, Індустрія 4.0, штучний інтелект, робототехніка, обробка Великих даних, Хмарні обчислення, електронні комунікації та багатьох інших.

6. Соціальні та цифрові трансформації призводять до істотної зміни системи і структури суспільних відносин як в цілому в суспільстві, так і в окремих його сегментах, що призводить до необхідності зміни правової моделі суспільства, що в свою чергу є причиною необхідності проведення відповідних теоретико-правових досліджень щодо пошуку шляхів вирішення правових проблем та подальшого удосконалення системи законодавства.

7. Оскільки важливою ознакою сучасного глобалізованого світу є наявність всепроникаючих взаємозв'язків і взаємозумовленостей об'єктів, суб'єктів, процесів і явищ як в локальному, так і в світовому вимірі, то стає необхідним проведення ґрунтовних системних міждисциплінарних досліджень змісту, особливостей та закономірностей планування та здійснення конкретних соціальних та цифрових трансформацій, а вже на базі отриманих результатів цих досліджень проведення міжгалузевих правових досліджень з метою формування ефективного правового забезпечення таких трансформацій.

8. Крім правових проблем, втілення в життя стратегії здійснення соціальних та цифрових трансформацій, як правило, буде вимагати подолання значної кількості бар'єрів: політичних, мотиваційних, ментальних, освітніх, організаційних, фінансово-економічних, техніко-технологічних, безпекових (кібербезпеки), конфіденційності, сумісності, стандартизації тощо, що, в свою чергу, буде вимагати проведення додаткових правових досліджень.

Використана література

1. E Weizsaecker, A Wijkman, Come On! Capitalism, Short-termism, Population and the Destruction of the Planet (Springer-Verlag New York 2018) 220 <https://www.clubofrome.org/2017/10/25/new-report-to-the-club-of-rome-come-on> (дата звернення: 10.08.2021).

2. А Бобрышев, М Тарабрин, К Тарабрин, 'Формирование бизнес-модели устойчивой производственной компании' (Московская академия рынка труда и информационных технологий, 04 июля 2015) <http://www.cfin.ru/management/controlling/business_model.shtml> (дата звернення: 10.08.2021).

3. Ю Сачков 'Динамические системы'. Новая философская энциклопедия. Москва: Мысль, 2000) <https://iphlib.ru/library/collection/newphilenc/document/HASH018ddae872549bb 629 6a3b8d> (дата звернення: 10.08.2021).

4. 'Самосохранение'. Толковый словарь русского языка / под ред. Д. Ушакова (Гос. изд-во иностр. и нац. слов., 1935-1940) <https://ushakovdictionary.ru/word.php?wordid=67702> (дата звернення: 10.08.2021).

5. 'Развитие'. Толковый словарь Ожегова <https://slovarozhegova.ru/word.php?wordid =25714> (дата звернення: 10.08.2021).

6. Н. Винер. Кибернетика, или управление и связь в животном и машине. Москва: Наука, Главная редакция изданий для зарубежных стран, 1983. 344 с.

7. С. Булдыгин ‘Концепция промышленной революции: от появления до наших дней’ (2017) 420. *Вестник Томского государственного университета* <https://cyberleninka.ru/article/n/kontseptsiya-promyshlennoy-revolyutsii-ot-poyavleniya-do-nashih-dney> (дата звернення: 10.08.2021).

8. L Yongxin and others, ‘The impact of the fourth industrial revolution: a cross-country/region comparison’ (SciELO, 2018) <https://www.scielo.br/j/prod/a/hRmXgtCKq6qbwMkK4nVkj8g/?lang=en> (дата звернення: 10.08.2021).

9. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services (World Economic Forum, 2015) 39 <http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf> (дата звернення: 10.08.2021).

10. The Future of Jobs. Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution (The World Economic Forum, 2016) 157 <www3.weforum.org/docs/WEF_Future_of_Jobs.pdf> (дата звернення: 10.08.2021).

11. World Summit on the Information Society (ITU, WSIS 2015) <http://www.itu.int/net/wsis/basic/about.html> (дата звернення: 10.08.2021).

12. Declaration of Principles. Building the Information Society: a global challenge in the new Millennium (ITU, WSIS, 12 December 2003 <http://www.itu.int/net/wsis/docs/geneva/official/dop.html> дата звернення: 10 серпня 2021.

13. Plan of Action (ITU, WSIS 12 December 2003) <http://www.itu.int/net/wsis/docs/geneva/official/poa.html> (дата звернення: 10.08.2021).

14. Tunis commitment (ITU, WSIS, 18 November 2005) <http://www.itu.int/net/wsis/docs2/tunis/off/7.html> (дата звернення: 10.08.2021).

Tunis agenda for the information society (ITU, WSIS, 18 November 2005) http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (дата звернення: 10.08.2021).

15. ‘Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels’ Report of the Secretary-General United Nations (UNCTAD, 13 Jan 2020). <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2625> (дата звернення: 10.08.2021).

16. О Баранов, Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія (Київ: Едельвейс 2014) 497.

17. О Баранов, ‘Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом’ (2018) 4 *Інформація і право*. 46.

18. О Баранов, ‘Правові аспекти національних стратегій розвитку штучного інтелекту’ (2019) 7 *Юридична Україна.* 21.

19. О Баранов, ‘Інтернет речей і штучний інтелект: витоки проблеми правового регулювання’ ІТ-право: проблеми та перспективи розвитку в Україні: ІІ-а Міжнародна науково-практична конференція (НУ “Львівська політехніка”, 2017). 18.

20. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics - Strasbourg. European Parliament 16 February 2017 <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect> (дата звернення: 10.08.2021).

21. О Баранов, Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар’єри, проблеми правового регулювання: монографія (Видавничий дім “АртЕк” 2018). 344.

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

УДК 342.951

МАЄТНИЙ М.І., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-9123-0706.

ШТУЧНІ НЕЙРОННІ МЕРЕЖІ: ПЕРСПЕКТИВИ ВИКОРИСТАННЯ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Анотація. *Проаналізовано окремі заходи у рамках виконання зарубіжного законодавства, присвячені питанням використання штучних нейронних мереж. Обґрунтовано результативні показники впровадження штучних нейронних мереж у правоохоронну діяльність. Розглянуто здобутки, отримані за результатами використання штучних нейронних мереж у правоохоронну діяльність. Окреслені загальносвітові тенденції розвитку та використання штучних нейронних мереж для потреб правоохоронної діяльності.*

Ключові слова: *інформаційне забезпечення, штучні нейронні мережі, штучний інтелект, цифрові технології, злочинність, система безпеки, кримінальна статистка.*

Summary. *Some measures within the framework of foreign legislation on the use of artificial neural networks are analyzed. The effective indicators of introduction of artificial neural networks in law enforcement activity are substantiated. The achievements obtained as a result of the use of artificial neural networks in law enforcement are considered. The general tendencies of development and using of artificial neural networks for the needs of law enforcement activity are outlined.*

Keywords: *information support, artificial neural networks, artificial intelligence, digital technologies, crime, security system, criminal statistics.*

Аннотация. *Проанализированы отдельные мероприятия в рамках исполнения зарубежного законодательства, посвященного вопросам использования искусственных нейронных сетей. Обоснованы результативные показатели внедрения искусственных нейронных сетей в правоохранительную деятельность. Рассмотрены достижения, полученные в результате использования искусственных нейронных сетей в правоохранительной деятельности. Очерчены общемировые тенденции развития и использования искусственных нейронных сетей для потребностей правоохранительной деятельности.*

Ключевые слова: *информационное обеспечение, искусственные нейронные сети, искусственный интеллект, цифровые технологии, преступность, система безопасности, уголовная статистика.*

Постановка проблеми. В сучасних умовах інформаційно-комунікаційні технології стали невід'ємною частиною сучасних управлінських систем у всіх галузях економіки, сферах державного управління, оборони, безпеки держави та забезпечення правопорядку, протидії злочинності. Разом з тим застосування сучасних цифрових технологій та штучного інтелекту формують нові платформи побудови взаємовідносин між громадянами, державними інституціями, громадянським суспільством, Інтернет речей тощо. Використовуючи розширені можливості комунікацій та відповідні онлайн-платформи, держава намагається контролювати цифрову інфраструктуру, відстежувати та здійснювати моніторинг переконань та уподобань тих чи інших соціальних груп населення. Проте міжнародно-правові механізми, які дозволяють відстоювати суверенне право держав на регулювання інформаційного простору, у тому числі, у національному сегменті мережі Інтернет, остаточно не встановлені. Більшість країн світу вимушені

“на ходу” адаптувати своє законодавство та впроваджувати державне регулювання сфери інформаційних технологій, у тому числі й цифрових.

Зусилля переважної більшості держав світу спрямовані на пріоритетний розвиток національної інформаційної сфери та її складових. Популярність цифрової економіки як принципово нової моделі розвитку глобальної економічної системи постійно зростає. У зв’язку із постійним збільшенням чисельності населення планети, цифровізації суспільства, активізації формату споживання різноманітних ресурсів, електронна економіка здатна вплинути на кожний аспект життєдіяльності людини у сучасному світі, зокрема у таких кластерах, як: промисловість, охорона здоров’я, освіта, соціальна політика, сільське господарство, культура. Збільшуються темпи зростання сучасних технологій, створених на основі передових знань (нано- та біотехнології, штучний інтелект, альтернативні джерела енергії). Створення, обробка та поширення інформації значно перевищили можливості більшості людей в опануванні та застосуванні знань, що призвело до появи нової моделі сприйняття великих масивів інформації, яка значно спрощує масштабне поширення та використання інформаційно-цифрових технологій та штучного інтелекту у повсякденному житті пересічних громадян та у питаннях державного управління, правоохоронної діяльності тощо.

Інформація являє собою велику цінність, а розвиток технологій її передачі та обробки визначив подальший розвиток широкого спектру злочинної діяльності, пов’язаної з незаконним доступом до інформації та її подальшого протиправного використання. Таким чином, формування сегменту сучасних економічних відносин у поєднанні з передовими технічними досягненнями, глобальною мережею та інформаційними системами являє собою цифрову економіку, а головним фактором її ефективного забезпечення стає впровадження технологій обробки даних, що дає змогу значно зменшити витрати під час виробництва товарів та надання послуг. За таких умов саме новітні цифрові технології та штучний інтелект визначатимуть майбутнє та сприятимуть динамічним змінам різноманітних соціальних регуляторів у світовому вимірі.

В сучасних умовах існує чимало технологічних рішень, які застосовуються з метою централізованого моніторингу і спостереження за кримінальною обстановкою у “розумних” містах. У світових масштабах сучасні реалії мегаполісів і більш дрібних міст такі, що під наглядом повинна знаходитися якомога більша кількість вулиць, кварталів, житлових і промислових об’єктів тощо. Інтелектуальні системи безпеки, які керовані командними центрами у поєднанні з системами відеоспостереження, дійсно ефективні у питаннях спостереження, запобігання терористичним атакам, диверсіям та іншим злочинам. В розбудові інфраструктури смарт-міст процесам забезпечення безпеки відводиться одна з ключових ролей. На цьому фоні тематика розвитку штучних нейронних мереж та цифрових технологій та їх використання у масштабах правоохоронної діяльності набуває неабиякої актуальності.

Результати аналізу наукових публікацій. Технології штучного інтелекту та їх вплив на стан забезпечення кібербезпеки певною мірою досліджували у своїх працях такі науковці: В. Брижко [1], О. Бусол [2], В. Савченко [3] тощо. Питання правового врегулювання засад розвитку штучного інтелекту розглядали: О. Баранов [4], А. Бежевець [5], О. Косілова [6], О. Кривецький [7], О. Радутний [8] тощо. Проте вбачаються недостатньо висвітленими питання використання штучних нейронних мереж у правоохоронній діяльності, у зв’язку із чим потребують детального розгляду зарубіжні ініціативи, які впроваджуються останнім часом у цій площині.

Метою статті є узагальнення кращих практик зарубіжного досвіду використання штучних нейронних мереж та на підставі їх аналізу визначення дієвих шляхів удосконалення з покращення результативності правоохоронної діяльності.

Виклад основного матеріалу. Сучасні штучні нейронні мережі складаються з великої кількості простих процесорних елементів з деякою кількістю локальної пам'яті (нейронів), об'єднаних за допомогою дискретних або неперервних комунікаційних каналів. Задачі, що вони розв'язують, підлягають декомпозиції на множину локальних завдань, кожне з яких може бути розв'язане за допомогою окремого нейрону шляхом реалізації певного алгоритму обробки локальних даних. Вірогідно, що у сучасних умовах для більшості передових держав світу штучний інтелект та новітні цифрові технології як важливі складові цифрової економіки мають вирішувати не тільки звичайні повсякденні завдання, а також стати ефективним інструментом у боротьбі з організованою злочинністю та корупцією.

Так у КНР вирішили подолати корупцію за допомогою саме штучних нейронних мереж та їх активного впровадження. Китай, безумовно, є однією з найбільш високотехнологічних держав у світі, яка потужно розвиває штучний інтелект та цифрові технології вже застосовує удосконалені системи у сфері державного менеджменту. Так, наприклад, в деяких регіонах КНР з 2012 року працює національна система безпеки, що відстежує громадян за допомогою системи розпізнавання обличчя та ідентифікації особи. Інші ж цифрові технології успішно допомагають контролювати роботу правоохоронних органів та навіть захищають державні бази даних від стороннього несанкціонованого втручання.

У 2012 році в КНР розпочала функціонування система "Zero Trust" (нульова довіра) на основі штучного інтелекту. Розроблена Китайською академією наук для "внутрішнього контролю, оцінки або втручання в роботу і особисте життя державних службовців", назараз "Zero Trust" працює тільки у 30 регіонах та містах, – понад 1 % від адміністративних територій КНР у форматі пілотного проекту. Повномасштабне запровадження цієї системи у КНР очікується у найближчій перспективі, оскільки існує формат "недовіри" політиків до сучасних цифрових технологій. Система "Zero Trust" має доступ до 150 захищених баз даних, може створити аналітику поведінки державних службовців, виявляти підозрілі операції відчуження чи набуття власності, факти незаконного будівництва, придбання землі або знесення будинків, незаконного збагачення з використанням тіньових схем.

Операційно система також передбачає постійний аналіз великого масиву даних, що зумовлює використання інформації з абсолютно різних джерел. Наприклад, можливо залучення супутників для того, щоб відстежити, що гроші на будівництво сільської дороги дійсно були витрачені за цільовим призначенням, чи провести аналіз інформації з банківських рахунків, на випадок, якщо помічено підозріле збагачення або покупка на велику суму. За переконанням розробників, головною проблемою системи "Zero Trust" став той факт, що штучний інтелект допомагав декларувати потенційну корупційну активність, але не завжди надавав пояснення, яким саме чином системні алгоритми це вирахували. Враховуючи такий стан справ, ця технологія залишається тільки допоміжним інструментом, а кінцеве рішення повинні приймати правоохоронні органи, які здійснюють боротьбу з корупційними злочинами.

Проте, навіть функціонування китайської системи "Zero Trust" у тестовому режимі за шість років з 2012 по 2018 роки, надала змогу викрити або попередити незаконні дії майже 9000 державних службовців, більшість з яких зберегли свої посади, але отримали попередження або мінімальні покарання. Лише деякі з них були засуджені до реальних

строків тюремного ув'язнення. За стратегічним задумом метою діяльності системи "Zero Trust" мало стати попередження корупційних ризиків, адже до політиків, вина яких була доведена, замість дисциплінарних заходів, застосовувалися занадто жорсткі покарання, що, певним чином, стурбувало співробітників державного апарату. Щодо подальшої долі системи штучного інтелекту технології "Zero Trust" поки невідомо, але деякі китайські політики вже виносять на обговорення питання про її законність, оскільки доступ комп'ютерних або роботизованих систем до закритих баз даних законодавчо жодним чином не регламентовано на території КНР. Деякі експерти прогнозують, що вона швидше за все буде працювати на загальнонаціональному рівні лише вибірково. Враховуючи такий стан справ, Китай вирішив відмовитися від впровадження такої антикорупційної системи, враховуючи її високу ефективність. Також політична влада КНР ще у липні 2017 року анонсувала, що до 2030 року планує побудувати індустрію штучного інтелекту з обігом $150 млрд. США. При цьому саме протидія злочинності має стати основною функцією штучного інтелекту. Однією із найбільш амбіційних розробок Китаю у цій сфері має стати система "Поліцейська хмара", яка, за задумом, повинна збирати інформацію з історій покупок у торгівельній мережі, замовлень доставок їжі, відвідувань лікарень, під час яких збираються зразки ДНК та з інших джерел. Система схожа до методів збору даних для визначення соціального рейтингу громадян та інтегрує масиви даних, починаючи від ip-адреси, аккаунтів, телефонних номерів, вхідних та вихідних дзвінків і закінчуючи придбанням даних про користувачів у приватних компаній, отримуючи при цьому доступ до *mac*-адрес персональних комп'ютерів та інформації з їх роутерів.

Слід також зазначити, що штучні нейронні мережі активно використовуються поліцейськими США з метою профілактики та попередження злочинності. Ще у 2009 році приватна американська компанія "Palantir Technologies" розробила сучасне програмне забезпечення під кодовою назвою "Palantir" з метою прогнозування поширення злочинності [9]. Ця компанія відома співпрацею із спецслужбами та урядовими установами, кілька років тому потайки запровадила у одному з міст США поліцейську технологію з метою прогнозування правопорушень. Секретна програма виявляла та відстежувала зв'язки членів банд. Вона аналізувала соцмережі та передбачала ймовірність того, що ті чи інші особи вчинять злочин або стануть жертвами. Співпраця стартапу з владою Нового Орлеану активно розпочалася у 2012 році. Тоді "Palantir Technologies", одним із постійних замовників якого було Центральне розвідувальне управління, надав своє ПЗ у вигляді неофіційної благодійної допомоги. Більшість урядовців Нового Орлеану – окрім вузького кола на чолі з мером Мітчем Ландре – не знали про цей проект.

Основний операційний функціонал цієї програми спрямований на візуалізацію великих масивів інформації, що допомагає працівникам правоохоронних органів встановлювати причино-наслідковий зв'язок між поведінкою осіб та скоєними ними правопорушеннями. Після тривалого використання поліцейськими Нового Орлеану та спецслужбами США "Palantir Technologies" запатентував свою систему прогнозування злочинності, зокрема терористичної діяльності. Використання поліцією алгоритмів полягає у прогнозуванні злочинної поведінки. Наприклад, один із інструментів програми зазначеної компанії "HunchLab" об'єднує статистику злочинності із соціально-економічними даними, іншою оприлюдненою інформацією з метою визначення найбільшої вірогідності скоєння правопорушення. Практичне використання цієї системи поліцейськими Чикаго дозволило завдяки новітнім технологіям суттєво знизити рівень злочинності. Інша програма – "Готем" використовується поліцейськими для

розпізнавання та затримання майбутніх злочинців. Інформація з протоколів затримань, матеріалів кримінальних справ завантажується в єдину базу, яка формує відповідний список осіб, які мають відношення до криміналітету. У США програми прогнозування злочинності досить часто мають непублічний характер, у зв'язку з чим громадян не попереджають про використання таких систем, оскільки актуальним питанням у США стала легітимність підстав для обміну даними та конфіденційність такої інформації. Саме тому деякі міста (Сієтл, Окленд) схвалили відповідні місцеві закони, а інші мегаполіси на рівні муніципалітетів ще й досі обговорюють питання забезпечення конфіденційності інформації в епоху цифрових технологій. Протягом двох років функціонування програми аналізу компанії "Palantir Technologies" відбулося різке зменшення кількості вбивств та актів насильства з використанням зброї, проте згодом результати практичного застосування продемонстрували зменшення її ефективності. Інші розроблені інструменти під назвою "Strategic Subject's List" та "ShotSpotter" визначають вірогідність місць вчинення злочинів на основі активності вуличних банд та продавців наркотиків. У 2017 році в Каліфорнії відкрили "Кримінологічний центр режиму реального часу", який займається прогнозуванням можливостей скоєння злочинів та визначає "потенційний ступінь загрози" з боку окремих категорій громадян.

За переконанням вчених та поліцейських штучний інтелект не є панацеєю, оскільки він не може впливати на причини та передумови, які породжують злочинність, наприклад такі як недоступність освіти або відсутність економічних можливостей у певної особи. Проте позитивним моментом впровадження штучного інтелекту у правоохоронну діяльність стало розширення можливостей прогнозування, оскільки воно стає швидшим, дешевшим і якіснішим. Цей інструмент має тенденцію до більш широкого використання. Для використання штучного інтелекту потрібно обов'язково додати камери та пристрої радіолокації й лазерної локації (LIDAR), за допомогою яких він отримуватиме дані та намагатиметься передбачити, які можуть бути подальші дії злочинця. Про намір залучити роботів до служби в поліції повідомили в прес-службі поліцейського управління Дубаї. Спочатку заплановано використовувати їх для проставлення штампів на документах, нагадування про справи та важливі робочі моменти, фіксації різного роду порушень роботи, а прикордонники мають намір обладнати аеропорти системою розпізнавання не задекларованих речей.

У Великобританії створена власна система профілактичних заходів з метою запобігання використанню мобільних телефонів під час руху за кермом. Щоб зрозуміти, чому дорожній безпеці приділяється так багато уваги в усьому світі, звернемося до офіційних даних: наприклад, у США мобільні телефони стають причиною 70 тисяч ДТП на рік, а у Великобританії розмова по телефону за кермом призводить до одного летального випадку кожні 10 днів.

Профілактика ДТП приносить свої результати і велике значення тут мають сучасні технології, а саме системи штучного інтелекту. В Австралії, наприклад, поліція впроваджує нові дорожні камери, призначені для відстеження водіїв, які розмовляють по телефону під час руху. Після успішного тестового періоду, що завершився у жовтні 2018 року, штрафи отримали понад 11 тисяч водіїв. Працює така технологія на основі сенсорних радарних систем, що роблять фотографії водіїв через вітрове скло. Потім зроблені фото передаються до нейронної мережі, яка аналізує знімок людини на предмет наявності мобільного телефону. Неправомірність дій водія можна легко довести на підставі фотографії. З появою платформи iOS 11 користувачам iPhone стала доступною нова вбудована функція "Не турбувати під час водіння". У цьому режимі блокуються вхідні дзвінки і будь-які повідомлення. Ця технологія також доступна на смартфонах з

ОС Android. Сучасні глобальні системи безпеки реагують на погодні умови, тремтіння камери, тіні і навіть ворушіння листя, використовують технологію розпізнавання обліч. Сейсмічні датчики вміють розрізняти транспортні засоби або людей.

Для запобігання масовим заворушенням, терактам, забезпечення безпеки на концертах або інших масових скупченнях людей теж розробляються спеціальні технологічні рішення. Наприклад, компанія "Evolv Technology" розробила машину безпеки на базі штучного інтелекту, що працює через додаток "Evolv Pinpoint" і використовує функцію розпізнавання обліч. Конструкцію можна встановити на вході у комерційні установи, школи, торгові центри, аеропорти, нічні клуби, ресторани і т.д. Для перевірки людині досить пройти через конструкцію як через звичайний металошукач. Пропускна можливість такого детектора становить 600-900 осіб на годину. Перевірка проводиться вбудованою камерою, алгоритми "Evolv Pinpoint" зіставляють особи відвідувачів з особами в списку спостереження, завантаженому у базу даних системи. Якщо з'ясовується, що відвідувач представляє інтерес для поліції або інших служб, його зображення і особисті дані відображаються на планшеті співробітника служби безпеки, що підсвічуються червоним кольором. Жовте підсвічування говорить про неперевірену загрозу. Тоді профіль перевіряється у реальному часі протягом декількох секунд.

Проте штучні нейронні мережі не позбавлені недоліків. Оскільки штучний інтелект базується лише на даних, які відомі, він може працювати некоректно у деяких випадках. Так, якщо злочинець раніше не стикався з правоохоронними органами і не був засуджений, про нього не буде інформації. Відтак програма вважатиме, що він становить меншу загрозу для суспільства.

Україна динамічно рухається у цьому напрямку. Так, задля забезпечення громадської безпеки, збору доказів злочину, пошуку і затримання злочинців, охорони власності, дотримання правил дорожнього руху Національна поліція України використовує системи відеоспостереження силових структур і приватних власників [10]. У вересні 2020 року Міністерство юстиції України анонсувало сучасний пілотний проект, у рамках якого запроваджується програмне забезпечення з елементами штучного інтелекту для того, щоб аналізувати злочинців та визначити, чи можуть вони в майбутньому знову порушувати закон. Нова розробка Мін'юсту з елементами штучного інтелекту під назвою "Касандра" використовується з метою аналізу ймовірності повторного порушення закону певним злочинцем. Програмне забезпечення "Касандра" – це не окрема програма, а фактично одна з вкладок єдиного реєстру засуджених і взятих під варту, яка включає в собі оцінку ризиків і потреб.

Ця розробка фактично автоматизує процес створення досудової доповіді, де характеризується особистість обвинуваченого та його схильність до повторного скоєння злочинів. Наразі розглядається можливість аналізування "Касандрою" реєстрів не лише Міністерства юстиції, а й інших відомств. На даний час програма не лише поповнюється даними з реєстру, а здійснює попередню обробку анкет людей, виставляючи їм бали. З роками "Касандра" стане більш оперативною та, маючи великі масиви даних, почне перевіряти, чи адекватно надано оцінку ймовірності рецидиву в кожному конкретному випадку. В сучасних умовах "Касандра" формується вручну, але при наповненні реєстру максимально можливими даними, цей процес буде відбуватиметься автоматично. Можливості для подальшого використання цього інструменту є дуже широкими як і для контролю за правопорушниками, так і для запобіжних аспектів. Йдеться про належне проведення з ними спеціальної виховної роботи тощо. Таким чином, програмне забезпечення "Касандра" працює у форматі підсистеми Єдиного реєстру засуджених осіб та осіб, взятих під варту.

Висновки.

Впровадження штучних нейронних мереж в різноманітні сфери життя здатне якісно його змінити, що сприятиме підвищенню результативності будь-якої діяльності, у тому числі й правоохоронної. Найбільш активно застосовуються штучні нейронні технології в таких країнах, як США, Японія, Китай, Німеччина. Інтелектуальна реальність сьогодні передбачає широку практику застосування, зміст якої формує низку перспективних напрямків розвитку розумних технологій. Очікується, що довіра до інтелектуальних технологій в рамках діяльності правоохоронних органів буде активно зростати і стимулювати появу нових унікальних рішень.

Ключовим аспектом у реалізації інноваційних проектів стане розуміння представниками влади необхідності зміцнення співпраці з дослідницькими і науковими центрами, а також доцільності належного фінансування сфери інновацій. Саме штучні нейронні системи за допомогою відповідних програм, камер і датчиків руху здатні стежити за порядком на вулицях міста і в місцях масового скупчення людей, прогнозувати виникнення небезпечних та кризових ситуацій і навіть впізнавати обличчя злочинців. Також розумні системи штучного інтелекту здатні з точністю проводити звірку документів, запобігаючи крадіжкам персональних даних.

Штучний інтелект неможливо убезпечити від помилок і впливу зовнішніх чинників. Не можна недооцінювати роль та значення сучасних розробок штучного інтелекту та передових цифрових технологій, які впроваджуються у зарубіжних країнах з метою профілактики та боротьби зі злочинністю.

Враховуючи таку динаміку, міжнародними експертами прогнозується, що до 2030 року у світі будуть мінімізовані прояви поширення злочинності. Отже, технічні та технологічні досягнення, зокрема штучні нейронні мережі, суттєво допомагають та спрощують роботу правоохоронців в усьому світі. Окрім того, вони захищають правоохоронців від нещасних випадків чи надмірної агресії. До того ж штучний інтелект працює над алгоритмами пошуку серійних вбивць та маніяків для того, щоб зробити людське життя більш безпечнішим та комфортнішим.

Вбачається, що ключовими напрямами підвищення конкурентоздатності цифрових інформаційних та комунікаційних технологій мають стати: стимулювання створення організацій та суб'єктів господарювання, які здійснюють діяльність, спрямовану на розвиток усього спектру сервісів цифрової економіки (екосистеми економіки); забезпечення трансферу іноземних технологій та застосування кращих практик зарубіжного досвіду у сфері впровадження інформаційних технологій у правоохоронну діяльність. У зв'язку з великою швидкістю та інтенсивністю еволюційних процесів більшість інформаційних систем вітчизняних правоохоронних органів, що були створені понад 10 років, потребують модернізації. Це, наприклад, Інтегрована міжвідомча інформаційно-телекомунікаційна система контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон.

Основними напрямами такої модернізації має стати використання засобів електронної ідентифікації, захищених електронних каналів передачі даних, систем контролю якості інформації, систем аналізу даних, систем управління інформаційною безпекою. Безумовно, передовий зарубіжний досвід у сфері інформаційного забезпечення заходів у сфері боротьби зі злочинністю доцільно адаптувати у роботі вітчизняних правоохоронних органів. Також потребує прискорення запровадження дієвий механізм взаємодії та налагодження конструктивної співпраці між правоохоронними органами та науково-дослідними установами, спеціалізованими у ІТ-промисловості. В даному контексті вважається доцільним впровадити в поліцейську діяльність відповідне

програмне забезпечення систем штучного інтелекту, у тому числі й з використанням системи трансферу технологій.

Саме штучні нейронні мережі та сучасні цифрові технології допоможуть швидко обробляти великі масиви інформації, які доцільно опрацьовувати під час здійснення розслідування та попередження будь-якої злочинної діяльності. Також доцільно визначити на державному рівні перелік потенційних ІТ-компаній, які виступають розробниками відповідних програм штучного інтелекту та аналізуватимуть інформаційні системи правоохоронних органів, державних реєстрів, інших інформаційних джерел з метою пошуку потенційних злочинців. Впровадження цифрових технологічних досягнень в діяльність правоохоронних органів надасть змогу значно підвищити ефективність їхньої роботи, забезпечити громадську безпеку.

Використана література

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

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

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

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

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

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

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

8. Радутний О.Е. Кримінальна відповідальність штучного інтелекту. *Інформація і право*. № 2(21)/2017. С. 124-132.

9. Американський стартап таємно випробував систему передбачення злочинів. URL: https://techno.nv.ua/ukr/innovations/velikij-brat-amerikanskij-startap-tajemno-viprobuvav-u-novomu-orleani-sistemu-peredbachennja-zlochiniv-2455319.html

10. Мордвинцев М.В. Хлєстков О.В., Ницюк С.П. Сучасний стан систем інтелектуального відеоспосереження які використовуються в діяльності Національної поліції України: зб. матеріалів круглого столу *Застосування інформаційних технологій у діяльності правоохоронних органів,* м. Харків, 9 грудня 2020 р. – (МВС України, Харк. нац. ун-т внутр. справ). Харків: ХНУВС, 2020. С. 88-90.

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

УДК 347.77.78:004.738.5 (045)

ІЗБАШ О.О., *кандидат юридичних наук, доцент,* доцент кафедри загальноправових дисциплін Національного університету "Одеська морська академія".

ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ У ЦИФРОВОМУ ПРОСТОРІ

Анотація. *У статті розглядається сучасний погляд на мистецтво у цифровому просторі та питання регулювання інтелектуальної власності у зв'язку з цим феноменом. Автор розкриває поняття блокчейну та невзаємозамінного токену, їх розвиток та вплив на права творців. Зараз перед цифровими художниками існує багато викликів. Одним із них є те, що предмети цифрового мистецтва можна легко копіювати, і робити це скільки завгодно. Так, багато хто скаже, що можна просто зберегти собі картинку й таких збережених копій може бути безліч, які не відрізняються від оригіналу. Але є один нюанс, а вірніше можливість, яку дає саме NFT – це право володіти оригінальною версією роботи. Це наче мати оригінал картини, яку виставлено в Луврі, а інші репродукції й копії поза його межами будуть лише популяризувати та збільшувати вартість цієї роботи, адже вона ставатиме більш впізнаваною. Отже, NFT дозволяє зафіксувати ваші інтелектуальні права, що підтверджуються в блокчейні. Застосування NFT може стати новим інструментом у сфері менеджменту інтелектуальної власності, сформувати нові можливості для ринку та його учасників, зробивши його зручнішим, адже операції з токенами дешеві, прості і швидші, ніж операції з реальними об'єктами, до яких вони прив'язані. Варто зауважити, що ажіотаж навколо використання NFT не створює революцію в мистецтві, комп'ютерних іграх чи самій інтелектуальній власності, але воно дає суттєві нові можливості, які заслуговують уваги.*

Ключові слова: *блокчейн, невзаємозамінний токен, інтелектуальна власність.*

Summary. *The article examines the modern view of art in the digital space and the regulation of intellectual property in connection with this phenomenon. The author reveals the concept of blockchain and non-fungible token, their development and impact on the rights of creators. There are many challenges for digital artists today. One of them is that digital art objects can be easily copied as many times as you want. Yes, many will say that you can just save a picture and such saved copies would not differ from the original. But there is one nuance, or rather the opportunity provided by NFT – it's the right to own the original version of the work. It is like having an original painting on display at the Louvre, and other reproductions and copies outside it will only promote and increase the value of this work, as it will become more recognizable. Therefore, NFT allows you to capture your intellectual property rights, which are confirmed in the blockchain. The use of NFT can be a new tool in the field of intellectual property management, creating new opportunities for the market and its participants, making it more convenient, because transactions with tokens are cheap, simple and faster than transactions with real objects to which they are tied. It is worth noting that the hype surrounding the use of NFT does not revolutionize art, computer games, or intellectual property itself, but it does offer significant new opportunities that deserve attention.*

Keywords: *blockchain, non-fungible token, intellectual property.*

Аннотация. *В статье исследуется современный взгляд на искусство в цифровом пространстве и регулирование интеллектуальной собственности в связи с этим явлением. Автор раскрывает концепцию блокчейна и невзаимозаменяемого токена, их развитие и влияние на права создателей. Сегодня перед цифровыми художниками стоит много вызовов. Один из них заключается в том, что объекты цифрового искусства можно легко копировать и делать это сколько угодно. Да, многие скажут, что можно просто сохранить картинку и таких сохраненных копий может быть много, не отличающихся от оригинала. Но есть один нюанс, а точнее возможность, которую предоставляет NFT – это право владеть оригинальной версией произведения. Это похоже на то, что оригинал картины выставлен в Лувре, а другие репродукции*

и копии за его пределами будут только повышать ценность этой работы, поскольку она станет более узнаваемой. Таким образом, NFT позволяет вам зафиксировать ваши права интеллектуальной собственности, которые подтверждены в блокчейне. Использование NFT может быть новым инструментом в области управления интеллектуальной собственностью, создавая новые возможности для рынка и его участников, делая его более удобным, потому что транзакции с токенами дешевле, проще и быстрее, чем транзакции с реальными объектами, с которыми они связаны. Стоит отметить, что шумиха вокруг использования NFT не революционизирует искусство, компьютерные игры или интеллектуальную собственность, но предлагает значительные новые возможности, заслуживающие внимания.

Ключевые слова: *блокчейн, невзаимозаменяемый токен, интеллектуальная собственность.*

Постановка проблеми. Основну цінність фізичного предмета мистецтва представляє можливість довести право на його володіння, і де-небудь цей предмет продемонструвати, що більш ніж реально в цифровому світі. Тому група зацікавлених цифрових художників негайно почала експериментувати. З'явилися платформи для публікації цифрового мистецтва: SuperRare, Known Origin, MakersPlace і Rare Art Labs, а такі художники, як JOY і Josie використовували смарт-контракти, створивши собі справжній бренд.

2020 став роком активного розвитку для індустрії NFT-токен (англ. – *nonfungible tokens*) – "невзаємозамінних токенів"[*]. NFT – це унікальний, невзаємозамінний запис в блокчейні, свого роду віртуальний "цінний папір" в цифровому світі, вартість якого визначається її творцем, що підтверджує право власності на цифровий актив. Це новий рівень у менеджменті інтелектуальної власності, що пов'язаний з новими технологіями, від темпу розвитку яких сучасне законодавство декілька відстає. Аби скоротити відстань між нормами права у сфері інтелектуальної власності та новими розробками у цифровому просторі, а також уніфікувати законодавство на міжнародному рівні, в мовах відсутності кордонів у цифровому електронно-інформаційному середовищі, необхідно не тільки вивчити явище блокчейнів, токенів та їх алгоритм існування та взаємодії, але й виявити переваги та недоліки digital-системи регулювання та захисту прав авторів творів мистецтва, а також закріпити єдині правила для цього явища.

Технологія була створена в 2017 р. на основі смарт-контрактів блокчейна Ethereum. У них може бути тільки один офіційний власник одночасно, і вони забезпечені блок-ланцюжком Ethereum – ніхто не може змінити запис про право власності або скопіювати, вставити новий NFT, підкреслюється на сайті *//www.ethereum.org*.

Результати аналізу наукових публікацій. NFT-технологія є дуже молодою, але стрімко набуває популярності та відкриває нові можливості для художників для маркування, переходу та захисту інтелектуальної власності. Наукові дослідження в цій сфері представлені в основному у вигляді стислого огляду вузьких спеціалістів або аналітиків, які мають подекуди ще й протилежні погляди на переваги та недоліки нових розробок системи блокчейнів та їх вплив на права авторів. Через технічні

[*] *Прим. від ред.* Токен (англ. *token* – "ключ, символ; жетон") – термін, що має кілька значень: монетовидний жетон, що використовується в якості замінника грошей; щодо криптовалюти – одиниця обліку, призначена для представлення цифрового балансу в деякому активі; щодо інформаційної безпеки – обладнання у вигляді USB-брелока, призначеного для авторизації користувача, захисту електронної переписки, безпечного дистанційного доступу до інформаційних ресурсів, зберігання даних. "Невзаємозамінний токен" – це токен, який містить ідентифікаційну інформацію, записану в смарт-контрактах. Визначає та надає право власності на цифрове мистецтво й дозволяє творцеві зберігати й записувати авторські права. Токени, а отже, і твори цифрового мистецтва, можна купувати й продавати точно так само, як і фізичні здобутки.

характеристики NFT нелегко зіставити з існуючими концепціями власності, оскільки вони відносяться до цифрових об'єктів. Це має важливі юридичні наслідки щодо передачі права власності на авторські права.

Оскільки велика частина цифрового контенту, пов'язаного з транзакціями NFT, відноситься до творчого вираження, виникає питання, як розглядати NFT з точки зору закону про авторське право, зокрема, щодо відповідного законодавства ЄС.

Метою статті є оцінка застосування блокчейн-технології у сфері мистецтва, а також огляд міжнародного досвіду у формуванні правових напрацювань у цій сфері.

Виклад основного матеріалу. На початку березня в Брукліні публічно спалили картину Morons (White) відомого вуличного художника Бенксі. Картину спалив представник блокчейн-компанії Injective Protocol, який особисто купив її за $95 тис. Знищене творіння Бенксі конвертували в токен, який був тут же виставлено на аукціон і проданий в чотири рази дорожче – за 228,69 ETH[**] (більше $380 тис. США). Акт спалення картини Бенксі став одним з перших відомих випадків перетворення фізично існуючого об'єкта мистецтва в "nonfungible tokens" або NFT.

Блокчейн (буквально "ланцюг з інформаціних блоків") – технологія, що лежить в основі роботи криптовалюти. Вона організовує базу даних, що складається з ланцюжка блоків, в кожному з яких зберігається інформація про попередній блок. Ця база даних децентралізована, тобто зберігається вона на всіх комп'ютерах учасників системи, так само, як і всі вчинені транзакції відображаються відразу на всіх комп'ютерах. Цю систему складніше зламати, вона прозора і надійно захищена.

О. Сальников, співзасновник і директор по продукту Rarible, називає блокчейн-технологію рішенням проблеми відсутності права власності на інформацію в Інтернеті.

Сама технологія блокчейн не нова, але її активна інтеграція в світ мистецтва почалася недавно, і за останні кілька років з'явилося безліч стартапів, які використовують блокчейн-інструменти для підтвердження автентичності та унікальності творів цифрового мистецтва, продажі традиційних предметів мистецтва в індивідуальне або колективне володіння. Перша платформа для сертифікації творів мистецтва Verisart була запущена в 2015 році британським підприємцем і колекціонером Р. Нортоном (раніше співзасновником платформи Sedition art для діджитал-художників і директором Saatchi Online).

Один з найдорожчих в світі художників Д. Херст зробив крок в сторону блокчейна і виставив на онлайн-платформі Heni Leviathan серію з восьми принтів "The Virtues", що зображують квітучі вишневі дерева. Кожен принт був оцінений в $3000 США, а покупці вперше могли оплатити покупку творів криптовалютою Bitcoin або Ethereum. Принти названі за переліком чеснот етичного кодексу самураїв – Justice, Courage, Mercy, Politeness, Honesty, Honor, Loyalty, Control.

Для того щоб перенести твори мистецтва в блокчейн, його потрібно "токенізувати". Зробити це можна двома способами – випустити один токен для одного твору або розбити твір на кілька токенів, що дозволяють продати його в колективне володіння. Припустимо, ви художник, який займається *digital*-мистецтвом та викладає свої твори в інстаграм, у вас достатня кількість фоловерів (читачів) і до вашої творчості проявляє інтерес художнє співтовариство. Для продажу робіт ви можете піти традиційним шляхом через галерею (яка візьме комісію від продажу вашої роботи), а можете самостійно "токенізувати" твір на одному з криптомаркетплейсів, призначити йому ціну і дочекатися покупця.

[**] *Прим. від ред*. ETH – цифрові гроші, скорочене позначення криптовалюти Ethereum.

Покупець NFT-об'єкта отримує блокчейн-сертифікат, що зберігається в цифровому гаманці і підтверджує володіння об'єктом. Інформація про це володіння і про всі його подальші зміни буде доступна всім учасникам системи, відкрито і прозоро. Сам твір мистецтва, будь то анімація, картинка або відео, при цьому продовжує жити в Інтернеті в загальному доступі.

Основними майданчиками для продажу і покупки є криптомаркетплейси і онлайн-платформи, навколо кожної з яких формується спільнота зацікавлених колекціонерів.

У 2017 році в США М. Лібманом і А. Алехіним була заснована "Snark Art" – технологічна лабораторія і платформа для створення творів мистецтва, що використовує блокчейн як креативне середовище. Найвідоміший кейс з'єднання IT-технологій з мистецтвом – арт-проект 2018 року 89 Seconds Atomized зі знаменитою художницею Ів Суссман. Її 10-хвилинна відеоробота, що заснована на картині Веласкеса "Меніни", знаходиться в колекціях кількох світових музеїв, але виставляється досить рідко. Snark Art запропонували художниці розбити твір на 2000 фрагментів-атомів і поекспериментувати з концепцією колективного володіння арт-об'єктом. Так, відеоробота вартістю $200 тисяч США була розділена на шматочки екрану розміром 20/20 пікселів вартістю всього $100 США. Щоб подивитися роботу цілком, власники фрагментів повинні домовитися між собою і "позичити" атоми у інших учасників.

Rarible – один з провідних майданчиків для створення NFT і торгівлі ними, була організована в 2019 році О. Фаліним і О. Сальниковим. У лютому цього року американська актриса Л. Лохан випустила свій токен з початковою ціною $59,4 тисячі США (33 ETH), заявивши, що вірить в фінансову децентралізацію світу, а біткоїни – це його майбутнє.

The Art Exchange – платформа, орієнтована на тих, хто хоче купувати традиційне мистецтво, що відрізняє його від перерахованих вище майданчиків, націлених все-таки на Діджитал-арт. Його засновниця, видавець The Art Newspaper І. Баженова сама збирає класичне мистецтво, тому вирішила створити інструмент, що дозволяє знизити "поріг входу" в середовище колекціонерів і дати більш широкій аудиторії доторкнутися до володіння визнаними шедеврами. Тут можна стати співвласником творів Ботічеллі або Рембрандта, такий цифровий актив не втратить ліквідності, а токен може бути переданий у спадок. Самі картини при цьому продовжують подорожувати по виставках, як це часто відбувається з роботами з приватних колекцій – власники іноді їх і не бачать.

Malevich – придуманий заступником глави аукціону Philips С. Марич блокчейн-проект працює по краудфандінговій моделі і пропонує користувачам інвестувати в "матеріальний" твір мистецтва на стадії його створення, тобто на виручені гроші художник створює роботу для майбутньої виставки. А учасники одержують токен з правами на роботу, який в разі успіху твору можна буде продати дорожче. Можна і просто придбати Artwork token робіт Є. Антуфьєва, П. Пепперштейна або К. Бранкузі, які фізично залишаться доступні для публіки в музеї або галереї, а ви будете знати, що цей твір з вашої колекції.

25 лютого цифровий художник М. Вінкельман, відомий як Beeple, виставив на аукціоні Christie's роботу "Everydays: the first 5000 days", існуючу як NFT-об'єкт і представляє собою колаж з 5000 унікальних зображень, які з 2007 по 2021 рік він щодня викладав в свій інстаграм. Аукціон завершився 11 березня, а ставки перевищили позначку $3 млн. США. Christie's став першим зі світових аукціонних будинків, які виставили на торги NFT-арт-об'єкт, що стало певним визнанням нової технології авторитетним гравцем арт-ринку і вивело її в мейнстрім.

Ще раніше, в жовтні 2020 року колекціонер Пабло Родрігес-Фрайле придбав аутентифіковане на блокчейні 10-секундне відео “Beeple” з лежачим на траві намальованим гігантським тілом Дональда Трампа за $67 тис. США, а в кінці лютого цього року продав його за $6,6 млн. на аукціоні Nifty Gateway.

Співачка і подруга І. Маска Grimes нещодавно виставила на тому ж Nifty Gateway колекцію цифрових артефактів і заробила $6 млн. США від продажу десяти об’єктів. Основну частку продажі склали два лоти “Earth” і “Mars” – короткі відео з оригінальними саундтреками, у кожного є тисячі копій, на торгах було продано близько 700 примірників на загальну суму $5,18 млн. США. Унікальне відео “Death of the Old” з літаючими під пісню “Grimes” ангелами було продано за $389 тисяч США і стало найдорожчим об’єктом аукціону. Торги тривали всього двадцять хвилин після того, як “Grimes” оголосила про них в своєму твіттері.

За даними Nonfungible.com, в 2020 році обсяг продажів на ринку NFT перевищив $350 млн. і виріс майже на 300 % в порівнянні з 2019-м. Є передумови вважати, що в 2021 році це зростання продовжиться.

У багатьох традиційних колекціонерів принцип NFT-мистецтва викликає сумніви і скепсис, бо, по суті, ти володієш не фізичним об’єктом, який можна повісити вдома на стіну або виставити на виставці, а самим “правом володіння” зображенням, яке цілком може знаходитися в вільному доступі в мережі.

Важко судити про частку сірого ринку мистецтва, але очевидно, що блокчейн-технології зроблять транзакції мистецтва більш прозорими. Для самих художників стежити за подальшим переміщенням робіт по світу стане безумовним бонусом (зібрати ранні роботи для ретроспективи зрілому художнику сьогодні дуже важко, а блокчейн дозволить залишатися в контакті з останнім власником), і крім того NFT стане революційною технологією в області авторських відрахувань: платформа Rarible, наприклад, дозволяє закласти в угоду відсоток відрахувань художнику при наступних перепродажах – наприклад 10 %, які художник буде отримувати кожного разу, як хтось з вигодою перепродасть його роботу.

Власник NFT може розпоряджатися токеном як завгодно, в тому числі перепродувати його. Поки що це відбувається мало коли – ринок невзаємозамінних токенів знаходиться на самому ранньому етапі свого розвитку, тому кількість перепродажів NFT залишається незначною. Повноцінної біржової інфраструктури для вторинного обігу токенів поки не існує, і це може впливати на формування справедливої вартості виставлених на продаж NFT.

Через відсутність достатнього числа верифікованих майданчиків з прозорим механізмом перепродажів, скептики критикують NFT-активи. Рідкісні угоди, які здійснюються на вторинному ринку, як правило, проходять в рамках аукціонів, що значно розтягує у часі процес їх покупки або продажу.

На тлі цього серйозною проблемою стає “воштрейдинг” (англ. – Wash Trading) – таким терміном описують ситуацію, при якій продавець штучно завищує торговельну активність з токеном, купуючи і продаючи актив у самого себе. Це досить поширене явище на криптовалютному ринку, наприклад, зовсім недавно біржа “Coinbase” виплатила штраф розміром $6,5 млн. США за такі дії з боку своїх користувачів і навіть одного зі своїх співробітників.

На ринку NFT ця проблема ускладнюється ще й тим, що оцінити масштаби такої форми шахрайства вкрай важко – ринок поки занадто малий, щоб можна було легко відстежувати такі операції. Проте такі випадки вже були зафіксовані, наприклад,

аналітики Nonfungible помітили, як за допомогою воштрейдингу завищували вартість персонажів в іграх “Blockchain Cuties” і “CryptoKitties”.

Ще одна причина поширення воштрейдингу на ринку NFT пов’язана з можливістю отримувати керуючі маркери за активну участь в роботі платформи – саме за такою схемою працює проект Rarible. Творці Rarible не відкидають цю проблему – за словами творця маркетплейсу О. Сальникова, більше 40 % від загального обсягу угод з NFT на загальну суму $750 тис. США, що скоєні в серпні 2020 року, були так чи інакше пов’язані з воштрейдингом. За його словами, щоб знизити цю частку, платформа поступово підвищує розмір комісій за транзакції.

Від того, чи зуміють учасники ринку вирішити ці проблеми, багато в чому буде залежати його доля. До ринку NFT починають придивлятися американські регулятори, а юристи вже висловлюють побоювання, що NFT може чекати доля Bitcoin-ETF. Новому інструменту потрібно довести, що він може використовуватися не тільки в спекулятивних цілях. Розвиток вторинного ринку з зрозумілими правилами гри може стати першим кроком у цьому напрямку.

Закон і мистецтво часто доповнюють один одного, особливо зараз, з появою технології блокчейна, що може грати ключову роль в таких питаннях, як доказ походження, а так само створення правових рамок пайового володіння творами мистецтва. І з цією метою першопроходець в області смарт-контрактів, OpenLaw, щойно запустив систему, на основі блокчейн, для допомоги художникам в безпечному контролі й отриманні прибутку від інтелектуальної власності, що, без сумніву, буде цікаво багатьом юристам, а не тільки тим, хто займається мистецтвом.

Технологія блокчейн широко пов’язана з обміном взаємозамінними цифровими активами, від платіжних систем, таких як Zcash (ZEC) і Libra, до платформ, таких як Ethereum і Substrate, з використанням так званих взаємозамінних (англ. – *fungible*) токенов. Предмет, що є замінним, взаємозамінний з іншим ідентичним предметом.

Однак невзаємозамінні токени (NFT) не мають подібної властивості. Хоча ця особливість може здатися непрактичною, особливо з урахуванням торгової корисності токенів, вона дуже бажана, якщо метою є захист вартості активу. З цієї причини NFT-токени зробили революцію у володінні предметами мистецтва та праві інтелектуальної власності. Одна з причин, по якій блокчейни настільки потужні, полягає в тому, що вони дозволяють нам визначати і забезпечувати дотримання меж і прав власності без залежності від централізованої, застарілої державної системи обліку.

Ці можливості дають надію на відкриття нових ділових можливостей для художників і працівників медіаіндустрії, де поширення вільно доступних цифрових копій підриває здатність власників контенту монетизувати і поширювати творчі роботи, за винятком часто спотворених моделей реклами.

Нові стандарти NFT в поєднанні з інструментами, створеними OpenLaw, будуть підтримувати поширення ліцензійних угод, заснованих на розумних контрактах, ліцензійних платежів та інших угод з управління і монетизації створення робіт. З OpenLaw і NFT сторони отримують можливість маркувати виняткові та невиключні права інтелектуальної власності поряд з іншими правами власності та гарантувати, що ці права криптографічно пов’язані з одним або кількома юридично обов’язковими угодами.

Після завантаження в IPFS художник може створити необмежену кількість ліцензійних прав, включаючи видачу токенізованих невиключних ліцензій і частин пайового володіння для даного твору мистецтва. Власність і права власності, що представлені NFT-токеном, можуть включати в себе різні класи власності, ліцензійні права та права на перепродаж роялті в оригінальному творі мистецтва.

Інструменти OpenLaw відкривають нові можливості для пайового володіння творами мистецтва. Наприклад, якщо художник вирішує продати частку володіння в своєму цифровому творі мистецтва, при цьому кожна дрібна частка становить 1 % володіння, він тепер може це зробити. Прив'язуючи смарт-контракти до токену, художник може забезпечити постійне отримання роялті (тобто 10 % від ціни продажу) кожен раз, коли токенізована ліцензія передається іншому покупцеві.

Використовуючи комбінацію коду та розумного контракту, що підтримує NFT, художники мають можливість отримувати роялті при перепродажі відповідно до вимог Європейського Союзу (відповідно до Директиви 2001/84/ЄС) та Сполученого Королівства (відповідно до Положення про право інтелектуальної власності художників від 2006 року).

NFT також використовується для представлення ліцензійних прав. Прикріплюючи метадані до токену та посилаючись на метадані в положеннях і умовах для кожної ліцензії в створеній угоді OpenLaw, токени можуть представляти невиключні ліцензійні права, що можна вільно продавати, купувати і перепродавати, як і будь-які інші криптографічні активи.

Самі по собі умови смарт-контрактів, які застосовуються при токенізації цифрових активів, можуть бути цілком звичними для законодавства з інтелектуальної власності більшості юрисдикцій (щодо переходу прав, виплати винагороди, наданням дозволу на певні види використання та контролю за таким використанням). Тому забезпечення відповідності вимогам та нормам поширення творів як об'єктів авторського права із національними законодавствами за допомогою NFT – не критична проблема. Але все ж вона потребує уваги та вирішення. Особливо це стосується визначення правової природи самого токену як цифрового активу. Зважаючи, що "можна токенізувати все", інколи проблематично визначити його як нематеріальний/цифровий актив, майнові права чи цінні папери. Чи можна їх лише конвертувати у валюту, чи використовувати як самостійний об'єкт (для інвестування, кредитування, чи включення в статутний капітал підприємств)? Однозначних відповідей на ці запитання сьогодні немає.

В Україні токенізація активів не є популярною й достатньо розвиненою, оскільки існують особливості законодавчої бази. Позитивними зрушеннями в цьому напрямку можемо вважати прийняття Верховною Радою України в першому читанні законопроєкту "Про віртуальні активи" № 3637. Законопроєкт передбачає зміни, що застосовуються до правовідносин, що виникають у зв'язку з обігом віртуальних активів в Україні, визначає права та обов'язки учасників ринку, засади державної політики у сфері обігу віртуальних активів.

Висновки.

Оскільки ми живемо в цифрову епоху, існує нагальна потреба швидко адаптуватися до змін та впроваджувати нові інструменти, які допомагають оцифровувати та зберігати активи, які представляють для нас цінність. Прийняття вищезгаданого законопроекту – впевнений крок на шляху до цього!

Варто зазначити, що застосування інструменту NFT важливо для авторського права не через зміну парадигми та основ інтелектуальної власності, а через створення для авторів та правовласників нових можливостей безпечної та вигідної дистрибуції своїх творів.

NFT відкриває великі можливості для діджитал-художників для продажу своїх творів, але водночас розмиває поняття експертності стосовно художників. Чи спростить платформа процедуру входу на арт-ринок художникам-початківцям?

Слід зазначити, що деякі фахівці вважають, що NFT не зовсім відповідають нормам закону про авторське право. Проте, як і у випадку з будь-якою появою нових технологій, які отримують достатнє суспільне визнання, вони надають можливість переглянути основні доктрини Закону про авторське право, такі як володіння, розповсюдження, вичерпання, перепродаж та управління колективними правами.

У певному сенсі NFT представляють собою концепцію мета-володіння, яка спирається на код, що дозволяє здійснювати цифрове поширення, подібне володіння, вичерпання ресурсів, перепродаж за винагороду і примусове виконання в контексті системи, заснованої на блокчейні. При цьому NFT пропонують творцям привабливу нову модель винагороди. Однак здебільшого аффорданс NFT не супроводжується відповідними юридичними наслідками в тому, що стосується Закону про авторське право. Це створює серйозні проблеми для творців, інших правовласників і користувачів, якщо вони очікують, що транзакція NFT в блокчейні буде відображати транзакцію поза мережею для еквівалентної роботи. Разом з проблемами, пов'язаними з можливістю неправильної атрибуції (і пов'язаними з цим проблемами автентичності), а також з порушенням виняткових і немайнових прав.

Незважаючи на недоліки, починається нове майбутнє цифрового мистецтва, яке обіцяє допомогти зменшити викривлення першої Інтернет-хвилі і забезпечити більшу компенсацію для художників по всьому світу. За допомогою OpenLaw і NFT творці контенту мають більше можливостей, що, в свою чергу, повинні допомогти створити більш справедливий і не просто творчий ландшафт в дусі Web 3.0.

Використана література

1. Про авторське право і суміжні права: Закон Украины від от 23.12.93 р. № 3792-XII. URL: https://zakon.rada.gov.ua/laws/show/3792-12

2. Лиханова Елена. Что такое NFT? Криптоискусство в вопросах и ответах. URL: https://rb.ru/story/nft-wat

3. Протокол. URL: https://protocol.ua/ru/realii_hhi_veka_zashchita_avtorskih_prav_s_pomoshchyu _ai_to_be_continued

4. Цьвок Данило. Що таке NFT і як продати цифрове мистецтво за мільйони. URL: https://ain.ua/2021/03/18/nft-renesans-abo-yak-prodati-cifrove-mistectvo-za-miljoni

5. Peter Mezei, Joao Pedro Quintais, Alexandra Giannopoulou, Balazs Bodo. The Rise of Non-Fungible Tokens (NFTs) and the Role of Copyright Law. URL: http://copyrightblog.Kluweriplaw.com/2021/04/22/the-rise-of-non-fungible-tokens-nfts-and-the-role-of-copyright-law-part-ii

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

УДК 342.951

ЮШКОВ А.Г., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-4912-478X.

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ БОТОФЕРМ НА ШКОДУ ДЕРЖАВНИМ ІНТЕРЕСАМ УКРАЇНИ: МЕХАНІЗМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ

Анотація. *Розглянуто поняття та види ботів. Визначено ознаки та сфери діяльності ботоферм. Окреслено алгоритм створення та поширення фейкових сторінок. Деталізовано процедури реагування на поширення неправдивої і недостовірної інформації в рамках чинного законодавства України. Висвітлено здобутки вітчизняної спецслужби за напрямом протидії злочинній діяльності ботоферм, які координуються кураторами з РФ. Узагальнено завдання діяльності проросійських ботоферм в Україні. Визначено засади державної політики боротьби з фейками та пропагандою у соціальних мережах. Уточнено шляхи удосконалення організаційно-правових засад щодо системної протидії функціонування злочинних ботоферм як загроз державним інтересам України.*

Ключові слова: *ботоферма, аккаунт, державні інтереси, національна безпека, цифрові технології, фейки,деструктивна діяльність, спецслужба.*

Summary. *The concepts and types of bots are considered. The signs and spheres of activity of bot farms are determined. The algorithm for creating and distributing fake pages is outlined. Procedures for responding to the dissemination of false and unreliable information within the current legislation of Ukraine are detailed. The achievements of the domestic special services in the direction of counteracting the illegal activities of bot farms, which are coordinated by curators from the Russian Federation, are highlighted. The task of pro-Russian bot farms in Ukraine is generalized. The principles of the state policy of combating fakes and propaganda on social networks are determined. The directions of improvements of the organizational and legal framework for the systematic counteraction to the functioning of crime bot farms as a threat to the state interests of Ukraine are specified.*

Keywords*. bot farm, account, state interests, digital technologies, fakes, destructive activity, secret service.*

Аннотация. *Рассмотрены понятие и виды ботов. Определены признаки и сферы деятельности ботоферм. Очерчен алгоритм создания и распространения фейковых страниц. Детализированы процедуры реагирования на распорстранение неправидивой и недостоверной информации в рамках действующего законодательства Украины. Освещены достижения отчественной спецслужбы по направлению противодействия преступной деятельности ботоферм, которые координируются кураторами из РФ. Обобщены задачи деятельности проросийских ботоферм в Украине. Определены основы государственной политики борьбы с фейками и пропагандой в социальных сетях. Уточнены направления усовершенствования организационно-правовых основ системного противодействия функционирования преступных ботоферм как угроз государственным интересам Украины.*

Ключевые слова: *ботоферма, аккаунт, государственные интересы, цифровые технологии, фейки,деструктивная деятельность, спецслужба.*

Постановка проблеми. З метою маніпулювання свідомістю пересічних громадян, інспірування соціальної напруги, а також поширення забороненої законом інформації кураторами з РФ та їх сателітами активно використовуються новітні технології, зокрема

соціальні мережі та системи мікроблогів на шкоду державним інтересам України та з метою здійснення протиправної діяльності проти нашої держави. За таких умов соціальні мережі в Україні залишаються найбільш вразливими з точки зору можливостей оприлюднення інформації антиукраїнського змісту та проведення інформаційних кампаній та акцій на шкоду інтересам держави. Організацію протидії використанню Інтернету в протиправних цілях ускладнює відсутність визначених законодавством норм, які б змушували суб'єктів надання телекомунікаційних послуг встановлювати обладнання для фільтрації Інтернет-трафіку та виявлення осіб, які здійснюють протиправну діяльність. Серед проблемних аспектів у цій сфері експерти виокремлюють також надчутливу реакцію громадськості на будь-які ініціативи щодо запровадження жорсткого контролю, що може тлумачитися як порушення прав та свобод людини, в т.ч. на рівні міжнародних недержавних правозахисних організацій.

За таких умов, актуальним є запровадження комплексу заходів (виявлення деструктивних інформаційних акцій або ознак їх підготовки, визначення зацікавленої сторони) з метою адекватного реагування на відповідні виклики та формування Україною власної наступальної інформаційної політики (в т.ч. в медіа-просторі закордонних держав). Таким чином, блокування поширення в Інтернет-просторі матеріалів, що містять заклики до посягання на державний суверенітет, територіальну цілісність України, розпалювання міжнаціональних, міжконфесійних конфліктів, пропаганду війни є пріоритетним завданням правоохоронних органів в умовах гібридної війни. Це завдання є особливо актуальним в контексті посилення спроможностей з обмеження деструктивного впливу на громадську думку.

Тобто за результатами моніторингу ресурсів мережі Інтернет (видання, соціальні мережі, блогосфера, форуми, особисті сторінки) ключовим завданням держави є виявлення, блокування та припинення використання зазначених інформаційних ресурсів найбільш активними радикально налаштованими представниками громадсько-політичних організацій, окремих мас-медійних структур для поширення резонансної інформації тенденційного характеру, оприлюднення закликів до організації масових протестних акцій, їх анонсування і координації тощо. Останнім часом має прояв загрозлива тенденція використання ботоферм на шкоду державним інтересам України. Через фейкові аккаунти поширюється деструктивна інформація в мережі Інтернет з метою створення панічних настроїв серед населення. Зокрема, за їх допомогою розміщувалися повідомлення з дискредитації української влади і поширювалися заклики до повалення конституційного ладу. Також ботоферми дедалі частіше оприлюднюють неправдиву інформацію загрозливого тенденційного характеру, що є різновидом підривної діяльності проти України, яка здійснюється з метою завдання репутаційного удару, нівелювання дієвих кроків української влади. У зв'язку із викладеним, висвітлення механізмів запобігання діяльності ботоферм є актуальним та своєчасним в сучасних реаліях.

Результати аналізу наукових публікацій. Питання соціалізації мережі Інтернет та уточнення шляхів та заходів запобігання поширенню фейків й пропаганди у соціальних мережах розглядали у свої працях О. Зінченко [1], М. Кіца [2], О. Курбан [3], О. Пригорницька [4], Н. Токарева [5] та інші. Проте практичні питання блокування діяльності злочинних ботоферм як однієї із загроз державним інтересам України залишаються малодослідженими, що посилює актуальність тематики цієї наукової статті.

Метою статті є визначення дієвих шляхів організаційно-правового характеру щодо контролю та блокування діяльності злочинних ботоферм, які спричиняють шкоду національним інтересам України в умовах гібридної війни України з РФ.

Виклад основного матеріалу. Сьогодні трохи більше як чверть українців основним джерелом новин для себе вважають соціальні мережі. З них більше двох третин користуються “Facebook”, у якій активно використовуються боти. Боти – це програми для рішення однотипних задач, які створюють та керують фейковими акаунтами у соціальних мережах. Остання тенденція сучасності – це масове створення ботоферм – компаній, які створюють не існуючих користувачів з їх коментарями, переважно з використанням “Facebook”.

Загалом виділяється відомих 4 типи ботів.

Перший тип – це соціальні боти в електронній комерції. Боти-менеджери з продажу. Їхня ідентифікуюча ознака: стилізація під сервіс свого власника. Їх, як правило, ніхто і не приховує.

Другий тип – SEO-боти**,** лайкателі, накручувальники і репостери. Їх ознаки: величезна кількість груп, підписок, репоста і повна відсутність особистої інформації.

Третій тип – це боти-багатоденки. Ознака: активне посилання на сторонній сервіс в профілі або на стіні користувача з приписку “тут рідко буваю”, “шукайте мене за посиланням”.

Четвертий тип – це виключно політично тематичні боти. Як правило, такі боти підключені до систем спілкування і можуть односкладово відповідати на будь-які повідомлення. Тобто зоною активності ботів є саме сучасні соціальні мережі.

У більшості випадків це акаунти, створені людьми та керовані також людьми. Вони можуть писати оригінальні коментарі або копіювати вже заздалегідь створений та погоджений із замовником список меседжів. Є також акаунти, якими керують роботи. В такому випадку залучення людини мінімальне. Але таких акаунтів мало, і, як правило, ботами керують все-таки люди. Водночас поведінка бота, навіть якщо ним керує людина, дуже сильно відрізняється від поведінки реальних користувачів “Facebook”.

Ми виділили вісім характеристик ботів: у середньому швидкість написання ботом коментаря в 15 разів вище звичайної людської (середня різниця в часі між двома сусідніми коментарями); більше половини ботів мають “напарників” по коментуванню – акаунти, які коментують разом із ними один і той самий пост. У реальних акаунтів людей така поведінка спостерігається тільки в одному випадку з восьми (13 %); боти у чотири рази частіше пишуть під політичними постами, ніж реальні люди; у ботів у середньому в чотири рази менше друзів на сторінці; тільки в половині випадків бот має аватарку з обличчям, а люди – у 92 % випадків. Тільки 20 % ботів мають коментарі під власними постами. У людей цей показник – 80 %.

Соціальні мережі, у свою чергу, постійно оголошують та реалізують курс на боротьбу з протиправною діяльністю деяких ботоферм, але по факту блокують лише декілька відсотків від багатомільйонної кількості існуючих фейкових акаунтів. З іншого боку, соціальним мережам навіть вигідна наявність ботоферм і шаленого трафіку, оскільки це дозволяє їм гарно заробляти. У соціальних мережах боти можуть впливати на підсвідомість людей і формувати громадську думку, формувати репутацію певного політика чи громадського діяча. Іноді буває навпаки. Боти, ботоферма більш ефективна коли потрібно сформувати негативну думку про когось або про щось, ніж позитивну. На формування позитивної думки боти впливають дуже опосередковано і швидше за все погано. Є цікавий феномен, коли політики знають, що ажитація в мережі викликана ботами, за яких вони платять цілеспрямовано, але вони рано чи пізно починають вірити, що ця підтримка дійсно щира. Оскільки боти для формування позитивної громадської думки працюють погано, то розчарування неминуче.

Слід ще раз зазначити, що *ботоферми* – це компанії, які масово *створюють несправжніх користувачів соцмереж і від їхнього імені пишуть тисячі коментарів*. В сучасних умовах, хто завгодно може придбати ботоферму для підтримки свого позитивного рейтингу або політичного іміджу. Навіть невелика ботоферма оперує мільйонними бюджетами й платить зарплату в конвертах. Цей тіньовий ринок послуг сягає мільйонів доларів на рік. Формат роботи ботоферми – написання коментарів. Наприклад, вийшов пост, і необхідно написати на підтримку по 20 коментарів для того, щоб вони почали розкручуватися. Проте під постами, реальні люди залучаються тільки тоді, коли вже є якась активність. Щодня ботоферма готує мінімум 200 – 300 коментарів для різних політичних сил, або для певних замовників. Когось у цьому форматі підтримують, а когось мають критикувати. У ботів навіть є спеціальні прийоми для того, щоб сприйматися цільовою аудиторією реальними людьми за допомогою створення діалогів між різними фейковими акаунтами.

Алгоритм створення фейкових сторінок є досить простим: співробітники ботоферми викрадають фотографії реальних людей із соцмереж “Вконтакте”, “Одноклассники” нині заборонених в Україні. Потім завантажують ці фотографії на порожню сторінку у “Facebook” з вигаданим іменем і прізвищем.

Функції в ботів можуть бути доволі різні. Від атак на опонентів певного політика й створення негативного образу до привернення уваги до конкретної події чи допису з метою маніпуляції громадською думкою. Ботів можливо залучати у випадку, коли треба терміново “розігнати” інформацію або, навпаки, відволікти увагу від скандалу або неприємної ситуації. Для цього можна “купувати” додаткових ботів в інших ферм, але їхня вартість буде вищою. Напрям діяльності ботоферми визначається завдяки процесу “таргетування”, тобто існує необхідність проведення дослідження, на яку аудиторію треба сфокусуватися ботофермі.

Такий стан справ потребує втручання держави з метою протидії протиправній діяльності ботоферм з метою реагування на ключові теми, за якими поширюється неправдива тенденційна інформація або маніпуляційна інформація. Протидія відбуватиметься через складання карти виявлених ботоферм і здійснення заходів щодо їх блокування. Також чинне законодавство України передбачає реагування на поширення дезінформації, не використовуючи самого слова “дезінформація”. Проте в законодавстві прописано процедури реагування на поширення неправдивої і недостовірної інформації. При чому реагування розділено на три рівні, залежно від ступеня суспільної небезпеки поширення такої інформації.

Перший рівень реагування – це цивільно-правова відповідальність. Відповідно до частини четвертої статті 32 Конституції України, кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім’ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріального і морального збитку, завданого збиранням, зберіганням, використанням та поширенням такої недостовірної інформації. Більш детально процедуру спростування, відповіді і припинення поширення шкідливої інформації про фізичну особу розкрито в положеннях Цивільного кодексу України, Законі України “Про інформацію” тощо. Зокрема, стаття 278 Цивільного кодексу України надає суду право заборонити поширення такої шкідливої інформації в газеті, книзі, кінофільмі, теле-, радіопередачі тощо, заборонити (припинити) їхнє розповсюдження до усунення цього порушення, а якщо усунення порушення неможливе – вилучити наклад газети, книги тощо для його знищення. Реалізація зазначеного права має широку судову практику, яка, зокрема, враховує прецедентні рішення Європейського суду з прав людини, намагаючись знайти баланс між реалізацією

права на свободу слова і запобіганням такій реалізації на шкоду законим інтересам, правам і свободам фізичних і юридичних осіб. Таким чином, у разі поширення неправдивої, недостовірної, перекрученої інформації щодо фізичних, юридичних осіб (зокрема, органів державної влади, їхніх посадових осіб, їх дій тощо) чинне законодавство України передбачає реагування у вигляді спростування, відповіді, відшкодування завданої шкоди, а в деяких випадках – вилучення накладу газети, журналу тощо за рішенням суду. Окремо треба зазначити, що ця процедура реагування стосується будь-якого способу поширення інформації, незалежно від того, чи поширюється вона через зареєстроване ЗМІ чи в Інтернеті за допомогою соцмереж тощо.

Другий рівень реагування – адміністративна відповідальність. Насамперед це стосується телебачення і радіомовлення, щодо яких існують спеціальні процедури державного контролю, виписані в Законі України "Про телебачення і радіомовлення". Зокрема, стаття 7 цього Закону містить для телерадіоорганізацій низку обмежень у діяльності. Не припускається використання телерадіоорганізацій для:

поширення відомостей, що становлять державну таємницю, або іншої інформації, яка охороняється законом;

закликів до насильницької зміни конституційного ладу України;

закликів до розв'язування агресивної війни або її пропаганди та/або розпалювання національної, расової чи релігійної ворожнечі та ненависті;

необґрунтованого показу насильства;

пропаганди винятковості, зверхності або неповноцінності осіб за ознаками їхніх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження;

трансляції програм та передач, у яких телеглядачам та/або радіослухачам надаються послуги з ворожіння, а також платні послуги щодо народної та/або нетрадиційної медицини;

трансляції програм або відеосюжетів, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, якщо вони мають змогу їх дивитися;

трансляції телепередач, виготовлених після 1 серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, виправдовують чи визнають правомірною окупацію території України. Для цілей застосування цієї норми використовуються визначення та критерії, встановлені Законом України "Про кінематографію";

трансляції аудіовізуальних творів (фільмів, телепередач, крім інформаційних та інформаційно-аналітичних телепередач), одним з учасників яких є особа, занесена до Переліку осіб, що створюють загрозу національній безпеці, оприлюдненому на вебсайті центрального органу виконавчої влади, який забезпечує формування державної політики у сферах культури та мистецтв. Водночас учасником аудіовізуального твору вважається фізична особа, яка брала участь у його створенні під власним ім'ям (псевдонімом) або як виконавець будь-якої ролі, виконавець музичного твору, що використовується в аудіовізуальному творі, автор сценарію та/або текстів чи діалогів, режисер-постановник, продюсер;

розповсюдження і реклами порнографічних матеріалів та предметів;

пропаганди наркотичних засобів, психотропних речовин з будь-якою метою їхнього застосування;

поширення інформації, яка порушує законні права та інтереси фізичних і юридичних осіб, зазіхає на честь і гідність особи;

інших вчинків, за якими настає кримінальна відповідальністю.

Закон містить також положення, спрямовані на захист прав телеглядачів і радіослухачів, прав неповнолітніх, суспільної моралі тощо. Відповідно до статті 71 вказного Закону, відповідають за порушення законодавства про телебачення і радіомовлення телерадіоорганізації, провайдери програмної послуги, їхні керівники та працівники, інші суб'єкти господарської діяльності, посадовці органів державної влади та органів місцевого самоврядування. Відповідно до частини шостої статті 72 цього закону, Національна рада може застосовувати до телерадіоорганізацій та провайдерів програмної послуги такі санкції:

оголошення попередження;

стягнення штрафу;

анулювання ліцензії на підставі рішення суду за позовом Національної ради.

Обмеження передбачаються також щодо друкованих засобів масової інформації та інформаційних агентств. Зокрема, відповідно до статей 3, 18 Закону України "Про друковані засоби масової інформації (пресу) в Україні", суд має право заборонити випуск друкованого видання, якщо воно використовується для:

закликів до захоплення влади, насильницької зміни конституційного ладу або територіальної цілісності України;

пропаганди війни, насильства та жорстокості;

розпалювання расової, національної, релігійної ворожнечі;

розповсюдження порнографії, а також для вчинення терористичних актів та інших кримінально караних діянь;

пропаганди комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки;

популяризації або пропаганди держави-агресора та її органів влади, представників органів влади держави-агресора та їхніх дій, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України;

втручання в особисте і сімейне життя особи, крім випадків, передбачених законом;

заподіяння шкоди честі і гідності особи;

розголошення будь-якої інформації, яка може призвести до вказання на особу неповнолітнього правопорушника без його згоди і згоди його законного представника.

Окрім адміністративної відповідальності для юридичних осіб – засобів масової інформації Кодексом України про адміністративні правопорушення передбачено адміністративну відповідальність для окремих фізичних осіб. Наприклад, згідно зі статтею 173-1 КпАП, поширення неправдивих чуток, що можуть спричинити паніку серед населення або порушення громадського порядку, незалежно від способу такого поширення (усно, через соцмережі в інтернеті, за допомогою розвішування інформації в громадських місцях тощо), має наслідком накладення штрафу від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян або виправних робіт на строк до одного місяця з відрахуванням 20 % заробітку.

Третій, найвищий рівень реагування – кримінальна відповідальність за поширення інформації (незалежно від її правдивості або неправдивості), яка має на меті заподіяння шкоди суспільству загалом. Зокрема, Кримінальний кодекс України (далі – КК України) встановлює відповідальність фізичних осіб (незалежно від їхнього статусу, громадянства, способу поширення інформації на невизначене коло осіб) за публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій (ст. 109 КК України). При чому в разі, якщо такі заклики поширюються організованою групою (зокрема, за допомогою "ботоферми") або з використанням засобів масової інформації,

покарання є більш суворим. КК України встановлює відповідальність за заклики до зміни меж території або державного кордону на порушення порядку, встановленого Конституцією, надання іноземній державі, іноземній організації або їхнім представникам допомоги в проведенні підривної діяльності проти України, зокрема інформаційної. КК України передбачає відповідальність також за інші види поширення дезінформації або суспільно шкідливої інформації: наприклад, свідомо неправдиве повідомлення про підготування вибуху, підпалу або решту дій, які загрожують загибеллю людей чи іншими тяжкими наслідками (ст. 250), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної або банківської таємниці (ст. 232) тощо.

Таким чином, сучасне законодавство України вже передбачає всі необхідні і достатні засоби реагування з боку державних органів на поширення дезінформації як явища без створення додаткових наглядових органів або організацій, що фінансуються з державного бюджету. Те, що часто уповноважені державою посадові особи не використовують передбачених законом правових механізмів, не вирішиться ухваленням нового закону. Ця проблема може бути вирішена лише через навчання відповідних посадовців та притягнення їх до відповідальності за бездіяльність у випадках, коли вони були зобов'язані вжити певних заходів.

Протиправна діяльність ботоферм перебуває у фокусі уваги вітчизняних правоохоронців. Так, важливим та актуальним завданням правоохоронних органів є виявлення та блокування роботи ботоферм, які поширюють деструктивний контент, зокрема з РФ. Існують числені ботоферми, які працюють на замовлення кураторів РФ з метою проведення підривної діяльності на шкоду державним інтересам України. У цьому році чимало випадків блокування роботи ботоферм, які працювали на шкоду державним інтересів України та керувалися кураторами з РФ. Як переконливо засвідчує набутий досвід, існують непоодинокі випадки поширення у мережі Інтернет сепаратистських матеріалів, які мають за мету сприяння розпалюванню міжнаціональної ворожнечі, поширення протестних настроїв, соціального невдоволення.

У 2020 році у місті Києві була викрита міжрегіональна ботоферма, яка використовувала не тільки облікові записи в соціальних мережах і е-мейли, а й електронні гаманці з фейковими персональними даними. Встановлено, що для реєстрації акаунтів зловмисники використовували, крім українських, також російські та європейські SIM-карти мобільних операторів. Виконуючи замовлення на ескалацію конфлікту на сході України, організатори ботоферм здійснювали інформаційні "вкидання", сприяли поширенню негативних настроїв і дискредитували українську владу як всередині країни, так і за її межами.

Міжрегіональна ботоферма також використовувалася організаторами для масового поширення деструктивних публікацій в соцмережах і меседжерах, розсилки неправдивих повідомлень про "замінування", а також інших дій, спрямованих на дестабілізацію загальної ситуації в Україні.

Так, у травні 2021 року у місті Чернігові було припинено діяльність ботоферми. Співробітники вітчизняної спецслужби встановили, що через ботоферму зловмисники поширювали фейкову інформацію для створення панічних настроїв серед населення. Зокрема, вони розміщували повідомлення для дискредитації української влади і закликали до повалення конституційного ладу. Виконавці з числа жителів обласного центру використовували спеціалізований апаратно-програмний комплекс, через який було створено та використовувалось майже 2,5 тисячі бот-акаунтів, якими дистанційно керували організатори злочинної схеми з РФ. Під час обшуку за місцем проживання організатора, де знаходилась ботоферма, правоохоронці вилучили: сім 16-ти канальних

GSM-шлюзів; 2 SIM-банки на 128 карток кожен; 370 SIM-карток російського мобільного оператора; 3 ноутбуки, через які здійснювалось керування телекомобладнанням ботоферми.

У лютому 2021 року у Львові Служба безпеки України заблокувала мережу ботоферм, яка дискредитувала вакцинацію та підтримувала так звані "Л/ДНР". Було встановлено, що зловмисників фінансували з території РФ через електронні гаманці санкційних платіжних систем. Під час обшуків правоохоронці вилучили зокрема сотні сім-карток та комп'ютерну техніку зі спеціалізованим програмним забезпеченням. Правоохоронці відкрили кримінальне провадження за частиною 2 статті 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

У травні 2021 року у Черкасах спецслужба заблокувала діяльність ботоферми, яку проросійські Інтернет-агітатори використовували для пропаганди. У ході розслідування встановили, що ботоферму "утримував" черкащанин у підсобному приміщенні власного підприємства. Він забезпечував використання анонімних IP-адрес для безпеки Інтернет-агітаторів. Підприємець використовував SIM-картки українських операторів мобільного зв'язку. Розрахунок за послуги отримував криптовалютою та через російські віртуальні платіжні системи, заборонені на підставі рішення РНБО України. Через ботоферму Інтернет-агітатори розповсюджували дезінформацію про події в ОРДЛО, проросійську пропаганду, спрямовану на штучну дестабілізацію ситуації в державі, повалення конституційного ладу і територіальної цілісності нашої країни. Під час проведення обшуку правоохоронці вилучили комп'ютерну техніку, телекомунікаційне обладнання та понад 400 SIM-карток мобільних операторів.

Таким чином, системна робота вітчизняної спецслужби дозволяє виявляти та блокувати діяльність ботоферм, які діють на шкоду державним інтересам України та поширюють матеріали деструктивного характеру. У складі спецслужб РФ, як і в складі багатьох інших спецслужб іноземних держав, діють спеціальні підрозділи, безпосереднім функціональним завданням яких є створення сталих позицій впливу в інформаційному просторі, проведення інформаційних операцій, спеціальних інформаційних акцій, в тому числі підривних та деструктивних. Лише за 2020 рік вітчизяна спецслужба заблокувала понад 2,5 тисячі спільнот у соцмережах з мільйонною аудиторією та понад 20 ботоферм з потужністю більш ніж 60 тисяч акаунтів, нейтралізовано понад 600 кібератак на ресурси органів державної влади. Усі ці дії координувалися із території РФ.

Слушно та об'єктивно вказує Н. Ткачук, що з огляду на актуальні загрози кібербезпеці України та досвід провідних країн саме Служба безпеки України повинна займати ключове місце в національній системі кібербезпеки для забезпечення її ефективності та підвищення спроможностей держави із протидії актуальним кіберзагрозам [6, с. 55].

Висновки.

Таким чином, метою діяльності проросійських ботоферм залишається дискредитація міжнародного іміджу України та усієї системи політичної української влади. На постійній основі фіксується неабиякий бурхливий сплеск активності проросійських ботоферм у соціальних мережах. Україна перебуває у перелік країн, де з 2017 року виявили найбільшу кількість ботоферм у соціальних мережах.

Слід зазначити також те, що тільки у 2020 році "Facebook" заблокував чисельну мережу акаунтів російських спецслужб, які працювали в Україні. Для мережі створювали фейкових осіб, які діяли на форумах блогів та часто одразу на кількох платформах соцмереж. Кожен такий акаунт вимагає часу та грошей на створення, тому їх намагалися створити максимально правдоподібно і помітити їх було нелегко. Так, наприклад, коли

журналісти перевіряли якусь “персону” у “Facebook”, вона могла мати акаунт і в “Instagram”, що могло створити враження, що це справді жива людина. Такі боти видавали себе за журналістів та намагалися зв’язатися з політиками, справжніми медійниками та громадськими діячами якогось регіону. Однак попри “витончений характер” операцій з такими ботофермами вони не мали значного успіху чи впливу.

Загальновідомо, що Україна увійшла до топ-5 країн-джерел мереж скоординованої неавтентичної поведінки (CAB) або ж ботоферм. Також Україна увійшла до переліку країн, щодо яких найчастіше здійснювалися операції впливу (ІО), що у “Facebook” розуміють як скоординовані зусилля з метою маніпулювання чи впливу на громадську думку. Україна активно долучає свою частку зусиль до міжнародної боротьби з пропагандою та фейками. На цьому фоні потребує активізації діяльність, спрямована на нейтралізацію впливу дезінформації та маніпуляцій, впровадження швидкого та проактивного реагування на ключові теми, у межах яких поширюють фейки та пропаганду. Тому в сучасних умовах доцільним є розробка змін до законодавства про удосконалення санкцій за поширення фейкової інформації та дезінформації.

Також необхідно прискорити складання карти виявлених злочинних ботоферм та посилити правоохоронні заходи з їх перспективного блокування, у тому числі в співпраці з “Facebook”. Має сенс розробити законодавчі зміни щодо вдосконалення санкцій за поширення дезінформації, налагодити проактивне інформування суспільства через соціальні мережі щодо позиції України з питань, які потенційно можуть стати загрозливими. Наслідками цього мають стати: оперативна реакція на повідомлення з дезінформацією та маніпуляціями; забезпечення оперативного донесення офіційної позиції держави щодо повідомлень, які місять дезінформацію; поінформованість суспільства про матеріали, які свідчать про поширення РФ деструктивних матеріалів та повідомлень, що містять дезінформацію й маніпуляції. Вагома роль у зазначених ініціативах відводиться Центру протидії дезінформації як робочому органу РНБО України, утвореному в Україні в березні 2021 року [7].

Використана література

1. Зінченко О.В. Мережеві фейки як психологічна проблема. URL: https://www.newlearning.org.ua/system/files/sites/default/files/zagruzheni/zinchenko_olexandr_2020.pdf

2. Кіца М.О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. URL: http://nz.uad.lviv.ua/static/media/1–52/36

3. Курбан О. Фейки у сучасних медіа: ідентифікація та нейтралізація. *Бібліотекознавство. Документознавство. Інформологія*. 2018. № 3. С. 96-103. URL: http://nbuv.gov.ua/UJRN/bdi_2018_3_15

4. Пригорницька О. Фейкова інформація в соціальних медіа: виявлення, оцінка, протидія. *Наукові праці Національної бібліотеки України імені В.І. Вернадського*. 2017. Вип. 48. С. 439-452. URL: http://irbis-nbuv.gov.ua/everlib/item/er-0003055

5. Варіативність соціалізації особистості в умовах сучасного інформаційного суспільства: монографія / Н.М. Токарева, А.В. Шамне, О.О. Халік та ін.; ред. Н.М. Токаревої. Київ: ТОВ НВП “Інтерсервіс”, 2017. 220 с.

6. Ткачук Н. Роль і місце Служби безпеки України в національній системі кібербезпеки. *Журнал східноєвропейського права*. 2017. № 44. С. 50-57.

7. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року “Про створення Центру протидії дезінформації”: Указ Президента України від 19.03.21 р. № 106. URL: https://www.president.gov.ua/documents/1062021-37421

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

УДК 343.9:343.235.2-057.874

ВЕДЕРНІКОВА А.О., ад'юнкт Луганського державного університету внутрішніх справ імені Е.О. Дідоренка.
ORCID: https://orcid.org/0000-0002-4526-1277.

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРБУЛІНГУ ТА ЙОГО ВИДІВ

Анотація. *У роботі досліджується поняття кібербулінгу та висвітлено його особливості, а також наведені приклади з вітчизняної судової практики. На основі наукових поглядів надано основні та похідні види кібербулінгу, їхні короткі кримінологічні характеристики. Здійснене структурування видів кібербулінгу. Проаналізовано статистичні показники проявів кібербулінгу в Україні. Визначаються світові тенденції щодо відповідальності за окремі види кібербулінгу, такі як харасмент, кіберсталкінг, грумінг, секстинг та наклеп.*

Ключові слова: *кібербулінг, цькування, види кібербулінгу, харасмент, кіберсталкінг, флемінг, персонація, кіберсексуальний булінг.*

Summary. *The article clarifies that there is no stable scientific and legislative definition of cyberbullying. It is proposed to consider that cyberbullying is a violent actions of participants in the educational process using electronic communications against a minor or such a person, causing interference in the educational process, significant non-compliance with school discipline, violation of the rights of participants in the educational process or caused them moral, physical, mental or material damage. It was found that cyberbullying is a subspecies of traditional bullying, but has specific properties: anonymity of the attacker; the victim and the offender located in different physical spaces; lack of time frame; the possibility of exponential growth of the audience; reusability. In addition, the article provides examples from domestic case law. The basic and derivative types of cyberbullying and their short criminological characteristics are given. An attempt has been made to structure these types of cyberbullying. The article also briefly analyzes the statistical indicators of various manifestations of cyberbullying in Ukraine. Finally, current global trends in liability for certain types of Internet abuse, such as such as harassment, cyberstalking, grooming, sexting and denigration, are also briefly analyzed.*

Keywords: *cyberbullying, bullying, types of cyberbullying, harassment, cyberstalking, flaming, impersonation, cybersexual bullying.*

Анотация. *В работе исследуются понятие кибербуллинга и освещено его особенности, а также приведены примеры из отечественной судебной практики. На основе научных взглядов представлены основные и производные виды кибербуллинга, их краткие криминологические характеристики. Осуществлено структурирование видов кибербулинга. Проанализированы статистические показатели проявлений кибербуллинга в Украине. Определены мировые тенденции относительно ответственности за отдельные виды кибербуллинга, такие как харасмент, кіберсталкинг, груминг, секстинг и клевета.*

Ключевые слова: *кибербуллинг, травля, виды кибербуллинга, харассмент, кіберсталкинг, флеминг, персонация, киберсексуальный буллинг.*

Постановка проблеми. Сучасні темпи поширення комп'ютерних технологій породжують нові форми насильницьких проявів – кібербулінг, тобто булінг (англ. *bullying* – "навмисне цькування", "переслідування"), який здійснюється із використанням інформаційно-комунікативних технологій. А в умовах карантинної ізоляції зі зменшенням реальної взаємодії, коли життя підлітків переходить у віртуальний вимір, ризик стати жертвою кібербулінгу значно підвищується.

За даними ЮНІСЕФ і Спеціальної представниці Генерального секретаря ООН з питань насильства щодо дітей, опитування 2019 року показало, що третина молодих

людей у 30 країнах світу стають жертвами онлайн-булінгу, а кожна п'ята молода людина змушена пропускати заняття в школі через кібербулінг та насильство. В Україні 29 % опитаних підлітків були жертвами онлайн-булінгу, а 16 % були змушені пропускати через це шкільні заняття [1].

Результати аналізу наукових публікацій. Кібербулінг досліджували такі зарубіжні вчені як: D. Olweus, S.P. Limber, N.E. Willard, M. Nuccitelli, K.L. Mason, A. Czesławiak, T. Porsch, S. Pieschl тощо. Вони розглядали кібербулінг здебільшого з позицій психології, педагогіки, соціології. А наявні окремі кримінологічні праці мають більш статистичний характер, ніж онтологічний.

У вітчизняній науці зазначену проблематику також з позицій психології, соціології, педагогіки, лінгвістики досліджували О.Ю. Міхєєва, М.М. Корнієнко, Л.П. Бутузова, В.О. Бондар, Н.М. Дайнека. Але є й доробки, які розглядають це негативне явище з позицій кримінології. Це стосується окремих праць присвячених кібербулінгу та його видам І.Г. Лубенця, Т.В. Миронюка, А.К. Запорожця, Б. Мойса. Проте вони розглядають кібербулінг у широкому значенні та надають характеристику лише основним видам кібербулінгу, залишаючи без уваги їх похідні форми, що мають самостійне кримінологічне значення.

З позицій кримінології явище кібербулінгу майже не досліджене, хоча у світовій науковій спільноті є усталеною думка, що цькування у закладах освіти, і тим більше з використанням інформаційних технологій, є криміногенним фактором, а їх жертви мають підвищений ризик причетності до делінквентної поведінки та злочинів.

Це зумовлює необхідність детального кримінологічного дослідження кібербулінгу та його видів щоб виробити дієві заходи протидії.

Метою статті є визначення видів кібербулінгу, що здійснюється у закладах освіти, їх структурування та надання кримінологічної характеристики задля визначення напрямів профілактичних заходів.

Виклад основного матеріалу. Понятійний апарат даного явища ще не сформований, оскільки в Україні відсутнє кодифіковане визначення кібербулінгу. Наукова література не має сталої термінології та єдності думок щодо розглянутого феномена. Деякі вчені розмежовують "традиційний" булінг та кібербулінг. Проте Д. Олвеус та С. Лімбер вважають, що кібербулінг є підкатегорією або конкретною формою булінгу [2]. Виходячи з цього, визначення кібербулінгу залежить від підходу до розуміння родового поняття "булінг". Так, у широкому розумінні кібербулінгом є будь-яка агресія, насильницькі дії із застосуванням засобів електронних комунікацій [3]. У вузькому значенні – це підвид булінгу між учасниками освітнього процесу, що здійснюється із використанням електронних засобів зв'язку [4].

Так Миронюк Т.В. вважає, що кібербулінг – це негативна, агресивна, суспільно небезпечна, протиправна поведінка умисного характеру із застосуванням морального, фізичного насильства чи будь-які інші дії, учинені з метою дошкулити, нашкодити, принизити людину, що посягають на життя, здоров'я, волю, честь і гідність особи шляхом використання інформаційно-комунікаційних засобів: Інтернету (електронної пошти, форумів, чатів, ICQ), мобільних телефонів, соціальних мереж тощо [5, с. 282].

На погляд Лубенець І.Г., кібербулінг – це систематичні умисні дії з боку особи або групи осіб (частіше підлітків) із використанням інформаційно-комунікаційних засобів, спрямовані проти іншої особи (осіб), що характеризуються створенням ворожої, принизливої, образливої обстановки й метою або наслідком яких є залякування, порушення права на безпечне навчання, повагу, честь, гідність, майно, здоров'я і життя, обмеження свободи волевиявлення особи (осіб) тощо. Тобто, це форма конфліктної,

агресивної поведінки систематичного характеру, яка підсилена технологічним оснащенням [6, с. 179].

Як зазначають Міхеєва О.Ю. і Корнієнко М.М., кібербулінг – це умисні дії, які скоєні однією особою або групою осіб відносно іншої особи, посередництвом електронних засобів комунікації, з метою завдання шкоди, що можуть здійснюватися напряму, або анонімізовано і можуть призвести до низки негативних наслідків в результаті створення ситуації напруження, тиску, залякування, переслідування [7, с. 248].

Більшість українських дослідників розглядають кібербулінг у широкому розумінні. Але, враховуючи специфіку українського законодавства, вважаємо за необхідне розглядати кібербулінг у вузькому значенні. На наш погляд, *кібербулінг – це насильницькі дії учасників освітнього процесу із застосуванням засобів електронних комунікацій, що вчиняються стосовно неповнолітньої особи або такою особою, і спричинили втручання у навчальний процес, суттєве недодержання шкільної дисципліни, порушення прав учасників освітнього процесу або завдали їм моральних страждань, фізичної, психічної, матеріальної шкоди.*

Використання інформаційно-комунікативних технологій в поєднанні з юнацькою імпульсивністю, ризикованою поведінкою, викликаною недостатнім життєвим досвідом, представляє унікальні проблеми безпеки для користувачів в Інтернеті. У судовій практиці зустрічається чимало випадків притягнення до відповідальності за кібербулінг.

Наприклад, у м. Синельникове Дніпропетровської області наприкінці 2019 року дві малолітні особи здійснювали кібербулінг по відношенню до вчителя, а саме створили сторінку в мережі Instagram та складали про неї історії сексуального характеру, чим завдали потерпілій моральної шкоди[8].

У м. Олександрія Кіровоградської області 18 лютого 2020 року малолітня особа на території навчального закладу ЗНЗ № 9 вчинила відносно іншої малолітньої особи булінг, а саме побиття останнього та поширення відеозапису із вказаною бійкою у соціальній мережі [9].

Кібербулінг, хоча і походить від звичайного булінгу, але має свої особливості, які значно підвищують його суспільну небезпечність у порівнянні з останнім. По-перше, булер і жертва можуть не знаходитися в одному фізичному просторі. По-друге, він може виникати в будь-який час, і не пов’язаний з навчальним розкладом, та в будь-якому місці – жертві навіть не обов’язково знаходитись онлайн, знущання можуть проходити позаочі. По-третє, аудиторія може зростати експоненційно з одного одержувача до невизначеного числа за секунди. По-четверте, злочинець може бути анонімним. По-п’яте, існує можливість повторного перегляду негативного контенту [10, с. 212].

Загалом вчені виділяють такі ознаки кібербулінгу: умисне ставлення до шкоди; довготривалість у часі; дисбаланс сили між сторонами, який проявляється через більшу технологічну компетенцію агресора; широка аудиторія; анонімність агресора [11, с. 30].

Деякі науковці ставлять під сумнів необхідність для кібербулінгу такої ознаки як системність. Аргументом є той факт, що розміщена інформація може переглядатися та пересилатися в Інтернеті неодноразово і онлайн-зміст часто доступний протягом багатьох років після початкового інциденту [12, с. 131].

Поведінці кібербулінгу серед підлітків можуть сприяти три фактори: ефект дезінгібіції, перехід ідентичності від приватного до соціального, і відсутність взаємодії дорослих, що проявляється у поганому моніторингу дій неповнолітніх в Інтернеті та відсутності емоційного контакту з батьками. Ефект дезінгібіції – це зменшення стурбованості про самопрезентацію та судження інших, зумовлене анонімністю, яку забезпечує кіберпростір. Інтернет-користувачі розслабляються та починають

висловлюватися більш відкрито, таким чином нормальні поведінкові обмеження можуть загубитися або знехтуватися, а як результат – може проявитися агресивна поведінка [4, с. 328].

Кіберпростір дає підліткам контекст, у якому вони вільні від впливу соціальних очікувань і можуть дослідити альтернативні аспекти власних "Я". Так званий, "ефект кабіни" – людина, що сидить перед екраном монітора, як пілот-винищувач, він не бачить страждань жертв, що в свою чергу може призвести до відсутності співчуття та емпатії [13, с. 234]. Перехід ідентичності від приватного (особистого) до соціального (публічного) рівня проявляється у тому, що користувачі менше прислухаються до внутрішніх переконань та починають дотримуватися групових норм. Кібербулери відмовляються від звичного соціального контролю і стають більш імпульсивними, ірраціональними та агресивними [4, с. 330].

Більшість негативних наслідків кібербулінгу такі ж самі, як і у "традиційного" булінгу: депресія, низька самооцінка, тривожність, суїцидальні думки, спроби самогубства [2, с. 231]. У багатьох жертв кібер-знущань може розвинутися ряд симптомів подібних до посттравматичних розладів [13, с. 242]. Нові дослідження показали, що кібербулінг пов'язаний з низкою психосоматичних проблем, у тому числі: труднощі сприйняття, емоційні проблеми та складнощі з однолітками, головний біль, періодичні абдомінальні болі, труднощі зі сном, відсутність почуття безпеки в школі, гіперактивність, антисоціальна поведінка, часте куріння, пияцтво та поведінкові проблеми [14, с. 183]. Більшість підлітків повідомляють про негативні наслідки кібербулінгу і щонайменше 20 % – про серйозний (психологічний) стрес спричинений кібер-знущаннями. Крім того, дівчата часто мають більші або гірші наслідки, ніж хлопчики [15, с. 10]. Тому світова спільнота акцентує свою увагу саме на дослідженні кібербулінгу та навіть криміналізації деяких його форм.

На думку Лубенець І.Г., кібербулінг може здійснюватися у двох основних формах: персоніфікованій, яка передбачає адресну розсилку інформації жертві, та неперсоніфікованій, що полягає в розповсюдженні інформації жертві й поширенні її в публічному інформаційному просторі для невизначеного кола осіб, створюючи навколо жертви в референтних соціальних групах негативну обстановку неповаги, приниження, засудження, ізоляції тощо. Друга форма кібербулінгу є значно більш суспільно небезпечною. Також авторка зазначає, що кібербулінг може бути відкритий (прямий) та латентний. Так, наприклад, надсилання повідомлень, листів, відео, фотографій образливого, погрожуючого характеру; розповсюдження персональних даних (правдивої або неправдивої інформації), яка дискредитує жертву; зйомка бійок, знущань за допомогою сучасних ґаджетів із подальшою демонстрацією таких фото, відео – є відкритим кібербулінгом. В свою чергу, прихована агресія, за якої поведінка кібербулера замаскована під звичайну бесіду, дискусію із застосуванням сарказму, іронії, провокативної поведінки, образ, дошкуляння, провокація конфлікту, здобуття інформації про особу з подальшим її використанням у хуліганських або злочинних цілях – це латентний кібербулінг [6, с. 179].

Існують різні підходи до класифікації кібербулінгу: Мічаел Нусцітеллі виділяє 38 підвидів; Лауріе-Анн М. Неллстен – 18 основних та 3 підвиди; веб-сайт "Kaspersky" – 10 видів, а Віллард Н.Е. – 8 форм. Основні з них:

- Харасмент, домагання (*harassment*) [16, с. 266; 17] – односторонній агресивний вербальний та/або невербальний вплив одного чи декількох агресорів на одну жертву, що дратує, тривожить, або призводить до істотного емоційного страждання. Наприклад, повторювані, образливі повідомлення, відправлені жертві найчастіше через особисті

канали комунікації, такі як електронна пошта, стільниковий телефон. Якщо вони мають сексуальний характер чи коментарі про тіло, зовнішність, стать – то це вже сексуальні домагання (*sexual harassment*). Лауріе-Анн М. Неллстен до харасменту також відносить: гріфінг, фламінг та онлайн-геймінг [18];

- Гріфінг (*griefing*) – харасмент, який відбувається у онлайн-іграх і ніколи не проявляється у вербальній площині. Гріфери навмисно шкодять іншим гравцям, оскільки зацікавлені не у перемозі в конкретній грі, а в руйнуванні гри іншим гравцям [19, с. 235];

- Онлайн-геймінг (*Interactive, Online Gaming Harassment*) – вербальне жорстоке поводження під час онлайн-ігор, використання погроз та нецензурної мови, блокування гри для інших, передача неправдивої інформації про особу, зламування облікового запису [18];

- Кібер-переслідування (*cyber-persecution*) – постійний і повторний харасмент, приниження, образи та погрози [20, с. 165];

- Кіберсталкінг (*cyberstalking*) [16, с. 266; 21; 17] – онлайн-залякування, використання агресивних, здебільшого анонімних, електронних повідомлень для переслідування іншої особи з метою дратування, домагання або вчинення подальших злочинів, зокрема сексуального насильства або побоїв. Значно небезпечніший за харасмент;

- Погрози, залякування (*threats, eIntimidation*) [22] – тактика, яка використовується для того, щоб вселити страх, повідомляючи про прямі загрози або натякаючи на їх імовірність, наприклад, щодо руйнування стосунків, небезпеки родині, майну, фізичному здоров'ю, навіть, погрози смертю;

- Флемінг (*flaming*) [16, с. 265; 17] – ворожі, образливі мовленнєві випади, вербальна конфліктна взаємодія між Інтернет-користувачами, часто з використанням нецензурної лексики, як правило, в результаті жвавого обговорення проблемних питань у сфері політики, релігії тощо, в публічному оточенні (наприклад, чати), а не в приватному обміні електронними повідомленнями, з метою завдання соціальної та психологічної шкоди і руйнування авторитету;

- Троллінг (*trolling*) [21] – стратегічно спланований та провокативно спрямований флемінг, часто постає як гіперболізована увага до незначних деталей у обговорюваній темі;

- Наклеп (*denigration, dissing, Spreading Rumours*) [16, с. 266; 17; 21] – надсилання або розміщення відомостей про інших осіб, фотографій чи відеозаписів, що є принизливими і не відповідають дійсності, з наміром завдати шкоди стосункам та репутації людини;

- "Вбивство веб-сайтом" (*Web Page Assassination*) – створення веб-сайту, який ображає або загрожує конкретній дитині [22];

- Блогобулінг (*Blogobullying*) – створення Інтернет-блогу, центральною темою якого є конкретна особа, з метою розміщення принизливої та неправдивої інформації. Зневажливі пости можуть розміщуватись на першій сторінці Google [18];

- Публічне викриття (*outing, exposure, revealing secrets*) [16, с. 266; 17; 21] – оприлюднення персональних даних приватного змісту, спільних фотографій, відео чи листування без дозволу суб'єктів даних;

- Персонація/уособлення (*impersonation, Impersonating YOU, "Imping"*) [16, с. 266; 17] – кривдник видає себе за жертву та, використовуючи пароль жертви, надсилає негативну, образливу чи недостовірну інформацію від імені жертви, з наміром зіпсувати стосунки жертви або занапастити її. Часто цей вид кібербулінгу тісно пов'язаний із, так званим, кетфішінгом;

- Кетфішінг (*catfishing*) – викрадення онлайн-ідентичності неповнолітнього для відтворення профілю у соціальних мережах для оманливих цілей [21];
- Фрепінг (*fraping*) – зміна деталей на чиїйсь обліковій сторінці, коли вони залишають її відкритою [21]. Лауріе-Анн М. Неллстен вважає, що фрепінг є складовою персонації;
- Маскарад (*masquerade, Impersonating Others, Creating Fake Profiles*) – створення підробленої особистості для цькування когось [20, с. 165];
- Шахрайство (*trickery, phishing*) [16, с. 266; 21; 17] – отримання відомостей, що містить приватну, конфіденціальну, компрометуючу інформацію, шляхом обману і встановлення довірливих стосунків з жертвою, через інформаційно-комунікативні канали з подальшим оприлюдненням цього змісту;
- Виключення/остракізм (*exclusion/ostracism*) [16, с. 266; 17] – виключення або вилучення з онлайн-соціуму, реалізується у невербальній площині у вигляді мовчазного бойкотування;
- Хеппі слеппінг (*Happy Slapping*) – фізичний напад на особу або її збентеження з метою фіксації реакції жертви на відео, яке потім розміщуються в Інтернеті [22];
- Секстинг (*sexting*) – розповсюдження фотографій сексуального характеру іншої особи без згоди цієї особи [22];
- Слатшеймінг (*Slut Shaming*) – тактика кібербулінгу, спрямована на особу жіночої статі. А саме, запис зображення чи відеозапису конкретної дитини, які легко можуть бути розтлумачені як сексуально провокуючі, та їх оприлюднення. Часто зображення зроблені без згоди дитини та без її відома [22];
- Секскастінг (*sexcasting*) – схожий на секстинг, але він включає відео високої чіткості із явно сексуальним змістом [20, с. 166];
- Сексторція (*Sextortion*) – неповнолітні особи експлуатують інших неповнолітніх задля сексуальних дій, шантажуючи їх розкриттям принизливої інформації [22];
- Грумінг (*grooming*) – встановлення емоційного зв'язку з дитиною чи її сім'єю для схилення неповнолітньої особи до дій сексуального характеру [20, с. 166];

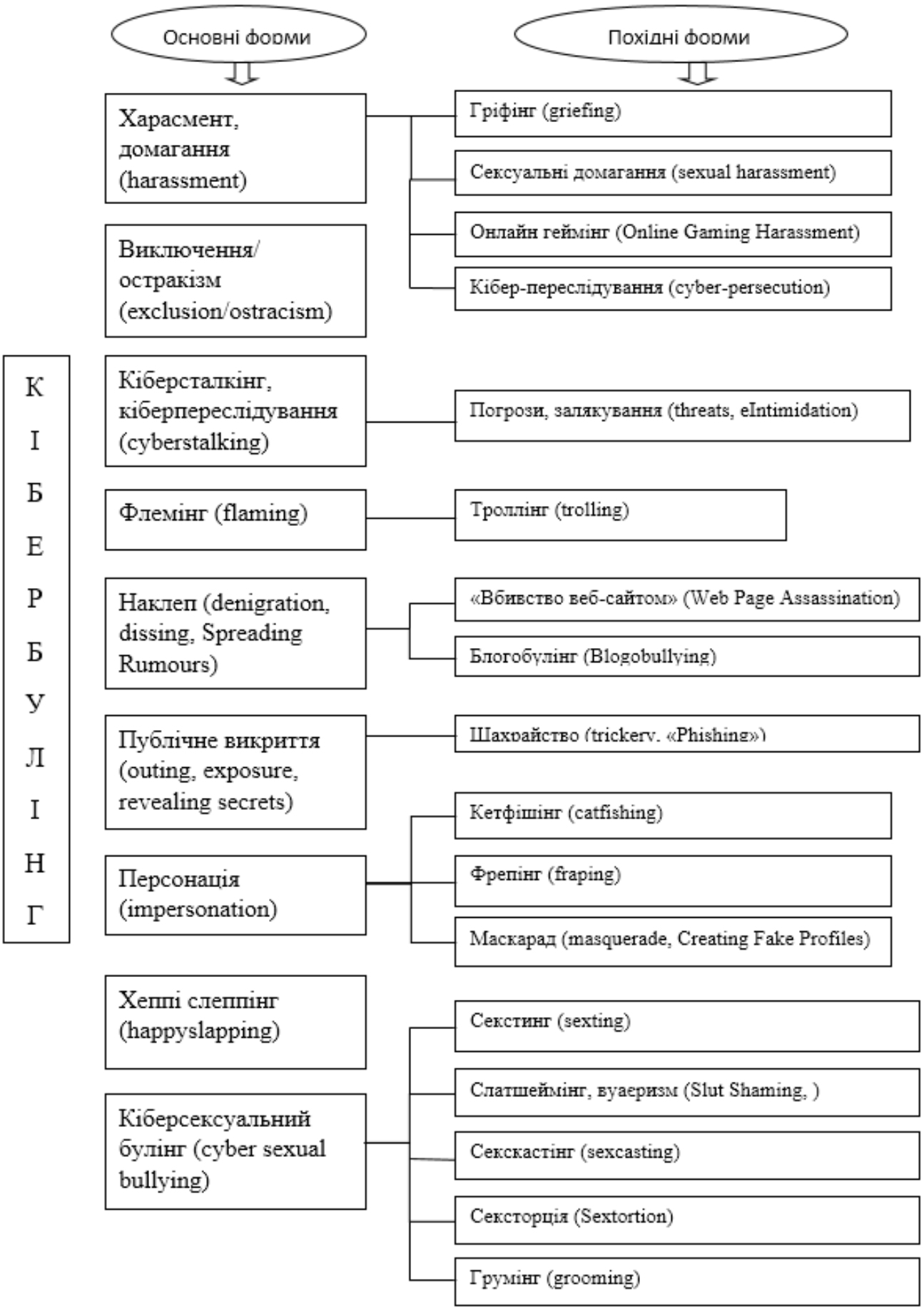
Проаналізувавши наявну інформацію, узагальнімо та схематично відобразимо основні та похідні форми кібербулінгу (див. далі Схему).

Вважаємо, що основними формами кібербулінгу є: харасмент або домагання; соціальне виключення (остракізм); кіберсталкінг, тобто переслідування із застосуванням засобів електронних комунікацій з погрозою завдання шкоди офлайн; флемінг у формі агресивних мовленнєвих випадів; наклеп; оприлюднення персональних даних, компрометуючої конфіденційної інформації; видавання себе за іншу особу (обман у персоналізації); фільмування булінгу (хеппі слеппінг); кіберсексуальний булінг.

Праворуч у схемі зображені похідні форми кібербулінгу, які утворюються від основних форм та мають з ними спільні риси, але є вужчими за своїм змістом через додавання ознак, які стосуються лише частини родового поняття, бо містять специфічні видові ознаки. Такий підхід є перспективним для розробки більш ефективних заходів протидії, бо похідні форми кібербулінгу хоча і утворюються від основних форм, проте мають самостійне кримінологічне значення.

За даними, наведеними "Ла Страда-Україна", на гарячу телефонну лінію за 2017 – 2018 роки надійшов 13381 дзвінок, що стосувався небезпеки для дітей в Інтернеті. Зокрема, звернення стосувались: секстингу (2845 дзвінків), троллінгу (1632), грумінгу (1385), мобінгу – групового цькування (1230), кібербулінгу (925) [23, с. 5]. Це демонструє значну поширеність цих негативних явищ.

Схема. Класифікація форм кібербулінгу



За останній рік, у зв'язку з необхідністю обмеження соціальних контактів через пандемію CoVID-19, кібербулінг за частотою прояву знаходив свій вияв у: відправці систематичних погрозливих, образливих повідомлень; створенні спільнот з метою цькування та впливу на школярів; пропозицій проголосувати "за" чи "проти" когось в образливому опитуванні; розповсюдженні (спаму) відео та фото порнографічного характеру; створенні підробних сторінок у соцмережах та систематичне користування такими сторінками [24, с. 341].

В Україні ні в доктринальній, ні в законодавчій літературі ці питання чітко не визначені, хоча зарубіжні експерти акцентують свою увагу саме на дослідженні кібербулінгу та деяких його підвидів: харасмент, кіберсталкінг, секстинг, грумінг, вуаєризм. А у деяких країнах ці діяння підпадають під кримінально-правову заборону. Наприклад, харасмент криміналізований у США, Австрії, Бельгії, Великобританії, Італії, Румунії; кіберсталкінг – у Великобританії, Іспанії, Нідерландах, Португалії, Словенії, США, Франції; грумінг – у Великобританії та США; секстинг – у Великобританії, Австралії, США; а наклеп – у Австрії, Бельгії, Великобританії, Італії, Іспанії, Франції, Угорщині тощо.

Висновки.

Аналізуючи вищесказане, можна зробити висновок, що немає сталого наукового та законодавчого визначення кібербулінгу. На наш погляд, кібербулінг – *це насильницькі дії учасників освітнього процесу із застосуванням засобів електронних комунікацій, що вчиняються стосовно неповнолітньої особи або такою особою, і спричинили втручання у навчальний процес, суттєве недодержання шкільної дисципліни, порушення прав учасників освітнього процесу або завдали їм моральних страждань, фізичної, психічної, матеріальної шкоди*.

Хоча кібербулінг є підвидом традиційного булінгу, але має специфічні властивості: анонімність зловмисника; знаходження жертви і правопорушника у різних фізичних просторах; відсутність часових рамок; можливість експоненційного зростання аудиторії; можливість повторного перегляду. Вважаємо, що основними формами кібербулінгу є: харасмент; остракізм; кіберсталкінг; флемінг; наклеп; публічне викриття; персонація; хеппі слеппінг та кіберсексуальний булінг. В свою чергу, похідні форми кібербулінгу утворюються від основних форм та мають з ними спільні риси, але є вужчими за своїм змістом через додавання ознак, які стосуються лише частини родового поняття, бо містять специфічні видові ознаки. До них відносяться: гріфінг, сексуальні домагання, онлайн-геймінг, кібер-переслідування, погрози, залякування, троллінг, блогобулінг, "вбивство веб-сайтом", шахрайство, кетфішінг, фрепінг, маскарад, секстинг, слатшеймінг, вуаєризм, секскастінг, сексторція, грумінг тощо. Додаткове вивчення останніх є перспективним для вироблення комплексної національної стратегії та механізмів протидії кібербулінгу, а також виявлення та фіксації цих протиправних діянь. У національній науці тільки розпочали досліджувати кібербулінг та його види, хоча зарубіжні вчені приділяють дослідженню вказаної проблематики значну увагу, а у деяких країнах такі підвиди кібербулінгу, як харасмент, кіберсталкінг, секстинг, грумінг, вуаєризм, підпадають під кримінально-правову заборону.

В Україні в умовах карантинної ізоляції через пандемію CoVID-19 відбулося зменшення реальної взаємодії підлітків, що продукувало наступні прояви кібербулінгу: погрозливі та образливі повідомлення, створення спеціальних груп, опитувань у месенджерах чи соціальних мережах задля знущання, розповсюдження контенту порнографічного характеру, створення фальшивих профілів у соцмережах.

Вважаємо, що поширеність кібербулінгу зумовлює необхідність подальших емпіричних та кримінологічних досліджень щодо поширеності в Україні різних форм кібербулінгу задля вироблення ефективних заходів протидії цьому негативному явищу.

Вбачається за доцільне розгорнути девіантологічну дискусію про заявлене предметне поле та розвинути дослідницькі підходи до вивчення нових проявів кібербулінгу, який містить загрозу для життя та здоров'я підлітків.

Використана література

1. Опитування ЮНІСЕФ: понад третина молодих людей у 30 країнах світу потерпають від онлайн-булінгу. 04.09.2019. URL: https://www.unicef.org/ukraine/uk
2. Olweus, Dan & Limber, Susan. Some Problems With Cyberbullying Research. *Current Opinion in Psychology.* 2017. № 19. P. 225-240. URL: https://www.researchgate.net/publication/316260953
3. Dorothy Wunmi Grigg. Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance & Counselling.* 2010. Volume 20. Number 2 2010. Pp. 143-156. URL: https://www.academia.edu/17873258/Cyberbullying_Labels_Behaviours_and_Definition_in_Three_European_Countries?auto=download&email_work_card=download-paper
4. Mason K.L. Cyber Bullying: A preliminary assessment for school personnel. *Psychology in the Schools.* 2008. 45(4). P. 323-348. URL: https://doi.org/10.1002/pits.20301
5. Миронюк Т.В., Запорожець А.К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія. *Юридичний часопис Національної академії внутрішніх справ.* 2018. № 2. С. 275-284. URL: http://nbuv.gov.ua/UJRN/aymvs_2018_2_25
6. Лубенець І.Г. Кібернасильство (кібербулінг) серед учнів загальноосвітніх навчальних закладів. *Jurnalul juridic national: teorie şi practică.* 2016. № 3. С. 178-181. URL: http://www.jurnaluljuridic.in.ua/archive/2016/3/38.pdf
7. Міхєєва О.Ю., Корнієнко М.М. Кібербулінг як соціально-педагогічна проблема. *Молодий вчений.* 2018. № 11(63). С. 247-251. URL: http://molodyvcheny.in.ua/files/journal/2018/11/60.pdf
8. Постанова Синельниківського міськрайонного суду Дніпропетровської області від 28.01.20 р. у Справі № 191/4658/19, провадження № 3/191/1281/19. URL: https://reyestr.court.gov. ua/Review/87399833
9. Постанова Олександрійського міськрайонного суду Кіровоградської області від 13.03.20 р. у Справі № 398/702/20, провадження № 3/398/348/20. URL: https://reyestr.court.gov.ua/Review/88248218
10. Semerci A. Investigating the effects o personality traits on cyberbullying. *Pegem Eğitim ve Öğretim Dergisi*. 2017. № 7(2). P. 211-230. URL: http://dx.doi.org/10.14527/pegegog.2017.008
11. Giménez-Guado A., Arnaiz-Sánchez P., Cerezo-Ramírez F., Prodócimo E. Percepción de docentes y estudiantes sobre el ciberacoso. Estrategias de intervención en Primaria y Secundaria. *Revista Comunicar*. 2018. № 56 (26). P. 29-38. URL: https://doi.org/10.3916/C56-2018-03
12. Annalaura Nocentini, Juan Calmaestra, Anja Schultze-Krumbholz, Herbert Scheithauer, Rosario Ortega, Ersilia Menesini. Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Australian Journal of Guidance and Counselling.* 2010. Volume 20 Number 2. P. 129-142. URL: https://www.academia.edu/17873258/Cyberbullying_Labels_Behaviours_and_Definition_in_Three_European_Countries?auto=download&email_work_card=download-paper
13. Adam Czesławiak. Agresja elektroniczna i cyberbullying wśród dzieci i młodzieży a działania szkoły. 2013. P. 221-263. URL: https://bon.edu.pl/media/book/pdf/Agresja%20_elektroniczna_i_cyberbullying-AC.pdf
14. Magdalena Marczak, Iain Coyne. Cyberbullying at School: Good Practice and Legal Aspects in the United Kingdom. *Australian Journal of Guidance & Counselling.* 2010. Volume 20. Number 2. P. 182-193. URL: https://www.academia.edu/17873258/Cyberbullying_Labels_Behaviours_and_Definition_in_Three_European_Countries?auto=download&email_work_card=download-paper

15. T. Porsch, S. Pieschl. Cybermobbing unter deutschen Schülerinnen und Schülern. *Diskurs Kindheits- und Jugendforschung Heft.* 1-2014, S. 7-22. URL: https://www.budrich-journals.de/index.php/diskurs/article/download/19080/16600

16. Willard N.E. Cyberbullying and Cyberthreats: Responding to the challenge of Online Social Aggression, Threats, and Distress. APPENDIX K Parent Guide to Cyberbullying and Cyberthreats. 2007. Champaign, IL: Research Press. URL: http://www.embracecivility.org/wp-content/upload snew/2012/10/appK.pdf

17. Roshini Pillay, Glenda Sacks. Cyberbullying - A Shrouded Crime: Experiences of South African Undergraduate Students. *The Oriental Anthropologist: A Bi-annual International Journal of the Science of Man.* 2020. Volume 20. P. 370-386. doi:10.1177/0972558x20952986

18. An Introduction to Cyberbullying Laurie-ann M. Hellsten. Presentation. University of Macerata. March 23, 2017. URL: http://docenti.unimc.it/alessandra.fermani/teaching/2016/15583/files/lh_slide-1-seminario

19. Дайнека Н.М. Кібербуллінг: онтологічні ознаки та типологія. *Вісник Житомирського державного університету.* 2013. Вип. 4 (70). С. 233-238. URL: http://eprints.zu.edu.ua/9887/1/48.pdf

20. Virginia Dalla Pozza, Anna Di Pietro, Sophie Morel, Emma Psaila. Cyberbullying among Young People. Directorate - General for Internal Policies - Policy Department C: Citizens' Rights and Constitutional Affairs. Study for the LIBE Committee. 2016. 192 p. URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

21. 10 Forms of Cyberbullying. Kaspersky website. 27 October 2015. URL: https://kids.kaspersky.com/10-forms-of-cyberbullying

22. Michael Nuccitelli. Cyberbullying Examples and Types of Cyberbullying. URL: https://www.ipredator.co/cyberbullying-examples

23. Богдан Мойса. Протидія кібербулінгу та кібергрумінгу в Україні: попередній аналітичний огляд. 18 с. URL: https://cyber.bullyingstop.org.ua/storage/media-archives/Протидія кібербулінгу та кібергрумінгу в Україні.pdf

24. Бутузова Л.П., Бондар В.О. Наратив учнівського булінгу в умовах карантинних обмежень. *World science: problems, prospects and innovations. Abstracts of the 5th International scientific and practical conference.* Perfect Publishing. Toronto, Canada. 2021. P. 337-346. URL: https://www.researchgate.net/profile/Maka_Jishkariani/publication/348917586_Using_Google_Sheets_to_Analyze_Electricity_Tariffs_World_science_problems_prospects_and_innovations_Abstracts_of_the_5th_International_scientific_and_practical_conference_Perfect_Publishing_Toronto_Ca/links/601698e892851c2d4d0736f1/Using-Google-Sheets-to-Analyze-Electricity-Tariffs-World-science-problems-prospects-and-innovations-Abstracts-of-the-5th-International-scientific-and-practical-conference-Perfect-Publishing-Toronto.pdf#page=337

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

Інформаційна і національна безпека

УДК 342.951

ФИЦА В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6590-8082.

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СТВОРЕННЯ КІБЕРВІЙСЬК В УКРАЇНІ

Анотація. *Розглянуто питання інституційного забезпечення створення та функціонування кібервійськ. Визначено завдання та цілі кібервійськ. Висвітлено кращі практики зарубіжного досвіду у сфері розбудови кібервійськ та кіберкомандування. Акцентована увага на сучасних загрозах поширення мілітаризації кіберпростору. Визначено шляхи удосконалення державної політики у військовій сфері щодо утворення кібервійськ в структурі Міністерства оборони України.*

Ключові слова: *кібервійська, кіберкомандування, кібербезпека, кібероборона, спеціальні інформаційні операції, кіберпростір, кібератака, мілітаризація кіберпростору.*

Summary. *The issue of institutional support for the creation and functioning of cyber forces is considered. The tasks and goals of cyber forces have been defined. The best practices of foreign experience in the field of building cyber forces and cybercommand are highlighted. Emphasis is placed on current threats to the spread of cyber space militarization. The directions of the improvement of the state policy in the military sphere on the formation of cyber forces in the structure of the Ministry of Defense of Ukraine have been identified.*

Keywords: *cyber forces, cybercommand, cybersecurity, special information operations, cyberspace, cyber attack, militarization of cyberspace.*

Аннотация. *Рассмотрены вопросы институционального обеспечения создания и функционирования кибервойск. Определены задачи и цели кибервойск. Освещены лучшие практики зарубежного опыта в сфере создания кибервойск и киберкомандования. Акцентировано внимание на современных угрозах распространения милитаризации киберпространства. Определены направления усовершенствования государственной политики в военной сфере касаемо создания кибервойск в структуре Министерства обороны Украины.*

Ключевые слова: *кибервойска, киберкомандование, кибербезопасность, кибероборона, специальные информационные операции, киберпространство, кибератака, милитаризация киберпространства.*

Постановка проблеми. Останнім часом колосального масштабу у світі набула проблема захисту кіберпростору та елементів системи стратегічних комунікацій сектору безпеки і оборони від загроз несанкціонованого втручання. Практично безмежні можливості використання Інтернету підкреслюють глобальну загрозу кіберзлочинів, кібертероризму та ведення кібервійни. Анонімність глобальних інформаційних мереж, швидкість передачі інформації та простота їх використання одночасно дозволяють використовувати всі ці переваги для здійснення протиправних діянь. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть реагувати на це зростання. У багатьох країнах світу проголошено мілітаризацію кіберпростору. Таким чином, розбудова дієвої

системи кібербезпеки України вимагає чіткого визначення засад державної політики у цій сфері та випереджального організаційно-правового та техніко-технологічного реагування на динамічні зміни, що відбуваються у кіберпросторі. Сучасна війна неможлива без кіберзахисту і, на превеликий жаль, без кібератак. Так, власні кібервійська вже мають у своєму потенціалі США, Китай, Великобританія, Франція, Німеччина, Ізраїль, Південна Корея, Японія та інші провідні держави світу. Протиборство в кіберпросторі стає принципово новою сферою та фазою вирішення конфліктних ситуацій між державами, а терміни та визначення з префіксом "кібер" знайшли своє відображення у положеннях стратегій, доктрин та концепцій переважної більшості держав світу, а також міжнародних організацій, у т.ч. НАТО. Стрімкий зростаючий у світі інтерес до проблематики кіберпростору пов'язаний, у першу чергу, з питаннями забезпечення кібербезпеки та ведення сучасних кібервійн. За таких умов визначення інституційних засад створення вітчизняних кібервійськ набуває актуальності в умовах масштабного поширення гібридних загроз, особливо з боку інформаційної експансії РФ.

Результати аналізу наукових публікацій. Питання інституційно-функціонального створення та розбудови кібервійськ досліджували у своїх працях такі науковці як: Г. Красноступ [1], О. Косогов [2], Р. Лук'янчук [3], С. Паламарчук [4] та інші. Аналіз праць вказаних авторів дає змогу визначити, що інституційні засади створення кібервійськ недостатньо розглянуті, що зумовлює необхідність дослідження зазначених процесів з урахуванням позитивного зарубіжного досвіду. Особливо це питання актуально на фоні анонсованих у травні 2021 року ініціатив Секретаря РНБО України О. Данилова щодо прискорення створення кібервійськ в Україні.

Метою статті є визначення інституційних засад у сфері забезпечення створення кібервійськ з урахуванням кращих практик зарубіжного досвіду у цій сфері в умовах глобального геополітичного протиборства.

Виклад основного матеріалу. Розуміючи необхідність та доцільність мілітаризації кіберпростору, у багатьох країнах світу створено та функціонують спеціальні підрозділи – кібервійська, які використовуються як для військових, так і розвідувальних цілей. Спеціалізовані підрозділи з кібербезпеки офіційно використовуються у десятках країн, а неофіційно – вже майже у сотні іноземних держав. Найбільш потужну армію у кіберпросторі має США, а державне фінансування на її утримання складає понад $7 млдр. США на рік. Комплектування цих підрозділів здійснюється переважно за рахунок хакерів, які поповнюють ряди військових у кіберпросторі. Надійний захист кіберпростору та домінування у світовому масштабі – стратегічне завдання уряду США, що не виключає військових дій у кіберпросторі з урахуванням національних інтересів. Політичний вектор, закладений у стратегії національної кібербезпеки США, аргументовано декларує систему кіберзагроз, настання яких провокує необхідність проведення спеціальних інформаційних операцій, спрямованих на запобігання їм та недопущення будь-яких кібератак з боку інших держав. Основними напрямками діяльності кібервійськ є шпіонаж, у тому числі й промисловий, кібератаки, спеціальні інформаційні операції та навіть ведення війни у кіберпросторі. У військових структурах передових країн світу є навіть кіберкомандування та відокремлено персонал, який залучається для захисту інфраструктури військових кіберсистем. Перемога над супротивником у цифровій війні вважається більш пріоритетною, аніж перемога у класичному військовому протистоянні.

Цікавим видається у цій площині передовий досвід Естонії. На початку серпня 2018 року в естонській армії з'явився підрозділ, що відповідає за кібербезпеку країни. Поява власного підрозділу кіберкомандування в Естонії демонструє не тільки відданість

приписам НАТО, який у 2016 році визнав кіберпростір полем проведення військових операцій на рівні з повітрям, сушею та морем. І не тільки поширення тенденції до створення власних кібервійськ, як у Франції, де їх заснували у 2016 році, або у Німеччині, де вони діють з 2017 року. Проте у цій країні процес створення оперативного кіберкомандування має закінчитися у 2023 році, оскільки повинні бути виконані нормативно визначені завдання у повному обсязі. Основна ідея підрозділу кіберкомандування Естонії полягає в тому, щоб об'єднати в єдине ціле різні частини усієї оборонної системи, які використовуються для підтримання життєдіяльності кіберсфери, для більш ефективного використання наявних людських, технологічних та фінансових ресурсів. Об'єднаний центр кіберкомандування допоможе краще використовувати здібності захищати об'єкти критичної інфраструктури від потенційних комп'ютерних загроз.

Кібернетичне командування має наступальні спроможності і може завдавати удари у відповідь на будь-які атаки. Також у цій структурі окремо було створено волонтерський підрозділ з кібербезпеки, до якого входять цивільні особи з комп'ютерними навичками. Добровольці захищають естонський кіберпростір у вільний від роботи час. Мета наступальних операцій у кіберпросторі полягає в тому, щоб вразити ворога у кіберпросторі для збереження власної свободи пересування. Незалежно від розвинених наступальних можливостей кіберкомандування, основним завданням нового підрозділу є підтримка командування оборонних сил Естонії через надання та захист інформації. Наступальні кіберспроможності використовуються, у тому числі, для перевірки безпеки власних інформаційно-комунікаційних систем і створення реалістичного середовища для навчань оборонних підрозділів. Кіберкомандування виконує свої повноваження лише в межах завдань Міністерства оборони цієї країни. Головна місія кіберкомандування – проводити спеціальні операції у кіберпросторі і надавати підтримку міністерству оборони. Тож кіберкомандування не несе відповідальності за підтримку та захист національних електронних послуг, але тісно співпрацює з організаціями, які цим займаються. Чисельно в Естонії кібервійська складають усього 300 осіб персоналу. У свою чергу, німецьке кіберкомандування у 2021 році налічує 13,5 тисячі військовослужбовців, в американському спецпідрозділі 19 тисяч, а в російській кіберармії – щонайменше 1 тис. військовослужбовців. За таких умов, пошук та підбір кваліфікованих кадрів – важливе завдання комплектування підрозділу кібервійськ. Волонтерська ліга оборони, резервні служби та призовники є основним резервом кадрів для пошуку кваліфікованого персоналу. Модель національної оборони Естонії ґрунтується на військовому обов'язку призовної служби, а також резервній службі. ІТ-навички, яким навчають у загальноосвітніх школах, можуть бути застосовані в силах оборони. Тому використовуються призовники з конкретними навичками під час виконання ними військового обов'язку. Наразі у кібервійськах Естонії проходять службу приблизно 30 призовників, які підтримують щоденні кібероперації. Якщо майбутні призовники матимуть відповідні вміння та навички, вони теж зможуть проходити службу у підрозділі кіберкомандування.

Держава-агресор ще у 2014 році створила у складі Міністерства оборони війська інформаційних операцій. РФ входить до топ п'ятірки держав світу, які мають власні кібервійська, які активно використовуються для проведення наступальних спеціальних інформаційних операцій та проведення інформаційних війн. Орієнтовно чисельність російських кібервійськ складає 1 тис. осіб, а обсяг щорічного фінансування дорівнює $300 млн. Об'єктами посягань з боку РФ залишається, у першу чергу, Україна та її інформаційний простір.

В Україні, особливо в умовах російської агресії, питання забезпечення безпеки кіберпростору гостро стоять перед політичним керівництвом нашої держави. Починаючи з 2018 року РНБО України опрацьовує питання створення кібервійськ, тобто вивчаються кращі практики зарубіжного досвіду з метою його адаптації в українських реаліях для створення власних кібервійськ у складі Збройних Сил України. Це надасть змогу значно посилити спроможності держави у сфері забезпечення оборони в кіберпросторі. Необхідно також зазначити, що відповідно до Указу Президента України "Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" від 06.06.16 р. № 240/2016 [5], в нашій країні прийнято Стратегічний оборонний бюлетень, який слугуватиме дорожньою картою оборонної реформи із визначенням шляхів її впровадження відповідно до стандартів НАТО.

Зокрема передбачається, в рамках оборонного реформування, досягнення таких стратегічних цілей, як: удосконалення системи управління силами оборони; створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR); удосконалення системи кібербезпеки та захисту інформації; становлення та розбудова спроможностей сил оборони у сфері стратегічних комунікацій, спрямованих на підтримку формування та реалізації політики у сфері безпеки і оборони України, а також досягнення цілей оборони держави; впровадження ефективної політики, системи планування і управління ресурсами в секторі оборони з використанням сучасних євроатлантичних підходів тощо. У свою чергу, Стратегічний бюлетень охоплював довгостроковий період до кінця 2020 року. Тобто в рамках оборонного реформування передбачається: створення в Міністерстві оборони та Генеральному штабі Збройних Сил підрозділів із забезпечення кібербезпеки та кіберзахисту, протидії технічним розвідкам; впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC; створення воєнної команди реагування на комп'ютерні надзвичайні події (*milCert*); здійснення міжвідомчої координації з цих питань в інтересах забезпечення обороноздатності держави, оскільки забезпечення максимальної ефективності Збройних Сил України в кіберпросторі та їх здатність надавати адекватну відповідь реальним та потенційним кіберзагрозам залишаються важливими завданнями сучасності; створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях. У цьому контексті нормативно було встановлено, що до кінця 2020 року Міністерством оборони України спільно з Держспецзв'язку заплановано: створення відділу безпеки інформації та відділу кібербезпеки в Головному управлінні зв'язку та інформаційних систем (*J6*); забезпечення розвитку підрозділів захисту інформації та кібербезпеки інформаційно-телекомунікаційної системи Збройних Сил України; створення регіональних центрів захисту інформації та кібербезпеки в містах Вінниця, Чернігів, Миколаїв; посилення спроможності Збройних Сил України в напрямі створення системи захисту інформації та кібербезпеки з урахуванням базових стандартів НАТО; забезпечення виконання вимог нормативних документів у сфері захисту інформації та протидії технічним розвідкам тощо.

Таким чином, Міністерство оборони України, Генеральний штаб Збройних Сил України на виконання політичних рішень і нормативно-правових актів у рамках реформування сектору безпеки і оборони України поступово впроваджують заходи, спрямовані на повномасштабне забезпечення безпеки в кіберпросторі, здійснюючи це на планових засадах у військовій сфері. При цьому державна політика у сфері забезпечення

кібербезпеки також повинна враховувати заходи розвитку ринку сучасних інформаційних технологій та інновацій у контексті взаємодії ІТ-сектору та держави. Проте цей процес триває у нашій країні дуже повільно. Тільки у травні 2021 року питання щодо створення в Україні кібервійськ стало предметом розгляду на черговому засіданні РНБО України. Адже створення кібервійськ стосується не тільки закупівлі комп'ютерів та відповідного обладнання, а також побудови захищеного *data*-центру, пошуку кваліфікованих фахівців та формування відповідного людського ресурсу професіоналів.

Висновки.

Виклики та загрози у кіберпросторі сьогодні набагато небезпечніші, ніж поширення ядерної зброї. Головним безпековим аспектом у воєнній сфері на національному рівні залишається розв'язана Російською Федерацією гібридна війна проти України, яка ведеться у формі комбінації різноманітних дій прихованого застосування регулярних військ (сил), незаконних збройних формувань і терористичних організацій, використання пропаганди, саботажу, тероризму, вчинення диверсій, навмисного завдавання шкоди громадянам, юридичним особам та об'єктам критичної інфраструктури в Україні. Метою цих дій є посягання на територіальну цілісність, дестабілізація соціально-політичної ситуації, гальмування соціально-економічного розвитку, європейської та євроатлантичної інтеграції, відновлення свого впливу в Україні, зміна її територіального устрою, зокрема шляхом повномасштабного застосування воєнної сили проти України. На цьому фоні важливим напрямком залишається розвиток інституційних спроможностей Міністерства оборони України та інших складових сил оборони з метою посилення кібербезпеки. У зв'язку з цим Україна максимально підтримує ідею створення кібервійськ у НАТО, які можуть стати одним із найпотужніших альянсів, враховуючи рівень проникнення інформаційних технологій в усі сфери життєдіяльності держави.

В умовах потенційної ескалації Російською Федерацією збройної агресії проти України, можуть застосовуватися методи воєнної сили проти України шляхом проведення військових операцій з рішучими діями, що може супроводжуватись інформаційними кампаніями, інформаційно-психологічними операціями, кібероперераціями та спеціальними операціями проти України тощо. Зокрема, Російська Федерація активно реалізує концепцію інформаційного протиборства, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України. Країни ЄС, НАТО, провідні міжнародні компанії та експерти одностайно визнають Російську Федерацію та її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її розвідувально-підривна діяльність у кіберпросторі є частиною гібридної війни, яку вона веде проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів національної інформаційної інфраструктури.

Таким чином, кіберпростір визнано одним з можливих театрів воєнних дій. Тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили загальносвітова тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

За таких умов для України надзвичайно важливим є прискорення створення підрозділу кібервійськ. Тобто розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України є важливим та актуальним завданням політичного керівництва держави, що неможливе без досягнення Міністерством оборони України необхідних інституційних спроможностей з метою забезпечення формування та реалізації державної політики у воєнній сфері [6].

Використана література

1. Красноступ Г.М. Організаційно-правове забезпечення протидії інформаційній агресії іноземних держав. *Правова інформатика*. № 2(42)/2014. С. 129-131.

2. Косогов О.М. Сірик А.О. Сучасна політика безпеки кіберпростору в умовах його мілітаризації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2015. №3. С. 181-186.

3. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. 2015. № 4. С. 50-56;

4. Паламарчук С.А. Шемендюк О.В., Ляшенко Г.Т., Ткач В.О. Забезпечення захисту кіберпростору в провідних країнах світу. *Збірник наукових праць ВІТІ*. 2020. № 1. С. 58-64.

5. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України": Указ Президента України від 06.06.16 р. № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/240/2016#Text (дата звернення: 20.05.2021).

6. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.21 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661(дата звернення: 20.05.2021).

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

УДК 343.14

КОКІЗА С.В., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8111-9203.
СТЕПАНОВ В.А., *кандидат технічних наук,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5249-6883.

ВИМОГИ ПРАВООХОРОННИХ ОРГАНІВ ЄС ЩОДО ЗАКОННОГО ПЕРЕХОПЛЕННЯ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Анотація. *Стаття присвячена аналізу нормативно-правових актів та нормативних документів ЄС щодо перехоплення інформації в електронних комунікаційних мережах в контексті підготовки технічного регламенту єдиної системи технічних засобів.*

Ключові слова: *перехоплення інформації, об'єкт перехоплення, суб'єкт перехоплення, правоохоронний орган, електронна комунікаційна мережа.*

Summary. *The article is devoted to the analysis of regulatory and legal acts and normative documents of the EU on information interception in electronic communication networks in the context of preparation of technical regulations of the united system of technical means.*

Keywords: *interception of information, object of interception, subject of interception, law enforcement agency, electronic communications network.*

Аннотация. *Статья посвящена анализу нормативно-правовых актов и нормативных документов ЕС относительно перехвата информации в электронных коммуникационных сетях в контексте подготовки технического регламента единой системы технических средств.*

Ключевые слова*: перехват информации, объект перехвата, субъект перехвата, правоохранительный орган, электронная коммуникационная сеть.*

Постановка проблеми. В концептуальних документах з національної безпеки провідних країн світу особливе місце займають заходи з перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах. Зазначені заходи відбуваються в кожній окремій країні відповідно до національного законодавства та мають назву *"wiretapping", "phone-tapping", "lawful interception"* та інші. В Україні перехоплення інформації у телекомунікаційних мережах здійснюється уповноваженими органами під час проведення оперативно-розшукових, контррозвідувальних, розвідувальних заходів та негласних слідчих (розшукових) дій.

Особливе значення під час здійснення перехоплення інформації в електронних комунікаційних мережах надається забезпеченню додержання конституційних прав громадян. З цією метою в Службі безпеки України здійснюється нормативне забезпечення вказаного заходу відповідно до європейських норм з врахуванням національних особливостей його організації та проведення. Враховуючи викладене, потребують аналізу та систематизації згідно з реаліями сьогодення вимоги правоохоронних органів щодо перехоплення інформації в електронних комунікаційних мережах, наведені в актах законодавства та нормативних документах Європейського Союзу (далі – ЄС), в контексті підготовки технічного регламенту єдиної системи технічних засобів.

Результати аналізу наукових публікацій. Питання перехоплення інформації у телекомунікаційних мережах досліджували Б. Гольдштейн [1], С. Грищенко [2], В. Елагин [1], Дж. Макнамара [3], О. Манжай [4], І. Стішенко [5] та інші. В більшості наукових робіт досліджувались системні аспекти вказаного питання. В статтях Б. Гольдштейна та В. Елагина [1], Дж. Макнамара [3], В. Степанова та І. Стешенка [5] проведено порівняльний аналіз підходів щодо законного перехоплення інформації з телекомунікаційних мереж, відображених в існуючих нормативних документах провідних країн світового суспільства. В статтях В. Степанова, С. Грищенка [2] та О. Манжая [4] здійснено порівняння підходу, на якому базується український нормативний документ [6], з підходами, що визначені у стандартах, рекомендаціях, специфікаціях та інших нормативних документах ETSI, CALEA та COPM.

Праці зазначених науковців, безсумнівно, є вагомим внеском в дослідження цього питання. Проте, аналіз та систематизація вимог правоохоронних органів ЄС, що пов'язані з перехопленням інформації в електронних комунікаційних мережах, в контексті підготовки технічного регламенту технічних засобів залишаються не повною мірою висвітленими, а тому потребують додаткового дослідження.

Метою статті є систематизація вимог правоохоронних органів щодо перехоплення інформації в електронних комунікаційних мережах на основі аналізу актів законодавства та нормативних документів ЄС та в межах підготовки технічного регламенту єдиної системи технічних засобів

Виклад основного матеріалу. На даний час в Україні продовжуються процеси з унормування та законодавчого закріплення заходів з перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах. В пункті 2 статті 121 Закону України "Про електронні комунікації" [7] 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 статті [8, с. 124] під єдиною системою технічних засобів розуміють функціональне поєднання засобів управління та обробки органів, уповноважених на зняття інформації з електронних комунікаційних мереж, засобів захищених транспортних мереж та мережного комплекту, що відноситься до категорії електронного комунікаційного обладнання. Визначення вимог до характеристик зазначеної єдиної системи технічних засобів та законодавче встановлення процедурних положень та норм її розробки, впровадження та експлуатування, додержання яких є обов'язковим, є вельми актуальним. Вирішення цього питання можливо через підготовку та прийняття відповідного технічного регламенту. В статті 1 Закону України "Про технічні регламенти та оцінку відповідності" [9] визначено, що технічний регламент є нормативно-правовим актом, в якому визначено характеристики продукції або пов'язані з ними процеси та методи виробництва, включаючи відповідні процедурні положення, додержання яких є обов'язковим. В пункті 3 статті 9 цього Закону України також наведено, що технічні регламенти України розробляються на основі міжнародних стандартів та актів законодавства ЄС. Тому для підготовки підґрунтя технічного регламенту єдиної системи технічних засобів проведемо систематизацію вимог правоохоронних органів ЄС щодо перехоплення інформації в електронних комунікаційних мережах на основі аналізу актів законодавства та нормативних документів (стандартів).

З цією метою розглянемо зміст нормативних документів Європейського інституту телекомунікаційних стандартів ETSI (European Telecommunication Standards Institute) технічних специфікацій [10] та [11], а також актів законодавства ЄС ENFOPOL [12], Директиви [13] та Резолюції [14].

Умовно усі вимоги правоохоронних органів, що наведені в зазначених документах, систематизуємо в наступних блоках:

- загальні вимоги;
- вимоги щодо місцезнаходження кінцевих терміналів споживачів послуг (абонентів електронних комунікаційних мереж);
- вимоги до заходів з одночасного перехоплення інформації;
- вимоги до інтерфейсу передачі та управління (в термінології нормативного документа [6];
- вимоги про додержання принципів конфіденційності під час перехоплення інформації.

По-перше, в *загальних вимогах* відображені наступні аспекти:

- національне законодавство визначає зобов'язання постачальників електронних комунікаційних послуг (оператора мережі, провайдера доступу, провайдера послуг) щодо перехоплення трафіку (пункт 4.2.a технічної специфікації [10]);
- повний вміст інформації, пов'язаної з ідентифікаційною ознакою об'єкта перехоплення, має бути перехоплений протягом повного проміжку часу дії дозволів (пункт 4.2.b технічної специфікації [10], пункт 1 ENFOPOL [12], ст. 3 Директиви [13], пункт 1 Резолюції [14]);
- будь-який вміст зв'язку, пов'язаний з ідентифікаційною ознакою об'єкта перехоплення, котрий передається до технічних засобів зберігання інформації або надходить від них, має бути перехоплений протягом повного проміжку часу дії дозволів (пункт 4.2.2 технічної специфікації [10], пункт 5.2 ENFOPOL [12], ст. 3 Директиви [13], пункт 5.2 Резолюції [14]);
- доставка інформації, пов'язаної з перехопленням, має бути надійною; інформація, яка не може бути доставлена негайно, має буферизуватись (зберігатись) до того часу, поки не стане можливим її доставка (пункт 4.2.4 технічної специфікації [10], пункти 2 та 10 ENFOPOL [12], ст. 8 Директиви [13], пункти 2 та 10 Резолюції [14]);
- має забезпечуватись можливість перехоплення електронних комунікацій (телекомунікацій) споживачів послуг – суб'єктів перехоплення, які працюють в межах електронної комунікаційної (телекомунікаційної) системи постійно, наприклад, абонентів або власників облікового запису (пункт 4.2.c технічної специфікації [10], пункт 1.1 ENFOPOL [12], пункт 1.1 Резолюції [14]);
- має забезпечуватись можливість перехоплення електронних комунікацій (телекомунікацій) споживачів послуг, які працюють в електронній комунікаційній (телекомунікаційній) системі тимчасово, наприклад, гостьових мобільних абонентів або гостьових абонентів, що використовують мережу доступу для отримання послуг, що надаються в домашній мережі (пункт 4.2.d технічної специфікації [10], пункт 1.1 ENFOPOL [12], пункт 1.1 Резолюції [14]);
- усі результати перехоплення мають отримувати унікальні ідентифікаційні ознаки (пункт 4.2.f технічної специфікації [10]).

По-друге, до правоохоронних органів має надходити інформація про поточне *географічне, фізичне та логічне місцезнаходження кінцевого обладнання (терміналу) споживачів послуг* в визначених формах (пункт 4.4 технічної специфікації [10], пункт 1.5 ENFOPOL [12], ст. 1 пункту 2 та ст. 2 пункту 2 Директиви [13], пункт 1.5 Резолюції [14]):

- під час здійснення електронної комунікаційної (телекомунікаційної) діяльності, включаючи сеанси зв'язку або послуги;

- незалежно від того, чи має місце електронна комунікаційна (телекомунікаційна) діяльність одночасно із сеансами зв'язку або послугами;
- під час тимчасового надання послуг щодо об'єкта перехоплення;
- під час успішної або ні спроби встановлення сеансу зв'язку;
- під час надання послуг, постійно пов'язаних з об'єктом перехоплення.

По-третє, *вимоги до заходів з одночасного перехоплення інформації* (пункт 4.14 технічної специфікації [10], пункт А.3 технічної специфікації [11], пункт 8 ENFOPOL [12], пункт 8 Резолюції [14]) враховують наступне:

- можливість одночасного застосування більше ніж одного заходу перехоплення для одного і того ж об'єкта перехоплення;
- можливість одночасного перехоплення однієї послуги, пов'язаної з об'єктом перехоплення, більше ніж одним правоохоронним органом;
- можливість одночасного перехоплення різних послуг, пов'язаних з об'єктом перехоплення, одним і тим же правоохоронним органом;
- максимальна кількість одночасних перехоплень відносно одного і того ж споживача послуг залежить від специфіки мережі та має бути визначена за національною згодою;
- якщо активовано одночасне перехоплення, повинні вживатись запобіжні заходи для захисту ідентифікаційних ознак правоохоронних органів та забезпечення конфіденційності розслідувань;
- заходи одночасного перехоплення можуть відбуватись відповідно до різних дозволів;
- при здійсненні заходів одночасного перехоплення в мережі мають бути створені та налаштовані механізми для забезпечення своєчасного усунення затримок в потенційно вузьких місцях.

По-четверте, *інтерфейс управління та передачі* (в термінології нормативного документа [6]) має відповідати наступному (пункт 4.10 технічної специфікації [10], пункт 5 технічної специфікації [11], пункт 3 ENFOPOL [12], пункт 3 Резолюції [14]):

- забезпечувати перехоплення інформації протягом всього заходу;
- використанню його в тих електронних комунікаційних (телекомунікаційних) мережах, в яких національне законодавство передбачає проведення перехоплення інформації;
- конфігурація має забезпечити передачу результатів перехоплення інформації;
- конфігурація має гарантувати якість електронного комунікаційного (телекомунікаційного) трафіку не гіршу за якість, що пропонується послугами щодо об'єкта перехоплення для кожного конкретного сеансу зв'язку;
- передача до правоохоронних органів результатів перехоплення інформації має відбуватись загальнодоступними шляхами зі стандартними протоколами та принципами кодування;
- кожний об'єкт перехоплення має бути однозначно пов'язаним з окремим каналом або ідентифікатором;
- між інформаційними повідомленнями та службовою інформацією сеансів зв'язку (в термінології нормативного документа [6]) має визначатись однозначна кореляція;
- формат передачі перехопленої інформації має бути загальнодоступним;
- якщо постачальник послуг використовує кодування, стиснення або шифрування електронного комунікаційного (телекомунікаційного) трафіку, то перехоплення має забезпечуватись у вигляді, придатному до застосування правоохоронними органами.

По-п’яте, вимоги *про додержання принципів конфіденційності* під час перехоплення інформації визначають наступне (пункт 4.9 технічної специфікації [10], пункти 7.3 та 8.6 технічної специфікації [11], пункт 4 ENFOPOL [12], ст. 7 Директиви [13], пункт 4 Резолюції [14]):

- перехоплення має здійснюватись та управлятись таким чином, щоб жодна неуповноважена особа не могла помітити різницю із звичайним режимом;
- перехоплення має здійснюватись таким чином, щоб ніхто із сторін, які використовують електронну комунікацію (телекомунікацію), не зміг помітити різницю із звичайним режимом;
- функції управління послугами щодо об’єкта перехоплення та будь-яких інших послуг не мають змінюватись за результатами будь-яких заходів перехоплення;
- якість обслуговування послуг щодо об’єкта перехоплення та будь-яких інших послуг не має змінюватися за результатами будь-яких заходів перехоплення.

Висновки.

Результати систематизації вимог правоохоронних органів ЄС до перехоплення інформації в електронних комунікаційних (телекомунікаційних) мережах спрямовані на підготовку в подальшому технічного регламенту єдиної системи технічних засобів та на гармонізацію політики перехоплення інформації в Україні з державами-членами Європейського Союзу з метою включення її до національного законодавства.

Автори не претендують на те, що всі вимоги, наведені в статті, обов’язково мають бути застосовані в Україні. Вони можуть бути використані під час доповнення та уточнення мережних вимог і вимог до інтерфейсів управління та передачі, що розроблені.

Викладені в статті матеріали можуть бути враховані під час підготовки Технічним комітетом стандартизації ТК 196 “Спеціальні технічні засоби для зняття інформації з каналів зв’язку та інші технічні засоби негласного отримання інформації” відповідного стандарту України.

Використана література

1. Гольдштейн Б.С., Елагин В.С. Законный перехват сообщений: подходы ETSI, CALEA и СОРМ. *Вестник связи*. 2007. № 3. С. 1-11. URL: http://iks.sut.ru/publications/zakonnyy-perehvat-soobsheniy-podhody-etsi-calea-i-sorm (дата звернення: 29.04.2021).

2. Степанов В.А., Грищенко С.М. Особливості побудови системи законного перехоплення інформації з телекомунікаційних мереж. *Збірник наукових праць Нац. акад. СБУ*. 2019. № 69. С. 199-204.

3. Макнамара Дж. Секреты компьютерного шпионажа: тактика и контрмеры/ пер. с англ. под. ред. М. Молявко. *БИНОМ. Лаборатория знаний*. 2004. 536 с. URL: http:// padaread.com/?book=36641&pg=20 (дата звернення: 29.04.2021).

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. 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).

7. Про електронні комунікації: Закон України від 16.12.20 р. № 1089-IX. *Офіційний вісник України*. 2021. № 6. Ст. 306. – (26.01.2021 р.).

8. Грищенко С.М., Степанов В.А. Умови автономного доступу до інформації під час зняття інформації з електронних комунікаційних мереж. *Інформація і право*. № 1(36)/2021. С. 123-127. URL: http://repository.vsau.org/getfile.php/28071.pdf (дата звернення: 29.04.2021).

9. Про регламенти та оцінку відповідності: Закон України від 15.01.15 р. № 124-VIII. *Відомості Верховної Ради України*. 2015. № 14. Ст. 96. URL: https://zakon.rada.gov.ua/laws/show /124-19#.Text (дата звернення: 29.04.2021).

10. Telecommunications security. Lawful Interception. Requirements of Law Enforcement Agencies (Безпека систем зв'язку. Законне перехоплення. Вимоги правоохоронних органів): технічна специфікація ETSI TS 101 331 V1.7.1. URL: https://www.etsi.org/deliver/etsi_ts/101300_ 101399/101331/01.07.01_60/ts_101331v010701p.pdf (дата звернення: 29.04.2021).

11. Telecommunications security. Lawful Interception. Requirements for network functions (Безпека систем зв'язку. Законне перехоплення. Вимоги до мережних функцій): технічна специфікація ETSI TS 101 158 V1.3.1. URL: https://www.etsi.org/deliver/etsi_ts/ 101100_101199/ 101158/01.03.01_60/ts_101158v010301p.pdf (дата звернення: 29.04.2021).

12. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL): Директива Ради ЄС від 20.06.01 р. URL: https://zakon.rada.gov.ua/laws/show/994_234#Text (дата звернення: 29.04.2021).

13. On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/ЄС (Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку, та внесення поправок в Директиву 2002/58/ЄС): Директива Європейського Парламенту та Ради 2006/24/ЄС від 15.03.06 р. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32006L0024 (дата звернення: 29.04.2021).

14. Про законне перехоплення телекомунікацій: Резолюція Ради ЄС 96/C329/01 від 17.01.95 р. URL: https://zakon.rada.gov.ua/laws/show/994_235#Text (дата звернення: 29.04.2021).

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

УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., *доктор юридичних наук, професор,* головний науковий співробітник Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України", директор НДІ ВПЗ ім. академіка В.В. Сташиса НАПрН України.
ORCID: https://orcid.org/0000-0003-3879-2237.

КРИМІНОЛОГІЧНИЙ АНАЛІЗ ЗАГРОЗ ПРАВАМ І СВОБОДАМ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ ПІД ЧАС КАРАНТИНУ У ЗВ'ЯЗКУ З ПАНДЕМІЄЮ CoVID-19

Анотація. *У статті здійснено кримінологічний аналіз основних загроз правам і свободам людини, на які вона може наразитися в інформаційному просторі під час запровадження й реалізації карантинних заходів у зв'язку із пандемією CoVID-19. До таких загроз віднесено поширення неправдивої інформації, стигматизацію певних суб'єктів – окремих осіб, соціальних груп, народів, країн та правопорушення, вчинення яких стає можливим завдяки кіберпростору.*

Ключові слова: *інформаційний простір, пандемія CoVID-19, дезінформація, інфодемія, стигматизація, правопорушення.*

Summary. *The article provides a criminological analysis of the main threats to human rights and freedoms that may be encountered in the information space during the introduction and implementation of quarantine measures in connection with the CoVID-19 pandemic. Such threats include the dissemination of false information, the stigmatization of certain actors (individuals, social groups, peoples, countries) and offenses, which are made possible by cyberspace.*

Keywords: *information space, CoVID-19 pandemic, misinformation, infodemia, stigmatization, offenses.*

Аннотация. *В статье осуществлен криминологический анализ основных угроз правам и свободам человека, с которыми может столкнуться человек в информационном пространстве при введении и реализации карантинных мер в связи с пандемией CoVID-19. К таким угрозам отнесены: распространение ложной информации, стигматизация определенных субъектов (отдельных лиц, социальных групп, народов, стран) и правонарушения, совершение которых становится возможным благодаря киберпространству.*

Ключевые слова: *информационное пространство, пандемия CoVID-19, дезинформация, инфодемия, стигматизация, правонарушения.*

Постановка проблеми. Інформаційний простір як головний комунікатор соціуму є неодмінною складовою всіх процесів його життєдіяльності. Намагаючись розширити межі та можливості цього простору, людство завжди рухалося у напрямку відшукання нових засобів комунікації, що згодом призвело до формування інформаційного суспільства, феномен якого сьогодні досить активно досліджується у філософії, глобалістиці, соціології, інформатиці, педагогіці, мистецтві і навіть у футурології. У 2011 році вільний доступ до мережі Інтернет визнано ООН як фундаментальне право людини [1]. Наслідком цього є небачене раніше збільшення впливу інформаційної складової на соціальне буття, якими б концептуальними характеристиками ми його не наділяли – постіндустріальне, інформаційне, ринкове, громадянське [2, с. 5].

Разом із тим невпинний розвиток інформаційних технологій, що спостерігається у світі принаймні в останні кілька десятків років, супроводжується необхідністю

розв'язання низки супутніх проблем, як-от: осмислення можливостей єдиної системи комунікативних зв'язків, заснованих на "цифрі", як нової моделі соціальної кооперації та прояву глобалізації сучасного соціуму як такої; прогнозування сценаріїв переходу останнього до якісно нової фази свого розвитку – інформаційної (постіндустріальної, постмодернової); аналіз негативних і позитивних наслідків, що випливають із цього факту, та розробка шляхів блокування несприятливих сценаріїв у процесі повсюдного впровадження цифрових технологій у ті чи інші сфери життя – економіку, політику, медицину, освіту, культуру тощо; кримінологічний моніторинг ситуації із правопорушеннями, вчинення яких зумовлюється можливостями саме цього простору; та ін. Не заперечуючи проти того факту, що цифровий розвиток є безумовним драйвером світового прогресу, слід пам'ятати, що цифровізація, активне зростання технологій та інноваційних досягнень незмінно породжують ризики та загрози [3], що мають стали предметом ретельного кримінологічного вивчення.

Таким чином, у суспільстві склалася парадоксальна ситуація: загальний тренд покращення якості комунікації стикається із загрозами, котрі є сателітами цього тренду. У подібній діалектиці, за словами відомого американського письменника та статистика Насіма Талеба, чимало "чорних птахів – лебедів". Це означає, що ми живемо під знаком непередбачуваності. І така непередбачуваність криється не лише у тому, що суспільство дедалі більше входить у суперечливу епоху цифрових трансформацій, а й у дії, припустимо, природних чинників, розвиток яких на певному етапі важко піддається поясненню й прогнозуванню. Одним із таких чинників є поширення донині невідомих хвороб.

Результати аналізу наукових публікацій. Щоб уявити, який обсяг публікацій сьогодні присвячується проблемі пандемії CoVID-19 у цілому та аналізованій тематиці, зокрема, достатньо зазначити, що сьогодні коронавірус став одним з основних інфоприводів [4], тому близько 88 % актуальних новин в соцмережах присвячені коронавірусу [5]. Така лавиноподібна ситуація спостерігається й у науці. З огляду на це дуже важко здійснити хоча б поверхневий аналіз підготовленої літератури. Тому уявляється правильним обмежитися посиленням лише на доробок тих українських авторів, які, на наш погляд, системно висвітлюють проблему небезпек інформаційного простору для пересічної людини, а також здійснюють соціально-правове та кримінологічне вивчення негативних соціально-правових та кримінологічних наслідків пандемії CoVID-19. До числа фахівців першої групи належать Д.С. Азаров, В.М. Брижко, В.Д. Гавловський, О.В. Голубєв, О.Г. Данильян, О.П. Дзьобань, М.В. Карчевський, В.А. Ліпкан, В.Г. Пилипчук, Н.А. Савінова, В.Ф. Фурашев, А.О. Ярошенко та ін. Що стосується науковців, увага яких спрямована на набуття знання щодо подолання чисельних негативних наслідків пандемії, які проявляються у різних соціальних сферах, то вважаємо за доцільне у цій статті згадати лише про науковий доробок творчого колективу фахівців НДІ ВПЗ, адже останніми за підтримки Національного фонду досліджень України виконується проєкт "Соціально-правові та кримінологічні наслідки поширення пандемій та шляхи їх усунення в Україні" (В.І. Борисов (керівник проєкту), В.С. Батиргареєва, Д.П. Євтєєва, А.В. Каліліна, М.Г. Колодяжний, С.С. Шрамко). Поміж іншого, зазначеними науковцями розглядається й проблема впливу інформаційного простору на поточну ситуацію із подолання аналізованої пандемії. Разом із тим серед різноманіття чисельних загроз слід виділити й ті загрози правам і свободам громадян, нейтралізація яких є невідкладною справою вже зараз.

Метою статті є, по-перше, виділення та кримінологічний аналіз породжених інформаційним простором найбільш помітних негативних явищ, що створюють ризики, у тому числі криміногенні, та призводять до порушення прав і свобод людини; по-друге, з'ясування впливу та розкриття зв'язку цих негативних явищ із ситуацією пандемії

CoVID-19 та реалізацією карантинних заходів; по-третє, експозиція деяких пропозицій щодо запобігання та зменшення негативного ефекту для прав і свобод людини від загроз інформаційного простору за часів пандемії.

Виклад основного матеріалу. Станом на 18 червня 2021 р. від CoVID-19 у світі померло 3 842 377 осіб, в Україні – 54 091 [6]. У подібній ситуації нескладно уявити, наскільки інформаційний простір є перевантаженим відомостями про світову коронакризу та ситуацію через цю кризу в окремих країнах, а також відомостями, що так чи інакше з нею пов'язані. Сама якість і націленість (іншими словами, вплив) усіх цих відомостей на певні сфери життєдіяльності, групи осіб та ін. стають великою проблемою так званої гігієни сучасного інформаційного простору, адже інформаційний простір з усіма його можливостями стає придатним інструментом для вчинення різноманітних протиправних діянь, "палітру" яких навіть неможливо до кінця уявити. У відповідності до щорічної доповіді Всесвітнього економічного форуму (21 – 24 січня 2020 р.) стосовно головних ризиків, з якими може зіштовхнутися світ, серед п'яти основних загроз було вказано на проблеми з кіберзлочинністю та у сфері охорони здоров'я [7]. Як показали подальші події 2020 р., ці загрози в умовах коронакризи дійсно стали відчутними, як ніколи.

Беручи до уваги висловлене, введений з метою протидії пандемії CoVID-19 режим карантинних заходів, з одного боку, істотно прискорив процеси діджіталізації суспільства і навіть виявився стимулом для пошуку і масового започаткування нових режимів роботи – дистанційного та змішаного, активного впровадження інструментів е-урядування, розвитку форм онлайн-навчання, телемедицини, Інтернет-торгівлі, проведення zoom-зустрічей та ін. А з другого боку, інформація про це лихо завдяки можливостям глобалізації поширюється у найкоротший строк. Таким чином, захист прав і свобод людини в інформаційному просторі має будуватися з урахуванням низки факторів, як-от: характеру та видів можливих загроз, поширеності останніх, професійних, вікових, будь-яких особистісних та ін. якостей особи і, безумовно, загальної ситуації, в якій перебуває світ. Від захищеності прав і свобод, а отже, й самої людини буде залежати стан безпеки людини в інформаційному просторі. У зв'язку з цим, ще раз повторимося, на характер і способи захисту прав людини в інформаційному просторі у теперішній час накладатиме відбиток ситуація пандемії, що викликала введення режиму карантинних заходів. Не вдаючись у сутність цих заходів, лише зазначимо, що найбільш істотних обмежень у світі та в Україні зазнали насамперед права громадян на свободу пересування, освіту та мирні зібрання. Тією чи іншою мірою обмежень зазнали і права людини у сфері культури, праці, зайняття підприємницькою діяльністю, навіть у сфері медицини.

Сьогодні навіть складно уявити таку сферу життєдіяльності суспільства, яка була б абсолютно захищена від ризиків інформаційного характеру. Проте, виходячи з буквального, або вузького, тлумачення інформаційного простору, взятого в аспекті функціонування мережі інформаційних комунікацій, слід відзначити, що трьома головними загрозами для людини, які здатний генерувати, поширювати та підживлювати інформаційний простір в умовах карантину, є фейки, правопорушення та стигматизація, умовою існування яких є рух відповідної інформації за допомогою засобів та інструментів цього простору.

Якщо перелічені небезпеки, на які може наразитися людина в інформаційному просторі під час здійснення карантинних заходів, представити у вигляді умовної піраміди, то у підґрунті цієї піраміди знаходяться випадки генерування й поширення неправдивої інформації (найчастіше йдеться про так звані фейки, або фейкові новини). Інформація подібного роду може зачіпати інтереси максимально невизначеного кола

споживачів, а тому порушення права на отримання правдивої інформації носитиме масовий характер. Слід визнати, що рух фейків не обмежують ані державні кордони, ані соціально-економічні та політичні формули буття, ані релігійні системи. У свою чергу, середину такої піраміди складають випадки стигматизації певних суб'єктів. При цьому обсяги прояву стигматизації інколи виявляються вражаючими, оскільки піддаватися стигмі можуть цілі народи, країни, континенти. Нарешті, на вершині "карантинної" піраміди небезпек знаходяться правопорушення, за якими завжди стоять конкретні особи. Звісно ж, стигматизація та поширення неправдивої інформації так само можуть набувати ознак протиправних діянь, однак ці масові феномени, як правило, є не персоніфікованими, на відміну від протиправної поведінки, яка, повторимося, завжди є проявом "злої волі" конкретної особи.

Отже, першим блоком небезпек, здатних порушити права і свободи в інформаційному сегменті буття і тим самим створити стан небезпеки для людини, є недостовірна інформація, поширення якої сьогодні називають не інакше, ніж "мережева чума" [8].

В абз. 5 п. 15 постанови Пленуму Верховного Суду України (нині – Верховний Суд) "Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи" від 27.02.09 р. № 1 зазначається, що *недостовірною вважається інформація*, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені) [9].

Поряд із поняттям недостовірної інформації так само використовуються поняття дезінформування, дезінформації та фейків, або фейкових новин. Так, у ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення" від 01.01.98 р. у п. 7.5 дається *визначення дезінформування*, під яким розуміється спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації [10]. Що стосується інформаційних фейків (новин), то існує чимало їх визначень. Однак, уявляється, головне не в різноманітті визначень та пошуку універсального поняття, а в тому, якій сфері суспільних відносин подібна інформація може завдати шкоди.

На нашу думку, у кримінологічному сенсі під недостовірною інформацією, поширеною *в умовах запровадження карантинних заходів* під час епідемій та пандемій слід розуміти навмисне спотворення суспільно значимої інформації стосовно географії й темпів поширення хвороби, її клінічних проявів і наслідків, способів і методів лікування, вживаних державою та суспільством засобів убезпечення та інших питань, пов'язаних із подоланням хвороби та її наслідків, а так само вигадування інформації, що подається під виглядом достовірних відомостей і що може загрожувати інтересам національної безпеки в сфері публічного здоров'я. Подібна інформація дезорієнтує суспільство, змушує вдаватися до хибних кроків, сприяє виникненню масових панічних настроїв і безладу, ескалації соціальної напруги, підриває віру людини у власні сили та ін. Крім того, фейкові новини паразитують на страхах, стресі і нездорової цікавості людини, припустимо, до теорій глобальних змов, центральними темами яких є "відсів" зайвої людської маси, що не потрапила до "золотого мільярду", біологічні війни, коронакриза як аналог третьої світової війни, "революція" роботів і т. п.

Щоб розробити кримінологічну систему заходів нейтралізації негативного впливу недостовірної інформація на громадян під час запровадження у країні карантинних заходів, а відповідно й загальний рівень криміногенності у суспільстві, слід зупинитися на джерелах, з яких люди черпають відповідну інформацію. За результатами

зазначеного вище дослідження під назвою “Соціально-правові та кримінологічні наслідки пандемій та шляхи їх усунення в Україні”, з’ясовано, що найчастіше інформацію, припустимо, про поширення пандемії в Україні та за кордоном респонденти отримують по телебаченню, радіо, із друкованої преси (63,9 % від усіх опитаних). Ще 46,2 % респондентів користуються офіціальними каналами Всесвітньої організації охорони здоров’я (далі – ВООЗ), МОЗ України в соціальних мережах та месенджерах; 34,2 % звертаються до інформаційних порталів новин в Інтернеті. Офіційними сайтами МОЗ і Національної служби здоров’я України користуються 32,2 % респондентів. Для 21,6 % осіб головним джерелом інформації є знайомі, друзі, колеги. На інші джерела інформації вказали 1,93 % (офіційні сайти РНБО України, університету Дж. Хопкінса й інших установ; безпосередньо в медичних закладах, де працюють респонденти, або зі службових документів та ін.)[*] .

Частка перевірених інформаційних джерел є не такою вже й значною. А тому вирішення проблеми пандемії CoVID-19 поєднується із необхідністю адекватної рефлексії на будь-які випадки недостовірної інформації, фреймом для яких стає глобалізація сучасного соціуму. Такий тандем недостовірної інформації та пандемії, який отримав назву інфодемії, окрім іншого, відтепер має братися до уваги у розробці будь-якого сценарію розвитку економічних, політичних та кримінальних реалій як національного, так і планетарного масштабів. Зазначені явища у своїй сукупності виявилися свого роду невідомими змінними глобального характеру, що впливають, у тому числі, й на визначення вектору прогнозних розрахунків майбутнього кількісно-якісного стану злочинності (принаймні на найближчу перспективу) та розробку кримінологічних стратегій запобігання їй. Недаремно Генеральний директор ВООЗ Т.А. Гебрейэсус зазначив: “Ми не просто боремося з епідемією, ми боремося з інфодемією” [11].

У цьому плані цікаво навести досвід деяких країн.

Якщо звернутися до досвіду Китаю, то в цій країні з початку березня 2020 р. поширення дезінформації у соціальних мережах визнається кримінальним правопорушенням. Аналогічний закон існує в Індонезії та Саудівській Аравії. Встановлена кримінальна відповідальність за поширення “коронавірусної” дезінформації й у деяких країнах пострадянського простору – в Узбекистані, Молдові, РФ [12, с. 4].

Унаслідок відсутності у чинному законодавстві України відповідальності за систематичне умисне поширення недостовірної інформації (дезінформації, фейків) наразі й у нашій країні назріла така потреба.

Останніми роками у світі поширюється феномен соціальної стигматизації осіб, що захворіли на певні хвороби. Причому стигматизуються цілі соціальні групи, народи країн, що може призводити до актів дискримінації. Це зумовлюється виникненням нових вогнищ небезпечних хвороб та стрімкістю й масштабами їх розповсюдження на певних територіях. Коли хвороби вважаються смертельними, люди, які наражаються на великий ризик інфікування, подають свої страхи, звинувачуючи у нових спалахів хвороб когось або якусь групу людей [13]. За визначенням ВООЗ, *соціальна стигматизація в питаннях здоров’я* – це виникнення негативної асоціації певного захворювання з певною особою або групою осіб із спільними характеристиками, що під час спалаху захворювання може відбиватися у розповсюдженні упередженості, стереотипів, дискримінації та сегрегації щодо таких людей і/або в утраті ними свого статусу внаслідок передбачуваного у них зв’язку з хворобою [14]. Тому й невипадково, що

[*] *Прим. авт*. Сумарно кількість наданих відповідей перевищує 100 %, що пояснюється тим, що респонденти могли одночасно користуватися кількома джерелами інформації.

проблема соціальної стигматизації осіб, що захворіли на ті чи інші види психічних і фізичних недугів, є не лише предметом обговорення серед фахівців у галузі охорони здоров'я та інших наук про суспільство і людину, а й викликає необхідність ведення гострої соціальної полеміки у форматі "must know".

Фахівці роблять цікаве спостереження про те, що у наш час з'являється тривожна лексика, що нагадує про концтабір (іспанською): permiso para conducir ("перепустка"), permiso para circular ("дозвіл на пересування"), guetto ("гетто"), aislamiento ("ізоляція"), а так само виникають постапокаліптичні одиниці: nueva normalidad ("нова нормальність"), postpandemia ("постпандемія") [15, с. 1383]. Тому невипадково зазначається, що тема CoVID-19 знаходить нові грані як дослідницька проблема світового масштабу в соціокомунікативному і лінгвістичному аспектах [15, с. 1369]. ВООЗ наводить приклади бажаних і небажаних слів і словосполучень (виразів). Наприклад, стверджується, що бажано називати хворих "людьми з CoVID-19", "особами, які лікуються від CoVID-19", "одужують від CoVID-19" або "померли після зараження CoVID-19". У свою чергу, небажано називати хворих та людей, які можливо інфікувалися, "хворими на CoVID-19" або "жертвами коронавіруса", "підозрілими" або "підозрюваними на CoVID-19 пацієнтами". І зовсім неприпустимо говорити, що люди "поширюють CoVID-19", "заражають оточуючих" або "розносять вірус", оскільки під цим мається на увазі вина цих людей у навмисній передачі інфекції [14].

Що стосується сумного українського досвіду поширення стигматизації, то початок актів стигматизації мав місце наприкінці лютого 2020 р. у Нових Санжарах Полтавської області у вигляді протестів, причиною яких стало рішення Уряду розмістити у місцевому шпиталі Національної гвардії людей, евакуйованих із китайського міста Ухань, в якому на той час знаходився епіцентр хвороби [16]. Однак пройде небагато часу, і ця хвороба стане сприйматися як щось буденне, коли знаходження поряд з явно хворою людиною перестане викликати негативну реакцію із приводу недотримання останньою карантинних заходів. До речі, об'єктом стигматизації і дискримінації ставали й конкретні люди, які заразилися хворобою або стосовно яких є інформація, що вони можуть виявлятися безсимптомними носіями інфекції [17, с. 2716]. Сьогодні побічно свідчити про деяку стигматизацію осіб, які хворіли на CoVID-19, може й той факт, що 36,7 % українських громадян намагаються обмежувати контакти з такими особами. Разом із тим в Україні стигматизація осіб, хворих на коронавірусну хворобу, не досягає критичних масштабів, щоб поставало завдання вживання будь-яких невідкладних заходів. Однак із метою превенції вже сьогодні слід вживати відповідних заходів у правовій, інформаційній та морально-культурологічній площинах, що, по суті, є кримінологічним загальносоціальним запобіганням.

Нарешті, ще одним видом небезпеки, на яку може наразитися людина в інформаційному просторі під час здійснення карантинних заходів, є кримінально карані правопорушення. На думку фахівців, актуальність проблематики інформаційної безпеки зумовлена синергетичним ефектом, що головним чином визначається двома факторами, а саме: сплеском великої уваги до проблеми на рівні ЗМІ, що призвело до різкого зростання комп'ютерних вторгнень, заснованих на методах соціальної інженерії; карантинними заходами, які реалізують сучасні можливості віддаленої роботи, що змінило усталені режими безпечного і сталого функціонування систем в Інтернеті [5]. На додаток до цього, як правильно зазначається А.В. Калініною, у межах боротьби із загрозою для життя та здоров'я населення, якою є коронавірусна хвороба, влада багатьох держав запровадила жорсткі карантинні заходи, а отже, змінила звичний уклад життя соціальних груп [18, с. 40].

Під час запровадження карантинних заходів перебування людини в кіберпросторі призводить до збільшення ймовірності стати жертвою від низки правопорушень, фоном для яких стають саме умови соціальної ізоляції. На додаток до вже відомих загроз у кіберпросторі людина наражається на ризики, інформаційним лейтмотивом яких стає пандемія і все, що з нею пов'язано. Таким чином, загальним для цих злочинів моментом, що дозволяє виокремити та проаналізувати їх, є обстановка і засоби вчинення. Так, кіберзлочини вчиняються в обстановці реалізації карантинних заходів, що передбачають і соціальну ізоляцію, і присутність у буденному житті людини відповідних суб'єктів (лікарів, фармацевтів, працівників різних соціальних служб та ін.), "імітація" діяльності яких може ставати джерелом небезпеки для пересічного громадянина, і збільшення часу, проведеного людиною в кіберпросторі, який, власне, й стає основною загрозою правам і свободам людини, та ін. Крім того, засновуючись на положеннях розділу XVI Особливої частини КК України, можна визначити, що засобом вчинення кіберзлочинів є електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі і мережі електрозв'язку, тобто інформаційно-комунікаційні технології.

За свідченням Д.В. Дубова, ще у середині десятих років XXI ст. в Україні в повному обсязі були присутні всі ключові "класичні" кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо), кількість яких зростає щороку [19, с. 210]. Сьогодні в умовах реалізації карантинних заходів проблема кіберзлочинності лише загострилася. Експерти в галузі комунікаційно-інформаційних технологій виділяють три причини збільшення кількості кіберзлочинів. По-перше, саме карантин створив умови для хакерів-початківців, які з появою вільного часу активно "експериментують"; по-друге, злочинці використовують масову стурбованість людей темою захворювання на коронавірус, вдаючись до фішингу і так званої соціальної інженерії; по-третє, масовий перехід працівників на нові умови роботи в період карантину з віддаленим доступом до робочих комп'ютерних систем робить уразливою інформацію, яка створюється і передається інформаційно-комунікаційними засобами [20]. При цьому якихось принципово нових видів загроз не з'явилося, оскільки злочинцями використовуються ті самі методи доступу до "цікавої" інформації, як і раніше (інтернет-фішинг, СМС-фішинг, вішинг, скімінг, шимінг, шкідливі програми, спам, соціальна інженерія та ін.) або вчиняються інші протиправні діяння відповідної спрямованості (піратство у галузі інтелектуальної власності в Інтернеті, протиправний контент, мальваре, рефайлінг [21], голосові повідомлення, встановлення застосунків, спрямованих на стеження за людиною, та ін.). Єдине, що додалося нового, так це перенесення зловмисниками акцентів на те, в який спосіб "ефективніше" робити втручання, беручи до уваги перехід робітників на дистанційний режим роботи з використанням особистих комп'ютерних приладів. Наприклад, зафіксовані випадки, коли працівнику приходила розсилка нібито від служби IT-підтримки або відділу кадрів його компанії з інформацією про звільнення у зв'язку з необхідністю оптимізації штату у складних пандемічних умовах, і більш докладну інформацію про відповідне рішення пропонувалося дізнатися із прикріпленого до листа зараженого файлу або при переході за посиланням на сайт, який краде персональні дані (звісно ж, про загрози таких листів або посилань адресат не здогадувався). За такою схемою "працюють" й повідомлення, що надійшли нібито від страхової компанії із приводу закінчення терміну дії договору медичного страхування, податкових органів, благодійних некомерційних організацій, авіакомпаній, торговельних компаній щодо "суперпропозицій" і "суперакцій" тощо. У результаті збитків зазнавали як самі працівники, персональні дані яких потрапляли

третім особам, так і компанії, які наражалися на локальні і мережеві зараження [3]. За інформацією глави Національної поліції України, у 2020 р. у країні було зареєстровано понад 5 тис. кіберзлочинів, за вчинення яких вдалося оперативно затримати 106 осіб [22].

На наш погляд, масив кіберзлочинів у період реалізації карантинних заходів можна поділити на протиправні діяння, у "сценарії" вчинення яких ключовою є тема коронавірусу, та "традиційні" злочини, вчинення яких безпосередньо не зумовлюється коронавірусною тематикою, хоча їх кількість (у бік збільшення) корелює із загальною ситуацією у суспільстві. Це збільшення пояснюється, зокрема, тим, що до тих злочинців, які вже займалися Інтернет-шахрайством (фальшиві Інтернет-магазини, Інтернет-аукціони, "корисні" сайти різноманітних послуг, телекомунікаційні засоби зв'язку тощо), приєдналися нові віртуальні злочинці, які до періоду карантинних заходів займалися злочинною діяльністю в реальності, адже кіберпростір привернув увагу багатьох зловмисників тим, що в ньому злочинний дохід може виявлятися не меншим, ніж в реальному просторі, але при більш низькому рівні ризиків.

До першої групи нами віднесено продаж нелегального медичного обладнання і медичних препаратів за допомогою відповідних торговельних Інтернет-платформ; шахрайство з приводу придбання та продажу медичних засобів індивідуального захисту (захисних масок, масок-респіраторів, антисептичних засобів, ліків і т. п.), продуктів харчування, речей індивідуального вжитку, розповсюдження "високоефективних" ліків від коронавірусу або препаратів, які унеможливлюють зараження ним, пропозиції щодо дезінфекції приміщень, автомобілів, речей і т. п. від коронавірусу так само через мережу Інтернет [18, с. 41]; кібершахрайство, яке "засновується" на експлуатації відповідної тематики (наприклад, пропозиції надати грошову допомогу у зв'язку із поширенням CoVID-19 від держави, органів місцевого самоврядування, посадовців, банківських установ, приватного сектора та ін. [18, с. 41], здійснити перехід за посиланням на певні сайти, що нібито містять корисну інформацію про хворобу, або скачати додаток для ознайомлення з актуальною інформацією про епідеміологічний стан) і фактично є лише приводом для отримання доступу до кредитно-фінансової та іншої важливої для людини інформації з метою подальшого її використання; кібератаки на медичні установи та інші об'єкти критичної інфраструктури, діяльність яких пов'язана із протидією пандемії, тощо. Тому можна говорити про новий різновид кіберзлочинців (найчастіше шахраїв) – "пандемічних" кіберзлочинців. Так, ще у квітні 2020 р. повідомлялося, що кіберполіція з початку пандемії викрила низку підпільних ділків та вилучила понад тисячі несертифікованих тестів коронавірусу, понад 2,5 тисяч літрів підроблених антисептичних засобів, а також майже 35 тис. медичних масок та респіраторів [20]. До того ж, за даними ВООЗ, щодня створюється близько 2 тис. сайтів про коронавірус, чимало з яких, вочевидь, можуть бути вірусними (наприклад, зловмисники викрадають облікові дані, логіни та паролі за допомогою "карт поширення коронавірусу") [20].

Аналізуючи першу групу кіберзлочинів, кілька слів необхідно сказати про виклики та загрози у сфері охорони здоров'я. Сьогодні, на жаль, медичні установи, компанії розробників вакцин та гуманітарні організації входять до переліку об'єктів критичної інфраструктури, що найчастіше атакуються кіберзлочинцями. Причому йдеться не лише про "традиційні" фішингові атаки з метою розкрадання відомостей про персонал і пацієнтів, що знаходяться на лікуванні або самоізоляції, для подальшого продажу цих даних, а й про "експлуатацію" самої приналежності закладів з охорони здоров'я до тих установ, до яких пересічні громадяни апріорі мають довіру. Так, зловмисниками нібито від імені таких установ масово розсилаються бюлетені, новини, дайджести з інформацією

про ситуацію із поширенням хвороби в певному регіоні та заходи боротьби з нею. Насправді ж подібні відправлення є ні чим іншим, як листом з фішинговим посиланням чи вірусною програмою. Після того, як особа відкриє цей лист або перейде за посиланням, "сценарій" стає традиційним. Відносно новим об'єктом кібератак у частині можливого використання персональних даних у теперішній час є система телемедицини, що популярна на Заході під час домашнього лікування. До того ж останнім часом навіть ВООЗ стає об'єктом дедалі більшої кількості кібератак та кіберінцидентів. Наприклад, хакери намагалися викрасти логіни та паролі її співробітників, запустивши фішинговий сайт, що імітував внутрішню систему електронної пошти організації [20].

Інколи злочинці з корисливою метою вдаються до кібератак на інформаційні системи медичних закладів за допомогою комп'ютерного вірусу, що унеможливлює роботу всіх електронних ресурсів, в яких міститься, наприклад, інформація з медичних карт пацієнтів, призначення лікарських препаратів, проведення процедур тощо. І зовсім цинічними в умовах пандемії видаються випадки блокування злочинцями інформаційних систем медичних установ, що відповідають за коректну й безперебійну роботу високотехнологічного медичного обладнання – техніки, що підтримує життєдіяльність людського організму, забезпечує роботу томографів, апаратів штучної вентиляції легень, операційної апаратури тощо (так званий Інтернет речей). Це робиться зловмисниками так само з метою отримання коштів за розблокування програм, відповідальних за коректну роботу медичного обладнання. За свідченням О.С. Маркова, що засновується на частоті згадувань у мережі Інтернету про розглядувану проблему, сьогодні кібератаки на медичні заклади складають 4 % від усіх загроз у кіберпросторі, релевантних коронавірусу [5]. Отже, серед прав людини, що порушуються у такий своєрідний спосіб, насамперед йдеться про її право на життя та здоров'я, котрі у період розповсюдження коронавірусної інфекції стають, напевно, найістотнішими правами.

Що стосується групи "традиційних" злочинів, вчинення яких безпосередньо не корелює з коронавірусною тематикою, то в їх "бутті" спостерігаються свої закономірності, що існували ще до пандемії та будуть існувати й після її завершення.

Висновки.

Дослідження проблеми особливостей захисту прав, свобод і безпеки людини в інформаційному просторі в умовах карантинних заходів дозволяє зробити кілька висновків принципового характеру.

По-перше, трьома істотними видами загроз чисельним благам людини в інформаційному просторі під час пандемії CoVID-19 є: заповнення цього простору неправдивою інформацією, що набуває характеру інфодемії, множення випадків стигматизації певних суб'єктів та вчинення кримінально караних правопорушень. Тому кримінологічний аналіз саме цих видів загроз має покладатися у підґрунтя розробки напрямів протидії небезпечним викликам інформаційного простору.

По-друге, проблематика кримінологічних важелів інформаційного убезпечення прав і свобод людини стає надзвичайно актуальною в період запровадження режиму карантинних заходів. У ситуації надзвичайної активності зловмисників єдине, що залишається, – змінити загальну парадигму протидії кіберзагрозам із наступальної на оборонну, в якій пріоритет віддаватиметься саме захисту інформації та запобіганню можливим загрозам. А враховуючи те, що "світ вже не буде таким як раніше", слід максимально сконцентруватися на тому досвіді, який людство отримало в пандемічний період, поширивши його мейнстрими й на часи "постпандемії".

По-третє, якщо є надія, що сила впливу інфодемії та проявів стигматизації рано чи пізно ослабне, тощо стосується злочинних проявів, то це негативне явище, на жаль, "резистентне" до зміни векторів актуальності тих чи інших суспільних проблем.

Напевно, можна стверджувати, шо "виник" новий феномен – пандемічний злочинець, протиправна поведінка якого знаходить свій прояв насамперед в інформаційному просторі. Всі злочини пандемічного періоду доцільно поділити на ті, сутність вчинення яких зумовлена темою коронавірусу, та "традиційні" злочини, вчинення яких розвивається за власним "сценарієм", хоча загальна їх кількість й корелює із режимом карантину. При цьому особливу тривогу викликають кібератаки на об'єкти критичної інфраструктури, від коректної роботи яких залежить безпека громадян. Саме протидія таким проявам має стати стратегічним напрямом запобіжної діяльності під час реалізації у країні карантинних заходів.

Використана література

1. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. United Nations. A/HRC/17/27. URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_ en.pdf (дата звернення: 25.06.2021).

2. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти. Харків: Майдан, 2011. 244 с.

3. Ключевская Н. Информационная безопасность и CoVID-19: рекомендации для бизнеса и граждан. URL: https://www.garant.ru/article/1421147 (дата звернення: 28.06.2021).

4. Отт М. "Хіт-парад" вірусних новин. Як медіа писали про CoVID-19? https://voxukraine.org/virusni-novini (дата звернення: 30.06.2021).

5. Марков А. Информационная безопасность в условиях пандемии CoVID-19. URL:https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-CoVID-19 (дата звернення: 25.06.2021).

6. Коронавирус в мире: данные по странам и регионам. URL: https://www.bbc.com/russian/news-51706538 (дата звернення: 20.06.2021).

7. The Global Risks Report 2020. *World Economic Forum*. 15th Edition. Geneva: Marsh & McLennan and Zurich Insurance Group, 2020. 102 p.

8. Sherry Ricchiardi. Фактчекинг распространяется повсеместно благодаря этим ресурсам. https://ijnet.org/ru/story/фактчекинг-распространяется-повсеместно-благодаря-этим-ресурсам (дата звернення: 30.06.2021).

9. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України від 27.02.09 р. № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09 (дата звернення: 25.06.2021).

10. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97 від 01.01.98 р. URL: https://tzi.com.ua/478.html (дата звернення: 18.06.2021).

11. Дорошенко К. Світові інтелектуали про наслідки пандемії коронавірусу для людства. URL: https://suspilne.media/20654-svitovi-intelektuali-pro-naslidki-pandemii-koronavirusu-dla-ludstva (дата звернення: 25.06.2021).

12. Коваленко М., Беленькая М., Тарасенко П. Вакцина от фейков. Как мир борется с дезинформацией о пандемии. *Коммерсантъ.* 2020. № 57. С. 4. – (31 марта).

13. Michael McCauley, Sara Minsky, Kasisomayajula Viswanath. The H1N1 pandemic: media frames, stigmatization and coping. *BMC Public Health.* 2013. 13:1116. URL: http://www.biomedcentral.com/1471-2458/13/1116 (дата звернення: 22.06.2021).

14. Социальная стигматизация и CoVID-19 Руководство по предупреждению и преодолению стигматизации. URL: https://www.euro.who.int/__data/assets/ pdf_file/0007/432268/SocialStigmaAssociatedCoVID-19-rus.pdf (дата звернення: 29.06.2021).

15. Мустайоки А., Зорихина-Нильссон Н., Гусман Тирадо Р., Тоус-Ровироса А., Дергачева Д., Вепрева И., Ицкович Т. CoVID-19: катастрофа в языковом измерении разных стран. *Quaestio Rossica.* Vol. 8. 2020. No 4. P. 1369-1390.

16. Протесты в Новых Санжарах. URL: https://ru.wikipedia.org/wiki/Протесты_в_Новых_Санжарах (дата звернення: 30.06.2021).

17. Vladyslava S. Batyrgareieva, Oleh A. Zaiarnyi, Sabriie S. Shramko. Prevention of the stigmatization of individuals in response to digital tracking (concidering CoVID-19 issue). *Wiadomości Lekarskie*. 2020. Tom LXXIII nr 12 cz. II. P. 2715-2721.

18. Калініна А.В. Пандемія вірусу VS правопорядок: кримінологічний прогноз. *Питання боротьби зі злочинністю:* зб. наук. пр. / редкол.: Б.М. Головкін та ін. Харків: Право, 2020. Вип. 39. С. 39-45.

19. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

20. Стрій Є. Don’t click shit! Як вберегтися від кіберзлочинців у час пандемії. URL: https://investigator.org.ua/ua/publication/224967 (дата звернення: 25.06.2021).

21. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 28.06.2021).

22. У 2020 році Нацполіція викрила більше ніж 5000 кіберзлочинів. URL: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv (дата звернення: 16.06.2021).

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

УДК 343.985

КУЧИНСЬКА І.В., *кандидат фармацевтичних наук*, провідний науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України.
ORCID: http://orcid.org/0000-0002-0269-9463.

РОЛЬ ПРОФІЛЮВАННЯ НАРКОТИЧИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН ТА ПРЕКУРСОРІВ У ПРОТИДІЇ ЇХ НЕЗАКОННОМУ ОБІГУ

Анотація. *Зростання кількості підпільних лабораторій по виготовленню синтетичних наркотичних засобів, психотропних речовин та прекурсорів є однією з негативних тенденцій у світі. Після проведення синтезу забороненої речовини, кінцевий продукт містить домішки реагентів. Завдяки профілюванню цих домішок визначають шляхи синтезу речовини, походження прекурсорів, отримують інформацію про місцезнаходження виробництва, надаючи допомогу правоохоронним органам у боротьбі з незаконним виготовленням та обігом заборонених речовин. Результати досліджень та інформація щодо обставин конфіскації повинні фіксуватися у відповідних створених електронних базах даних для подальшого використання правоохоронними органами в оперативній та слідчій роботі, своєчасного виявлення та ліквідування підпільних нарколабораторій.*

Ключові слова: *підпільні лабораторії, синтетичні наркотичні засоби, психотропні речовини, прекурсори, заборонені речовини, домішки, профілювання, правоохоронні органи, бази даних.*

Summary. *Recently, there is a negative trend in the world – increasing number of synthetic drugs, psychotropic substances and precursors in the illicit trafficking of these substances. Specially equipped underground laboratories for their drug production are being set up to meet the demand for synthetic drugs. Synthetic drugs and psychotropic substances produced in underground laboratories can be synthesized in various ways. Various precursors and reagents are used for their synthesis, which leads to the appearance of impurities in the final product. Impurities help to determine the ways of synthesis of the illegal substance, the origin of the precursors, provide information about the location of production. Due to the presence of impurities, the connections between the removed substances are revealed. Specific impurities are used to determine the route of production, which, combined with other forms of investigation, will help to link different batches of a prohibited substance to the specific person who manufactured them. Impurities associated with the synthesis of substances seized in illegal laboratories are so-called marker compounds. They are a kind of marks that guide the expert chemist on the specific method used by criminals to obtain the substance. Marker compounds are of the greatest importance for the accurate establishment of the synthesis method. Marker compounds are determined by impurity profiling of samples of the prohibited substance. The main purpose of the profiling of impurities is to assist law enforcement agencies in combating the illicit manufacture and circulation of controlled substances. The results of research and information on the circumstances of the confiscation should be recorded in the relevant created electronic databases. In the profile database, two samples of a substance with a similar chemical profile can be linked together from the manufacturing stage to the distribution stage. Data on impurity profiles and fillers can be used to estimate the batch size, time and area of drug distribution. Databases are needed for use by law enforcement agencies in operational and investigative work. Databases are needed for the timely detection and liquidation of underground drug laboratories. The above aspects emphasize the importance of cooperation between investigative, operational services and forensic agencies in the process of effective detection and cessation of crimes related to the distribution of controlled substances.*

Keywords: *underground laboratories, synthetic drugs, psychotropic substances, precursors, banned substances, impurities, profiling, law enforcement agencies, databases.*

Аннотация. *Рост количества подпольных лабораторий по изготовлению синтетических наркотических средств, психотропных веществ и прекурсоров является одной из негативных тенденций в мире. После проведения синтеза запрещенного вещества, конечный продукт содержит примеси реагентов. Благодаря профилированию этих примесей определяют пути синтеза вещества, происхождение прекурсоров, получают информацию о местонахождении производства, оказывая помощь правоохранительным органам в борьбе с незаконным изготовлением и оборотом запрещенных веществ. Результаты исследований и информации об обстоятельствах конфискации должны фиксироваться в соответствующих созданных электронных базах данных для дальнейшего использования правоохранительными органами в оперативной и следственной работе, своевременного выявления и ликвидации подпольных лабораторий.*

Ключевые слова: *подпольные лаборатории, синтетические наркотические средства, психотропные вещества, прекурсоры, запрещенные вещества, примеси, профилирования, правоохранительные органы, базы данных.*

Постановка проблеми. Протягом останніх років однією з негативних тенденцій у світі є зростання частки синтетичних наркотичних засобів, психотропних речовин та прекурсорів у незаконному їх обігу. Протидія незаконному обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів є пріоритетним завданням діяльності правоохоронних органів.

Існує безліч можливих стратегій боротьби проти мереж незаконного обігу підконтрольних речовин на всіх етапах процесу – від їх виробництва до поширення та споживання з акцентом на превентивні або примусові заходи. Для правоохоронних органів це означає вибір найбільш ефективних оперативних методів та стратегій з урахуванням наявних ресурсів.

Основними цілями розслідувань злочинів, пов'язаних з незаконним оборотом наркотиків, є виявлення осіб, які виступають в якості ключових координаторів злочинної діяльності, забезпечення підтримки для майбутніх розслідувань та зусиль щодо запобігання.

Для обслуговування зростаючого попиту на синтетичні підконтрольні речовини, створюються спеціально обладнані підпільні лабораторії по їх виготовленню. Вказані тенденції характерні як для України, так і для більшості країн Європейського Союзу, США, країн Азії. Суспільна небезпека нарколабораторій полягає в масовому виробництві заборонених речовин.

Експерти Міжнародного комітету з контролю за наркотиками ООН зазначають, що підпільна нарколабораторія – це хімфабрика в мініатюрі. У таких лабораторіях можуть використовувати як високотехнологічне устаткування (спеціальні нагрівальні прилади, конденсаційні трубки, колби для реакцій, різний лабораторний посуд тощо), так і звичайний кухонний посуд. Крім того, у комплект лабораторного устаткування входять також прекурсори та різні реагенти, які використовують під час виготовлення наркотиків і психотропів. Ці лабораторії, на думку експертів, можуть бути розташовані в будь-якому місці: в ізольованих фермерських господарствах, міських житлових будинках і приміщеннях комерційних підприємств, у гірських районах. Устаткування підпільних лабораторій може бути різним: як примітивним, так і найсучаснішим. Працювати в них можуть фахівці різного рівня – від висококваліфікованих біохіміків до непрофесійних заповзятливих людей [1].

Динаміка зростання підпільних нарколабораторій обумовлена наступними факторами:

- виробництво та виготовлення синтетичних заборонених речовин відрізняється відносною простотою, не вимагає великих людських та (або) природних ресурсів, не потребує дорогого обладнання та особливих кліматичних умов (як, наприклад, у випадках з коноплею, опійним маком, кокаїновим кущем або з псилоцибін-вмісними грибами);

- докладний опис процесу виготовлення синтетичних наркотиків, а також інформація з пропозиціями щодо придбання необхідних прекурсорів та лабораторного обладнання знаходяться у відкритому доступі в мережі Інтернет;

- виробництво та виготовлення синтетичних підконтрольних речовин може бути налагоджено практично в будь-якому відносно компактному місці, при цьому висока щільність забудови обумовлює можливість маскування місцезнаходження підпільних лабораторій в приватних будинках великих густонаселених дачних селищ (садових товариств), а також в інших важкодоступних і прихованих від правоохоронних органів місцях (гаражних комплексах, складських приміщеннях);

- кінцевий продукт має низьку собівартість та високу прибутковість на ринку у зв'язку з постійним попитом та можливістю швидкої реалізації;

- наявність спеціалізованих Інтернет-магазинів, які торгують хімічними реактивами, прекурсорами, спеціальним лабораторним обладнанням;

- щоб обійти вплив заходів контролю, підпільні виробники переходять на предпрекурсори, які самі по собі не підпадають під дію заходів контролю та можуть бути легко перетворені в продукт.

Саме тому своєчасне виявлення та ліквідування підпільних нарколабораторій є одним із пріоритетних напрямків роботи правоохоронних органів щодо боротьби зі злочинністю у цілому.

Результати аналізу наукових публікацій. Проблемні питання кримінально-правової та кримінологічної протидії організації або утриманню місць для незаконного вживання, виробництва чи виготовлення наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів досліджували Ю.В. Баулін, В.І. Борисов, Л.В. Дорош, А.А. Музика, О.М. Стрільців, М.С. Хруппа [2 – 5].

Виявлення та ліквідація підпільних нарколабораторій працівниками оперативних підрозділів відображено в публікаціях А.М. Кислого, М.О. Сергатого, О.М. Стрільціва [4; 6; 7].

Питання, які ставляться слідчими органами на вирішення експерту під час проведення судово-хімічної експертизи вилучених речовин та обладнання підпільних нарколабораторій сформульовані О.П. Замощем [8].

Особливості експертизи обладнання для незаконного виготовлення наркотичних засобів, психотропних речовин та їх аналогів стало предметом досліджень В.В. Бондаренка, З.С. Галавана, В.О. Шаповалової, В.В. Шаповалова [9].

Питанням використання можливостей комплексу судово-хімічних експертиз по дослідженню наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів для проведення якісного експертного супроводження матеріалів кримінального провадження, об'єктами якого є лабораторії по нелегальному виготовленню наркотичних засобів, психотропних речовин чи прекурсорів, присвячені роботи В.В. Пасічника, М.С. Хруппи, В.М. Жмінька, О.Г. Дячука, О.П. Замощя, Р.М. Павленка, О.М. Стрільціва, С.В. Шкурдоди, О.О. Посільського [10; 11].

В свою чергу K. Andersson, K. Jalava, E. Lock, Y. Finnon, H. Huizer, E. Kaa, A. Lopes, A. Poort-man-van der Meer, M.D. Cole, J. Dahlen, E. Sippola звертають увагу, що вивчення домішок набуває все більшого значення, оскільки воно необхідне для визначення

можливих шляхів виробництва та ілюстрування зв'язків між окремими вилученнями [12]. Дослідження основних методів синтезу наркотичних засобів, психотропних речовин та визначення ключових домішок проводили Kunalan, N.N. Daeid, W.J. Kerr, H.A.S. Buchanan, A.R. McPherson [13 – 14].

В.В. Вартузов, С.А. Бабичев, В.І. Литвиненко запропонували аналітичну модель системи профілювання наркотичних речовин з метою оцінки імовірності шляху транзиту наркотиків і місця їх виготовлення, показали реалізацію запропонованої моделі на прикладі трьох лабораторій, шести дилерів, які постачають товар до місця призначення та чотирьох компонент наркотичної речовини, які додають дилери в процесі транспортування товару [15].

Про можливість використання профілювання амфетаміну для кращого розуміння структури ринку та реалізації середньострокових та довгостротрокових стратегій розслідування наголошували у своїх працях L. Aalberg, K. Andersson, C. Bertler, H. Borén, M.D. Cole, J. Dahlén, Y. Finnon, H. Huizer, K. Jalava, E. Kaa, E. Lock, A. Lopes, A. Poortman-van der Meer, E. Sippola [16].

На необхідності створення баз даних, що полегшить моніторинг ринку прекурсорів, ідентифікацію джерел прекурсорів заборонених речовин та встановлення зв'язків між кримінальними, справами керуючись походженням прекурсору наголошували W. Krawczyk, T. Kunda, I. Perkowska, D. Dudek [17].

Метою статті є оцінка досвіду профілювання наркотичних засобів, психотропних речовин, прекурсорів в європейських країнах та створення вітчизняних баз даних для своєчасного виявлення та ліквідування підпільних нарколабораторій.

Виклад основного матеріалу. Вироблені в підпільних лабораторіях синтетичні наркотичні засоби та психотропні речовини можуть бути синтезовані кількома шляхами з використанням, відповідно, різних прекурсорів та реагентів, що призводить до появи у кінцевому продукті домішок, залежно від ступеня чистоти вихідних речовин, шляху синтезу, умов проведення реакції, навичок підпільного хіміка. Кількість домішок та їх наявність істотно залежать від ступеню очищення кінцевого продукту.

Факт наявності цих домішок та співвідношення між ними можна використовувати для порівняння зразків забороненої речовини та розрізнення цих зразків, оскільки речовина, вироблена в межах однієї партії, майже напевно матиме однакові домішки та їх кількості. Зразки заборонених речовин, вироблені в різний час тією ж незаконною лабораторією, можуть виявляти схожість, тоді як зразки з непов'язаних лабораторій мають великі якісні та кількісні відмінності.

Домішки можуть полегшити визначення шляхів синтезу забороненої речовини, походження прекурсорів, а також надати інформацію про місцезнаходження виробництва. Виявлені специфічні для шляху синтезу домішки можуть бути використані для визначення маршруту виробництва, який у сукупності з іншими формами розслідування, допоможе пов'язати окремі партії підконтрольної речовини з конкретною людиною, що їх виготовляла.

Домішки, пов'язані з синтезом вилучених у нелегальних лабораторіях речовин, являються так званими маркерними сполуками, вони є своєрідними відмітками, що орієнтують експерта-хіміка на конкретний використаний злочинцями метод отримання речовини. Маркерні сполуки мають найбільше значення для точного встановлення методу синтезу.

Маркерні сполуки визначають шляхом проведення профілювання зразків домішок забороненої речовини.

Основною метою методу профілювання домішок є надання допомоги правоохоронним органам у боротьбі з незаконним виготовленням та обігом підконтрольних речовин. Визначення методу синтезу дає змогу правоохоронним органам на місцях зосередити розслідування на конкретних хімічних речовинах, у той час як встановлення зв'язків між окремими зразками заборонених речовин полегшує моніторинг незаконного обігу, встановлення джерел та маршрутів його переміщення [18]. Так, подібність або відмінності між вилученими зразками заборонених речовин можуть надати докази про зв'язки між постачальниками та споживачами, а інформація щодо методів синтезу цих речовин буде корисною для пошуку підпільних лабораторій шляхом моніторингу торгівлі прекурсорами та ключовими речовинами [19 – 20].

Щоб запропонувати можливий шлях синтезу, профілювання фокусується на ідентифікації домішок, а не на їх кількісному визначенні, оскільки для цього достатнім є лише виявлення та ідентифікація цільових домішок.

Більшість незаконно синтезованих речовин найчастіше знаходиться в обігу у вигляді порошку, що дає змогу на будь-якому етапі розповсюдження додавати до нього наповнювачі з метою збільшення обсягу кінцевого продукту та, відповідно, доходу. В якості наповнювача використовують креатин, ефедрин, саліциламід, парацетамол, феназон, цукор [12]. Таким чином, профіль наповнювачів може змінюватись на кожній ланці ланцюжка, що веде від виробника до дилера через оптовика. Такі фактори та варіації домішок можуть виявитися корисними для отримання цінної довідкової інформації криміналістами відносно вилучених зразків забороненої речовини та, можливо, їх походження. Чистота забороненої речовини у партії та комбінація наповнювачів надають інформацію, що дає змогу висувати гіпотези відносно стадії незаконного обігу, до якої належить вилучення.

Вбачається, що велика кількість окремих вилучень підконтрольних речовин у дилерів дають змогу збирати дані, які можуть стати корисною основою для розслідування – допоможуть спрямовувати подальшу оперативну роботу та призведуть до виявлення підпільних лабораторій по виготовленню цих речовин. З досвіду деяких європейських країн [17; 21] відомо, що створення електронних баз даних на основі таких окремих вилучень полегшили як моніторинг ринку підконтрольних речовин в цих країнах, так і встановлення джерел та зв'язків між зразками, що зберігаються у базах даних, і кримінальними справами на основі походження цих речовин з метою виявлення несподіваних зв'язків. Такі бази даних можуть включати профілі домішок підконтрольної речовини, результати досліджень (чистота, наповнювачі, цільові домішки), відповідні ідентифікаційні номери випадків, місце та дату вилучення, обставини справи, об'єм вилучення та інформацію щодо схожості зі зразками, які досліджувалися раніше, детальні дані про конфіскацію (імена, телефони, адреси причетних осіб).

У базі даних профілів два зразка речовини з аналогічним хімічним профілем можуть бути пов'язані між собою від стадії виготовлення до стадії розподілу.

В ході розслідування мереж поширення заборонених речовин слідчі здобувають велику кількість опосередкованої інформації. На основі цих даних вони роблять висновки та визначають зв'язки, які можуть існувати між різними людьми, що діють в мережі поширення наркотиків. Зв'язки, що виявлені із використанням традиційних методів розслідування також можуть бути підтверджені і на основі даних профілювання. У свою чергу, дані профілювання можуть бути використані для виявлення раніше невиявлених слідством зв'язків. Зворотній шлях підтвердження також має місце – дані традиційних методів розслідування можуть пов'язати два зразки, що відрізняються за профілем домішки.

Таким чином, два джерела інформації доповнюють один одного при побудові уявлення про мережу та її функціонування. Взаємодія свідчень розслідування та профілювання наркотиків дає змогу підтримувати базу даних та висновки, які можуть бути зроблені з неї в актуальному стані.

Встановлення зв'язків також допоможе ініціювати нові розслідування або визначити пріоритети дій та можуть виявити асоціації, які не виявляються за допомогою традиційних методів розслідування через численні спроби приховування інформації.

Дані щодо профілю домішки, включаючи наповнювачі, можна використовувати для оцінки її загального розміру, часу та території поширення партії.

Висновки.

Таким чином, профілювання дозволяє визначати шлях синтезу, ідентифікувати зразки та джерела походження наркотичних засобів, психотропних речовин та прекурсорів.

Результати досліджень та відомості щодо обставин конфіскації повинні фіксуватися у відповідних створених базах даних для подальшого використання правоохоронними органами в оперативній та слідчій роботі.

З метою максимізації ефективності зусиль з контролю за ринком заборонених речовин, правоохоронними органами має бути налагоджений обмін криміналістичними даними на місцевому, регіональному та міжнародному рівнях, що вимагає швидкого збору та обміну даними, які можна легко порівняти створюючи та використовуючи бази даних профілів домішки.

В такому випадку слідчі будуть мати в своєму розпорядженні відомості, що визначають всі епізоди, хімічно пов'язані зі злочином. Це дозволить вивчати зв'язки між різними джерелами інформації та формулювати гіпотези про структуру мереж торгівлі наркотичними засобами, психотропними речовинами, прекурсорами.

Розглянуті вище аспекти підкреслюють важливість взаємодії слідчих та оперативних служб із судово-експертними установами в процесі ефективного виявлення та припинення злочинів, пов'язаних із розповсюдженням підконтрольних речовин.

Зв'язки, встановлені за допомогою профілювання, в поєднанні з традиційною інформацією, можна буде використовувати для кращого розуміння структури ринку та реалізації стратегій розслідування.

Використана література

1. Подготовка кадров в области обеспечения законов о наркотиках: руководящие принципы для работников правоохранительных органов: Руководство ООН від 1990 р. 42 с.

2. Бауліна Ю.В., Дорош Л.В. Організований наркобізнес (поняття, форми, підстави кримінальної відповідальності). Харків, 2005. 256 с.

3. Музика А.А. Покарання за незаконний обіг наркотичних засобів: монографія. Хмельницький, 2010. 224 с.

4. Савченко А.В. Кримінально-правова протидія незаконному обігу наркотиків: міжнародні та національні стандарти: посібник. Київ, 2014. 146 с.

5. Хруппа М.С., Никифорчук Д.И., Семенюк В.А. Діяльність підрозділів по боротьбі з незаконним обігом наркотиків з виявлення та ліквідації підпільних нарколабораторій: посібник. Київ, 2004. С. 7.

6. Кислий А.М. Оперативно-розшукові заходи щодо припинення діяльності підпільних нарколабораторій. *Науковий вісник Київського національного університету внутрішніх справ*. 2009. № 5 (66). С. 152-157.

7. Сергатий М.О. Подолання ухилення від відповідальності учасників організованих злочинних груп, що займаються незаконним обігом наркотиків. *Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія "Юридичні науки"*. 2012. № 2 (3). С. 75-81.

8. Шаповалова В.О., Замошець О.П., Шаповалов В.В., Бондаренко В.В. Нелегальні нарколабораторії та роль спеціалістів із судової хіміко-фармацевтичної експертизи при розслідуванні справ даної категорії. *Ліки України*. 2005. № 9. С. 138-141.

9. Шаповалова В.О., Замошець О.П., Галаван З.С., Шаповалов В.В. Предмет, об'єкти та завдання судової хіміко-фармацевтичної експертизи наркотичних засобів, психотропних речовин і прекурсорів. *Фармацевтичний журнал*. 2006. № 1. С. 48-52.

10. Пасічник Г.В., Хруппа М.С., Жмінько В.М., Дячук О.Г., Замошець О.П., Павленко Р.М., Стрільців О.М. Виявлення та ліквідація підпільних лабораторій по виготовленню наркотичних засобів та психотропних речовин: методичні рекомендації. Київ, 2000. 24 с.

11. Пасічник В.В., Шкурдода С.В., Посільський О.О. Про практику використання можливостей комплексу хімічних експертиз по дослідженню наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів. *Криминалистика и судебная экспертиза*. 2015. № 60. С. 349-357.

12. K. Andersson, K. Jalava, E. Lock, Y. Finnon, H. Huizer, E. Kaa, A. Lopes, A. Poort-man-van der Meer, M.D. Cole, J. Dahlen, E. Sippola Development of a harmonised method for the profiling of amphetamines III. Development of the gas chromatographic method. *Forensic Science International*. 2007. № 169. P. 50-63.

13. V. Kunalan, N.N. Daeid, W.J. Kerr, H.A.S. Buchanan, A.R. McPherson, Characterization of route specific impurities found in methamphetamine synthesised by the Leuckart and reductive amination methods. *Journal of Analytical Chemistry*. 2009. № 81. P. 7342-7348.

14. UNODC, Recommended Methods for the Identification and Analysis of Amphetamine, Methamphetamine and their Ring-substituted Analogues in Seized Materials, United Nations, New York, 2006.

15. В. Вартузов, С. Бабічев, В. Литвиненко, А. Фефелов Модель аналітичної системи профілювання наркотичних речовин на основі мережі Байеса. *Вісник Національного університету "Львівська політехніка"*. 2012. № 744. С. 114-119.

16. L. Aalberg, K. Andersson, C. Bertler, H. Borén, M.D. Cole, J. Dahlén, Y. Finnon, H. Huizer, K. Jalava, E. Kaa, E. Lock, A. Lopes, A. Poortman-van der Meer, E. Sippola Development of a harmonised method for the profiling of amphetamines: I. Synthesis of standards and compilation of analytical data. *Forensic Science International*. 2005. № 2-3 (149). P. 219-229.

17. W. Krawczyk, T. Kunda, I. Perkowska, D. Dudek Impurity profiling/comparative analyses of samples of 1-phenyl-2-propanone. *Bulletin on Narcotics*. 2005. № 1-2 (LVII). P 33-62.

18. United Nations Office for Drug Control and Crime Prevention (Scientific Section), Drug Characterization/Impurity Profiling: Background and Concepts. 2001 (United Nations publication, Sales № E.01.XI.10).

19. Allan A., Ely R. In Crime Scene, Northwestern Association of Forensic Scientist (NWAFS). 2011. № 37. P. 15-25.

20. Stojanovska N., Fu S., Tahtouh M., Kelly T., Beavis A., Kirkbride K.P. A review of impurity profiling and synthetic route of manufacture of methylamphetamine, 3, 4-methylenedioxymet hylamphetamine, amphetamine, dimethylamphetamine and p-methoxyamphetamine. *Forensic Science International*. 2013. № 1 – 3 (224). P. 8-26.

21. S. Ioset, P. Esseiva, O. Ribaux, C. Weyermann, F. Anglada, S. Lociciro, P. Hayoz, I. Baer, L. Gasté, A.-L. Terrettaz-Zufferey, C. Delaporte, P. Margot Establishment of an operational system for drug profiling: a Swiss experience. *Bulletin on Narcotics*. 2005. № 1 – 2 (LVII). P 121-147.

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

УДК 355.402

СКУЛИШ Є.Д., *доктор юридичних наук, професор*, керівник Наукового центру національної безпеки і права ДНУ ІБП НАПрН України.
БАЛІЦЬКИЙ В.В., *кандидат юридичних наук, доцент*, професор СК-12 Академії зовнішньої розвідки України.

ЗАГРОЗИ ТЕРОРИСТИЧНОГО ХАРАКТЕРУ ЗАКОРДОННИМ ДИПЛОМАТИЧНИМ УСТАНОВАМ УКРАЇНИ

Анотація. *У статті здійснено аналіз конкретних терористичних загроз дипломатичним місіям України за кордоном, їх співробітникам і членам сімей, а також відрядженим за кордон українським громадянам, які обізнані у відомостях, що становлять державну таємницю. В ній відпрацьовані конкретні рекомендації щодо дій в екстремальних ситуаціях під час терористичних акцій в оточенні закордонних дипломатичних установ, зокрема, при блокуванні представництв терористами чи захопленні їх приміщень злочинцями, а також утримуванні дипломатичних співробітників як заручників.*

Ключові слова: *оперативна обстановка в країні перебування, терористичні загрози, стан екстремальної ситуації, безпека ЗДУ, безпека дипломатичного персоналу.*

Summary. *The article presents an analysis of specific terrorist threats to diplomatic missions of Ukraine abroad, their employees and families, as well as citizens of Ukraine, who are on their official missions abroad, who are informed about state secrets. It developed specific recommendations for actions in dangerous situations in the case of terrorist attacks in the area of DMU's location, especially, when the terrorist act is followed by blocking the mission, taking the stuff members for hostages.*

Keywords: *operational situation in the host country, terrorist threats, extreme situations, security of the diplomatic missions abroad, security of diplomatic missions' staff.*

Аннотация. *В статье осуществлен анализ конкретных террористических угроз дипломатическим миссиям Украины за границей, их сотрудникам и членам семей, а также откомандированным за границу украинским гражданам, осведомленных в сведениях, которые представляют государственную тайну. В ней отработаны конкретные рекомендации относительно действий в экстремальных ситуациях во время террористических акций в окружении заграничных дипломатических учреждений, в частности, при блокировании представительств террористами или захвате их помещений преступниками, а также содержании дипломатических сотрудников как заложников.*

Ключевые слова: *оперативная обстановка в стране пребывания, террористические угрозы, состояние экстремальной ситуации, безопасность ЗДУ, безопасность дипломатического персонала.*

Постановка проблеми. Негативні тенденції сучасного світового розвитку такі як: прояви міжнародного тероризму, організованої злочинності, контрабанди наркотиків і зброї, нелегальної міграції й торгівлі людьми; зростання екологічних і природних катастроф, загроз епідемій та пандемії; збереження ескалації заморожених конфліктів і поява нових джерел напруженості, виникнення кризових ситуацій, зокрема, активізація внаслідок подій на сході України терористичної та розвідувально-підривної діяльності спецслужб РФ, покладають на СЗР України та інші спеціальні державні органи завдання належним чином забезпечувати безпеку закордонних дипломатичних установ України (далі – ЗДУ), їх співробітників і членів сімей, а також відряджених за кордон українських громадян, обізнаних у відомостях, що становлять державну таємницю.

Саме комплексний характер вирішення проблем забезпечення безпеки ЗДУ, зокрема, під час терористичних акцій у країні акредитації, диктує необхідність їх глибокого наукового опрацювання. Результати такого роду роботи можуть стати підґрунтям для подальшого вдосконалення державних нормативно-правових актів, відомчих розпорядчих документів й інструкцій, а також практичних рекомендацій, якими безпосередньо керуватимуться співробітники та керівництво ЗДУ під час виконання своїх посадових обов'язків за кордоном.

Результати аналізу наукових публікацій. Дослідженню зазначеної проблематики останнім часом приділено належну увагу іноземними й українськими науковцями, зокрема, Крутовим В.В., Скулишем Є.Д., Владленовою І.В., Канцір В.С. та ін.

Теоретичною базою для цього наукового аналітичного дослідження стали законодавчі та відомчі нормативно-правові акти, наукові праці вітчизняних та зарубіжних авторів, що стосуються питань забезпечення безпеки відряджених за кордон українських громадян від терористичних загроз у країні перебування, і першочергово, забезпечення безпеки ЗДУ та їх співробітників, а також конкретні положення підзаконних нормативно-правових актів. Зокрема, це "Положення про безпеку закордонних дипломатичних установ України", затверджене Указом Президента України від 31.07.06 р.; Постанова КМУ від 24.03.04 р. "Про затвердження Порядку класифікації надзвичайних ситуацій техногенного та природного характеру за їх рівнями"; "Інструкція про порядок реагування системи органів дипломатичної служби на загрозу вчинення терористичного акту"; "Праксеологія у сфері комплексного забезпечення безпеки дипломатичних представництв, консульських та інших державних установ України за кордоном"; "Рекомендації щодо поведінки на випадок захоплення злочинцями" тощо.

Метою статті є пошук ефективних шляхів організації забезпечення безпеки ЗДУ України та їх персоналу від терористичних загроз у країнах акредитації та покращення чинного нормативно-правового регулювання.

Досягненню поставленої мети сприяло виконання конкретних завдань:

- проаналізувати існуючі підходи до визначення терористичних загроз ЗДУ у країнах акредитації згідно законодавства України;
- визначити роль керівництва ЗДУ й офіцера безпеки (далі – ОБ) у забезпеченні безпеки дипперсоналу під час терористичних акцій у країнах акредитації;
- узагальнити конкретні практичні висновки і рекомендації.

Виклад основного матеріалу. Кожна терористична загроза, що виникає в іноземній країні акредитованим закордонним дипломатичним установам України, разом з іншими негативними проявами, характеризується зростанням рівня радикального налаштування терористичних елементів, їх груп чи організацій. Закономірне наростання суперечностей у суспільстві під час загострення внутрішньополітичної ситуації в країні перебування ЗДУ породжує підстави й формує передумови для активізації діяльності екстремістськи налаштованих осіб та їх угруповань, які можуть, зокрема, вдаватися і до терористичних акцій як методу досягнення політичних чи інших амбітних цілей.

Чинний Закон України "Про боротьбу з тероризмом" дає наступні визначення основних понять терористичної діяльності [1]:

під терористичною діяльністю розуміється суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не повинних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей;

терористична група – група з двох і більше осіб, які об'єдналися з метою здійснення терористичних актів;

терористична організація – стійке об`єднання трьох і більше осіб, яке створене з метою здійснення терористичної діяльності, у межах якого здійснено розподіл функцій, встановлено певні правила поведінки, обов'язкові для цих осіб під час підготовки і вчинення терористичних актів. Організація визнається терористичною, якщо хоч один з її структурних підрозділів здійснює терористичну діяльність з відома хоча б одного з керівників (керівних органів) усієї організації;

міжнародний тероризм – здійснювані у світовому чи регіональному масштабі терористичними організаціями, угрупованнями, у тому числі за підтримки державних органів окремих держав, з метою досягнення певних цілей суспільно небезпечні насильницькі діяння, пов'язані з викраденням, захопленням, вбивством ні в чому не повинних людей чи загрозою їх життю і здоров'ю, зруйнуванням чи загрозою зруйнування особливо важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження;

заручник – фізична особа, яка захоплена і (або) утримується з метою спонукання державного органу, підприємства, установи чи організації або окремих осіб здійснити якусь дію чи утриматися від її здійснення як умови звільнення особи, що захоплена і (або) утримується.

Загострення оперативної обстановки в країні акредитації ЗДУ внаслідок політичних, соціальних, національних, етнічних, релігійних або інших причин виникнення напруженості часто призводить до вчинення масових безладів, погромів, активізації терористичних проявів, здійснення нападів на державні та інші офіційні установи, зокрема, й іноземні дипломатичні представництва, аж до їх можливого захоплення. Водночас, при цьому підвищується ймовірність нецивілізованих демаршів з боку місцевого населення, спрямованих безпосередньо проти конкретних іноземних дипломатичних місій та їх персоналу, зокрема, й України [4].

Тому серед об'єктів, на які може бути спрямована активність з боку терористичних й інших екстремістських організацій у країні акредитації, ймовірно перебувають і дипломатичні установи України, їх персонал та члени сімей, а також відряджені за кордон українські громадяни – володільці державної таємниці, особливо, в країні гібридної агресії Росії.

Головними завданнями, які першочергово слід вирішувати керівництву ЗДУ з метою забезпечення їхньої безпеки в екстремальних умовах, є [3]:

- запобігання можливих жертв серед співробітників дипломатичного представництва, членів їхніх сімей та інших відряджених до країни перебування громадян України, нанесення шкоди їхньому життю чи здоров'ю;
- недопущення захоплення злочинцями таємних документів, техніки та конфіденційних службових матеріалів, забезпечення їх надійного укриття або знищення;
- збереження будівель і приміщень дипломатичних представництв, їх майна та іншої державної власності України в країні перебування.

З метою належного виконання вказаних завдань від ОБ та всього особового складу ЗДУ вимагається психологічна витримка і, що дуже важливо, чіткі, рішучі й разом з тим обачливі дії. Очевидно, що це є можливим лише за умови вмілого управління персоналом і належної практичної підготовки особового складу ЗДУ, за що безпосередньо відповідають керівник дипломатичної установи й ОБ.

Під час виникнення реальної загрози терористичного нападу на ЗДУ першочерговими завданнями її керівництва є інформування відповідних державних органів України. Зокрема, Посол або особа, яка виконує його обов'язки та ОБ повідомляють у Міністерство закордонних справ і СЗР України про ситуацію, яка виникла в країні перебування та навколо дипломатичного представництва й просять відповідних розпоряджень та рекомендацій [4].

Не менш важливим є своєчасне інформування органів місцевої влади про терористичну загрозу, що виникає в оточенні ЗДУ органи місцевої влади. Посол або особа, яка його заміщає, інформує Міністерство закордонних справ країни перебування, ОБ ж – керівництво зовнішньої охорони, а черговий дипломат – місцеві правоохоронні органи про виникнення екстремальної ситуації навколо дипломатичного представництва, вірогідність реального нападу на нього терористів і вирішують питання про посилення зовнішньої охорони ЗДУ, вжиття інших заходів з протидії терористичній загрозі представництву і його персоналу.

Одним із першочергових оперативно-організаційних кроків у ЗДУ повинен стати перехід дипломатичної установи, її співробітників та членів сімей на особливий режим роботи та перебування в країні акредитації. Такий перехід здійснюється за відповідним розпорядженням Посла або особи, яка виконує його обов'язки та з відома ОБ.

Особливий режим роботи в ЗДУ передбачає [2]:

- заборону всім співробітникам виходити в місто чи за територію дипломатичної установи. Рішення про екстрений збір тимчасово відсутніх у ЗДУ співробітників приймається Послом в залежності від гостроти ситуації, що складається;
- термінове залишення приміщень і території дипломатичної установи всіма іноземцями, які там перебувають;
- закриття черговими комендантами всіх входів-виходів та в'їзних воріт на територію представництва, основних та запасних вхідних дверей до будівлі з одночасним переміщенням механіком-водієм та завідуючим господарства автотранспорту ЗДУ в гараж і запирання останнього;
- попередження з використанням телефонного зв'язку наявними співробітниками ЗДУ своїх родин, а черговим дипломатом і черговим комендантом родин відсутніх працівників про заборону виходити з помешкань та необхідність вжиття додаткових заходів безпеки;
- відповідні застереження передаються черговим дипломатом і комендантами персоналу інших українських представництв, які функціонують у країні перебування.

Всі наявні співробітники дипломатичної установи зачиняють вікна, кватирки та опускають жалюзі. Близько підходити до віконних отворів та дивитися через них на вулицю під час блокування ЗДУ суворо забороняється.

На випадок можливих спроб підпалу терористами дипломатичного представництва та намагань закинути у вікна чи на територію установи будь-які запалювальні суміші, підривні пакети тощо, завідуючий господарством, попередньо перекривши газопостачання до будинку, разом з протипожежною командою з числа співробітників ЗДУ приводять у стан повної протипожежної готовності всі наявні й додаткові можливості протипожежної безпеки та засоби пожежогасіння (наприклад, наповнення порожніх ємностей водою і т.п.).

Інші, не задіяні співробітники дипломатичного представництва, від'єднують від електромереж усі електроприлади, комп'ютери та телерадіоапаратуру і переміщують їх у кабінети, що розташовані з тильної сторони будинку.

Для недопущення несанкціонованого стороннього доступу до таємних документів і матеріалів, завідувач референтури забезпечує вивезення або знищення на місці секретної документації та спецтехніки. Безпосереднє їх знищення здійснюється попередньо створеною відповідно до плану на особливий період мобільною групою лише за вказівкою керівника дипломатичної установи та з відома ОБ. У виключних випадках, виходячи з реальної загрози захоплення ЗДУ, завідувач референтури може прийняти таке рішення самостійно.

З цією ж метою, за розпорядженням керівника ЗДУ або ОБ, співробітники дипломатичного персоналу установи відбирають службову документацію, яка містить конфіденційні відомості та є у них на виконанні і передають її завідувачу канцелярії (референтури) для знищення. Документація, що залишилась, та інші легкозаймисті речі переносяться у кабінети, що розміщуються з тильної сторони будинку.

Очевидно, що швидкість та першочерговість реалізації безпекових заходів згідно плану на особливий період щодо можливого нападу терористів забезпечується у відповідності з реаліями конкретної обстановки, яка складається в країні перебування.

Водночас керівництво ЗДУ спільно з ОБ розглядають можливість та доцільність проведення, залежно від характеру терористичної загрози, переговорів з особами, які беруть у ній найактивнішу участь, з метою поступового зниження рівня граничної напруженості та можливого відвернення нападу [3].

Якщо внаслідок подальшого наростання напруженості напад на дипломатичну установу стає невідворотним, співробітники дипмісії діють згідно з розподілом обов'язків за мобілізаційним планом функціонування установи в особливий період та адекватно до обстановки, що складається. З цією ж метою, з числа співробітників ЗДУ й дорослих членів сімей дипломатів формуються сплановані заздалегідь спеціалізовані мобільні групи внутрішньої фізичної охорони, зокрема, для "блокування спроб можливого прориву до дипломатичного представництва", "прикриття місць знищення таємної документації", "здійснення протипожежних заходів захисту приміщень" тощо.

На випадок не очікуваного нападу терористів на дипломатичне представництво, чергові коменданти зобов'язані здійснити, використовуючи всі наявні фізичні можливості та захисні засоби, адекватний опір нападникам, стримуючи їх спроби прорватися до приміщень ЗДУ на розрахунковий час (необхідний для знищення таємних документів і зразків). Саме тому дуже важливо, щоб вхідні двері були постійно замкнені, а будь-хто із співробітників, що опинився поруч, зобов'язаний надати черговим комендантам необхідну фізичну допомогу. Терміново інформуючи Посла або особу, яка його заміщає, про напад терористів, ОБ перевіряє замкненість запасних дверей до будинку, які виходять у двір установи, та злагодженість мобілізаційних дій усіх груп співробітників ЗДУ.

Керівник дипломатичної установи та ОБ, забезпечуючи додаткову допомогу черговим комендантам по здійсненню ними фізичної охорони представництва, одночасно з'ясовують характер нападу та кількість злочинців, засоби нападу, які ними використовуються, та терміново повідомляють про напад терористів до місцевих правоохоронних органів, вимагаючи негайної допомоги в його локалізації, припиненні та забезпеченні подальшого необхідного зовнішнього захисту ЗДУ. Одночасно інформується про терористичний напад на ЗДУ Міністерство закордонних справ держави перебування.

З урахуванням кількості нападників, характеру їхніх дій, оцінок реальної спроможності стримувати прорив до дипломатичного представництва, керівництвом ЗДУ й ОБ максимально вживаються всі передбачені мобілізаційним планом заходи,

головними й першочерговими з яких є запобігання можливому захопленню людей і таємних матеріалів.

Вірогідним варіантом подальшого розвитку подій може стати захоплення терористами приміщень дипломатичної установи й утримання її персоналу як заручників. Вважатимемо, що ще до стадії захоплення персоналу ЗДУ вдалося знищити всі таємні й конфіденційні матеріали (якщо ні, то відповідальні за це особи з допомогою інших співробітників вживають заходів для остаточного їх знищення), а владні органи країни перебування вже проінформовані про факт захоплення дипломатичної установи і вживають негайних антитерористичних заходів щодо її звільнення [6].

Подальші головні зусилля й поведінка керівного складу ЗДУ та кожного члена колективу, що потрапив до рук злочинців як заручник, повинні бути спрямовані на збереження їхнього життя та здоров'я. Виходячи з цієї мети та маючи на увазі вірогідність можливих крайнощів, до яких здатні вдатися злочинці, всім заручникам слід керуватися у своїй поведінці основними настановами, які викладені в "Рекомендаціях щодо поведінки на випадок захоплення злочинцями".

Слід також зазначити, що викрадення та захоплення людей як заручників з будь-якою метою останнім часом є одним із розповсюджених терористичних злочинів. Проте, стати заручником можливо і випадково, навіть при захопленні людей екстремістами чи пограбуваннях банків, магазинів, установ грабіжниками тощо [6].

Заручник, як утримувана особа, завжди перебуває під повною владою злочинців. Але це не означає, що він повністю позбавлений будь-якої можливості боротися за благополучне розв'язання екстремальної ситуації, в якій опинився. Навпаки, багато чого залежатиме саме від його поведінки, для правильного вибору якої йому необхідні і належний рівень попередньої підготовки, і виваженість та зібраність у надзвичайних умовах.

Класична схема викрадення чи захоплення конкретної особи або групи в заручники має наступний вигляд: збір інформації щодо визначеного об'єкта (об'єктів) захоплення, планування, підготовка, саме захоплення, укриття заручника чи заручників, спілкування і допити, ведення переговорів, отримання викупу або досягнення злочинцями іншої поставленої мети, звільнення або страта жертв [5].

Захоплення є центральною частиною злочинної акції терористів. Навіть поверховий аналіз таких ситуацій показує, що 90 % усіх викрадень і захоплень відбуваються у той момент, коли жертва перебуває на шляху слідування на роботу чи додому, здебільшого неподалік від місця проживання або служби. Тобто для захоплення заручника обирається, як правило, таке місце, де неможлива зміна його маршруту пересування, навіть у разі можливого відхилення від часу прибуття чи відбуття об'єкта.

У момент захоплення злочинці переважно діють безцеремонно, навіть жорстоко. Нерідко жертву позбавляють притомності ударом по голові, або застосовують сильнодіючі психотропні препарати. Робиться це з метою, щоб об'єкт не чинив опору, не спробував втекти, не привертав увагу сторонніх осіб та не міг зрозуміти, куди його везуть і чому приховують.

Реальною і здебільшого єдиною можливістю вирватися із рук злочинців на початковій стадії захоплення є саме момент нападу. Несподівані для злочинців та рішучі дії жертви здатні призвести до її порятунку. Але якщо вирватись їй однозначно неможливо, то краще не вдаватися до крайнощів, а діяти відповідно до обстановки, що склалася.

У момент захоплення злочинцями доцільно контролювати їхні дії і фіксувати все навколо, що може сприяти звільненню. Необхідно намагатися запам'ятати всі деталі

транспортування з місця захоплення: час та швидкість руху, підйоми та спуски, круті повороти, зупинки на світлофорах, залізничних переїздах, характерні звуки тощо. При найменшій можливості такі відомості слід повідомити тим, хто веде переговори зі злочинцями про звільнення заручників (якимось чином натякнути чи передати записку).

Зрозуміло, що такої можливості загалом може й не бути. Але за будь-яких обставин слід пам'ятати, що навіть незначна інформація про місце перебування заручників може сприяти їх звільненню, стати корисною для того, щоб викрити і присікти дії злочинців. Треба запам'ятовувати все побачене та почуте за час перебування в ув'язненні – розташування приміщень, вікон та дверей, навколишню обстановку тощо, особливо зовнішній вигляд та манери поведінки самих злочинців. Треба також спостерігати за їхніми стосунками між собою, уважно слухати їхні розмови, запам'ятовувати розподіл ролей. Важливо скласти для себе чіткий психологічний портрет кожного з терористів. Однак, робити такі речі слід дуже обережно, адже у разі їх виявлення злочинцями може неминуче наступити сувора розправа.

Особа стає жертвою в момент захоплення, і хоч це відбувається за різних умов, жертва завжди перебуває у стані сильного психологічного потрясіння або шоку. Це зумовлено раптовим різким переходом від фази спокою до фази стресу. Люди реагують на такий перехід неоднаково: одних страх буквально паралізує, інші пробують чинити опір. Тому життєво важливо заручникам якнайшвидше приборкати свої емоції, щоб поводитися раціональніше, відповідно збільшуючи свої шанси на порятунок [7].

Злочинці ж завжди поводяться з ув'язненими так, щоб максимально використати їх у власних інтересах. Усяким чином намагаються демонструвати свою зверхність та владу, навіть якщо жертва не чинить опору. Вони прагнуть придушити її волю й залякати. Тому кожен заручник повинен визначити свою позицію у взаєминах зі злочинцями. Як свідчить практика, безвільна поведінка, благання про пощаду, надмірна поступливість реальної користі не приносять. Злочинці у кожному разі діють відповідно до своїх планів та з урахуванням обставин, що складаються.

Тому зовнішня готовність до контактів зі злочинцями та обговорення питань, які їх цікавлять, повинна поєднуватися з головним правилом: діяти на користь собі, а не злочинцям. Адже надання злочинцям будь-якої інформації використовуватиметься ними врешті-решт на шкоду самим заручникам, їх близьким, родичам, колегам по роботі, співробітникам правоохоронних органів тощо. Тому дуже важливо зважено ставитися до запитань злочинців, зокрема, про можливу реакцію оточення, колег по роботі, близьких родичів на раптове їх зникнення чи можливу суму викупу або задоволення інших вимог [5].

Адже суть поведінки заручників полягає саме у тому, щоб своїми частковими відповідями на запитання злочинців допомогти людям, які прагнуть їх знайти та звільнити, а не нашкодити останнім, поставивши їх у більш скрутніше становище. Зокрема, аргументоване переконання злочинців у нереальності тих чи інших їхніх вимог може сприяти позитивному вирішенню конкретного інциденту. Проте, не можна діяти за принципом "усе або нічого". Реакція злочинців на очевидні факти нездійсненності їхніх задумів, у поєднанні зі збудженим психічним станом, в якому вони перебувають, може стати фатальною для заручників. До того ж терористи часто перебувають у стані алкогольного або наркотичного сп'яніння.

Заручникам варто намагатися пом'якшити ворожість екстремістів до себе, шукаючи можливості для встановлення індивідуальних контактів з окремими із них. Це потрібно хоч би тому, щоб пом'якшити фізичні страждання та поліпшити умови утримання. Але зовнішня готовність до спільної розмови зі злочинцями, участь в

обговоренні проблем, які їх хвилюють, не повинні суперечити зазначеному вище головному принципу – "допомагати собі, а не злочинцям". І тут заручникам може стати в нагоді ще одна стародавня народна мудрість: "розділяй і володарюй". Можливо стане ефективною спроба внести розлад у злочинну групу або схилити кого-небудь із них на свою сторону, шляхом обіцяння всього того, що реально можна зробити.

Практично завжди викрадених людей допитують. Допити можуть носити характер майже товариської бесіди, а можуть супроводжуватися фізичними катуваннями і тортурами.

Досвідчені злочинці спочатку пробують демонструвати дружнє ставлення, яке справляє на збентежених заручників позитивне враження, адже вони жадають психологічної підтримки хоча б на рівні емоцій. Крім того, терористи завжди вдаються до різних хитрощів. Так, терорист, який веде допит, погрожує, що у разі упертості жертви він буде змушений передати справу до рук свого помічника, людини більш жорсткої та тупої. Тому, мовляв, краще не впиратися марно, а піти на взаєморозуміння та співпрацю. Цей відомий у практиці допитів заручників трюк і на сьогодні ще достатньо дієвий [5].

Щоб зламати заручника психологічно, терористи використовують низку заходів фізичного тиску:

- обмежують рух, зір, слух, (тримають зв'язаними чи в наручниках, на ланцюгу або із зав'язаними очима, затикають вуха тощо);
- морять голодом і спрагою, позбавляють цигарок;
- створюють нестерпні умови утримання (тіснота, бруд, вологість, задушливість, сморід, холод тощо).

Для слабких людських особистостей усього зазначеного більш ніж достатньо, щоб виконати будь-які вимоги терористів. Адже у запасі в злочинців є ще й такий дієвий спосіб фізичного тиску, як тортури. За всю давню історію людство придумало величезну кількість тортур, багато з яких актуальні і до цього часу. Вони поділяються на дві основні групи: ті, які спричиняють сильний фізичний біль, і ті, які викликають непереборний людський страх. І як би це дивно не виглядало, фізичне катування перенести буває значно легше, ніж витримати психологічне залякування. Справа в тому, що існує так званий "поріг больової вразливості". Якщо фізичний біль пересилити, то у подальшому організм вже гостро його не сприймає. Що ж стосується впливу на людину психологічним тиском, шантажем та залякуваннями, то чинити їм належний опір завжди набагато важче.

Окремо слід розглядати питання вимоги терористами фінансового викупу. Злочинці добре усвідомлюють, що найбільшу небезпеку для них становить момент отримання грошей. Тому вони розробляють складні й багатоступінчаті схеми їх можливого отримання. Метою таких заходів є виключення вірогідності нападу із засідки, фіксації факту передачі грошей, встановлення конкретних особистостей злочинців. При цьому терористи самі призначають час та місце зустрічі, прибуття кур'єра із грошима, визначають маршрут, ведуть приховане стеження за його пересуванням та місцем передачі викупу [5].

Оскільки ініціатива завжди перебуває в руках у злочинців, то вони намагаються створити такі умови, які б не дали змоги співробітникам правоохоронних органів наблизитись до них на відстань, з якої можна було б ідентифікувати їх особи або навіть захопити. З цих же причин злочинці підбирають кур'єрів із числа осіб з найближчого оточення заручників, які є їм добре відомі ще з етапу підготовки та планування терористичної акції.

Отримання викупу або досягнення іншої терористичної мети не обов'язково тягне за собою звільнення заручників, скоріше навпаки – їх ліквідацію. Адже кожного із заручників у перспективі можливо використати як важливого свідка [6].

У випадках, коли злочинці самі відпускають на волю заручника, вони як правило, відвозять його в яке-небудь безлюдне місце і там залишають. Другий варіант – його залишають у замкнутому приміщенні, вихід з якого вимагає суттєвої затрати сил та часу. Третій варіант – заручника висаджують з машини на багатолюдній вулиці, подалі від постів та офісів поліції і тікають.

Особливо важливо для заручників правильно поводити себе у разі їх звільнення співробітниками правоохоронних органів. Під час таких операцій заручникам необхідно спробувати переконати терористів, що для них найдоцільніше здатися, бо тоді вони можуть розраховувати на більш м'який вирок. Якщо ж зазначений варіант не спрацьовує, слід намагатися переконати злочинців у тому, що їх подальша доля цілком залежить від долі самих заручників. Адже у разі їх ліквідації, всілякі переговори з терористами втратять сенс. Тоді залишиться тільки єдиний вихід – штурм їхніх позицій силами спецназу чи правоохоронних органів із застосуванням зброї і спецзасобів [7].

Під час проведення штурму бійцями спецпідрозділів правоохоронних і спеціальних органів заручникам обов'язково слід прикриватися від куль. Краще всього лягти на підлогу подалі від вікон і дверей, обличчям додолу та не на прямій лінії ведення вогню з віконних і дверних пройм. У момент штурму заручникам не варто брати до рук озброєння злочинців. Інакше штурмовики можуть переплутати їх зі злочинцями.

Нерідко терористи під час штурму намагаються сховатися серед заручників. Таким їхнім діям, за можливості, слід перешкоджати.

У випадках, коли місце утримання заручників та перебування злочинців встановлено, спецслужби, як правило, завжди намагаються використати наявні у них технічні засоби для прослуховування розмов, які ведуться в приміщеннях утримання. Про це слід пам'ятати і в розмовах зі злочинцями повідомляти інформацію, яка у разі її перехоплення буде корисною при підготовці штурму. Особливо важливо повідомляти відомості про видимі прикмети, які одразу дають можливість відрізнити злочинців від заручників, про їх озброєння, кількісний склад, місце перебування у приміщенні, моральний стан й амбітні терористичні наміри.

Висновки.

Збереження заручниками психологічної стійкості при тривалому перебуванні в ув'язненні – одна із найважливіших умов їх порятунку. Водночас, корисним є використання ними будь-яких прийомів і методів, які відволікають від неприємних почуттів та переживань і дозволяють зберігати ясність думок й адекватність оцінок.

Слід завжди бути ввічливими у своїх розмовах з терористами, не ображати їх, не говорити з ними про те, чого вони не бажають чути, не вступати у суперечки та не критикувати. Свою лінію на можливе звільнення доцільно проводити не запереченнями, а через досягнення погодження.

Досить важливо заручникам зважено ставитися до запитань терористів, особливо, про можливу реакцію оточення, колег по роботі, своїх близьких і родичів на факт зникнення, про суму викупу або про можливість задоволення інших вимог злочинців.

Результати проведеного дослідження можуть стати підґрунтям для подальшого наукового обґрунтування необхідності вдосконалення державних нормативно-правових актів, відомчих розпорядчих документів й інструкцій, а також практичних рекомендацій, якими безпосередньо керуються співробітники та керівництво ЗДУ під час виконання ними своїх повноважень за кордоном.

Використана література

1. Про боротьбу з тероризмом: Закон України від 12.08.14 р. № 1630-VII. URL: https://zakon.rada.gov.ua

2. Інструкція про порядок реагування системи органів дипломатичної служби на загрозу вчинення терористичного акту": наказ МЗС України від 04.06.10 р. № 114-дск.; погоджена з Антитерористичним центром СБ України.

3. Державна політика протидії тероризму: пріоритети та шляхи реалізації: збірник матеріалів "круглого столу"; за ред. М.Г. Гуцало. Київ: НІСД. 2011. 120 с.

4. Владленова І.В., Кальницький Е.А. Нанотероризм: нові можливості та соціальні загрози. *Вісник Національної юридичної академії України імені Ярослава Мудрого*. 2011. № 9. С. 64-79.

5. Канцір В.С. Тероризм як метод політичної боротьби: збірник наукових праць Національного університету "Львівська політехніка". 2015. № 45. С. 430-435.

6. Ключові тези саміту G7 в Італії: *Тероризм та пропаганда в мережі*, 25-26.05.2017 р. URL: httgs://www.eurointegration.com.ua/news/2018/06/9/7082884 (дата звернення: 19.08.2017).

7. I. Wallerstein. Typology of Crises in the World-System. URL: http://www.jstor.org/stable/40241112 (дата звернення: 30.11.2018).

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

УДК 343.9:343.326

БОХЕНКО В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-3579-4328.

УДОСКОНАЛЕННЯ СИСТЕМИ БОРОТЬБИ З ТЕРОРИЗМОМ: ДОСВІД США

Анотація. *Стаття присвячена аналізу системи боротьби з тероризмом у США. Наведено систему суб'єктів боротьби з тероризмом. Вказано новації в антитерористичній діяльності правоохоронних органів та спеціальних служб США. Розглянуто окремі нормативні акти США у сфері боротьби з тероризмом. Відзначається роль громадськості у боротьбі з тероризмом, висвітлюються механізми залучення населення до цієї діяльності.*

Ключові слова: *боротьба з тероризмом, США, національна безпека, суб'єкти боротьби з тероризмом, терористична загроза, американське законодавство.*

Summary. *The article is devoted to the analysis of the counter-terrorism system in the United States. The system of subjects of fight against terrorism, and also innovations in anti-terrorist activity of law enforcement agencies and special services of the USA is defined. Some US regulations in the field of counter-terrorism are considered. The role of the public in the fight against terrorism is noted, the mechanisms of public involvement in this activity are highlighted.*

Keywords*: fight against terrorism, USA, national security, subjects of fight against terrorism, terrorist threat, American legislation*

Аннотация*. Статья посвящена анализу системы борьбы с терроризмом в США. Приведена система субъектов борьбы с тероризмом. Указаны новации в антитеррористической деятельности правоохранительных органов и специальных служб США. Рассмотрены отдельные нормативные акты США в сфере борьбы с терроризмом. Отмечается роль общественности в борьбе с терроризмом, освещаются механизмы привлечения населения к этой деятельности.*

Ключевые слова*: борьба с терроризмом, США, национальная безопасность, субъекты борьбы с терроризмом, террористическая угроза, американское законодательство.*

Постановка проблеми. Сьогодні боротьба з тероризмом є одним з найбільш проблемних питань міжнародної безпеки, глобальної взаємодії та співпраці. Сучасний тероризм давно вже став явищем інтернаціональним, транскордонним, глобальним, й таким, що загрожує не тільки окремим державам, а й міжнародній безпеці в цілому. В цьому плані цікавим є американський досвід протидії тероризму, оскільки в США створено власну масштабну загальнодержавну систему виявлення, запобігання і припинення терористичної діяльності. Спецслужби та правоохоронні органи США активно взаємодіють з цією метою з спеціальними службами інших країн, проводять активні операції за кордоном. В лютому 2015 року відповідні служби США підписали дві нових угоди з Європолом щодо протидії нелегальній міграції та іноземним бойовикам. Це забезпечило платформу для обміну інформацією щодо осіб, які забезпечують вербування та переправлення іноземних бойовиків, а також джерел їх фінансування [1]. У результаті цієї діяльності рівень терористичної загрози порівняно з країнам Європи понизився. Водночас, на думку американських аналітиків, у 2020 – 2021 рр. терористична загроза у США значно зросте через декілька факторів: президентські вибори та реакцію на кризу, пов'язану з поширенням інфекційної хвороби CoVID-19 [2, с. 380].

Крім цього, посилення міграційних процесів створює додаткові можливості для активізації діяльності міжнародних терористичних організацій. З огляду на це, США вживають заходів щодо посилення прикордонного контролю, впровадження ефективних систем спостереження за мігрантами, запобігання нелегальній міграції, як важливих елементів системи попередження вчинення терористичних актів [1].

Результати аналізу наукових публікацій. Дослідженням досвіду боротьби з тероризмом займалися багато вчених: Б. Дженкінс, Г. Деникер, [3], В. Лакер [4], Р. Паркес [5], Р. Хантер, А. Шмід [6] та ін. Серед українських дослідників слід виділити праці В.Ф. Антипенка [7], В.П. Ємельянова [8], Б.Д. Леонова [9], В.В. Мокляка [10], А.В. Савченка, О.Г. Семенюка, О.В. Шамари та ін. Найбільш актуальним і дієвим, на нашу думку, є досвід США, де існує стабільна правова система, а правова діяльність у цій країні має вагому базу напрацювань у сфері запобігання терористичним актам.

Метою статті є оцінка сучасних тенденцій розвитку антитерористичної діяльності у США в контексті запозичення позитивного зарубіжного досвіду під час удосконалення державної політики у сфері боротьби з тероризмом в Україні.

Виклад основного матеріалу. Аналіз боротьби з тероризмом в США умовно можна поділити на два періоди: до 11.09.2001 р. і після цієї дати. Жахливі теракти 11 вересня 2001 року в США змінили свідомість американського суспільства, в тому числі його ставлення до терористичної загрози. Ці події призвели до активізації антитерористичної діяльності в США та за її межами, зокрема, під час здійснення воєнних операцій в Іраці та Афганістані.

З метою підвищення ефективності боротьби з міжнародними терористичними організаціями, а також координації діяльності різних суб'єктів боротьби з тероризмом були розроблено низку нормативно-правових актів. Вже у жовтні 2001 року був прийнятий Федеральний Закон "Патріотичний акт" (USA PATRIOT Act) [11], який істотно розширив можливості правоохоронних органів, спеціальних служб та органів національної безпеки у сфері запобігання тероризму з виявлення і попередження терористичних актів, що готуються як на території США, так і за кордоном. Вони визначили новий, більш системний підхід до протидії тероризму в XXI столітті [2, с. 72].

З моменту прийняття "Патріотичного акта" в американському суспільстві розпочалася критика багатьох його положень, а особливо тих, що стосувалися розширення процедури таємного нагляду за особами, що підозрюються у терористичній діяльності [10, с. 220]. Відтепер правоохоронним органам та спеціальним службам дозволялось: розкривати один одному службову й "таємну" інформацію, що тим чи іншим чином стосувалася кримінального переслідування осіб, що підозрюються у тероризмі; спостереження, тобто таке прослуховування за допомогою електронних засобів, коли воно проводиться не відносно конкретно зафіксованого номера телефону, а щодо розмов об'єкта спостереження з усіх телефонних апаратів при його пересуванні (розділ 206 Акта). Окрім цього, були розширені можливості електронного спостереження за підозрюваними у тероризмі: збільшено перелік даних, які повинен надавати провайдер на запит правоохоронних органів (підрозділи 209 – 212, 217 Акта); наділено юридичним імунітетом провайдерів та інші організації, що надають допомогу у розслідуванні, стосовно розголошених у зв'язку із цим даних (підрозділ 225 Акта); спрощена офіційна процедура застосування спеціальних пристроїв для негласного збору інформації у комп'ютерних мережах (підрозділ 216 Акта) [10, с. 220; 11].

За результатами антитерористичної реформи було створено або реорганізовано понад 263 державні установи для реалізації антитерористичної діяльності [12]. Проте,

реалізація ефективної стратегії боротьби зі злочинністю – справа, якою займалися всі держави не одне століття, помітних здобутків так і не досягла [3, с. 76-77].

Відповідно до Акта про національну безпеку від 25 листопада 2002 р. створено Міністерство національної безпеки США, яке об'єднало 22 федеральних відомства та агентства, а також Адміністрацію транспортної безпеки США [13]. Серед завдань Міністерства національної безпеки США варто відзначити: запобігання терористичній діяльності та транснаціональній злочинності; забезпечення безпеки кордонів; реалізацію імміграційної та митної політики; забезпечення економічної безпеки та кібербезпеки; запобігання стихійним лихам та іншим надзвичайним ситуаціям [14].

Крім Збройних Сил, до складу системи суб'єктів запобігання тероризму США також входять консультативні органи при президентові США для координації діяльності суб'єктів боротьби з тероризмом та вирішення проблем національної безпеки із зовнішньої політики та внутрішньої безпеки, серед яких виділяється Рада національної безпеки США, Рада внутрішньої безпеки США [15], Національний координатор з безпеки, захисту інфраструктури та боротьби з тероризмом та ін. [10, с. 223-224]. Важливе місце у системі боротьби з тероризмом займає Федеральне бюро розслідувань та Центр з відстеження терористичної активності.

ФБР наділене широким колом повноважень, достатнім матеріально-технічним забезпеченням, великим штатом професійних агентів, значним надбанням у розвідувальній і оперативній діяльності, завдяки цьому їм вдається якісно та рішучо попереджати терористичні акти у великих містах США. Співробітники ФБР значну увагу приділяють просвітницькій і профілактичній діяльності серед населення, застерігаючи людей захищати себе як у мережі, так і при особистій зустрічі, а також закликають одразу ж повідомляти про будь-яку підозрілу активність, із якою вони стикаються [2, с. 383].

Помітну роль у боротьбі з тероризмом відіграє Центральне розвідувальне управління, яке займається зовнішньою розвідкою терористичних загроз. При ЦРУ функціонує спеціальний підрозділ – Антитерористичний центр, який збирає інформацію про терористичні об'єднання в усьому світі. Спеціалісти цього підрозділу беруть участь у підготовці щорічних звітів про стан тероризму в світі [10, с. 225].

У США діє Національний контртерористичний центр, до завдань якого віднесено проведення міжвідомчих засідань щодо виявлення внутрішніх і зовнішніх загроз інтересам держави; аналітична діяльність і вироблення рішень з протидії тероризму, надання інформації щодо світової розробки інноваційних рішень у сфері боротьби з тероризмом. Також існує інформаційний центр вивчення тероризму ім. Меіра Аміта, метою діяльності якого є акумуляція, дослідження та розповсюдження інформації стосовно тероризму та розвідувальної діяльності.

Наприкінці 2018 р. Президент США затвердив Національну стратегію боротьби з тероризмом, яка втілює в собі новий еволюційний підхід у процесі стабілізації рівня терористичних актів і знешкодження терористичної загрози в усьому світі та на теренах Америки. Ця стратегія відрізняється від попередніх тим, що вона застосовує більш рухливий та експансивний підхід, який розглядає весь спектр терористичних загроз для США, включаючи зарубіжних ворогів та осіб, на яких вони прагнуть впливати та яких планують вербувати для вчинення насильства у США [2, с. 380]. Тобто центральна мета стратегії спрямована на захист американських свобод і непохитність у зобов'язанні перемогти всіх, хто застосовує насильство, намагаючись знищити, дестабілізувати чи погіршити стан суспільства [16; 2].

Основні цілі та задачі США у процесі запобігання терористичним актам, спрямовані на: зменшення рівня нападів терористів на території штатів; знищення фінансових,

матеріальних і матеріально-технічних джерел сили та підтримки терористів; ліквідацію спроможності терористів вербувати людей і надихати на реалізацію терористичних цілей; посилення охорони кордонів; покращення діяльності правоохоронних органів; протидію придбання терористами та використання ними зброї масового ураження; розширення кола партнерів із державного та приватного сектору, в т.ч. іноземних [17].

У процесі розробки та реалізації заходів запобігання терористичним актам у США опираються на три принципи, серед яких активне партнерство; масштабність, гнучкість та адаптованість; готовність діяти [2, с. 380; 18].

Не останню роль у боротьбі з тероризмом відіграють інформаційні технології без яких неможливо уявити сучасне суспільство. У зв'язку з сутнісними відмінностями сучасних інтелектуально насичених технологій ведення війни від традиційних, для ефективного функціонування системи антитерористичного захисту необхідно змінювати принципи і моделі антитерористичної діяльності, формувати інноваційно-креативне мислення, нові концепції, теорії, методи та технології інноваційного розвитку [19]. Основне завдання подібних технологій зводиться до розпізнавання, формалізації та оцінки загроз терористичного характеру для прогнозування терористичної активності.

Найбільшою перевагою застосування інформаційних технологій є швидкість, з якою адресат отримує інформацію, що має значення для розкриття кіберзлочинів. Цим скористалася компанія Palantir Technologies, послугами якої користуються ЦРУ, ФБР, Міноборони США, Військово-повітряні сили США, Корпус морської піхоти США, командування спеціальних операцій, Військова академія США. Інформаційна система Palantir аналізує інформацію про колишні правопорушення підозрюваних злочину, їх родичів та оточення, автомобільні номери та іншу супутню інформацію, яка прямо або опосередковано стосується підозрюваного [20].

Окремо слід виділити державну програму США з негласного збору інформації, яка передається каналами електрозв'язку – PRISM. Лише у 2010 році завдяки PRISM було перехоплено та зібрано близько 1,7 млрд. телефонних перемовин та електронних повідомлень, а також близько 5 млрд. геолокаційної точок місцезнаходження власників мобільної техніки. Як тільки особа, що несе інтерес з боку органів поліції або держбезпеки, потрапляє до бази даних Palantir, інформація про неї відразу розповсюджується відповідним співробітникам. Слідчі мають можливість отримувати повідомлення про осіб, які підпадають під завчасно визначені параметри пошуку: раса, стать, вік, зріст тощо. У штатному режимі працівники спецслужб вносять до бази даних інформацію про особу, яка причетна до тероризму [21]. Також Palantir реалізовано систему виставлення рейтингових балів залежно від ступеня небезпеки, яку несе особа, кількості скоєних правопорушень, затримань органами поліції тощо. Співробітникам спецслужб достатньо кількох хвилин, щоб мати уявлення про пряму чи опосередковану причетність осіб до терористичної діяльності [22].

Зацікавленість викликає ще один напрямок боротьби з тероризмом, який з'явився у США з огляду на особливості терористичної атаки у 2016 р. у м. Ніцца (Франція), де зловмисником використовувалась вантажівка. Передбачається, що у США до 2021 року до Інтернету речей буде приєднано близько 250 млн. транспортних засобів, управління якими може здійснюватися через Інтернет. Це надає терористам можливість перехоплювати управління такими засобами та вчиняти терористичні атаки дистанційно, навіть не перетинаючи державний кордон. З огляду на таку потенційну загрозу в Міністерстві юстиції США розпочала функціонувати окрема група, що опікується виключно питаннями Інтернету речей [1].

Особливим відділом ФБР по боротьбі з тероризмом було підготовлено та представлено на своєму сайті матеріал, присвячений мінімальним запобіжним заходам: громадянам пропонується ознайомитися з інформацією про місця підвищеної небезпеки, про рекомендовані дії у разі виявлення сумнівних пакетів і згортків на вулицях, у транспорті, в інших публічних місцях. На сайті містяться відомості щодо офіційної оцінки рівня терористичної загрози в конкретний момент, а також своєрідний "інструктаж" для тих, хто планує закордонні поїздки в "небезпечні" зони [23].

Важливе значення у сфері протидії тероризму має реалізація спеціальних програм та ініціатив під егідою Державного департаменту США. У Департаменті функціонує Бюро з протидії тероризму та насильницькому екстремізму, що займається розробкою скоординованих стратегій та підходів до боротьби з тероризмом за кордоном та забезпечує антитерористичне співробітництво міжнародних партнерів. Серед інших обов'язків Бюро реалізує такі програми та ініціативи: Програма допомоги у боротьбі з тероризмом, Програма протидії насильницькому екстремізму, Програма протидії фінансуванню тероризму, Фонд боротьби з тероризмом та багато ін. [24]. Також важливими аспектом антитерористичної діяльності в США є залучення громадськості до боротьби з тероризмом, яке надає допомогу правоохоронним органам для підтримання правопорядку.

Отже, система запобігання терористичним актам у США характеризується вагомою законодавчою базою, яка повністю забезпечує функціонування державних органів у цій сфері; широким спектром суб'єктів запобігання терористичним актам у великих містах, діяльність яких оперативна та скоординована між собою; активною участю фізичних осіб, громадських організацій, релігійних спільнот і представників приватної діяльності у попередженні злочинних намірів терористів; розгалуженою низкою заходів, серед яких – захист кордонів, захист уразливих об'єктів інфраструктури, викриття спроб вербування людей терористами у терористичну діяльність, мінімізація терористичної пропаганди через ЗМІ та Інтернет, міжнародне співробітництво та формування соціальної стійкості до терористичного акту [2, с. 384].

Висновки.

Дослідження досвіду США є важливим завданням суб'єктів боротьби з тероризмом в контексті удосконалення вітчизняної антитерористичної діяльності. В США існує розгалужена державна система боротьби з тероризмом, основу якої утворює значна кількість суб'єктів боротьби з тероризмом. Важливе значення має використання інформаційних технологій під час взаємодії таких суб'єктів, що значно підвищує ефективність обміну інформацією між ними. Важливу роль у цій діяльності відіграють громадські організації, які активно співпрацюють з правоохоронними органами у напрямі запобігання тероризму. Активне залучення громадян і суспільства в цілому до боротьби з цим небезпечним явищем дозволить підвищити ефективність такої діяльності і рівень довіри населення до відповідних уповноважених органів [1].

Використана література

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

2. Стукаліна О.В., Кулик Л.М. Міжнародний досвід запобігання терористичним актам у великих містах. URL: http://www.baltijapublishing.lv/omp/index.php/bp/ catalog/download/84/2184 /4720-1?inline=1 (дата звернення: 13.06.2021).

3. Деникер Г. Стратегия антитеррора: факты, выборы, требования. Новые пути борьбы с терроризмом. Терроризм в современном капиталистическом обществе. Москва, 1982. Вып. 2. С. 76-80.

4. Laqueur W. Postmodern Terrorism. *Foreign Affairs*. Vol. 75. № 5 (Sept./Oct.). 1996. P. 24-36.

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

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

7. Антипенко, В.Ф. Оптимізація антитероистичної системи держави в умовах міжнародної і регіональної інтеграції. Київ, 2008. 406 с.

8. Емельянов В.П. Терроризм и преступления с признаками терроризирования (уголовно-правовое исследование): монография. Москва: Nota Bene, 2000. 320 с.

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

10. Мокляк В.В. Сучасний досвід США у сфері запобігання тероризму. *Питання боротьби зі злочинністю.* 2017. № 34. С. 219-229. URL: http://nbuv.gov.ua/UJRN/Pbzz_2017 _34_20

11. Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 / Public Law 107-56 – OCT. 26, 2001. URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата звернення: 12.06.2021).

12. Green, Shannon N. Do we need a new strategy to prevent terrorist attacks on the United States? Center for strategic and international studies. URL: https://www.csis.org/analysis/do-we-need-new-strategy-prevent-terrorist-attacks-united-states (дата звернення: 09.06.2021).

13. Homeland Security Act of 2002. Public Law 107–296. URL: https:// legcounsel.house. gov/Comps/Homeland%20Security%20Act%20Of%202002. pdf (дата звернення: 13.06.2021).

14. Our Mission – Department of Homeland Security. URL: https:// www.dhs.gov/our-mission (дата звернення: 13.06.2021).

15. Homeland Security Presidential Directive-1. October 29, 2001. URL: https://fas.org/irp/off docs/nspd/hspd-1.htm (дата звернення: 13.06.2021).

16. National Strategy for Counterterrorism of the United States of America. URL: https://www.whitehouse.gov/ wp-content/uploads/2018/10/NSCT.pdf (дата звернення: 09.06.2021).

17. National Prevention Framework. Second Edition. URL: https://www.fema.gov/media-librarydata 146601720927983b/72d5959787995794c08/74095500b1/National_Prevention_Framework 2nd.pdf (дата звернення: 10.06.2021).

18. URL: https://www.fema.gov/medialibrarydata/146601720927983b72d5959787995794c08/74095500b1/National_Prevention72d5959787995794c08/74095500b1/National_Prevention_Framework2nd.pdf (дата звернення: 10.06.2021).

19. Блэкнер Ф. Информационные технологии и организации: уроки 80-х и перспективы 90-х. (Психология труда и организационная психология). Москва, 1995. 448 с.

20. Офіційний сайт Palantir. URL https://www.palantir.com (дата звернення: 12.06.2021).

21. PRISM (программа разведки). URL: https://ru.wikipedia.org/wiki/PRISM_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8) (дата звернення: 12.06.2021).

22. Terrorist Threat integration. URL: https://www.dni.gov/index.php/nctc-who-we-are/history

23. Safety and Security for the Business Professional Abroad. URL: https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view(дата звернення: 12.06.2021).

24. Programs and Initiatives – U.S. Department of State. URL: https://www.state.gov/j/ct/programs/index.htm#ISEG (дата звернення: 12.06.2021).

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

УДК 34.096

БОРИСОВ О., *магістр права*, аспірант ДНУ ІБП НАПрН України.

ОСОБЛИВОСТІ ПРАВОВОГО РЕЖИМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ, ЗУМОВЛЕНІ КОНСТИТУЦІЄЮ УКРАЇНИ

Анотація. *Стаття присвячена конституційним особливостям правового режиму забезпечення інформаційної безпеки України. Автором комплексно досліджено норми Конституції України, наукові напрацювання відносно поняття правового режиму і його особливостей, завдяки чому було виявлено ключові конституційні особливості правового режиму забезпечення інформаційної безпеки України і визначено відповідні конституційні засади, першочергові кроки реформування такого правового режиму.*

Ключові слова: *інформаційна безпека України, інформаційна війна, правовий режим, Конституція України.*

Summary. *The article is devoted to the constitutional features of the legal regime for ensuring information security of Ukraine. The author comprehensively investigated the norms of the Constitution of Ukraine, scientific developments regarding the concept of the legal regime and its features, due to which the key constitutional features of the legal regime of information security of Ukraine were identified and the relevant constitutional principles, priority steps of reforming such a legal regime were determined.*

Keywords: *information security of Ukraine, information war, legal regime, the Constitution of Ukraine.*

Аннотация. *Статья посвящена конституционным особенностям правового режима обеспечения информационной безопасности Украины. Автором комплексно исследованы нормы Конституции Украины, научные наработки относительно понятия правового режима и его особенностей, благодаря чему были выявлены ключевые конституционные особенности правового режима обеспечения информационной безопасности Украины и определены соответствующие конституционные принципы, первоочередные шаги реформирования такого правового режима.*

Ключевые слова: *информационная безопасность Украины, информационная война, правовой режим, Конституция Украины.*

Постановка проблеми. Минуло вже сім років з початку відкритої збройної агресії Російської Федерації проти України, наслідком якої стала анексія території АР Крим, частини Донецької і Луганської областей, істотні соціальна та економічна дестабілізація України.

Набутий Україною досвід протистояння з Російською Федерацією показав, що одним з ключових інструментів агресії нашого супротивника є цілеспрямований інформаційний вплив: пропаганда, поширення недостовірної та/або неповної, викривленої інформації, інформаційний тиск і провокації тощо.

Відповідно, як для протидії російській агресії, так і для упередження можливої агресії з боку інших держав Україні сьогодні вкрай необхідно сформувати і запровадити ефективний правовий механізм забезпечення інформаційної безпеки.

У свою чергу, дія правового механізму провадиться в життя засобами правового режиму, пристосованого під мету і цілі конкретної сфери правового регулювання. Тобто, правовий режим є своєрідним інструментарієм або арсеналом, застосування якого допускається в межах дії відповідного механізму правового регулювання.

Так, останнім часом в Україні спостерігається тенденція домінування засобів правового регулювання, притаманних імперативному методу, в першу чергу - заборон.

Зокрема, протягом періоду відкритого російсько-українського збройного конфлікту в Україні мають місце:

- обмеження на території України доступу до ряду російських веб-ресурсів;
- заборона функціонування ряду телевізійних каналів;
- застосування механізмів кримінально-правової охорони інтересів національної безпеки.

Такі дії держави значною мірою спрямовані саме на забезпечення інформаційної безпеки. Водночас, в інформаційній сфері зосереджені не лише інтереси національної безпеки держави, а й приватні права, свободи та інтереси людини і громадянина, пов'язані з інформацією. Відповідно, застосування засобів імперативного впливу в інформаційній сфері без їх належного збалансування менш жорсткими засобами правового регулювання може призвести до порушення соціальної стабільності, надмірного обмеження соціальних прав і свобод людини.

Відтак, питання збалансованого правового регулювання у сфері забезпечення інформаційної безпеки залишається для України досить актуальним. І для його вирішення доцільно звернутися саме до такого поняття як правовий режим, дослідити його особливості та визначити ключові засади, першочергові кроки подальшого реформування.

Основоположним нормативно-правовим актом в Україні є Конституція України, іменована також Основним законом [1]. Безпосередньо нормами Конституції України зумовлено цілий ряд особливостей правового режиму забезпечення інформаційної безпеки України. Відповідно, саме з дослідження норм Основного закону доцільно розпочати роботу над виявленням конституційних особливостей правового режиму забезпечення інформаційної безпеки України і визначенням відправних точок для ефективного реформування такого правового режиму. Даній проблематиці і присвячена ця стаття.

Результати аналізу наукових публікацій. Питанням забезпечення інформаційної безпеки України присвячено вже досить багато наукових статей, значну частину з яких складають напрацювання саме в галузі права. Доцільно згадати окремих науковців, праці яких було досліджено нами в межах підготовки цієї статті.

Так, доктор юридичних наук Бєлєвцева В.В. відзначає деякі особливості правового режиму інформаційних ресурсів [2]. Розкрита нею проблематика певною мірою є подібною до проблематики, що існує у сфері забезпечення інформаційної безпеки, зокрема, в частині незавершеності формування законодавчої бази, що забезпечує правове регулювання відповідної сфери.

Перун Т.С. розкрив особливості адміністративно-правового механізму забезпечення інформаційної безпеки України [3]. Огляд розкритої ним проблематики виявився доцільним в контексті індуктивного дослідження особливостей і проблем правового регулювання у сфері забезпечення інформаційної безпеки України.

Турчак А.В. комплексно оглядає механізми забезпечення інформаційної безпеки України як складової державної безпеки України [4]. Відповідні напрацювання були використані при дедуктивному дослідженні особливостей і проблем правового регулювання у сфері забезпечення інформаційної безпеки України.

Водночас, проблематика саме правового режиму забезпечення інформаційної безпеки України невиправдано залишається поза увагою переважної більшості науковців.

Метою статті є розкриття конституційних особливостей правового режиму забезпечення інформаційної безпеки України і визначення відповідних конституційних засад, першочергових кроків у реформуванні правового режиму.

Виклад основного матеріалу. Правовий режим (від лат. regimen – "управління, керівництво") – певна сукупність юридичних засобів, способів, що застосовуються в певній сфері суспільних відносин та забезпечують дію механізму правового регулювання. Правовому режиму притаманні певні особливості:

1) він встановлюється законодавством та забезпечується примусовою силою держави;

2) він є специфічним порядком правового регулювання, що складається із сукупності юридичних засобів, спрямованих на досягнення певної мети, й характеризується певним їх співвідношенням;

3) правовий режим особливим чином регламентує певні сфери суспільних відносин, виділяючи суб'єктів та об'єкти права;

4) в основу правового режиму покладено той чи інший спосіб правового регулювання – заборону, дозвіл чи позитивне зобов'язання [5, с. 716-717].

Із вищевикладеного можливо встановити такі чотири відповідні базові умови функціонування будь-якого правового режиму:

1) наявність належної законодавчої бази, якою закріплюється відповідний правовий режим, а також ефективного апарату державного примусу, яким такий правовий режим забезпечується;

2) юридичні засоби, застосовувані в межах запровадженого правового режиму, у своєму співвідношенні мають бути спрямовані на досягнення конкретної мети;

3) чітке виокремлення суб'єктів і об'єктів, взаємодія яких регулюється правовим режимом;

4) коректно обрані й пристосовані до цілей правового режиму способи (засоби) правового регулювання.

При цьому важливо відзначити, що серед перерахованих чотирьох умов перша є об'єднувальною відносно інших трьох. Тобто, відповідна мета, співвідношення і порядок застосування юридичних засобів правового режиму мають бути встановлені законодавством. Виокремлення суб'єктів і об'єктів, що взаємодіють в межах правового режиму, також здійснюється законодавчо. І закріплення способів (засобів) правового регулювання, які належить застосовувати в межах правового режиму, також здійснюється законодавчо.

Загальна ж непорушність функціонування запроваджених механізму правового регулювання, правового режиму забезпечується апаратом державного примусу. Втім, прикметно, що і порядок функціонування апарату державного примусу встановлюється законодавством.

Відтак, саме з огляду на первинну і об'єднувальну роль законодавства у питанні функціонування будь-якого правового режиму, дослідження правового режиму забезпечення інформаційної безпеки України доцільно розпочати із основоположного нормативно-правового акту України – Конституції України.

Системне дослідження норм Конституції України дозволяє дійти висновку, що вже на рівні Основного закону законодавцем закріплено ряд положень, що зумовлюють істотні особливості правового режиму забезпечення інформаційної безпеки України.

Так, стаття 1 Конституції України встановлює: "Україна є суверенна і незалежна, демократична, соціальна, правова держава". Стаття 3 Конституції України встановлює: "Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в

Україні найвищою соціальною цінністю". Водночас, частина 1 статті 17 Конституції України визначає: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу" [1].

На перший погляд може спостерігатись певна колізія між положеннями статтей 1, 3 Конституції України з одного боку і положеннями статті 17 Конституції України – з іншого.

Така колізія може вбачатись у тому, що найважливішими функціями держави визначено забезпечення безпеки самої держави, попри те, що найвищою соціальною цінністю в Україні є людина.

Втім, важливо підкреслити, що людина визнається в Україні найвищою соціальною (!) цінністю. Водночас, першою ознакою держави – України у ст. 1 Конституції України законодавець називає суверенність, другою – незалежність.

Першочерговою умовою збереження Україною суверенності і незалежності, беззаперечно, є належне забезпечення національної безпеки. При цьому вже самою Конституцією України додатково згадано такий компонент національної безпеки як інформаційна безпека, що надає її забезпеченню певний пріоритет, особливе значення.

Співвідношення пріоритетів забезпечення національної (в т.ч. інформаційної) безпеки і соціальних цінностей можливо чітко простежити на прикладі ряду статей Конституції України, якими гарантуються соціальні права і свободи.

Так, стаття 32 Конституції України передбачає заборону на втручання в особисте і сімейне життя людини; стаття 34 Конституції України закріплює право кожного на свободу думки і слова; стаття 36 Конституції України встановлює право громадян України на свободу об'єднання у політичні партії та громадські організації; стаття 39 Конституції України гарантує право громадян на мирні збори; статтею 44 Конституції України передбачено право працюючих на страйк.

Разом з тим, положення кожної із зазначених статей (32, 34, 36, 39, 44) Конституції України містять вказівку на можливість обмеження гарантованого відповідною статтею права. Перелік причини, з яких допускаються відповідні обмеження, не є ідентичним для зазначених статей, водночас, він завжди містить вказівку на інтереси національної безпеки України як на такі, що можуть стати причиною обмеження гарантованого Конституцією України права.

Відповідно, при такому взаємному співставленні положень Конституції України можна дійти висновку, що людина визнається в Україні найвищою соціальною (!) цінністю, а суверенність і незалежність – найвищою цінністю взагалі. І Основний закон неухильно слідує такому співвідношенню пріоритетів, дозволяючи державі відступати від ряду даних людині та громадянину гарантій, якщо цього вимагають інтереси національної безпеки.

Таким чином, у відповідності до вимог норм Конституції України при правовому регулюванні в державі найвищий пріоритет належить збереженню суверенітету і незалежності України. Водночас, реалізація цього пріоритету повинна здійснюватись не "будь-якою ціною", а в межах і у способи, які відповідають цілям і засадам демократичної, соціальної, правової держави. Тобто, наявність функції держави із вищим пріоритетом не виключає інші її функції та необхідність їх виконання.

Викладене дозволяє нам встановити одразу дві взаємопов'язані особливості правового режиму забезпечення інформаційної безпеки України, зумовлені Конституцією України:

1) найвища пріоритетність розвитку такого правового режиму;

2) необхідність забезпечення збалансованості такого правового регулювання, яка убезпечить інші пріоритети, встановлені Конституцією України, від утискання.

За таких обставин, оптимальним рішенням для задоволення вимог Конституції України є формування збалансованого правового режиму забезпечення інформаційної безпеки України. У межах такого правового режиму імперативні засоби правового регулювання мають поєднуватись із диспозитивними, рекомендаційними, заохочувальними.

Окремо слід зазначити, що XXI століття стало добою безпрецедентного технологічного розвитку людства у сфері зв'язку та комп'ютерних технологій. Безліч стратегічних процесів, пов'язаних із життєдіяльністю людини сьогодні нерозривно пов'язані із мережею Інтернет, яка продовжує свій стрімкий розвиток, як і її інфраструктура, супутні ринки технологій та послуг.

Як наслідок, ми є свідками небаченого раніше розширення можливостей доступу людини до інформації. Так, за даними Міжнародного союзу електрозв'язку, станом на кінець 2018 року доступ до мережі Інтернет мало близько 4-х мільярдів осіб, і це число невпинно зростає.

Ця обставина ставить під гострий сумнів ефективність заходів імперативного впливу в інформаційних правовідносинах, адже в реаліях сучасної правової держави повністю ізолювати людину від негативного інформаційного впливу просто неможливо. Як неможливо забезпечити інформаційну безпеку і силами самої лише держави.

У ч. 1 статті 17 Конституції України цілком логічно і виправдано зазначено, що забезпечення інформаційної безпеки України є не лише функцією держави, а й справою всього українського народу. Тобто сам законодавець на рівні основного закону заклав ідею про те, що забезпечення інформаційної безпеки має здійснюватись силами всього українського суспільства.

Таким чином, можемо назвати ще одну особливість правового режиму забезпечення інформаційної безпеки України: він повинен гарантувати можливість залучення до забезпечення інформаційної безпеки всього українського суспільства.

При цьому відомо, що добровільна діяльність особи завжди є більш результативною порівняно із примусовою. Усвідомлення цього факту свого часу стало одним із ключових факторів, що підштовхнув держави до відмови від рабовласницького/кріпацького устрою.

Відповідно, залучення народу, громадянського суспільства до справді ефективної діяльності із забезпечення інформаційної безпеки України можливе винятково за умови застосування для цього неімперативних засобів правового регулювання.

Базовими кроками для залучення до забезпечення національної, в тому числі інформаційної, безпеки України українського суспільства можуть бути зокрема такі:

– створення добровільних державних програм заохочення і підтримки фізичних та юридичних осіб, які беруть участь у забезпеченні інформаційної безпеки України (беруть участь у здійсненні національної пропаганди, піднятті внутрішнього і світового авторитету України, у провадженні правового виховання і правової пропаганди тощо);

– уповноваження компетентного суб'єкта(-ів) державної влади на організацію правового виховання, правової пропаганди серед усіх верств населення;

– організація, розширення і поглиблення міжнародної співпраці щодо обміну досвідом забезпечення інформаційної безпеки, протидії інформаційній агресії.

Повторно підкреслимо, що жоден із пропонованих кроків не може бути реалізований засобами, що притаманні імперативному методу правового регулювання.

Це наштовхує нас на висновок про те, що формування збалансованого правового режиму забезпечення інформаційної безпеки України є критичною умовою для ефективного забезпечення національної, в тому числі інформаційної, безпеки України.

Водночас, системний аналіз законодавства України дозволяє встановити, що нормативно-правове забезпечення діяльності держави, її взаємодії із суспільством у сфері забезпечення інформаційної безпеки України залишається на вкрай низькому якісному рівні.

Так, національна система законодавства не дозволяє чітко встановити ані мету і поточні завдання забезпечення інформаційної безпеки України, ані суб'єктів владних повноважень, уповноважених на діяльність у відповідній сфері, ані засоби правового регулювання, які дозволили б забезпечити належний і збалансований правовий вплив на відповідні правовідносини.

Нами в межах цієї статті вже було встановлено, що законодавче забезпечення відіграє первинну і об'єднувальну роль при формуванні правового режиму і забезпеченні дії механізму правового регулювання. Відповідно, формування в Україні належного нормативно-правового підґрунтя забезпечення інформаційної безпеки залишається ключовою умовою, пріоритетним кроком для запровадження ефективного правового режиму забезпечення інформаційної безпеки України.

Висновки.

Умовою ефективного правового регулювання у сфері забезпечення інформаційної безпеки України є формування збалансованого правового режиму, яким буде визначено конкретну мету і завдання правового регулювання у сфері забезпечення інформаційної безпеки України, виокремлено суб'єктів і об'єктів відповідного правового регулювання, врегульовано їх взаємодію, закріплено способи (засоби) правового регулювання, пристосовані до цілей правового режиму.

Розбудова відповідного правового режиму має здійснюватись на засадах, передбачених Конституцією України, ключовими з них є такі:

1) найвища пріоритетність розвитку правового режиму забезпечення інформаційної безпеки України;

2) необхідність забезпечення такої збалансованості правового режиму інформаційної безпеки України, яка убезпечить інші пріоритети, встановлені Конституцією України, від утискання;

3) правовий режим інформаційної безпеки України повинен гарантувати можливість залучення до забезпечення інформаційної безпеки всього українського суспільства.

Як видно з наданого нами матеріалу, такі засади є взаємозумовленими і взаємопов'язаними, а відтак – мають комплексно враховуватись при реформуванні правового режиму забезпечення інформаційної безпеки України.

З метою додержання вимог Конституції України в межах відповідного правового режиму доцільно передбачити взаємоузгоджене застосування як засобів правового регулювання, що відповідають імперативному методу правового регулювання, так і тих, що відповідають диспозитивному, рекомендаційному, заохочувальному методам.

При цьому першочерговим кроком (умовою) ефективного реформування правового режиму забезпечення інформаційної безпеки України залишається формування належної нормативно-правової бази. Відповідна система нормативно-правових актів має бути доопрацьована для забезпечення системності, узгодженості та повноти правового регулювання у сфері забезпечення інформаційної безпеки України.

Додатково слід зазначити, що правовий режим забезпечення інформаційної безпеки України повинен бути пристосованими не лише до викликів сучасності, а й до потенційних загроз інформаційній безпеці України.

Використана література

1. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Бєлєвцева В.В. Правовий режим інформаційних ресурсів. URL: http://ippi.org.ua/sites/default/files/11bvvrir.pdf

3. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні. URL: http://ena.lp.edu.ua/bitstream/ntb/45453/3/dysertaciya_na_zdobuttya_naukovogo_stupenya_kandydata_yurydychnyh_nauk_peruna_t.s.pdf

4. Турчак А.В. Механізми забезпечення інформаційної безпеки як складової державної безпеки україни. URL: https://ipk.edu.ua/wp-content/uploads/2020/04/dis-Turchak.pdf

5. Великий енциклопедичний юридичний словник; за ред. акад. НАН України Ю.С. Шемшученка. 2-ге вид., перер. і доп. Київ: Вид-во "Юридична думка", 2021. 1020 с.

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

УДК 343.983

КОВАЛЬЧУК Н.А., головний судовий експерт Центру спеціальних та судових експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.

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

АКТУАЛЬНІ ПИТАННЯ ЩОДО ВЖИВАННЯ ТЕРМІНОСПОЛУК У ВИСНОВКАХ ЕКСПЕРТА (ЗА МАТЕРІАЛАМИ ЕКСПЕРТИЗ ВІДЕО-, ЗВУКОЗАПИСУ)

Анотація*. У статті наведено тлумачення найуживаніших термінів і термінологічних сполук, подано практичні рекомендації щодо унормування варіантності термінів, що стане корисним експертам під час аналізу результатів та укладання висновку експерта.*

Ключові слова: *висновок експерта, терміни та термінологічні сполуки, тлумачення, калька, штамп.*

Summary*. The article provides an interpretation of the most commonly used terms and terminological components, provides practical recommendations for standartization of variance of terms, which will be useful to experts when analyzing the results and preparing expert conclusions.*

Keywords*: expert conclusion, terms and terminological components, interpretation, tracing paper, stamp.*

Аннотация. *В статье приведено описание часто употребляемых терминов и терминологических соединений, предоставлены практические рекомендации по поводу нормирования вариантности терминов, которые будут полезны экспертам в процессе анализа результатов и формулирования выводов эксперта.*

Ключевые слова: *вывод эксперта, термины и терминологические соединения, толкование, штамп.*

Постановка проблеми. У процесі дослідження експертові не тільки необхідно проникнути в суть самої комунікації, виявити характерні сталі ознаки усного мовлення певного диктора, належно оцінити їх, а також необхідно точно відображати результати проведеного дослідження і не допускати різних тлумачень найуживаніших термінів і терміносполук під час оформлення та укладання висновку експерта. Висновки повинні точно відображати результати проведеного дослідження і не допускати різних тлумачень.

Результати аналізу наукових публікацій. Питання добору нормативного терміна на сьогодні відзначається особливою актуальністю. Чимало дослідників вказують на те, що в мові офіційно-ділового стилю необхідно уникати двозначності терміна в межах однієї терміносистеми або субтерміносистеми. Проблему унормування термінології неодноразово описували українські дослідники [1 – 3], зокрема О. Тараненко, І. Кочан, Л. Василькова, Т. Лепеха.

Уніфікація термінології стосується усіх галузей знань і потребує чималих зусиль з боку і філологів, і фахівців певної галузі.

Вирішення питань структуризації термінології в аспекті уникнення варіантності дозволить підвищити якість і ефективність експертиз, сприятиме зменшенню кількості спірних моментів, а самим експертам дасть можливість звертатись під час оформлення результатів досліджень усного мовлення і матеріалів звуко-, відеозаписів до конкретного джерела.

Метою статті є вдосконалення професійної майстерності експертів, поліпшення якості та обґрунтованості їх висновків.

Виклад основного матеріалу. Іноді, під час укладання висновків, виникають суперечливі питання, які саме терміни та термінологічні сполуки доцільніше вживати, щоб чітко передати зміст. Висновки експерта повинні бути зрозумілими, повними, конкретними, повинні точно відображати результати проведеного дослідження і не допускати двозначних тлумачень. Яке слово вибрати?

Одним із виявів досконалого володіння мовою є вибір доречного, найбільш слушного в тому чи іншому випадку слова.

Досить часто плутають слова *виняток* і *виключення***,** а також похідні від них *винятковий* і *виключний***.**

У вислові *цей випадок не складатиме виключення* останнє слово недоречне, бо *виключення* означає "усування, унеможливлення, припинення дії". Коли йдеться про відхилення від чогось узвичаєного, слід уживати слово *виняток*, похідне від якого *винятковий* означає "особливий, надзвичайний". Тож правильно: *цей випадок не становитиме винятку*. Відповідно: *виняткові умови, винятковий випадок* тощо.

У свою чергу К. Городенська зазначає, що словосполука *не виключено, що…* – це дослівний переклад російського *не исключено, что…* Наголошує, що ним послуговуються деякі автори для вираження значення можливості, імовірності чого-небудь, припущення на тлі того, що вже гарантоване, реальне. Чи можна уникнути цієї кальки в українській мові? Звичайно, можна. Замість неї пропонує вживати словосполуки: *цілком можливо, що…; цілком імовірно, що…; припускають, що…; сподіваються, що… та ін.* [3, с. 60].

Під час укладання висновку експерта досить часто виникає запитання, яке формулювання правильно вжити: *доля чи частка (секунди)? Доля* – напрям життєвого шляху, талан; частка – частина чогось [2, с. 315]. Російські вислови перекладаються: *делить на равные доли* – ділити на рівні частини; *доля истины* – частка правди (істини); *судьба* – доля; *доля секунды* - частка секунди [11, с. 182]. Отже, правильно – частка секунди.

Також у експертів під час формулювання відповідей висновку постає питання, який термін доречно вжити: *імовірно* чи *ймовірно***.**

Імовірно - ймовірно – споріднені слова. *Імовірний/ймовірний* **–** той, що його можна тільки припустити, можливий (допустимий) [2, с. 500].

Для правильного написання необхідно послуговуватись правилами евфонії (милозвучності). "І" вживається, щоб уникнути збігу приголосних, важких для вимови: а) після приголосного або паузи, що на письмі позначається крапкою, комою, крапкою з комою, двокрапкою, перед словами з початковим приголосним звуком; б) на початку речення. Взагалі це правило поширюється для сполучників, але так само чергується початковий ненаголошений "і" з "й" у словах: *імовірний – ймовірний, іти – йти, ідеться – йдеться.*

Наприклад: "*можна зробити висновок про те, що усне мовлення особи з умовним індексом Д, яке міститься на досліджуваній сигналограм**і**, **й**мовірно (на досліджуваних сигналограма**х**, **і**мовірно) належить громадянину…".*

Актуальним є і добір таких терміносполук:

- *можна зробити висновок чи можливо зробити висновок*

можна – є умови, можливості для здійснення чого-небудь; дозволяється, дозволено [2, с. 629];

можливо – допустимо, може здійснитися; уживається для вираження припущення чого-небудь; вірогідність, імовірність, ірреальний, припущення; той, що його можна тільки припустити, *можливий* [2, с. 629].

Наприклад: *"*можна *зробити висновок", "*можна *відзначити високу збіжність формантної структури", "дикторський склад кожної з розмов по суті справи,* можливо, *складається з двох співрозмовників"*;

- *приймати чи брати (участь, до уваги):*

правильно – *брати участь або брати до уваги*, адже приймати ви можете когось або щось – ліки, друзів, папери, та тільки не участь, увагу.

Враховуючи зазначене, вважаємо за доцільне послуговуватись у висновках таким словосполученням: "Гр. ...*бере участь* у розмові…";

- *приймати чи уживати (уживати (вживати) заходів):*

правильно – *уживати (уживати (вживати) заходів),* нерідко доводиться чути і читати *вживати заходи* (помилка у виборі відмінка), у гіршому разі – *приймати міри;*

- *завідомо* чи *свідомо (неправдивий висновок):*

у мові українського законодавства узвичаївся штамп *завідомо неправдивий висновок (неправдиві свідчення/показання).* А став цей штамп звичним тому, що він є буквальним перекладом російського *заведомо неправдивый вывод (ложные свидетельства/показания).* Українською мовою його значення правильно передати як *свідомо неправдивий висновок (неправдиві свідчення/показання);*

- *свідомо,* прис. до *свідомий* – зроблений, заподіяний з певним наміром, навмисно; ужитий з певним наміром, з певною метою [2, с. 1297].

Зважаючи на зазначене вище, вважаємо, що у висновках правильно використовувати словосполучення: *свідомо неправдивий висновок (неправдиві свідчення/показання).*

- *рахувати чи вважати:*

вважати – мати свою думку, *рахувати* – займатися підрахунками чогось, лічити – послідовно називати цифри. Наприклад: *вважаємо за доцільне*;

- *строк чи термін:*

здавалося б, яка різниця – застосовувати слово *строк* чи *термін*? На сьогодні вирізняють два терміни, що свідчать про тривалість діяння: *строк* чи *термін*.

Строком є певний відрізок часу, зі спливом якого пов'язана дія чи подія, яка має юридичне значення.

Терміном є певний момент у часі, з настанням якого пов'язана дія чи подія, яка має юридичне значення [2, с. 1412, 1444].

Стаття 252 ЦК України містить наступні норми щодо визначення *строку* та *терміну*: *строк* визначається роками, місяцями, тижнями, днями або годинами, а *термін* – календарною датою або вказівкою на подію, яка має неминуче настати [14].

Тобто, говорячи простою мовою, *строк* – це період, після завершення якого процес закінчився, а *термін* – це момент початку якоїсь дії або події.

Наприклад: "*строк* дії договору – 2 роки з моменту підписання"; "*термін* виконання – 12.12. 2021"; "стосовно даної експертизи повідомляємо, що у разі неотримання у місячний *строк* зазначених матеріалів, експертизу буде виконано

відповідно до обсягу наданих експертам матеріалів";

- *продовжується чи триває дослідження:*

перевага надається не слову *продовжуватися* (калька з рос. "продолжаться"), а перевага надається укр. *тривати*, коли йдеться про вимір у часі: *дослідження (робота, розслідування) триває;*

- *вірна чи правильна відповідь:*

верный (рос. м.) – вірний, щирий, правильний, неминучий [11, с. 69];

правильний – коли йдеться про той, який відповідає дійсності, істинний; який відповідає встановленим правилам, нормам; безпомилковий. Отже правильна думка, відповідь;

спірний (відданий, незрадливий) помічник, друг; вірний, надійний, певний спосіб; неминуча поразка [2, с. 1789, 1100].

У висновках експерта варто послуговуватись: "персоніфікацію дикторів розпізнано *правильно*", "зміст розмови загалом встановлено *правильно*";

- *обробка чи опрацювання (даних, статті):*

у Великому тлумачному словнику сучасної української мови зазначається: *обробка* – дія за значенням обробляти [2, с. 824]; *обробка даних* – систематична цілеспрямована послідовність дій над даними; *автоматизована обробка даних* – обробка даних, що виконуються автоматичними даними; *опрацювання* – дія за значенням опрацювати, опрацьовувати [2, с. 858]; *опрацювання статті, тексту* – глибоко вивчати, докладно ознайомлюватися; покращувати якість, надавати викінченості, досконалості. Вважаємо за доцільне використовувати у висновках експерта: "цифрова *обробка*", "програма аналізу та *обробки* сигналів", "після *опрацювання* наданих на дослідження матеріалів";

- *присвоювати чи надавати (назву, номер, ім'я):*

присвоювати – у системах обробки інформації: а) операція зміни значення змінної, регістра або ін. елемента даних; б) надання пристрою або ін. ресурсу імені, за яким до них можуть звертатися програми;

коли мовиться про те, що комусь дано ордени чи якісь права, слід послуговуватись дієсловом *надати (надавати).*

Зважаючи на вищевказане, пропонуємо під час написання висновків послуговуватись: "*присвоєння* інвентарного номера", "формат імен експериментальних файлів, які *присвоюються* апаратом цифрового запису".

В офіційно-діловому вжитку, особливо в мові українського законодавства, узвичаївся штамп *приводити/привести щось у відповідність із чим-небудь (до чого-небудь).* А став цей штамп звичним тому, що він є буквальним перекладом російського *приводить/привести что-либо в соответствие с чем-нибудь.* Українською мовою його значення правильно передати як *узгоджувати/узгодити що-небудь із чимось,* напр.: *документ* рекомендовано *узгодити з нормами чинного законодавства.*

Отже, замість *приводити/привести щось у відповідність із чим-небудь (до чого-небудь)* потрібно *вживати узгоджувати/узгодити що-небудь із чимось.*

Також звертаємо увагу, що в різноманітних словосполученнях українська мова має неоднакові відповідники: "положительный (отрицательный) вывод" – позитивний (негативний) висновок, "положительный (отрицательный) отзыв" – позитивний (негативний) відгук, "положительный (отрицательный) ответ" – ствердна (заперечна) відповідь.

Поділяємо думку К. Городенської не вживати "*під цим розуміється…*", "*мається на увазі…*". Вона зазначає, що у наукових текстах, коли автор з'ясовує суть

використовуваного поняття чи терміна, іноді читаємо: *під суржиком розуміється…; під суржиком мається на увазі…*

В українській мові, на противагу російській, авторське застереження не можна виражати безособовими формами дієслів *розуміється* або *мається* (у словосполуці мається на увазі). Замість них потрібно вживати дієслова *визначати, тлумачити, витлумачувати, називати, кваліфікувати, трактувати* та ін. у формі 1-ої особи множини чи однини теперішнього часу. Коли ж треба повідомити про усталене трактування якогось поняття в певній галузі знань, то названі дієслова потрібно вживати у формі 3-ї особи множини теперішнього часу або у формі множини минулого часу [3, с. 70].

Наприклад: трактуємо (трактую), визначаємо (визначаю), називаємо (називаю) як…, кваліфікуємо (кваліфікую) як…, витлумачуємо (витлумачую) як…; трактують (трактували), визначають (визначали), називають (називали)…, кваліфікують (кваліфікували) як…, витлумачують (витлумачували) як…

Звертаємо увагу на використання в офіційно-діловому мовленні слів *скасувати чи відмінити.*

Великий тлумачний словник сучасної української мови подає: *скасовувати* (недок.), *скасувати* (док.) – а) визнавати, оголошувати що-небудь недійсним, незаконним; анулювати; б) те саме, що ліквідувати [2, с. 1328]; *відміняти, відмінювати* (недок.) *відмінити* (док.) – робити кого-, що-небудь інакшим; змінювати [2, с. 174].

Заходи скасовують або повідомляють про перенесення їх на інший день, а документи, що не відповідають за змістом чи формою чому-небудь, скасовують або анулюють.

Зокрема, на думку К. Городенської, українською мовою правильно вживати: *скасувати* виставу (засідання); *перенести на іншу дату* виставу (засідання); *скасувати* постанову (наказ, закон, акт); *анулювати* постанову (наказ, закон, акт) [3, с. 49].

Висновки.

Дотримання запропонованих рекомендацій сприятиме правильному використанню найуживаніших термінів і термінологічних сполук під час аналізу результатів та формулювання форм висновку експерта.

Оптимізація цієї ділянки роботи дозволить експертам різного ступеню підготовки уникнути можливих помилок.

Ця робота на сьогодні є актуальною і потрібною для практичного застосування, оскільки уніфікує й систематизує експертний досвід у галузі дослідження усного мовлення і матеріалів звуко-, відеозаписів.

Використана література

1. Василькова Л. Лексика на позначення правових відносин: зб. наук. праць *Українська термінологія і сучасність.* 2001. Вип. IV. С. 36-38.

2. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В.Т. Бусел. Київ, 2005. 1728 с.

3. Городенська К.Г. Українське слово у вимірах сьогодення. Київ, 2014. 124 с.

4. ДСТУ 2737-94. Записування і відтворення інформації. Терміни і визначення. – (Чинний від 1995-07-01). Київ: Держстандарт України, 1994.

5. Про судову експертизу: Закон України від 25.02.94 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення 21.05.2021).

6. Кочан І. Варіанти і синоніми термінів з міжнародними компонентами. *Вісник Нац. ун-ту "Львівська політехніка". Серія "Проблеми української термінології"*. № 620. 2008. С. 14-19.

7. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. URL: https://zakon.rada. gov.ua/laws/ show/4651-17 (дата звернення 21.05.2021).

8. Лепеха Т. Лексико-семантичні особливості термінів судово-медичної експертизи: зб. наук. праць *Українська термінологія і сучасність*. 1998. Вип. VII. С. 141-145.

9. Методика криміналістичного дослідження матеріалів і засобів звуко- та відеозапису. Київ: ДНДЕКЦ МВС України, 1998.

10. Методика ідентифікації особи за фонограмами російської мови на автоматизованій системі "Діалект"/ Н.Ф. Попов та ін.; за ред. А.В. Фісенка. М., 1996.

11. Новітній російсько-український словник / уклад. Л.П. Коврига. Харків, 2006, 1072 с.

12. Сегай М.Я. Методология судебной идентификации. Київ: РИО МВД Украины, 1970. 254 с.

13. Тараненко О. Нормативні тенденції в сучасній українській мові і явище варіантності: зб. наук. праць. *Українська термінологія і сучасність.* 2007. Вип. VII. С. 25-37.

14. Цивільний кодекс України: Закон України 16.01.03 р. № 435-IV. URL: https://zakon. rada.gov.ua/laws/show/435-15#Text (дата звернення 20.06.2021).

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

УДК 001.89

АЛЕКСЕЄВА О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6629-3606.

ПРАВОВІ АСПЕКТИ РЕЄСТРАЦІЇ ТА ОБЛІКУ НАУКОВО-ДОСЛІДНИХ І ДОСЛІДНО-КОНСТРУКТОРСЬКИХ РОБІТ В СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Анотація. *Стаття присвячена питанням здійснення реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт, виконуваних в сфері забезпечення національної безпеки держави, на прикладі Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України. Досліджуються правові підстави виконання заходів із зазначеної тематики. Аналізується наявний стан справ щодо порушеного питання.*

Ключові слова: *науковий потенціал, науково-технічна сфера, реєстрація науково-дослідних та дослідно-конструкторських робіт, національна безпека, законодавство.*

Summary. *The article is devoted to the issues of registration and accounting of research and development work performed in the field of national security, by the example of the Ukrainian scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine. The legal bases for actions on the specified subjects are investigated. The current state of affairs on the raised issue is analyzed. Some issues that arise during the registration procedure are highlighted.*

Keywords: *scientific potential, scientific and technical sphere, registration of research and development works, national security, legislation.*

Аннотация. *Статья посвящена вопросам осуществления регистрации и учета научно-исследовательских и опытно-конструкторских работ, выполняемых в сфере обеспечения национальной безопасности государства, на примере Украинского научно-исследовательского института специальной техники и судебных экспертиз Службы безопасности Украины. Исследуются правовые основания выполнения мероприятий по указанной тематике. Анализируется существующее состояние дел по данному вопросу.*

Ключевые слова: *научный потенциал, научно-техническая сфера, регистрация научно-исследовательских и опытно-конструкторских работ, национальная безопасность.*

Постановка проблеми. Недостатній рівень висвітлення у наукових джерелах питань щодо реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт (далі – НДДКР), зокрема виконуваних в сучасних умовах для забезпечення, у тому числі й національної безпеки держави, спонукає пропагувати антиформальне ставлення до процедури реєстрації та обліку НДДКР, аби уникати спотворення викладеної під час реєстрації та обліку відповідним чином оформленої інформації, яка є підґрунтям для всеукраїнських баз даних науково-технічних результатів, досягнення яких відбувається завдяки використанню здебільшого коштів держави. Крім того, ситуація, що склалася, змушує проаналізувати особливості здійснення процесу реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт, зокрема державної. При цьому, потребує уваги й розгляд наявних суперечностей.

Результати аналізу наукових публікацій. Питання розвитку науково-технічної сфери розглядали у своїх наукових працях такі науковці, як О.О. Скорик, Д.В. Смерницький, Й.С. Ситник, Г.В. Скиба та інші. Проте, на жаль, в їх дослідженнях

не достатньо приділино уваги питанням актуалізації процесу реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт, а також питанням, що виникають під час практичної реалізації зазначених заходів з метою належного виконання вимог відповідних нормативних документів з реєстраційної діяльності. Таким чином, не зайвим буде вкотре акцентувати увагу на тонкощах організації відповідної процедури реєстрації та обліку у вказаних межах, окремо зосередивши увагу на державній реєстрації та обліку відповідних робіт.

Метою статті є розгляд на базі аналізу наукових і практичних матеріалів та нормативно-правових актів стосовно реєстрації та обліку науково-дослідних і дослідно-конструкторських робіт особливостей організації діяльності з реєстрації та обліку НДДКР на прикладі Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України, а також деяких суперечливих питань вказаної діяльності.

Виклад основного матеріалу. Указом Президента України "Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" визначено поточні та прогнозовані загрози національній безпеці та національним інтересам України, джерела загроз незалежності України, її суверенітету і демократії тощо [1].

При цьому визначено, що пріоритетним завданням держави є захист прав, свобод і законних інтересів громадян України, який можливо забезпечити, у тому числі й завдяки використанню в умовах сьогодення новітніх (модернізованих) зразків спеціальних технічних засобів та спеціальної техніки, що використовуються оперативними підрозділами задля протидії зазначеним загрозам.

На жаль, постійний дефіцит фінансових ресурсів, вочевидь обумовлений обмеженістю та вичерпністю державного "гаманця", неабияк ускладнює виділення відповідних коштів для забезпечення закупівлі у необхідних обсягах сучасних зразків озброєння та військової техніки.

Усе вищезазначене "провокує" та в деякій мірі мотивує з подвійним завзяттям використовувати наявний науково-технічний потенціал країни, у тому числі "користуватися послугами" наукових установ, основна діяльність яких відповідно до статті 1 Закону України "Про наукову і науково-технічну діяльність" полягає у проведенні прикладних наукових досліджень і науково-технічних (експериментальних) розробок, що є основними видами науково-технічної діяльності, спрямованої на одержання та використання нових знань для розв'язання технологічних, інженерних тощо проблем в суспільстві, зокрема забезпечення безпеки як держави в цілому, так й кожного громадянина окремо [2].

Отже, з огляду на викладене, а також спираючись на визначення, викладене у статті 1 Закону України "Про наукову і науково-технічну діяльність", саме наукові (науково-дослідні тощо) установи є виконавцями науково-дослідних (далі – НДР), дослідно-конструкторських (далі – ДКР) та інших робіт.

Відповідно до положень Закону України "Про Службу безпеки України" від 25.03.92 р. № 2229-XII державним органом спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку країни, є Служба безпеки України, до складу якої входять у тому числі й навчальні, науково-дослідні та інші заклади, що забезпечують виконання обов'язків Служби безпеки України, покладених пунктом 15 статті 24 вказаного Закону, зі здійснення наукових досліджень та виконання дослідно-конструкторських робіт, а також впровадження їх результатів в практику діяльності Служби безпеки України [3].

Одним з таких підрозділів СБУ є Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (далі – ІСТЕ СБУ), який у взаємодії з підрозділами, органами, закладами СБУ та Штабом АТЦ при СБУ здійснює за рахунок коштів державного бюджету України відповідні заходи науково-технічної діяльності в системі Служби безпеки України, спрямовані на проведення науково-технічних розробок, виготовлення спеціальних технічних засобів та спеціальної техніки, проведення ремонтних і регламентних робіт, у тому числі виконання секретних НДДКР.

У цілому, ІСТЕ СБУ в рамках реалізації відповідних заходів з виконання науково-технічної діяльності на підставі нормативних актів Міністерства освіти та науки України, а також відомчих нормативних актів Служби безпеки України здійснює відповідні заходи стосовно:

- формування планових документів з виконання НДДКР для отримання наукових результатів, а також робіт за оперативно-технічними завданнями (далі – ОТЗ) [4];
- відомчий облік НДДКР та ОТЗ [5];
- державну реєстрацію та облік НДДКР [6; 7].

З метою розуміння тонкощів здійснення зазначених заходів має сенс більш детально розглянути кожну позицію наданого переліку.

Не є великою таємницею, що будь-яку діяльність, орієнтовану на отримання відповідних результатів бажано розпланувати задля, у тому числі, здійснення адекватного контролю з метою досягнення цілей її виконання та уникнення несподіваних (непрогнозованих) наслідків. Отже, виконавці науково-дослідних та дослідно-конструкторських робіт (ІСТЕ СБУ не виключення) мають також планувати свою науково-технічну діяльність з огляду на наявність відповідних потреб та кошторисних призначень на них, а саме складати відповідні тематичні плани щодо науково-технічної діяльності на відповідний період (зокрема, на поточний рік). За необхідності до цих планових документів під час виконання заходів, передбачених ними, за аргументованих причин різного характеру вносяться відповідні зміни та доповнення (щодо термінів виконання, назви, очікуваних результатів тощо) шляхом формування відповідних додатків. Подальша діяльність виконавців НДДКР розгортається саме в межах передбачених плановими документами заходів у сфері науково-технічної діяльності.

Одним із завдань, обов’язкових до виконання після фактичного початку заходів НДДКР, передбачених вищевказаними плановими документами, є здійснення процедури реєстрації та обліку відповідних робіт. Аналізуючи джерела у мережі Інтернет, можна дійти висновків, що виконавці НДДКР (здебільшого наукові установи, підпорядковані Міністерству освіти та науки України) задля вирішення організаційних питань стосовно здійснення діяльності, пов’язаної з процедурою реєстрації та обліку НДДКР, складають положення (порядки), в яких виписують алгоритм взаємодії відповідних підрозділів з метою якісного та своєчасного виконання цієї діяльності. Такі документи є в Центральноукраїнському національному технічному університеті, Східноєвропейському університеті ім. Р. Аблязова, Дніпропетровському національному університеті імені О. Гончара, ДП “ДержавтотрансНДІпроект” тощо.

Слід зауважити, що в СБУ також є документ аналогічного спрямування – Інструкція з організації централізованого обліку та реєстрації робіт науково-технічного спрямування в Службі безпеки України (далі – Інструкція), затверджена наказом Центрального управління СБУ від 29.09.15 р. № 638. На виконання вимог цієї Інструкції та здебільшого для уникнення дублювання тематик й шифрів НДДКР і ОТЗ ІСТЕ СБУ здійснює централізований (відомчій) облік усіх розпочатих НДДКР та ОТЗ (не залежно від обсягів та джерел фінансування на їх виконання), що відбувається наступним чином [5]:

- ведеться Єдиний електронний реєстр (далі – Реєстр), який формується кожного року після затвердження тематичного плану науково-технічної діяльності та складається з переліку нових до виконання у відповідному році робіт. До складу відомостей цього Реєстру входить, зокрема, обліковий номер відповідної роботи (номер відомчої реєстрації), який присвоюється на підставі планових показників виконання цієї роботи;

- складається узагальнена облікова картка кожної фактично завершеної роботи на підставі інформації з Реєстру та відомостей про закриття замовлення на виконання цієї роботи.

Терміни виконання вказаних заходів на підставі вимог Інструкції можна викласти у схематичному вигляді [4], див. Рис.1.

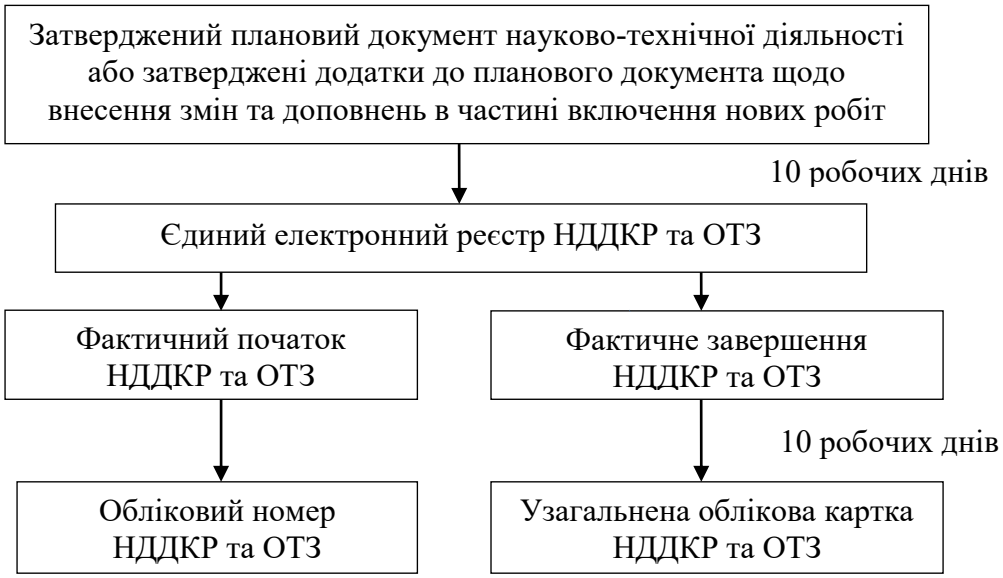


Рис.1. Терміни виконання основних заходів в межах відомчої реєстрації робіт науково-технічного спрямування

Зазначена Інструкція визначає порядок здійснення в СБУ централізованого обліку усіх (без винятку) робіт науково-технічного спрямування, у тому числі робіт за оперативно-технічними завданнями, що є роботами, які виконуються в один етап для створення і разового виготовлення науково-технічної продукції, потреба в якій зумовлена оперативною необхідністю, а також у випадках, пов’язаних із незначним (нескладним) доопрацюванням окремої науково-технічної продукції за специфікою (умовами) її використання за призначенням [4]. З огляду на необхідність унеможливлення дублювання робіт, виконання яких передбачено тематичними планами науково-технічної діяльності, надання кожній (без винятків) новій роботі облікового номеру є, звісно, слушним й, навіть, обов’язковим заходом. Стосовно необхідності складання узагальнених облікових карток є певні сумніви через те, що обумовлено це завдання лише Інструкцією. Але, як то кажуть здавна: “що написане пером, то не вирубаєш сокирою”. Отже, сьогодні вимоги Інструкції, у тому числі стосовно необхідності складання узагальнених облікових карток на всі роботи науково-технічного спрямування, що визначені до виконання відповідними тематичними планами науково-технічної діяльності, є чинними та мають бути виконані в повному обсязі. При цьому така обов’язковість змушує виконувати додатковий досить вагомий обсяг паперової праці, спрямованої на акумулюванні всієї інформації за відповідними НДДКР та ОТЗ, хоча більшість тих відомостей зберігається в окремих справах за відповідними роботами.

Крім того, ІСТЕ СБУ відповідно до своїх статутних положень виконує науково-дослідні та дослідно-конструкторські роботи, фінансування яких, як вже було зазначено, відбувається за рахунок державного бюджету України. Ця діяльність передбачає відповідно до статті 11 Закону України "Про науково-технічну інформацію", а також постанов Кабінету Міністрів України від 31.03.92 р. № 162 "Про державну реєстрацію науково-дослідних, дослідно-конструкторських робіт та дисертацій" (для відкритих НДДКР) та від 10.03.94 р. № 155 "Про державний облік засекречених науково-дослідних, дослідно-конструкторських розробок і дисертацій" здійснення взаємодії з уповноваженим органом, а саме державною науковою установою "Український інститут науково-технічної експертизи та інформації" (далі – УкрІНТЕІ).

Вказана взаємодія відбувається шляхом формування ІСТЕ СБУ як виконавцем науково-дослідних та дослідно-конструкторських робіт, відповідних комплектів документів та надсилання їх до УкрІНТЕІ з метою присвоєння роботам, щодо яких складено ті документи, відповідних державних номерів.

Зазначена діяльність в залежності від грифа секретності НДР (ДКР) відбувається з деякими відмінностями, а саме.

- для НДР (ДКР) з грифом секретності "нетаємно" та "для службового користування" відповідно до вимог Порядку державної реєстрації та обліку відкритих науково-дослідних, дослідно-конструкторських робіт і дисертацій, затвердженого наказом Міністерства освіти та науки України від 27.10.08 р. № 977;

- для НДР (ДКР) з грифом секретності "таємно" відповідно до вимог Порядку державного обліку секретних науково-дослідних, дослідно-конструкторських робіт і дисертацій, затвердженого наказом від 09.06.09 р. № 494.

Відповідно до вимог Порядків до УкрІНТЕІ з метою достовірного та повноцінного висвітлення стану виконання та витрачання коштів державного бюджету України на відповідну роботу науково-технічного спрямування мають надходити такі матеріали:

- реєстраційна картка;

- облікова картка (висвітлює відомості стосовно виконання окремого етапу роботи або виконання роботи в цілому);

- інформаційна картка.

Узагальнюючи вищевикладену інформацію, хронологію подій щодо кожної НДДКР, яка має бути зареєстрована та облікована в УкрІНТЕІ, можна представити у вигляді наступної схеми [5; 6], див. Рис 2.

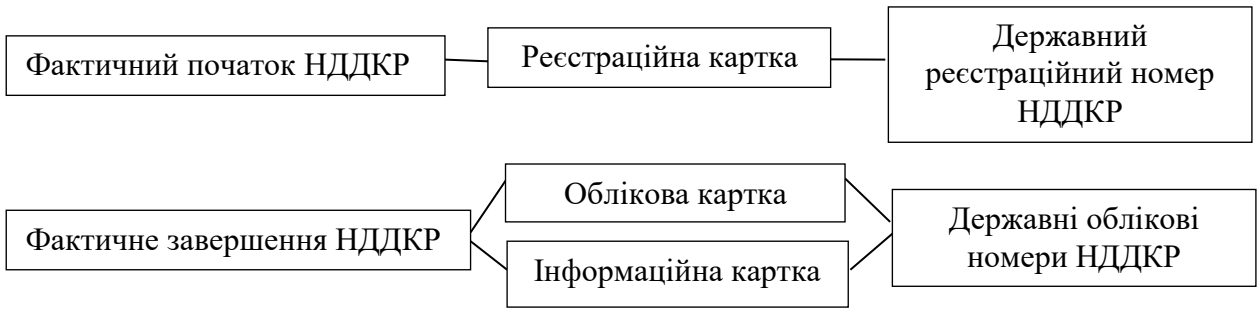


Рис. 2. Послідовність виконання основних заходів в межах державної реєстрації робіт науково-технічного спрямування

Слід зазначити, що надання в обумовлені Порядками строки вищевказаних карток, складених за формами, визначеними УкрІНТЕІ, може відбуватися у різний спосіб залежно від грифу секретності НДР (ДКР), див. Рис. 3.

Рис. 3. Способи надсилання документів до УкрІНТЕІ

Має сенс детальніше зупинитися на деяких питаннях з практики оформлення відповідних матеріалів, що виникають під час їх підготування.

Не можна не погодитися з Д.В. Смерницьким, який у своєму дослідженні звернув увагу на неоднозначність сприйняття поняття “власні кошти” під час визначення обов’язковості здійснення державної реєстрації та обліку науково-дослідних та дослідно-конструкторських робіт. Особливо це визначення, наведене у пунктах 1.4 Порядків, спантеличує по відношенню до державних установ, які виконуючи певну науково-технічну діяльність, заробляють певні кошти, й, звичайно, хотіли б вважати їх власними. Проте не зрозуміло, якою мірою отримані кошти є власними, адже роботи в рамках науково-технічної діяльності виконуються у приміщеннях, що є державною власністю, а співробітники цих установ отримують за свою працю з того ж приводу заробітну платню з державного “гаманця”. Крім того, слушною є думка Д.В. Смерницького про доцільність державної реєстрації та обліку всіх НДДКР, що забезпечить максимальне наповнення інформаційних баз даних щодо результатів науково-технічної діяльності [8].

Разом з цим, під час складання реєстраційно-облікових матеріалів маємо не зовсім однозначне визначення поняття підстави для проведення НДР (ДКР), де з переліку відповідей маємо обрати одну, що поміж інших є згадане вище поняття “власні кошти” та “договір з міністерством, іншим центральним органом влади”. Адже в сфері створення спеціальних технічних засобів та спеціальної техніки, як й в будь-якій іншій, виконавцем НДДКР може виступати підпорядкований замовнику підрозділ, який спроможний виконувати відповідні роботи на підставі вищезгаданих тематичних планів науково-технічної діяльності без складання відповідного договору.

Висновки.

В умовах сьогодення, існує потреба у створенні силами вітчизняних талантів сучасної конкурентоспроможної науково-технічної продукції, у тому числі й спеціальних технічних засобів та спеціальної техніки, які б дозволили гідно протистояти наявним викликам безпеці держави, зокрема кожного громадянина.

З огляду на вищевикладене, можемо дійти висновку, що відповідно до нормативно-правових актів як державного, так й відомчого рівня науково-технічна діяльність неодмінно пов’язана з процедурою реєстрації та обліку науково-дослідних та дослідно-конструкторських робіт, у тому числі державних. Потреба щодо цього обґрунтована не тільки обов’язковістю виконання вимог певних нормативних документів, а й необхідністю наповнення відповідних інформаційних баз з порушеного питання. Саме здійснення зазначеної реєстрації створює умови для уникнення дублювання НДДКР та відповідно ірраціонального витрачання, особливо державних, коштів.

Аналізуючи стан справ щодо державної реєстрації та обліку науково-дослідних та дослідно-конструкторських робіт, бачимо певні суперечливості щодо неоднозначності

розуміння деяких понять під час оформлення реєстраційно-облікових документів. Можливо, ці непорозуміння, не є, на щастя, глобальними, але прикро, коли їх наявність загальмовує процес державної реєстрації через витрачання певних зусиль та часу на з'ясування "істини".

Проте, незважаючи на певні питання, що виникають в тлумаченні деяких понять під час реєстрації робіт, виконувати цю працю потрібно, бо "те, що нас не вбиває, робить нас міцнішими", більш мотивованими та рішучими для виховання відповідального, деякою мірою майстерного, ставлення до підготовки відповідних матеріалів під час здійснення зазначеної роботи.

Більш того, вочевидь, що без відповідності оформлених бланків реєстраційних, облікових, інформаційних карток вимогам вищевказаних Порядків в УкрІНТЕІ робота не буде зареєстрована або буде зареєстрована з недостовірними даними. З метою унеможливлення спотворення реального висвітлення стану справ в науково-технічній сфері має сенс кожному, хто долучається до процесу, у тому числі реєстрації та обліку НДДКР, бути пильним, максимально відповідальним, а за необхідності ініціативним для обґрунтованого внесення змін (за необхідності доповнень) до відповідних нормативних актів, наприклад з означених вище питань задля удосконалення процесу реєстрації робіт науково-технічного спрямування, зокрема в сфері створення спеціальних технічних засобів та спеціальної техніки.

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 (дата звернення: 02.05.2021).

2. Про наукову і науково-технічну діяльність: Закон України від 26.11.15 р. № 848-VIII *Відомості Верховної Ради (ВВР).* 2016. № 3. Ст. 25. URL: https://zakon.rada.gov.ua/laws/show/848-19#Text (дата звернення: 02.05.2021).

3. Про Службу безпеки України: Закон України від 25.03.92 р. № 2229-XII. *Відомості Верховної Ради (ВВР).* 1992. № 27. Ст. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 02.05.2021).

4. Про затвердження Інструкції про порядок планування та проведення науково-технічних розробок, виготовлення спеціальних технічних засобів та спеціальної техніки, проведення ремонтних і регламентних робіт в Українському науково-дослідному інституті спеціальної техніки та судових експертиз Служби безпеки України: наказ Центрального управління СБУ від 25.03.21 р. № 100.

5. Про затвердження Інструкція з організації централізованого обліку та реєстрації робіт науково-технічного спрямування в Службі безпеки України: наказ Центрального управління СБУ від 29.09.15 р. № 638.

6. Про затвердження порядку державної реєстрації та обліку відкритих науково-дослідних, дослідно-конструкторських робіт і дисертацій: наказ Міністерства освіти та науки України від 27.10.08 р. № 977. URL: https://zakon.rada.gov.ua/laws/show/z0312-09#Text (дата звернення: 02.05.2021).

7. Про затвердження порядку державного обліку секретних науково-дослідних, дослідно-конструкторських робіт і дисертацій: наказ Міністерства освіти та науки України від 09.06.09 р. № 494. URL: https://zakon.rada.gov.ua/laws/show/z0606-09#Text (дата звернення: 02.05.2021).

8. Смерницький Д.В. Інформаційне забезпечення науково-технічної діяльності. URL: http://elar.naiau.kiev.ua/bitstream/123456789/1862/1/%D0%A1%D0%BC%D0%B5%D1%80%D0%BD%D0%B8%D1%86%D1%8C%D0%BA%D0%B8%D0%B9%20%D0%94.%20%D0%92.pdf (дата звернення: 09.05.2021).

9. Про науково-технічну інформацію: Закон України від 25.06.93 р. № 3322-XII. *Відомості Верховної Ради (ВВР).* 1993. № 33. Ст. 345. URL: https://zakon.rada.gov.ua/laws/show/3322-12# Text (дата звернення: 02.05.2021).

10. Про державну реєстрацію науково-дослідних, дослідно-конструкторських робі та дисертацій: Постанова Кабінету Міністрів України від 31.03.92 р. № 162. URL: https://zakon.rada.gov.ua/laws/show/162-92-%D0%BF#Text (дата звернення: 02.05.2021).

11. Ситник Й.С. Розвиток наукового потенціалу України як передумова інтелектуалізації економіки і менеджменту. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/23351/1/12-75-86.pdf (дата звернення: 09.05.2021).

12. Скорик О.О. Сутність та складові елементи науково-технологічного потенціалу держави. *Державне управління: удосконалення та розвиток*. – (Електронний журнал). 2015. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=920 (дата звернення: 09.05.2021).

13. Скиба Г.В. Сучасний стан науково-технічного потенціалу України: вітчизняні реалії та зарубіжний досвід. URL: http://elar.khnu.km.ua/jspui/bitstream/123456789/5357/1/%D0%A1%D0%BA%D0%B8%D0%B1%D0%B0.pdf (дата звернення: 09.05.2021).

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

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

УДК 342.7

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.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПОЛІТИЧНИХ ПРАВ ГРОМАДЯН УКРАЇНИ: СУЧАСНИЙ СТАН, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Анотація. *У статті досліджено сучасний стан нормативно-правового забезпечення формування та реалізації політичних прав громадян України. Проаналізовано основні положення Конституції України, законів України, міжнародно-правових договорів, підзаконних нормативно-правових актів. Обґрунтовано необхідність удосконалення нормативно-правового забезпечення права на мирні зібрання, а також права на громадський контроль, який є складовою права на управління державними справами.*

Ключові слова: *політичні права, нормативно-правовий акт, закон, підзаконний нормативно-правовий акт.*

Summary. *The article examines the current state of regulatory and legal support for the formation and implementation of political rights of citizens of Ukraine. The main provisions of the Constitution of Ukraine, laws of Ukraine, international legal agreements, bylaws are analyzed. The necessity of improving the regulatory and legal support of the right to peaceful assembly, as well as the right to public control, which is a component of the right to manage state affairs, is substantiated.*

Keywords: *political rights, regulatory and legal act, law, by-law regulatory act.*

Аннотация. *В статье исследовано современное состояние нормативно-правового обеспечения формирования и реализации политических прав граждан Украины. Проанализированы основные положения Конституции Украины, законов Украины, международно-правовых договоров, подзаконных нормативно-правовых актов. Обоснованно необходимость совершенствования нормативно-правового обеспечения права на мирные собрания, а также права на общественный контроль, который является частью права на управление государственными делами.*

Ключевые слова: *политические права, нормативно-правовой акт, закон, подзаконный нормативно-правовой акт.*

Постановка проблеми. Нормативно-правове забезпечення політичних прав та свобод є актуальною та важливою темою дослідження, що обумовлено особливою роллю та значенням політичних прав та свобод. Зважаючи на відсутність чіткого уніфікованого переліку політичних прав, наявність "умовно-політичних" прав, тобто таких, які відносяться до громадянських та політичних одночасно, важливо зосередити увагу на аналізі нормативного забезпечення так званих "чистих" політичних прав та свобод, визначити якісний рівень їх правового регулювання, наявні правові прогалини та напрямки удосконалення нормативно-правового забезпечення.

У зв'язку з вищезазначеним, у межах даної статті проаналізовано сучасний стан нормативно-правового забезпечення прав і свобод громадян України, які здійснюються у конвенційних формах та базуються на формальній політичній участі. Конкретизуючи викладені положення, до "класичних" політичних прав ми відносимо: виборчі права (право обирати та бути обраним); право брати участь у загально-державних та місцевих референдумах; право на об'єднання у політичні партії; право брати участь у мітингах та демонстраціях (мирні збори), які мають політичну мету; право в управління державними справами.

Результати аналізу наукових публікацій. Дослідження нормативно-правого забезпечення політичних прав, а також самого змісту політичних прав та свобод в Україні здійснювали П.М. Рабінович, У.В. Ільницька, М.М. Антонович, В.Л. Федоренко, Ю.І. Римаренко, Л.Ю. Бельо, О.В. Совгиря, М.В. Савчин та інші науковці. Дослідженню нормативно-правої бази у цьому напрямку, класифікації нормативно-правових актів, аналізу судових рішень присвячені роботи Г.І. Дутки, Р.С. Мельника, М.І. Смоковича, В.М. Олуйко, О.С. Лисенкова, В.М. Гайворонського та інших.

Метою статті є оцінка сучасного стану та виявлення прогалин у нормативно-правовому забезпеченні реалізації політичних прав і свобод громадян України.

Виклад основного матеріалу. Нормативно-правове забезпечення політичних прав забезпечується нормами різних галузей та підгалузей права, до яких відносимо конституційне право, адміністративне, кримінальне тощо. Важливо зазначити, що нормативно-правове забезпечення (регламентація) політичних прав здійснюється за допомогою матеріальних та процесуальних норм. Зокрема, процесуальні норми визначають порядок проведення виборів та референдумів, порядок реєстрації громадських об'єднань та політичних партій, порядок формування та склад громадських рад при органах державної влади тощо, тоді як матеріальні норми фіксують та визначають зміст самих політичних прав, їх властивості, права та обов'язки громадян, щодо реалізації принципів народовладдя, здійснення громадського контролю, управління державними справами тощо. У сукупності матеріальні й процесуальні норми встановлюють певний порядок дій громадян та державних органів, окремих державних службовців; забороняють здійснення певних дій, надають можливість вибору одного з встановлених варіантів поведінки, дозволяють діяти (або не діяти) на свій розсуд.

Найактуальнішим для правового поля України є загальний поділ за юридичною чинністю на закони та підзаконні нормативні акти і поділ за суб'єктами правотворчості, де більш ґрунтовно класифіковано саме підзаконні нормативно-правові акти [1].

Основоположним законом, що закріплює конституційний лад, права і свободи людини та громадянина, визначає форму правління і державного устрою, правовий статус органів державної влади є Конституція України [2]. Юридичним підґрунтям для здійснення політичних прав та свобод є положення, закріплені у ст. 5 та ст. 69 Конституції України, що мають фундаментальне значення. У вказаних статтях закріплені ключові положення, що носієм суверенітету і єдиним джерелом влади в Україні є народ. Народ здійснює владу безпосередньо і через органи державної влади та органи місцевого самоврядування. Право визначати і змінювати конституційний лад в Україні належить виключно народові і не може бути узурповане державою, її органами або посадовими особами. Ніхто не може узурпувати державну владу. Народне волевиявлення здійснюється через вибори, референдум та інші форми безпосередньої демократії. Політичні права закріплено у розділі ІІ Конституції України, а саме: ст. 36-37 регламентують право на свободу об'єднання у політичні партії, ст. 38 закріплює право на участь в управлінні державними справами, право брати участь в референдумах

та виборах; ст. 39 закріплює право на мирні збори, у тому числі, й з політичною метою; ст. 40 закріплює право направляти індивідуальні чи колективні звернення.

Перелік законів, що регулюють реалізацію політичних прав, є досить широкий. До законів у сфері регулювання політичних прав і свобод можемо віднести, зокрема, закони України: "Про політичні партії" [3], "Про місцеве самоврядування" [4], "Про звернення громадян" [5], "Про громадські об`єднання" [6], "Про доступ до публічної інформації" [7], "Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань" [8] тощо.

Важливе значення має прийняття Закону України "Про народовладдя через всеукраїнський референдум" [9]. Нагадаємо, що тривалий час в Україні була правова прогалина у цьому питанні: Закон України "Про всеукраїнський та місцеві референдуми" [10] втратив чинність 28.11.12 р. на підставі прийняття нового Закону України "Про всеукраїнський референдум" від 06.11.12 р. [11]. Однак новий Закон № 5475-VI було визнано неконституційним на підставі рішення Конституційного Суду України від 26.04.18 р. [12]. У новому Законі № 1135-IX вперше пропонується запровадження електронних процедур: організації проведення та голосування на референдумі. Передбачено створення автоматизованої інформаційно-аналітичної системи із забезпечення електронного голосування, що потребуватиме окремих видатків із державного бюджету. Прикінцевими положеннями на реалізацію положень Закону передбачено внесення змін до "Кодексу адміністративного судочинства України" [13], законів України "Про Конституційний Суд України" [14], "Про запобігання корупції" [15], "Про політичні партії в Україні" [3], "Про Центральну виборчу комісію" [16]. Водночас, у Законі України № 1135-IX не здійснено нормативного регулювання місцевих референдумів. Наявний Закон України "Про місцеве самоврядування в Україні" закріплює право громадян на проведення місцевих референдумів, водночас не містить процесуальних норм щодо його реалізації. Слід зазначити, що станом на сьогоднішній день вже зареєстровано та подано до розгляду Верховною Радою України законопроект "Про місцевий референдум" [17].

Серед кодифікованих нормативно-правових актів особливо слід відзначити "Виборчий кодекс України", який об'єднав у собі нормативні положення про проведення місцевих виборів, виборів до Верховної Ради України, виборів Президента України. "Виборчий кодекс України" [18] замінив низку законів, які регламентували виборче право та виборчий процес: "Про вибори Президента України" [19], "Про вибори народних депутатів України"[20], "Про місцеві вибори" [21].

"Виборчим кодексом України" передбачено і вже були внесені зміни до "Кримінального кодексу України", зокрема у ст. 157-160 [22] та "Кодексу України про адміністративні правопорушення" у ст. 212-22, 212-23, 212-24 [23], що уможливлюють проведення необхідних для розслідування проваджень щодо порушення виборчих прав слідчих дій, затримання порушників безпосередньо на виборчій дільниці, притягнення до відповідальності кандидатів, які погоджуються балотуватись за отримання незаконної винагороди, чітке розмежування адміністративної та кримінальної відповідальності за непрямий підкуп виборців тощо. Передбачена юридична відповідальність за підкуп виборців, учасника референдуму, члена виборчої комісії або комісії з референдуму (ст. 160).

Як прогалину у нормативному забезпеченні політичних прав слід розцінювати відсутність спеціального закону, який регулював би суспільні відносини у сфері мирних зібрань. На сьогоднішній день окремі питання реалізації права на мирні зібрання висвітлені в рішенні Конституційного Суду України № 1-30/2001 у справі щодо

завчасного сповіщення про мирні зібрання [24], ініційованій поданням Міністерства внутрішніх справ України щодо офіційного тлумачення положення частини першої ст. 39 Конституції України про завчасне сповіщення органів виконавчої влади чи органів місцевого самоврядування про проведення зборів, мітингів і демонстрацій.

Також доцільно було б прийняти спеціальний закон про громадський контроль, який визначає права управління державними справами. Наразі окремі положення про громадський контроль врегульовано Законом України "Про національну безпеку" [25] у межах Розділу ІІІ "Демократичний цивільний контроль" та низки підзаконних нормативно-правових актів.

Важливе значення для нормативного забезпечення політичних прав мають міжнародні договори, згоду на обов'язковість яких надано Верховною Радою України и, котрі є частиною національного законодавства згідно із ст. 9 Конституції України, а також ті міжнародні договори, які було укладено Українською РСР до проголошення незалежності України і зобов'язання за якими Україна підтвердила відповідно до Закону України "Про правонаступництво України" від 12.11.91 р. [26]. Серед базових міжнародних договорів – "Міжнародний пакт про громадянські та політичні права" [27] (набув чинності, в тому числі для України, 23.03.76 р.), "Загальна декларація прав людини" від 10.12.48 р. [28], "Перший Протокол до Конвенції про захист прав людини і основоположних свобод" (дата підписання 20 березня 1952 року, ратифікація 17 липня 1997 року) [29]. Згідно зі ст. 3 "Право на вільні вибори" Першого Протоколу до Конвенції, Договірні Сторони зобов'язуються проводити вільні вибори з розумною періодичністю шляхом таємного голосування в умовах, які забезпечують вільне вираження думки народу у виборі законодавчого органу.

Юридичну силу міжнародного договору мають і прецеденти Європейського суду з прав людини (далі – ЄСПЛ), рішення якого визнані в Україні джерелом права, відповідно до ст. 17 Закону України "Про виконання рішень та застосування практики Європейського суду з прав людини" від 23.02.06 р. № 3477-IV [30]. Як слушно зазначає М.І. Смокович, правові позиції ЄСПЛ мають значну цінність для розуміння справжнього змісту положень Конвенції, а деякі з формулювань Суду слід розглядати як принципові доктринальні положення, що істотно впливають на тлумачення багатьох норм як міжнародних документів, так і національного законодавства [31].

Рішення ЄСПЛ є підставою для перегляду рішень національних судів України, якщо вони допустили порушення прав громадянина при розв'язанні конфлікту, в тому числі й виборчого спору. Крім того ЄСПЛ після розгляду справи національними судами України може вирішити справу по суті. Порушень у сфері виборчого права стосуються ухвали ЄСПЛ стосовно заяви № 43476/98 "К.А. Бабенка проти України" [32], заяви № 3239/98 "С. Головатий проти України" [33], справи № 40269/02 – "Корецький проти України" [34]. Результатом розгляду справи "Корецький проти України" стало приведення чинного законодавства України у відповідність до Конвенції про захист прав людини і основоположних свобод і прийняття Закону України "Про громадські об'єднання" від 22.03.12 р. [6].

Важливе значення у нормативно-правовому забезпеченні політичних прав та свобод мають підзаконні нормативно-правові акти, прийняті компетентними органами державної влади чи уповноваженими державою іншими суб'єктами на підставі закону, відповідно до закону і в порядку його виконання. Серед них особливе значення мають постанови Верховної Ради України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, нормативно-правові акти центральних органів виконавчої влади, ЦВК, акти суб'єктів системи місцевого самоврядування,

найвагомішими серед яких є акти місцевих референдумів та акти представницьких органів місцевого самоврядування. Зважаючи на значну кількість та різноманітність підзаконних нормативно-правових актів, наведемо лише деякі, які мають пряме відношення до забезпечення реалізації окремих політичних прав громадян України.

За останні десять років нормативно-правова база щодо активізації участі громадськості у державних справах поповнилася низкою документів, серед яких укази Президента України, постанови Кабінету Міністрів України.

Зокрема, в Указі Президента України "Про Національну стратегію у сфері прав людини" від 24.03.21 р. № 119/2021 [35] визначено завдання щодо запровадження системного підходу до забезпечення прав і свобод людини, узгодженості дій органів державної влади, органів місцевого самоврядування, інститутів громадянського суспільства, суб'єктів господарювання, створення в Україні ефективного механізму реалізації та захисту прав і свобод людини, усунення недоліків системного характеру, які лежать в основі порушень, виявлених ЄСПЛ. В інших указах Президента України – "Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади" [36], "Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики" [37] визначено пріоритетні напрямки діяльності центральних органів виконавчої влади щодо поглиблення співпраці з інститутами громадянського суспільства та забезпечення прав і свобод громадян, у тому числі й у політичній сфері. Зокрема, в Указі Президента України "Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики" наголошено на необхідності створення ефективних організаційних та правових умов для всебічної реалізації громадянами конституційного права на участь в управлінні державними справами, забезпечення відкритості діяльності органів виконавчої влади, врахування громадської думки у процесі підготовки та організації виконання їх рішень тощо.

Серед нормативних актів, що приймаються Кабінетом Міністрів України слід відзначити ті, що покликані забезпечити партнерство органів виконавчої влади з громадянським суспільством: "Про затвердження порядку сприяння проведення громадської експертизи діяльності органів виконавчої влади" від 05.11.08 р. [38], "Про забезпечення участі громадськості у формуванні та реалізації державної політики" від 03.11.10 р. [39].

Сприяти поглибленню взаємодії громадянського суспільства та органів державної влади мають громадські ради, які діють як тимчасові консультативно-дорадчі органи, утворені для сприяння участі громадськості у формуванні та реалізації державної, регіональної політики, її завдання, компетенції, порядок роботи тощо, що нормативно закріплено у "Типовому положенні про громадську раду" [40], в якому визначено їх правовий статус.

Важливе значення для забезпечення політичного права на створення політичних партій мають накази Міністерства юстиції України. Зокрема державна реєстрація створення політичної партії здійснюється на основі наказів: "Про затвердження Порядку підготовки та оформлення рішень щодо легалізації об'єднань громадян та інших громадських формувань" [41], "Про затвердження Порядку державної реєстрації юридичних осіб, фізичних осіб-підприємців та громадських формувань, що не мають статусу юридичної особи" [42].

Слід згадати нормативні акти ЦВК, обов'язкові для використання в роботі виборчих комісій та комісій з референдумів, роз'яснень і рекомендацій з питань застосування законодавства України про вибори і референдуми, наприклад "Про форму

списку громадян, які мають право брати участь у всеукраїнському референдумі за народною ініціативою" [43] та низки інших актів.

Висновки.

Нормативно-правове забезпечення політичних прав і свобод громадян України здійснюється комплексно, за допомогою цілісної системи законів та підзаконних нормативно-правових актів. Загалом, під нормативно-правовим забезпеченням політичних прав та свобод, на нашу думку слід розуміти сукупність усіх діючих матеріальних та процесуальних норм, закріплених у нормативних актах органів державної влади, а також міжнародні договори, ратифіковані Верховною Радою України и, які прямо чи опосередковано регламентують та забезпечують порядок реалізації політичних прав, визначають передумови та вимоги для суб'єктів реалізації ними своїх законних політичних прав, їх прав та обов'язків при реалізації ними цих прав.

Серед законів України центральне місце займає Основний Закон, який має установче значення для всіх політичних прав, що закріплено у Розділі ІІ "Права, свободи та ~~обов~~'~~язки~~ обов'язки людини і громадянина". Забезпечення політичних прав та свобод закріплено низкою ординарних законів України, які визначають порядок, спосіб та форми реалізації політичних прав. До таких актів ми відносимо Закони України: "Про політичні партії", "Про місцеве самоврядування", "Про звернення громадян", "Про громадські об'єднання", "Про народовладдя через всеукраїнський референдум", "Про доступ до публічної інформації", "Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань" та ряду інших.

Важливим кроком у формуванні правового поля України є ухвалення Виборчого кодексу України, який об'єднав у собі нормативні положення про проведення місцевих виборів, виборів до Верховної Ради України, Президента України та Закону України "Про народовладдя через всеукраїнський референдум", який заповнив правову прогалину у цьому питанні.

На сьогодні у нормативно-правових актах чітко визначені інституції, що відповідають за формування й реалізацію політичних прав: Верховна Рада України, Президент України, Кабінет Міністрів України, центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, судові та правоохоронні органи.

Вагомим внеском у створення цілісної нормативно-правової бази є прийняття підзаконних нормативно-правових актів, таких як: укази Президента України "Про Національну стратегію у сфері прав людини", "Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади", "Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики"; постанови Кабінету Міністрів України, які покликані забезпечити партнерство органів виконавчої влади з громадянським суспільством: "Про забезпечення участі громадськості у формуванні та реалізації державної політики"; "Про затвердження порядку сприяння проведення громадської експертизи діяльності органів виконавчої влади", "Про забезпечення участі громадськості у формуванні та реалізації державної політики" тощо.

Як прогалину у нормативному забезпеченні політичних прав слід розцінювати також відсутність спеціального закону, який регулював би суспільні відносини у сфері мирних зібрань. Також доцільно було б прийняти спеціальний закон про громадський контроль, який є складовою права на управління державними справами. Потребує нормативного врегулювання інститут місцевого референдуму, який проект якого наразі зареєстрований та поданий до розгляду ~~профільним~~ ~~комітетом~~ Верховної Ради України.

Використана література

1. Гайворонський В. Джерела права. *Вісник Академії правових наук України*. 2001. № 3. С. 56-65. URL: https://dspace.nlu.edu.ua/handle/123456789/4582

2. Конституція України від 28.06.96 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80#Text

3. Про політичні партії: Закон України від 05.04.01 р. № 2365-III. URL: https://zakon.rada.gov.ua/laws/show/2365-14#Text

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

5. Про звернення громадян: Закон України від 02.10.96 р. № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text

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

7. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

8. Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань: Закон України від 15.05.03 р. № 755-IV. URL: https://zakon.rada.gov.ua/laws/show/755-15#Text

9. Про народовладдя через всеукраїнський референдум: Закон України від 26.01.21 р. № 1135-IX. URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69060

10. Про всеукраїнський та місцеві референдуми: Закон України від 03.07.91 р. № 1286-XII – (втратив чинність на підставі Закону України від 06.11.12 р. № 5475-VI). URL: https://zakon.rada.gov.ua/laws/show/1286-12#Text

11. Про всеукраїнський референдум: Закон України від 06.11.12 р. № 5475-VI – (визнаний неконституційним від 26.04.18 р.). URL: https://zakon.rada.gov.ua/laws/show/5475-17#Text

12. Рішення Конституційного Суду України від 26.04.18 р. № 4-р/2018. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/KS18076.html

13. Кодекс адміністративного судочинства України: Закон України від 06.07.05 р. № 2747-IV. URL:https://zakon.rada.gov.ua/laws/show/2747-15/print

14. Про Конституційний Суд України: Закон України від 13.07.17 р. № 2136-VIII. URL: https://zakon.rada.gov.ua/laws/show/2136-19#text

15. Про запобігання корупції: Закон України від 14.10.14 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text

16. Про Центральну виборчу комісію: Закон України від 30.06.04 р. № 1932-IV. URL: https://zakon.rada.gov.ua/laws/show/1932-15#Text

17. Про місцевий референдум: проект закону від 19.05.21 р. № 5512. URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71942

18. Виборчий кодекс України: Закон України від 19.12.19 р. № 396-IX. URL:https://zakon.rada.gov.ua/laws/show/396-20#Text

19. Про вибори Президента України: Закон України від 05.03.99 р. № 474-XIV. URL: https://zakon.rada.gov.ua/laws/show/474-14#Text

20. Про вибори народних депутатів України: Закон України від 17.11.11 р. № 4061-VI. URL: https://zakon.rada.gov.ua/laws/show/4061-17#Text

21. Про місцеві вибори: Закон України від 14.07.15 р. № 595-VIII. URL: https://zakon.rada.gov.ua/laws/show/595-19#Text

22. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

23. Кодекс України про адміністративні правопорушення: Закон України від 27.04.21 р. № 80731-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text

24. Рішення Конституційного суду України від 19.04.01 р. № 1-30/2001. URL: https://zakon.rada.gov.ua/laws/show/v004p710-01#Text

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

26. Про правонаступництво України: Закон України від 12.09.91 р. № 1543-XII. URL: https://zakon.rada.gov.ua/laws/show/1543-12#Text

27. Міжнародний пакт про громадянські і політичні права: ратифіковано Указом Президії Верховної Ради Української РСР від 19.10.73 р. № 2148-VIII. URL: https://zakon.rada.gov.ua /laws/ show/995_043#Text

28. Загальна декларація прав людини від 10.12.48 р. URL: https://zakon.rada.gov.ua/laws/ show/995_015#text

29. Протокол до Конвенції про захист прав людини і основоположних свобод: Закон України від 17.07.97 р. № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/994_535#Text

30. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.06 р. № 3477-IV. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text

31. Смокович М.І. Правове регулювання розгляду виборчих спорів: теоретичний і практичний аспекти: монографія. Київ: Юрінком Інтер, 2014. 576 с.

32. Ухвала ЄСПЛ щодо прийнятності заяви № 43476/98 "К.А. Бабенка проти України". URL: https://minjust.gov.ua/m/str_194

33. Ухвала ЄСПЛ щодо прийнятності заяви № 43476/98 "С. Головатий проти України". URL: https://zakon.rada.gov.ua/laws/show/980_015#Text

34. Ухвала ЄСПЛ щодо прийнятності заяви № 40269/02 "Корецький проти України". URL: https://zakon.rada.gov.ua/laws/show/974_446#Text

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

36. Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади: Указ Президента України від 01.08.02 р. № 683. URL: https://zakon.rada.gov.ua/laws/ show/683/2002#Text

37. Про забезпечення умов для більш широкої участі громадськості у формуванні та реалізації державної політики: Указ Президента України 31.07.04 р. № 854/2004. URL:https:// zakon.rada.gov.ua/laws/show/854/2004#Text

38. Про затвердження Порядку сприяння проведенню громадської експертизи діяльності органів виконавчої влади: Постанова КМУ від 05.11.08 р. № 976. URL: https://zakon.rada. gov.ua/laws/show/976-2008-%D0%BF#Text

39. Про забезпечення участі громадськості у формуванні та реалізації державної політики: Постанова КМУ від 03.11.10 р. № 996. URL: https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text

40. Типове положення про громадську раду від 03.11.10 р. № 996: в редакції Постанови КМУ від 24.04.19 р. № 353. URL: https://zakon.rada.gov.ua/laws/show/353-2019-%D0%BF#Text

41. Про затвердження Порядку підготовки та оформлення рішень щодо легалізації об'єднань громадян та інших громадських формувань: наказ Міністерства юстиції України від 08.07.11 р. № 1828. URL: https://zakon.rada.gov.ua/laws/show/z0855-11#Text

42. Про затвердження Порядку державної реєстрації юридичних осіб, фізичних осіб-підприємців та громадських формувань, що не мають статусу юридичної особи: наказ Міністерства юстиції України від 09.02.16 р. № 359/5. URL: https://zakon.rada.gov.ua/laws/ show/z0200-16#Text

43. Про форму списку громадян, які мають право брати участь у всеукраїнському референдумі за народною ініціативою: Постанова ЦВК від 16.04.00 р. № 8. URL: https://zakon. rada.gov.ua/laws/show/v0008359-00#Text

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

УДК 351/354

ЯЩЕНКО В.А., *доктор юридичних наук, професор,* головний науковий співробітник ДНУ ІІБП НАПрН України.
ORCID: https://orcid.org/0000-0002-2257-318X.

ДІАЛЕКТИКА ЦИВІЛЬНО-ВІЙСЬКОВИХ ВІДНОСИН

Анотація. *У запропонованій статті здійснено критичний аналіз підходів до розуміння цивільно-військових відносин не лише як контрольного чинника, а й більш широкого соціального феномену. З'ясовано, що останній виконує функцію своєрідного соціального інтегративного фактору сфери безпеки та оборони України. Висвітлення проблеми здійснюється через призму діалектичних категорій змісту та форми, сутності і проявів, загального і окремого, єдності і відмінності цивільних та військових зв'язків тощо. Автор не обмежується констатацією наявно існуючих досягнень у становленні цих відносин, а ставить питання їх подальшого плідного розвитку у системі права України.*

Ключові слова: *діалектика, сутність та прояви, зміст та форма, цивільно-військові відносини, демократичний цивільний контроль, об'єктивний та суб'єктивний контроль.*

Summary. *The proposed article provides a critical analysis of approaches to understanding civil-military relations not only as a control factor, but also a broader social phenomenon. It was found that the latter serves as a kind of social integrative factor in the field of security and defense of Ukraine. The problem is covered through the prism of dialectical categories of content and form, essence and manifestations, general and separate, unity and difference of civil and military relations, etc. The author does not limit himself to stating the existing achievements in the formation of these relations, but raises the question of their further fruitful development in the legal system of Ukraine.*

Keywords: *dialectics, essence and manifestations, content and form, civil-military relations, democratic civil control, objective and subjective control.*

Аннотация. *В предложенной статье осуществлен критический анализ подходов к пониманию гражданско-военных отношений только лишь как контрольной функции, но и как более широкого социального феномена, который выступает определяющим фактором общественного согласия в сфере безопасности и обороны Украины. Установлено, что эти отношения выполняют функцию своеобразного социального интегративного фактора сферы безопасности и обороны Украины. Освещение проблемы осуществляется через призму диалектических категорий содержания и формы, сущности и явлений, общего и отдельного, единства и отличия гражданских и военных связей и опосредований. Автор не ограничивается констатацией существующих достижений в становлении этих отношений, а ставит вопрос их дальнейшего развития в системе права Украины.*

Ключевые слова*: диалектика, сущность и явления, содержание и форма, гражданско-военные отношения, демократический гражданский контроль, объективный и субъективный контроль.*

Постановка проблеми. В сучасній українській юридичній науці дедалі більше звертається увага не лише на висвітлення питань правосвідомості, а й правобуття, тобто, проблеми правовідносин. Серед них особливо актуальною постала проблема цивільно-військових відносин, викликана необхідністю мобілізації суспільства на відповідь новим загрозливим викликам його існування.

Водночас підходи до висвітлення цих відносин неоднозначні, часто-густо вузько професійні і не розкривають повністю їх змісту. Пропонується застосувати для їх аналізу

діалектичний метод в його конкретизації до цивільно-військової реальності, що є основною проблемою і, водночас, надає цим відносинам статусу соціально-безпекового чинника.

Результати аналізу наукових публікацій. Останніми роками обсяг праць з питань цивільно-військових відносин значно зріс. В той же час теоретичний їх аналіз не виходить за межі, визначені американським вченим С. Гантінгтоном ще у 50-і роки XX століття, який фактично створив їх теорію. Однак більшість вітчизняних публікацій часто-густо зводять ці відносини до функції демократичного цивільного контролю за сектором безпеки і оборони України і залишають поза висвітленням всю їх багатоманітність. Між тим, ці відносини нині набули особливого безпеко-оборонного чинника у всіх цивілізованих країнах і потребують зваженого критично-наукового аналізу, що на нашу думку, можливо здійснити на основі діалектики. Виходячи з цього вважаємо, що актуальним є потреба з'ясування феномену цивільно-військових відносин як визначального чинника сектору безпеки і оборони держави, що не знайшов ще належного наукового висвітлення.

Метою статті є розкриття природи цивільно-військових відносин і їх функціональні особливості та визначення шляхів і способів їх удосконалення.

Розв'язання проблеми пропонується шляхом обґрунтування необхідності внесення змін до чинного законодавства терміну "цивільно-військові відносини", який нині в цих актах відсутній.

Виклад основного матеріалу. З'ясування діалектики цивільно-військових відносин зумовлено, на нашу думку, перш за все зростанням їх ролі як чинника безпеки України, забезпечення надійного стабільного існування соціуму. Врешті-решт мова буде йти про необхідність якісного оновлення цих відносин у сфері безпеки і оборони України.

Цивільно-військові відносини (далі – ЦВВ) визначаються як взаємовідносини між військовими інституціями, з одного боку, та цивільним урядом, неурядовими інституціями, організаціями та громадянами, з іншого. Отже, цивільно-військові відносини – це сукупність правових взаємовідносин між суспільством та складовими частинами Воєнної організації держави, які охоплюють політичні, фінансово-економічні, соціальні та інші процеси у сфері національної безпеки і оборони [14, с. 1]. Це визначення, з точки зору діалектики, не зовсім вдале, оскільки одиничне, окреме (військове) виводиться за сферу загального, суспільного, до якого воно належить.

Таким чином, навіть у буденній свідомості цивільні та військові відносини не існують самостійно, відірвано один від одного, а органічно пов'язані між собою, де цивільний чинник виступає пріоритетним, як більш загальний по відношенню до військової складової безпеки і оборони. Діалектика і визначає тип і характер цього зв'язку.

Формування і функціонування цих відносин фактично є визначальним чинником, що зумовлює наявність політичних, економічних, соціальних, господарських та ін. зв'язків між цивільними і військовими. Одразу зауважимо, що значна частина дослідників та законотворців, як правило, ці обставини не враховує, а все багатство ЦВВ звужується лише до контрольної прерогативи, розглядаючи ці відносини через призму демократичного цивільного контролю.

В узагальненому вигляді цю точку зору висловлюють М.В. Сіцінська, Г.Д. Рябоконь та ін. науковці. На думку М.В. Сіцінської: "…актуальність цивільно-військових відносин і цивільного контролю значно зростає на переломних етапах розвитку нашого суспільства. Тому саме сьогодні демократичний цивільний контроль над сектором безпеки і оборони являє собою зміст і головну частину цивільно-

військових відносин" [2, с. 83]. Практично аналогічною щодо цього питання є позиція Г.Д. Рябоконя: "Головною складовою формування системи цивільно-військових відносин є запровадження цивільного контролю над силовими структурами, що визнається однією з головних ознак стабільного політичного режиму в країні, а також демократичної зрілості самого суспільства" [3, с. 1].

Однак і в окремих міжнародних нормативних актах прерогатива теж віддається демократичному цивільному контролю, але йому фактично надається більш узагальнена функція цивільно-військових відносин. Так, згідно п. 20 Кодексу поведінки стосовно військово-політичних аспектів безпеки ОБСЄ: "Держави-учасниці розглядають демократичний політичний контроль над військовими і воєнізованими силами, силами внутрішньої безпеки, а також розвідувальними службами і поліцією, як невід'ємну складову стабільності і безпеки. Вони сприятимуть інтеграції своїх збройних сил із громадянським суспільством як важливому прояву демократії" [4].

Що стосується національного законодавства з питань безпеки і оборони, то в ньому термін "цивільно-військові відносини" теж не використовується, а застосовується поняття "демократичний цивільний контроль", хоча фактично цей контроль представляються в інтегрованому безпеко-забезпечувальному вигляді. Зокрема, стаття 13 Закону України "Про оборону України" передбачає, що Міністерства, центральні та інші органи виконавчої влади у взаємодії з Міністерством оборони України у межах своїх повноважень:

організовують і забезпечують виконання законодавства у сфері оборони, сприяють Збройним Силам України у виконанні ними завдань, здійснюють їх належне забезпечення за напрямами діяльності;

узгоджують з Генеральним штабом Збройних Сил України та забезпечують проведення заходів щодо розвитку системи зв'язку, шляхів, транспорту, інших об'єктів інфраструктури і території держави та підготовки своїх галузей до оборони, забезпечують їх територіальну оборону в межах своїх повноважень та ін. кроки. Регламентується також діяльність Ради міністрів Автономної Республіки Крим, місцевих державних адміністрацій у сфері оборони, діяльність органів місцевого самоврядування, права та обов'язки громадян України у сфері оборони: Захист Вітчизни, незалежності та територіальної цілісності України є конституційним обов'язком громадян України [5].

Визначення термінів "військова безпека", "громадська безпека і порядок", "державна безпека" у Законі України "Про національну безпеку України" функціонально поєднується і вони являють собою цільність цивільно-військових відносин. Більш того, як в Кодексі поведінки стосовно військово-політичних аспектів безпеки ОБСЄ, у цьому Законі демократичний цивільний контроль теж зводиться практично до рангу ЦВВ. Зокрема, п. 5 ст. 1 Закону передбачає: "демократичний цивільний контроль – комплекс здійснюваних відповідно до Конституції і законів України правових, організаційних, інформаційних, кадрових та інших заходів для забезпечення верховенства права, законності, підзвітності, прозорості органів сектору безпеки і оборони та інших органів, діяльність яких пов'язана з обмеженням у визначених законом випадках прав і свобод людини, сприяння їх ефективній діяльності й виконанню покладених на них функцій, зміцненню національної безпеки України" [6].

Закон України "Про Збройні Сили України"(ст.ст. 1, 11, 12), вказуючи на обмеження політичної діяльності у ЗСУ, теж передбачає недопустимість незаконних дій по відношенню до цивільного населення, його майна та навколишнього середовища, дотримання верховенства права, законності та гуманності, поваги до людини, її

конституційних прав і свобод; гласності, відкритості для демократичного цивільного контролю [7].

На нашу думку, в даному випадку має місце абсолютизація закономірностей одиничного (контролю) і недостатня увага до загального (ЦВВ). У практиці це призводить до того, що не враховуються важливі складові цих відносин. Наприклад, соціальна реабілітація військових, цивільно-військове співробітництво, проведення операцій з підтримання миру та ін., які явно виходять за межі лише контрольної функції.

Тому В.І. Білошицький, аналізуючи досвід НАТО, вважає за необхідне розширити цю функцію ЦВВ і не зводити її лише до виконання контрольної місії: "Такі відносини більш широко мають розглядатись в ракурсі забезпечення національної безпеки. При цьому не слід забувати, що саме слово "відносини" висвітлює дві взаємодіючі сторони – громадянське суспільство та його воєнну організацію" [8, с. 26]. У підтвердження цієї позиції він наводить приклад роботи Групи цивільно-військової співпраці "Північ", яка отримала статус Міжнародного військового штабу НАТО: "Завдяки цій групі командувачі НАТО і цивільні установи можуть створити потрібні умови для налагодження зв'язку між цивільними та військовими протягом усього періоду проведення операцій. А особливо при проведенні післяконфліктних заходів з підтримання миру. Отже, ЦВВ – це ще й значний фактор гуманітарної допомоги, допомоги з подолання наслідків катастроф, інших операцій у разі надзвичайних ситуацій цивільного характеру, які виконують національні або міжнародні військові сили" [9, с. 8].

На нашу думку, вище згадувані оцінки феномену ЦВВ певною мірою правомірні, але з точки зору методології недостатні, щоб розкрити всю повноту і багатство цих відносин, що й спонукає нас звернутися до найбільш загальної, діалектичної методології філософсько-правового аналізу.

По-перше, мова має йти про з'ясування родової належності цивільно-військових відносин. Це, очевидно, різновид суспільних відносин, які складаються з виробничих відносин, відносин обміну і відносин соціальних груп. Згідно енциклопедичних даних, суспільні відносини – "багатоманітні зв'язки, що складаються між людьми в процесі їх діяльності в різних сферах суспільного життя і визначаються способом виробництва їх матеріального життя, виникають з появою суспільного виробництва. Суспільні відносини – це відносини між різними людськими колективами, соціальними групами, класами та всередині них" [1, с. 117]. Саме до останніх тобто, відносин соціальних груп і належать цивільно-військові відносини, що втілюють в собі аспект соціальності зв'язків і опосередкувань. Очевидно, не слід забувати, що категорія зв'язку є фундаментальним принципом діалектики, і в даному випадку ЦВВ означають такі опосередкування, які є необхідними, суттєвими, атрибутивними, і лише за цієї умови вони набувають статусу відносин.

Тому й цивільні відносини часто розглядаються як синонім соціальності, цивілізованості, тобто, досягнень демократії і культури. Отже, ця цивільна складова соціальних відносин є їх змістовною складовою, яка визначає всі інші різновиди і форми соціальних зв'язків.

На відміну від цього військові відносини є формою соціальних, які здійснюються в особливій, навіть унікальній сфері військового буття. Вони, звісно, мають свою самостійність, але ця самостійність відносна, вона володіє статусом автономності.

Таким чином, цивільні і військові відносини – це не антиподи, це суперечності не протиставлення, а залежності, взаємозв'язку, взаємодії, взаємопереходів, тобто, протилежності не типу невирішених антиномій, а суперечливості між змістом та формою: цивільні відносини складають їх зміст, а формою є продовження (розповсюдження) цього

змісту на військову сферу і розвиток, збагачення цього змісту в залежності від багатоманітності та багатогранності військового життя.

Але, як ми зазначали, самостійність військових відносин не є істиною абсолютною, а відносною і визначається в кінцевому рахунку сутністю соціальних відносин, яка втілюється у політичному режимі: авторитарному чи демократичному.

Що стосується тоталітарного режиму, то при ньому держава набуває характеру воєнізованого середовища, коли цивільні (громадянські) відносини воєнізуються з метою виправдання і підтвердження легітимності влади і тоталітарного режиму (мілітаризація економіки і всього суспільного життя), іншими словами, мілітаризація цивільних відносин.

При авторитарному режимі цивільно-військові відносини формально мають місце і відповідно задекларовані, але військові домінують, оскільки саме від них залежить міцність вертикалі влади і існуючого ладу. Це характерно по відношенню до сучасної Росії, де патріотизм, національна свідомість мілітаризуються і набувають агресивно войовничого характеру, що не виключає і ескалації збройного конфлікту як способу захисту від уявних, примарних загроз. В такому випадку, на нашу думку, спотворюється головний урок Другої Світової війни – ненависть до війни.

Отже, цивільно-військові відносини – це своєрідний синтез громадянських та військових взаємин, військових та невійськових, воєнних та невоєнних зв'язків, де цивільні відносини складають зміст, а військові – його особливу унікальну форму, при визначеній ролі цивільних, як загально соціальних зв'язків.

Характеризуючи ці зв'язки, відомий теоретик цивільно-військових відносин С. Гантінгтон класифікує їх, поділяючи на об'єктивні та суб'єктивні, в залежності від типу політичних режимів [12, с. 80]. Позитивним при цьому є те, що С. Гантінгтон теж відстоює пріоритетність цієї істини. Що ж стосується поділу їх на об'єктивні та суб'єктивні, то він, на нашу думку, надто умовний і навряд чи може бути прийнятий. Справа в тому, що всі зв'язки між людьми (виробничі, обміну, соціальних груп, цивільні, військові та ін.) носять лише об'єктивну природу за своїм змістом, оскільки вони не залежать від волі та свідомості людей, а існують наявно. Тому поділ на об'єктивні та суб'єктивні відносини не розкриває їх сутності.

На нашу думку, суб'єктивною може бути лише форма прояву цієї сутності, тобто, суб'єктивне розуміння і реалізація цих зв'язків. В такому випадку діалектика передбачає не стільки суб'єктно-об'єктну класифікацію, скільки вияв змісту та форми цих відносин, де змістовну функцію виконують цивільні зв'язки як загально соціальні, а статус форми їх реалізації належить військовим.

Цей зміст і форма поєднуються в особливості та унікальності феномену національної безпеки, яка надає ЦВВ безпекового характеру. Адже саме забезпечення національної безпеки виступає рушійною силою формування та розвитку ЦВВ, бо безпека є атрибутом існування суспільства. Вона, по-перше, диктує спрямованість цих відносин на забезпечення існування соціуму, його конструктивного розвитку і, як наслідок, озброює спроможністю передбачати протидіяти загрозам та небезпекам як внутрішнього, так і зовнішнього характеру.

По-друге, в цій спрямованості закладена потреба регулювання цих відносин з метою їх упорядкування, що зумовлює створення системи суб'єктів забезпечення національної безпеки. І ця суб'єктність (не суб'єктивність) саме і є виразом суті цивільно-військових відносин, які в кінцевому рахунку і формують стратегію і тактику діяльності цих суб'єктів. Тобто, ці відносини є основою, на якій базується безпекова політика держави як її невід'ємний атрибут. Ця безпекова політика, в силу своєї

значущості, має конституційний статус. Цим самим ЦВВ набувають функції регулятора безпекової діяльності.

І сама практика ЦВВ випереджує ці теоретичні недоопрацювання і йде шляхом їх розвитку через налагодження цивільно-військового співробітництва. З цією метою у Збройних Силах України створені відповідні підрозділи, на які покладені наступні функції: "систематична, планомірна діяльність Збройних Сил України по взаємодії з органами виконавчої влади, органами місцевого самоврядування, громадськими об'єднаннями, організаціями та громадянами у районах дислокації військових частин та підрозділів Збройних Сил України з метою формування позитивної громадської думки про діяльність Збройних Сил України і забезпечення сприятливих умов для виконання покладених на них завдань та функцій" [13].

Інший аспект цивільно-військових відносин пов'язаний з реалізацією Міжнародного гуманітарного права ("права війни", далі – МГП): саме Збройним силам України судилася практична місія втілення в життя світових та європейських цивілізаційних досягнень, що впроваджені у МГП.

Це, по-перше, радикально змінює саму ментальність військовослужбовців, наділяючи їх атрибутами носіїв світової та європейської культури і, разом з тим, подальшого ствердження їх національної самобутності, а по-друге, що на наш погляд є головним, посилює їх роль, як чинника впливу на всі інші структури суспільства та сфер його функціонування. Мова йде про те, що ЗСУ, маючи високий ступінь суспільної довіри, як захисників Вітчизни, у той же час сприяють залученню України до світових цінностей та стандартів. Вважаємо, що це не кон'юнктурно-політична їх акція, а об'єктивно зумовлена необхідність.

Отже, як стверджує І.О. Остапенко: "Можемо зробити висновок, що розуміння необхідності налагодження та підтримання взаємодії військового компоненту з об'єктами цивільного середовища забезпечує досягнення максимального ефекту при виконанні Збройними Силами України поставлених перед ними завдань. Ми переконані, що цивільно-військове співробітництво є найбільш ефективним та результативним сегментом відносин між суспільством і збройними силами, а також між збройними силами і політичною владою. На нашу думку, в умовах сьогодення глибоке осмислення змін щодо ведення сучасних операцій (бойових дій), неординарний підхід до виконання поставлених завдань та вміння командира налагодити ефективну взаємодію з об'єктами цивільного середовища стали велінням часу, що, у свою чергу, потребує подальшого розвитку та удосконалення" [10, с. 50].

Водночас, як зазначалось нами, у чинному законодавстві України термін ЦВВ не застосовується, хоча фактично їх змістовна наповненість розкривається без вказівки на те, що мова йде саме про ці відносини. Тобто, констатується їх необхідність, наявність як безпекового чинника, який діє через призму цивільного контролю за сектором безпеки і оборони України, що не дає можливості охопити весь феномен цих відносин у повному обсязі. Причини цього вбачаємо в першу чергу в механічному перенесенні положень міжнародних актів в національне законодавство, а також у теоретичному недоопрацюванні суті і змісту таких відносин.

У вище згадуваній праці С. Гантінгтона "Солдат та держава…" саме ця цілісна безпеко-оборонна функція ЦВВ окреслена однозначно, а щодо всеосяжного цивільного контролю над воєнною організацією держави та її діяльністю, він зазначає, що це апріорно приречено на провал. На його думку, значна частина контролю повинна бути організована у воєнній сфері зсередини і залишена за військовими, в усякому разі, поки офіцери та службовці діють відповідно до законів і директив легітимних органів

державної влади. Тому збройні сили та військові формування існують якомога далі від партійно-політичної боротьби за владу, що може бути забезпечено лише налагодженням повноцінних цивільно-військових відносин [12, с. 86-88].

Таким чином ЦВВ, як ми вище аргументували, є фактором визначальним, що зумовлює формування та здійснення безпекової політики і тому законодавство у сфері безпеки і оборони має вибудовуватись, виходячи з пріоритетності їх засад. На нашу думку, ця соціальна характеристика ЦВВ визначає їх роль як чинника консолідації суспільства, розвитку його провідних громадянських начал, де військові, закономірно, є рівноправними членами соціальної спільноти, і, разом з тим, професійної корпоративності, що є невід'ємною складовою функціонування соціуму.

Концентрація уваги дослідників на питанні демократичного цивільного контролю над сектором безпеки оборони України, а не ЦВВ, очевидно, викликано тим, що автори, і це відповідає дійсності, вважають такий контроль одним із важливих засобів формування та розвитку цивільно-військових відносин, розвитку громадянського суспільства. Тому, очевидно, і законодавці України теж пішли цим шляхом.

В той же час зазначимо, що абсолютизація контрольної функції небажана, і перш за все тому, що будь який контроль, при всій його конструктивності, суб'єктивно, в силу своєї імперативності, не сприяє повноцінності реалізації відносин, оскільки підконтрольна сторона не відчуває себе рівнозначним суб'єктом відносин, тобто, партнером. Тому вкрай важливо законодавчо створити чіткі обмеження з реалізації контрольної функції і передбачити відносну автономність відносин, причому в цьому питанні слід погодитися з С. Гантінгтоном: "об'єктивний контроль передбачає визнання існування у збройних силах особливих, залишених професійним військовим автономних, вільних від політики сфер (наприклад, бойова підготовка, оволодіння навичками застосування різ них видів зброї тощо). У такий спосіб політична діяльність цивільних груп у збройних силах мінімізується. У своїй сфері військові самі здійснюють контроль" [12, с. 83-85].

Більш того, об'єктивно, контроль побудований на політиці обмежень, що навряд чи є виправданим. Навпаки, вважаємо, більш конструктивною є політика широкого залучення військових до суспільних процесів, щоб соціально-психологічний стереотип побудови суспільства на правових, демократичних засадах став для військових таким же обов'язковим, як і для цивільних.

Отже, характер взаємозв'язку й взаємодії армії і політики може бути різним. Він визначає рівень стабільності суспільно-політичного устрою і владних відносин. Усвідомлення ролі та місця Збройних сил у суспільстві, визначення сутності армії у контексті взаємодії з владою, дослідження чинників і факторів, що зумовлюють різні моделі і форми взаємозв'язку армії і політики, – важлива й актуальна проблема, яка потребує подальшого вирішення.

З іншого боку, законодавче закріплення ЦВВ дасть можливість поєднати діяльність суб'єктів безпеки та оборони в єдиний комплекс дій, що відповідатиме потребі удосконалення військової складової безпеко-оборонної сфери, інтересам всього громадянського суспільства.

Таким чином ці відносини у законотворчій практиці визнаються і реально виступають регулятивним чинником безпеково-оборонної сфери. Але вважаємо що цього недостатньо, оскільки осторонь залишаються цілі пласти безпекової реальності громадянського суспільства. Зокрема, не враховується аспект національної культури, як джерела самоідентифікації нації, що нині вкрай важливо для збереження і розвитку національної самосвідомості, загрози якій сьогодні особливо відчутні.

Висновки.

Визначений нами статус цивільно-військових відносин як базового чинника безпеки і оборони держави зумовлює потребу його унормування і подальшого використання з метою консолідації українського суспільства і орієнтації на подальше зміцнення обороноздатності країни.

Застосування діалектичної методології дало можливість відносно повно розкрити сутнісні особливості ЦВВ, піднести їх до рівня важеля вирішення значущих соціальних проблем національного безпеко творення. Разом з тим, зроблено висновок, що ЦВВ існують об'єктивно і так чи інакше впливають на всі сторони суспільного життя, вони потребують подальшого правового визначення і розвитку.

Використана література

1. Философская энциклопедия. Т. 4 / под ред. Ф.В. Константинова. Москва: Советская энциклопедия, 1967. 592 с.

2. Сіцінська М.В. Проблеми українського суспільства у сфері цивільно-військових відносин. *Вісник Національної академії державного управління.* 2013. С. 82-89.

3. Рябоконь Г.Д. Питання демократичного цивільного контролю над воєнною організацією правоохоронними органами держави. URL: https://minjust.gov.ua/m/str_954

4. Кодекс поведінки стосовно військово-політичних аспектів безпеки ОБСЄ. Organization for Security and Co-operation in Europe. 3 грудня 1994.

5. Про оборону України: Закон України. *Відомості Верховної Ради України (ВВР).* 1992. № 9. Ст. 106.

6. Про національну безпеку України: Закон України. *Відомості Верховної Ради (ВВР)*. 2018. № 31. Ст. 241.

7. Про Збройні Сили України: Закон України. *Відомості Верховної Ради України (ВВР)*. 1992. № 9. Ст. 108.

8. Білошицький В.І. Специфіка прояву цивільно-військових відносин у державах Євросоюзу. *Вісник НТУУ "КПІ". Політологія. Соціологія. Право*. Вип. 1/2 (25/26). 2015. С. 25-29.

9. Білошицький В.І. Цивільно-військові відносини в країнах НАТО: історія та сучасність. *Вісник НТУУ "КПІ". Політологія. Соціологія. Право*. Вип. 4 (20) 2013. С. 7-13.

10. Остапенко І.О. Перспективи розвитку цивільно-військового співробітництва в Україні: тези доповідей XV Міжнародної науково-практичної конференції *Військова освіта і наука: сьогодення та майбутнє,* Секція 7. Актуальні проблеми військового права (частина 2). С. 49-52. м. Київ, 29 лист. 2019 р. Київ: Військовий інститут Київського національного університету імені Тараса Шевченка, 2019.

11. Про затвердження Порядку в'їзду осіб, переміщення товарів на тимчасово окуповані території у Донецькій та Луганській областях і виїзду осіб, переміщення товарів з таких територій: Постанова Кабінету Міністрів України від 17.0719 р. № 815. (Із змінами, внесеними згідно з Постановами КМ).

12. Huntington S. The Soldier and the State. *The Theory and Policies of the Civil-Military Relations.* The Cambridge: Belknap Press of Harvard University Press, 1957.

13. Про затвердження Тимчасової настанови з цивільно-військового співробітництва у ході підготовки та застосування Збройних Сил України: наказ Генерального штабу Збройних Сил України від 02.04.19 р. № 131.

14. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави: Закон України. *Відомості Верховної Ради України (ВВР)*. 2003. № 46. Ст. 366. – (Закон втратив чинність на підставі Закону № 2469-VIII (2469-19) від 21.06.18 р.).

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

УДК 338.439.5:339.162.3

КРИВЕНКО А.Л., співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.

ПРАВОВЕ РЕГУЛЮВАННЯ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ: ДОСВІД ЕС

Анотація. *У статті здійснено аналіз процесу розвитку та становлення інституту публічних закупівель в Україні та іноземних державах, досліджено організаційно-правове регулювання публічних закупівель в Україні, визначено нормативно-правове регулювання публічних закупівель, а також розроблено шляхи впровадження в Україні досвіду законодавства Європейського Союзу у сфері публічних закупівель.*

Ключові слова: *інститут публічних закупівель, державний бюджет, європейський досвід, публічні закупівлі, фінансовий контроль.*

Summary. *The article analyses the development process and establishment of the public procurement institute in Ukraine and foreign countries, examines the organizational and legal regulation of public procurement in Ukraine, identifies legal regulation of public procurement in the European Union and ways to implement the experience of European legislation in the field of public procurement in Ukraine.*

Keywords: *public procurement institute, State budget, European experience, public procurement, financial control.*

Аннотация. *В статье осуществлен анализ процесса развития и становления института публичных закупок в Украине и отдельных зарубежных странах, исследовано организационно-правовое регулирование публичных закупок в Европейском Союзе, а также разработаны пути внедрения в Украине опыта законодательства Европейского Союза в сфере публичных закупок.*

Ключевые слова*: институт публичных закупок, государственный бюджет, европейский опыт, публичные закупки, финансовый контроль.*

Постановка проблеми. В умовах сучасної економічної ситуації, що склалась в Україні, необхідно визначити роль і можливість вдосконалення механізму здійснення публічних закупівель. Крім того, необхідно проаналізувати сучасний стан законодавства, а також з метою його удосконалення запропонувати варіанти змін до чинних нормативно-правових актів з урахуванням європейського досвіду.

Одним з найперспективніших шляхів збалансування державного бюджету в сучасних умовах ринкової економіки вважається інститут публічних закупівель. Саме за допомогою цього механізму держава має змогу забезпечувати свої потреби за єдиною централізованою системою.

Актуальність теми дослідження полягає в тому, що інститут публічних закупівель є однією з головних складових економіки будь-якої держави. Саме тому вітчизняне правове регулювання цієї сфери потребує значних змін та доповнень з боку законодавця. Вагомість дослідження та покращення механізму реалізації публічних закупівель в Україні в контексті світових принципів державної закупівельної політики визначається слабким економічним розвитком країни, а також нерезультативною діяльністю економічних структур та неефективним використанням бюджетних ресурсів. Сьогодні система публічних закупівель перебуває на стадії зародження, яка супроводжується невирішеними проблемами щодо законодавчого спрямування, регламентації планування

та контролю за суб'єктами державних закупівель. Тому сьогодні існує гостра потреба у побудові нових моделей організації державних закупівель, що сприятиме забезпеченню стабільного соціально-економічного розвитку держави.

Результати аналізу наукових публікацій. Серед українських та зарубіжних науковців, у працях яких досліджувалась окреслена проблематика, варто назвати таких, як: Ю.І. Пивовар, Л.В. Фалько, І.В. Влялько, А.О. Олефір, Н.Ю. Цибульник, Я.В. Петруненко та ін. Крім того, заслуговує на увагу наукові розробки вчених-економістів, таких як В.В. Зубар, Г.І. Пінькас, О.А. Нагорнічевський. Однак, на сьогодні відсутні комплексні наукові роботи по дослідженню перспективних напрямів використання у господарському законодавстві України позитивного зарубіжного досвіду у сфері регулювання публічних закупівель як одного з дієвих господарсько-правових засобів забезпечення ефективного використання державних коштів, що вказує на важливість вивчення даної проблематики.

Аналіз соціально-економічних проблем українського суспільства показав, що формування інституту державної закупівельної діяльності вимагає системного підходу. Існує потреба в уточнені понятійного апарату економічної науки у сфері впровадження інституту державних закупівель, обгрунтуванні та розробці концептуальних засад розвитку системи державних закупівель, удосконалення механізму бюджетного фінансування державних закупівель шляхом введення процедури попереднього контролю, розвитку.

Метою статті є розробка теоретичних та практичних питань удосконалення чинного законодавства України у сфері регулювання публічних закупівель.

Для досягнення поставленої мети вважаємо за необхідне проаналізувати організаційно-правове регулювання публічних закупівель в Україні та окремих країнах, визначити нормативно-правове регулювання публічних закупівель у Європейському Союзі, описати перспективи та шляхи впровадження в Україні досвіду європейського законодавства у сфері публічних закупівель.

Виклад основного матеріалу. Потужним важелем впливу держави на економіку є система державних замовлень, закупівель продукції, робіт та послуг для державних та муніципальних потреб. Оскільки державні закупівлі займають значне місце у витратній частині бюджету більшості розвинених країн, то вони є дієвим інструментом управління економікою. За допомогою державних контрактів багато держав вирішують свої соціально-економічні проблеми, а також забезпечують проведення наукових досліджень, створення і впровадження нових технологій і розробок.

Ефективність публічних закупівель визначається насамперед додержанням усіма учасниками цієї системи вимог щодо економії та справедливості під час її організації. Від ефективності здійснення публічних закупівель залежить успішність функціонування економіки загалом. Відповідно, є актуальним питання подальшого розвитку системи публічних закупівель та підвищення ефективності використання державних коштів з метою забезпечення українського населення якісними товарами та послугами. У середньому обсяги державних закупівель в країнах ЄС становлять від 8 % у Швейцарії до 25 % ВВП у Нідерландах. Проте обсяг цих закупівель не завжди свідчить про їх ефективність, оскільки цей сектор у кожній країні має свої корупційні складові. Обов'язки державних закупівель за Угодою про державні закупівлі Світової організації торгівлі (СОТ) оцінюються приблизно в 1,3 трлн. Євро.

Однією з ключових проблем у сфері публічних закупівель є недосконале законодавче врегулювання організаційно-правових відносин між учасниками торгів, а саме законодавчі прогалини та проблеми у застосуванні законодавства, що яскраво

виражено в наявності певних колізій, які ускладнюють його застосування суб'єктами господарювання. Законодавцем не розроблена та не закріплена система внутрішнього та зовнішнього, поточного, попереднього, подальшого контролю. Крім того, наявна недосконаліть в Україні фінансової системи, проблеми якої негативно впливають на діяльність системи публічних закупівель.

У спробах підвищити якість публічних закупівель, Україна взяла курс на євроінтеграцію, запозичуючи досвід європейських держав, зокрема і у цій сфері.

Однак, поруч з цим залишаються невирішеними ряд питань, наприклад, встановлення цінової політики для проведення конкурсних торгів. О.С. Мельников зауважив, що ціни для застосування процедури проведення торгів збільшувались, тобто це залежить від інфляції в країні, що властива економіці кожної держави в цілому [1].

У більшості випадків при здійсненні державних закупівель товарів мають враховуватися не тільки цінові межі, а й якісні характеристики предмета закупівлі. Від ефективності закріплення критеріїв на законодавчому рівні залежить результат здійснення державних закупівель, оскільки на сьогодні основним правилом, яким керуються на практиці, є цінові межі. На жаль, не завжди переможець торгів, тобто учасник, який запропонував найнижчу ціну, може забезпечити належний рівень якості торгів, робіт або послуг. Ця позиція обгрунтовується тим, що між ціною та якістю завжди існує прямий зв'язок. Тому доцільним буде встановлювати в документації конкурсних торгів чіткі вимоги до якості предмета закупівлі. Відразу після цього постає й інше не менш важливе питання: як перевірити достатній рівень кваліфікації членів комітетів, оскільки від їх кваліфікації залежить встановлення належних та якісних критеріїв для предмета закупівлі.

На разі ще одним дискусійним запитанням залишається взаємодія системи державних закупівель із природними монополіями. У таких випадках, коли предмет закупівлі може постачатися одним постачальником, немає сенсу у проведенні конкурсних процедур закупівель. При цьому, постачальник має необмежений контроль над ціною предмета закупівлі, що призводить до нераціонального використання коштів з державного бюджету. Зазначена позиція є незадовільною, і тому в законодавстві має бути чітко прописано механізм щодо регулювання ціни пропозиції від природних монополій.

Перелік прогалин в законодавстві можна продовжувати: інформаційне забезпечення конкурсних торгів, порядок оскарження результатів, механізм корегування договірних цін, необхідність введення акредитації членів комітетів з конкурсних торгів.

Майбутнє вдосконалення законодавства у сфері державних закупівель повинне проводитись на базі системного аналізу процесів, які відбуваються у цій сфері. Для реалізації цих положень необхідно чітко визначити критерії визначення доцільності застосування процедур конкурсних торгів, розробити необхідні методи та методики оцінки пропозицій учасників торгів з чітко встановленими критеріями, врегулювати питання публічних закупівель товарів та послуг у природних монополій. Раціонально буде також конкретизувати в законодавстві вимоги, які стосуються якості товарів, послуг, що є об'єктом закупівлі. Для реалізації цієї мети необхідно спиратися на вимоги державних стандартів серій ISO 9000 та ISO 14000.

Не дивлячись на те, що система публічних закупівель яскраво виділяється у засобах масової інформації, достатньо уваги приділяється державою, але все одно вона залишається непрозорою. О.В. Грибовський зауважив, що результати оцінки системи державних закупівель, які здійснювалися аудиторською групою за критерієм економії ресурсів, свідчать про наявність проблем, через які втрачається близько 20-25 %

державних бюджетних ресурсів. Наявність прогалин у функціонуванні системи державних закупівель підтвердили і результати анкетування, згідно з якими наявна система не задовольняє близько 60 % бюджетних установ та 65 представників комерційних структур. Крім того, у анкетах 60% опитуваних указали, що дана система є малоефективною, а 24 % – взагалі не мають до неї довіри [2].

Основними факторами, які впливають на негативні результати є:

- законодавчі прогалини та проблеми у застосуванні законодавства, що яскраво виражено в наявності певних колізій, які ускладнюють його застосування суб'єктами господарювання;

- законодавцем не розроблена та не закріплена система внутрішнього та зовнішнього, поточного, попереднього, подальшого контролю;

- недосконаліть наявної в Україні фінансової системи, проблеми якої негативно впливають на діяльність системи публічних закупівель;

- незацікавленість керівництва у реалізації системи публічних закупівель у найекономніший спосіб. При укладенні договорів відсутня вимога про обов'язкову оцінку ефективності роботи керівника протягом року;

- відсутність достатнього інформаційного середовища про ринок товарів та послуг.

Анкетування показало, що при проведенні публічних закупівель розпорядники державних коштів майже не користуються електронними та друкованими ресурсами, що містять інформацію про ціни на товарному ринку. Внаслідок вказаного ми маємо глибоку необізнаність суб'єктів господарювання про товари, послуги, ціни в регіоні і державі.

Що стосується питання організації, регулювання та спроб вдосконалення публічних закупівель в Україні на законодавчому рівні, то варто зазначити, що Законом України від 16.11.14 р. № 1678-VII [3] було ратифіковано Угоду про асоціацію між Україною, з однієї сторони, Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Так, у частині 1 статті 153 глави 8 розділу IV даної Угоди передбачено, що Україна забезпечує поступове приведення існуючого та майбутнього законодавства у сфері державних закупівель у відповідність до acquis ЄС у сфері державних закупівель [4], а також визначено необхідність імплементації Директив Європейського Союзу, а саме № 2014/24/ЄС та №2014/25/ЄС.

Окрім цього, пунктом 5 "Децентралізація та реформа державного управління" Указу Президента України від 12.01.15 р. № 5/2015 "Про стратегію сталого розвитку "Україна – 2020" визначено, що пріоритетом в управлінні публічними фінансами має стати підвищення прозорості та ефективності їх розподілу та витрачання. Процес здійснення державних закупівель повинен стати максимально прозорим, корупційна складова під час здійснення державних закупівель має бути ліквідована [5].

Також Розпорядженням Кабінету Міністрів України "Про Стратегію реформування системи державних закупівель ("дорожню карту")" від 24.02.16 р. №175-2016-р до 2022 року передбачено основні напрями реформування системи державних закупівель, що об'єднують: а) гармонізацію національного законодавства з правилами Європейського Союзу шляхом імплементації положень директив ЄС вітчизняним законодавтством; б) розвиток інституційної структури, вдосконалення й оптимізацію функцій контролюючих органів; в) міжнародне співробітництво у сфері державних закупівель; г) розвиток електронних закупівель; д) навчання і професіоналізацію у сфері деражавних закупівель [6].

Стандартизація законодавства у сфері регулювання публічних закупівель держав необхідна для майбутніх постачальників товару, послуг, продукції, оскільки, вони мають можливість брати участь у тендерах різних держав, але головною ознакою є рівні умови участі. Саме такі цілі і ставилися перед українським законодавством, під час розробки законодавства у сфері державних закупівель.

Законодавство Європейського Союзу встановлює ряд принципів, за якими має реалізуватися процес державних закупівель в державах-членах ЄС: відсутність дискримінації; прозорість процедур здійснення закупівель; інформування про вибрану процедуру присудження контракту; відповідність технічним вимогам; прозорість процедур добору підрядників і присудження контрактів через використання завчасно сформульованих об'єктивних критеріїв [7].

Одним з важливих нормативних актів, які слід проаналізувати, є Генеральна угода про тарифи і торгівлю, яку було укладено у рамках Уругвайського раунду 15 квітня 1994 року між 22 урядами, а головним чином між Сполученими Штатами Америки і державами-членами Європейського Союзу. Дана угода набула чинності лише 1 січня 1996 року і відкрила ринок публічних закупівель у багатьох сегментах держав-учасниць. Базовими принципами, які були покладені в основу даної угоди, є здійснення державних закупівель на рівних умовах, а також недопущення дискримінації при реалізації прав та свобод у даній сфері. Положення Угоди визначають також умови про рівноправність, тобто рівне ставлення до вітчизняних та іноземних постачальників, відсутність будь-яких дискримінаційних положень у законах, постановах, процедурах тощо.

У рамках Європейського Союзу та Світової організації торгівлі було розроблено всеохоплюючу регулятивну базу для державних закупівель, вартість яких значно перевищує відповідні порогові показники. Усі держави-члени Угоди мають імплементувати дані положення в національне законодавство.

Загалом, принципи і правила GPA за своєю суттю не відрізняються від принципів та правил, що були прописані в Директивах щодо закупівлі у межах держав Європейського Союзу.

Наступним етапом у розвитку нормотворчої бази у сфері публічних закупівель стали Римські угоди у 1957 році, якими було створено дві організації: Європейське економічне співтовариство, а також Європейське співтовариство атомної енергії [7].

Початкові правила державної закупівлі містилися у Римській угоді, але вони були досить неточними для вільного застосування закупівельними товариствами. Комісія Європейського Союзу разом з державами-членами розробила відповідні директиви щодо державної закупівлі для того, щоб Римські угоди почали нормально функціонувати і здійснили свою поставлену мету. Дані директиви містять більш детальні правила, які мають виконуватися органами виконавчої влади [7].

Необхідно зауважити, що одним з основних актів регулювання здійснення державних закупівель став Лісабонський договір 2007 року, яким не передбачалося внесення змін у правове регулювання сфери державних закупівель, так як забезпечення основних свобод недискримінації залишаються незмінними. Але варто звернути увагу й на те, що Лісабонський договір таки вніс деякі доповненя до сфери здійснення державних закупівель, наприклад з'явилися нові статті з метою сприяння та використання ефективних та сумісних метоів закупівель для Європейського оборонного агенства. При аналізі вторинного права Європейського Союзу на сучасному етапі, не можна не помітити, що в правовому регулюванні держзакупівель спостерігалась чітка дихотомія цієї сфери, тобто поділ на два сектори: традиційний (закупівля товарів, послуг, робіт тощо), а також особливий (постачання води, енергоресурсів, поштові

послуги тощо). Положення цих Директив забороняють будь-яку дискримінацію або будь які обмеження щодо усіх контрактів незалежно від їх вартості, а також автоматично застосовуються до всіх державних закупівель, навіть якщо в договорі немає посилання на ту чи іншу директиву [7]. Мета прийняття Директив – це не погодження усіх національних правил державної закупівлі, а створення єдиної процедури, якої мають дотримуватися держави-члени, навіть за умови, що очікувана вартість закупівель перевищує порогові показники. Кожна Директива регулює певну сферу державних контрактів, тоді як загальні принципи, які прописані у Римській угоді, мають застосовуватися до всіх контрактів, незалежно від сфери використання та їх вартості [7].

Одним з основних документів, який акумулював весь наявний міжнародний досвід і практичні напрацювання в сфері публічних, а також громадських закупівель є Типовий закон ЮНСІТРАЛ "Про закупівлі товарів (робіт) та послуг" від 1994 року, який був прийнятий на 27-й сесії Комісії ООН по праву міжнародної торгівлі. Основними цілями, які були покладені в основу Типового закону, визначено: максимальний розвиток конкуренції; забезпечення справедливого ставлення до постачальників; підвищення рівня відкритості та об'єктивності при проведенні держзакупівель. Зазначений нормативний акт рекомендується застосовувати у всіх випадках проведеня державних закупівель, але з певними винятками, а саме з тими, які забезпечують національну оборону і безпеку.

Наступним по значущості міжнародним доументом є багатостороння Угода про державні закупівлі (Agreementon on Government Procurement), що прийнята за результатами Уругвайського раунду багатосторонніх торгових переговорів у 1994 році. Даний документ є частиною Генеральної угоди з торгівлі та тарифів (ГАТТ). Підписання Угоди не є головною умовою для вступу країни до Світової організації торгівлі, але протягом останніх десяти років з'явилася чітка тенденція: провідні держав-членів Світової організації торгівлі вважають за необхідне підписати її у ході двосторонніх переговорів.

Розробники даного акту поклали в основу досягнення таких цілей: заборона на дискримінацію іноземних постачальників, забезпечення прозорості законодавства та застосовуваних процедур закупівель. Отже, замовники мають проводити конкурс на рівних умовах для всіх учасників, тобто їм заборонено надавати певні пільги окремим учасникам. Також розроблена заборона на встановлення до закуповуваної продукції технічних вимог, що обмежують міжнародну торгівлю; технічні вимоги до товарів, робіт та послуг мають відповідати встановленим міжнародним правом стандартам.

Закупівлі держав, що входять до Європейського Союзу, як і раніше, здійснюються органами державного управління згідно з національним законодавством. Однак до уваги беруться не тільки національні правила закупівель, але й законодавство та рекомендації Європейського співтовариства, встановлені в раніше згадуваних директивах.

Одним із найбільш ефективних інструментів для створення системи публічних закупівель, подібної до такої, що є в Європейському Союзі, та побудованої на засадах прозорості та дієвості, є створення комплексного законодавства із фінансового контролю, результатом чого стане зменшення фіскального тиску на підконтрольні об'єкти та забезпечення чіткої регламентації процесу контролю за здійсненням закупівель. Це пояснюється не лише дефіцитом державного бюджету, а й необхідністю закупівлі якісних товарів, робіт та послуг за обґрунтованими цінами.

О.А. Нагорнічевський зазначає, що шляхами вдосконалення механізму проведення публічних закупівель є: вдосконалення регулюючого відносини у сфері державних закупівель законодавства, метою якого є спрощення закупівельних процедур;

впровадження системи електронних закупівель; розвиток конкурентного середовища; боротьба з корупцією; впровадження відповідальності за нові та посилення відповідальності за вже існуючі правопорушення у галузі публічних закупівель; імплементація міжнародних стандартів у національну правову систему [8].

Враховуючи досвід згаданих в цій роботі держав, одним із найбільш результативних шляхів розвитку держави та втілення в життя концепції раціонального та ефективного використання бюджетних коштів вбачається впровадження єдиної структурованої, побудованої на принципах децентралізації, прозорості, конкуренції, недискримінації системи у сфері закупівель для державних потреб.

Отже, існує об'єктивна необхідність у впровадженні низки заходів законодавчого та методичних рівнів, метою яких є створення об'єктивного середовища та всіх умов для добросовісної конкуренції, а також запобігання, перешкоджання та боротьба з проявами корупції в даній сфері.

Одним із напрямків вдосконалення вітчизняної системи проведення публічних закупівель є її децентралізація, яка дозволить більш гнучко реагувати на потреби ринку та забезпечить значно більшу мобільність у обороті товарів та послуг у закупівельній сфері. Деякі вчені вважають, що про децентралізацію у вітчизняній сфері регулювання закупівель прямо свідчить законодавче визначення широкого кола розпорядників бюджетних коштів.

При цьому не можна не визнати переваги і за централізованим методом регулювання даної сфери. Зокрема, як зазначається у [9] – якщо децентралізовані закупівлі за своєю природою є гнучкими та оперативними в їх проведенні, проте досить витратними, то централізовані навпаки дають можливість укладати договори за значно нижчими цінами, що у свою чергу, пов'язане зі значними оптовими закупівлями, проте не мають тієї мобільності та, що особливо принципово, не враховують індивідуальні особливості задоволення потреб замовників Тобто, значну роль у питанні удосконалення вітчизняної системи закупівель приділяється питанню дослідження та аналізу суб'єктного складу проведення державних закупівель.

16 березня 2016 року на умовах рішення Комітету з державних закупівель Світової організації торгівлі GPA/133 від 16 листопада 2015 року Україна приєдналася до Угоди про державні закупівлі, укладеної 15 квітня 1994 року в м. Марракеші [10]**.** Даною Угодою було відкрито можливість долучатися до глобального ринку публічних закупівель для українських замовників. Таким чином, національний бізнес отримав змогу брати участь у державних закупівлях 45 держав-членів вищезгаданої Угоди. Завдяки цій реформі держава підвищила обізнаність учасників публічних закупівель, а торговельні майданчики шляхом застосування стандартів відкритих даних GPA отримали статус децентралізованих.

Впровадження платформи для проведення електронних торгів безсумнівно є одним із шляхів удосконалення вітчизняної системи публічних закупівель. Адже для того, щоб оптимізувати сферу публічних закупівель державним установам необхідно проводити узагальнення і систематизацію інформації про витрати на закупівлі, стимулювати, змінювати та заохочувати до цього інших суб'єктів, займатися оптимізацією процедури закупівель і вдосконалювати, відповідно, організаційну модель. Сукупність цих процесів, що спрямовані на модернізацію та покращення вже існуючих механізмів реалізації поставлених завдань у даній сфері, є важливим елементом реформування системи публічних закупівель. З цього приводу Франческо Гарден вважає що, саме електронні закупівлі можуть призвести до позитивного впливу та ефективного результату конкурентоспроможності та прозорості даної сфери. Введення електронних

закупівель у державному секторі – це далеко не просто технологічне питання; це масштабні зусилля з боку усіх учасників процесу для створення більш ефективної культури закупівель [11]. Саме через це електронні публічні закупівлі гарантовано сприятимуть оптимізації державних витрат у зв'язку з підвищенням організаційних показників, а також посилюватимуть підзвітність зацікавлених сторін закупівель як уповноваженими органами, так і державними постачальниками послуг.

Застосування інформаційних і комунікаційних технологій у сфері публічних закупівель товарів, робіт та послуг дає змогу усунути низький рівень ефективності використання бюджетних коштів та підвищити результативність заходів у сфері державного управління. Впровадження автоматизованих інформаційних систем електронних закупівель для державних потреб забезпечує вдосконалення процедери закупівель завдяки автоматизації всіх етапів і стадій процесів планування, формування та здійснення закупівель, а також функцій аналізу й контролю їх реалізації. Прозорість механізму закупівель на всіх стадіях і рівнях сприятиме запобіганню скороченню бюджетних витрат під час закупівель продукції для державних потреб, а також підвищенню економічної ефективності праці виконавчих органів державної влади на всіх рівнях [12]. Що стосується безпосередньо такої системи, то внаслідок проведення вищезгаданої реформи державних закупівель у 2015 році було створено систему публічних електронних закупівель “Prozorro”. Зазначається, що дана реформа була проведена з метою системного викорінення корупції, підвищення прозорості в даній сфері, переходу на електронний документообіг та товарообіг, викорінення дискримінації за різними признаками учасників публічних закупівель, залучення громадськості до проведення та контролю за здійсненням публічних торгів та їх виконанням [13].

Окрім цього, у сучасному українському законодавстві відсутні вимоги підтвердження законності діяльності, здійснюваної учасником торгів, яке мало б офіційне документальне підтвердження.

На нашу думку, задля покращення ситуації та вирішення даної проблеми об’єктивно необхідним є вичерпне нормативно-правове визначення кваліфікаційних критеріїв, що мають висуватися до потенційних учасників торгів, що, у свою чергу, унеможливить зловживання як із боку замовників, так і з боку недобросовісних учасників публічних закупівель. Прикладом тому є норми ст. 46 – 48 Директиви 2004/18/ЄС, де представлений вичерпний список економічних, професійних, фінансових, технічних вимог до потенційних учасників, названо типи документів, що їх підтверджують [14].

На окрему увагу заслуговують способи удосконалення системи публічних закупівель в контексті національної безпеки.

Саме тому, зважаючи на пріоритетність завдань держави щодо попередження розкрадання бюджетних коштів, відбувається тісна взаємодія органів внутрішніх справ та органів контролю з органами Державної аудиторської служби України та іншими органами, компетентними у сфері публічних закупівель [15]. Адже очевидним є те, що проведення прозорих, гласних процедур публічних закупівель, побудованих на засадах конкурентності, є запорукою успіху в питанні використання коштів для задоволення власних потреб для будь-якої держави.

В останні роки однією із визначальних особливостей правової системи України є прийняття великої кількості різноманітних нормативно-правових актів, подання тисячі законопроектів, більшість з яких написана малоосвіченими в конкретній сфері громадянам. Всі ці дії робляться для того, щоб якнайшвидше вибірково підлаштувати ті чи інші національні закони під законодавство Європейського Союзу. Це стосується, у тому числі, питань регулювання публічних закупівель відповідними Директивами ЄС.

Проте, на жаль, спроби адаптації вітчизняних правових норм до європейських спричиняють протиріччя та неузгодженість актів між собою, не відповідають реаліям українського суспільства. Як правило, кількісна величина прийнятих нормативно-правових актів не завжди супроводжується високою якістю. Тому чинна нормативно-правова база багатогранна, заплутана та переповнена порушеннями правил юридичної техніки, на що при опрацюванні в комітетах з власної чи чужої вигоди у компетентних осіб закриваються очі.

Для того, щоб розпочати трансформацію законодавства Європейського Союзу у сферу публічних закупівель в Україні потрібно розробити рекомендаційну систему, яка стосувалася б вдосконалення процедури прийняття нормативно-правових актів або внесення змін до них. Після чого затвердити її як обов'язкову до застосування на всіх рівнях законотворчого процесу.

Крім того, на засіданнях Комітету Громадської ради при Міністерстві юстиції України з питань міжнародного співробітництва та адаптації законодавства України до права Європейського Союзу є можливість підняти питання щодо вдосконалення законодавства у сфері публічних закупівель в Україні шляхом виконання норм Європейського Союзу. Після чого підготувати подання для розгляду порушених питань на засіданні Громадської ради.

Таким чином, прийнятим на засіданні Громадської ради рішенням можна ініціювати перед Міністерством юстиції України розробку змін до законодавства, які при задоволенні пропозиції будуть внесені до орієнтовного плану проведення консультацій з громадськістю, винесені на обговорення департаменту та при підтримці передані на розгляд Кабінету Міністрів України.

Висновки.

Проаналізувавши деякі принципи функціонування публічних закупівель у державах-членах Європейського Союзу, визначивши позитивні та негативні аспекти даного функціонування та виділивши серед них ті, що могли б бути перейняті Україною задля покращення власної системи публічних закупівель, варто зазначити таке.

Закупівлі на конкурсній основі є основним механізмом закупівель товарів, робіт і послуг для державних потреб у більшості країн світу. Процедури проведення конкурсів регламентуються законодавством і різного роду рекомендаціями державних органів або громадських організацій.

Регулювання державних закупівель у всьому світі є об'єктом уваги з боку законодавця, оскільки в даному випадку сам покупець, тобто держава, зацікавлена у ефективності процесу. Важливим питанням у цій діяльності є боротьба за чесну конкуренцію, яка, відповідно до економічної теорії, повинна спричинити зниження цін.

Стандартизація законодавства у сфері регулювання публічних закупівель держав необхідна для майбутніх постачальників товару, послуг, продукції, оскільки, вони мають можливість брати участь у тендерах різних держав, але головною ознакою є рівні умови участі. Саме ці цілі і ставилися перед українським законодавцем під час розробки законодавства у сфері державних закупівель.

Одним із найбільш ефективних інструментів для створення системи публічних закупівель, подібної до такої, яка існує в Європейському Союзі, та побудованої на засадах прозорості та дієвості, є створення комплексного законодавства із фінансового контролю, результатом чого стане зменшення фіскального тиску на підконтрольні об'єкти та забезпечення чіткої регламентації процесу контролю за здійсненням закупівель. Це пояснюється не лише дефіцитом державного бюджету, а й необхідністю закупівлі якісних товарів, робіт та послуг за обґрунтованими цінами.

Використана література

1. Мельников О.С. Організація системи державних закупівель у країнах ЄС. *Теорія та практика державного управління*. № 3 (38). С. 433-440.

2. Грибовський О.В. Державні закупівлі: проблеми функціонування в Україні. URL: //www.dkrs.gov.ua (дата звернення: 11.01.2021).

3. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.14 р. № 1678-VII. URL: //www.zakon.rada. gov.ua (дата звернення: 11.01.2021).

4. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 30.11.15 р. № 984_011. URL: //www.zakon.rada.gov.ua (дата звернення 11.01.2021).

5. Про Стратегію сталого розвитку "Україна – 2020": Указ Президента України від 12.01.15 р. № 5/2015. URL: //www.zakon.rada.gov.ua (дата звернення: 11.01.2021).

6. Про Стратегію реформування системи публічних закупівель ("дорожню карту"): розпорядження Кабінету Міністрів України від 24.02.16 р. № 175-р. URL: //www.zakon.rada.gov. ua (дата звернення 11.01.2021).

7. Державне регулювання закупівель в умовах реалізації адміністративної реформи. Івано-Франківськ: Івано-Франківський центр науки, інновацій та інформатизації. 2012. С. 8-48.

8. Нагорнічевський О.А. Основні напрямки удосконалення державного управління у сфері державних закупівель в Україні в контексті національної безпеки. *Ефективність державного управління*. 2015. № 43. С. 184-192.

9. Олефір А.О. Угода про державні закупівлі СОТ: правові наслідки для України. *Підприємництво, господарство і право*. 2017. № 3. С. 79-84.

10. Про приєднання України до Угоди про державні закупівлі: Закон України від 16.03.16 р. № 1029-VIII. URL: //www.zakon.rada.gov.ua (дата звернення: 11.01.2021).

11. Francesco Garden. A model to measure e-procurement impacts on organization performance. *Journal of Public Procurement*. Vol. 13. Issue 2. 2013. P. 215-242.

12. Цибульник Н.Ю. Адміністративно-правове забезпечення публічних закупівель в Україні: дис. …канд. юр. наук: 12.00.07. Запоріжжя. 2018. 222 с.

13. Загальні положення про PROZORRO. URL: https://e-tender.ua/training-tenders/teoriya-zakupivel-3/zagalni-polozhennya-pro-prozorro-5 (дата звернення: 11.01.2021).

14. Директива 2004/18/ЄС Європейського Парламенту та Ради від 31 березня 2004 року стосовно координації порядків надання державних контрактів щодо виконання робіт, постачання товарів та надання послуг. *Офіційний вісник Європейського Союзу*. 2004. С. 1-126.

15. Афонін Е.А., Суший О.В. Транспарентність влади в контексті європейської інтеграції України: конспект лекцій. – (НАДУ). 2010. 48 с

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

До відома авторів

"**ІНФОРМАЦІЯ І ПРАВО**" – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   - *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   - *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   - *відстань між рядками – 1 інтервал;*
   - *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов'язкові структурні елементи:

   - УДК.
   - Ім'я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.
   - Назва статті (укр. та англ. мовами).
   - Анотація та ключові слова (укр., англ. та рос. мовами).
   - **Розв'язання проблеми,** шляхом наукового вирішення завдання:
     - **постановка проблеми** *(загальна характеристика);*
     - **результати аналізу наукових публікацій** – надаються відомості про стан вирішення проблеми та ПІБ авторів, з обов'язковим посиланням на їхні роботи (в […]), повний опис бібліографії яких вказується в підрозділі "Використана література"; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;
     - **формування мети** *(постановка завдання)* статті;
     - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
   - **Висновки** за результатами розв'язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
   - **Використана література.** Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання" або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.
   - Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- ***Актуальність теми***.
- ***Новизна та обґрунтованість одержаних результатів***.
- ***Наукова (практична) цінність результатів***.
- ***Висновок про можливість відкритої публікації***.

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України "Про затвердження порядку формування переліку наукових фахових видань України" від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов'язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту**.

Реквізити для оплати робіт:

Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України". Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 *(з приміткою – за науковий журнал).*

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада НДІІП НАПрН України не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
  Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за додержання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:

– відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;

– внесення до статті змін редакційного змісту у зв'язку з обмеженням обсягу загального матеріалу.

* * * * * * * * * *

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 3(38)/2021

Засновники журналу:	- Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"; - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини "Україна".
Видавець:	© ДНУ ІІБП НАПрН України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України". Тел.: 234-94-56; e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	URL: //www.ippi.org.ua – ДНУ ІІБП НАПрН України; URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.

Founders of journal:	- State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; - Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine; - Open International University of Human Development "Ukraine"
Publisher:	© IISL of the NALS of Ukraine.
Address of release:	01032, Kyiv, Saksaganskogo str., 110-V. State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine". Phone: 234-94-56; e-mail: bvm777@ ukr.net
Web-pages of journal in the network Internet:	URL: //www.ippi.org.ua – IISL of the NALS of Ukraine; URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.