Науково-дослідний інститут інформатики і права
Національної академії правових наук України

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

Відкритий міжнародний університет розвитку людини “Україна”

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 3(34)/2020

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

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

м. Київ

Scientific Research Institute of Informatics and Law
of the National Academy of Law Sciences of Ukraine

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

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND LAW

SCIENTIFIC PROFESSIONAL JOURNAL

№ 3(34)/2020

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

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

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * * *

З М І С Т

Інформаційне право

Інформаційна і національна безпека

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

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. 10.6. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ "Видавничий дім "АртЕк".
04050, м. Київ, вул. Мельникова, буд. 63. Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІІП НАПрН України, протокол № 9 від 15.09.20 р.

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

Informative Law

Informative and National Safety

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

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 9 dated 15.09.20.

Інформаційне право

УДК 351/354:351.746

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

ЛАТЕНТНІСТЬ ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Анотація. *В статті досліджується питання щодо існування феномену, яким є "латентна" публічна інформація в інформаційному просторі України, надається визначення терміну "латентність публічної інформації", розкривається її структура – внутрішня і зовнішня валідність, види валідності інформації та направленість дії зазначеної інформації; наводяться приклади існування згаданої інформації, як сучасних внутрішніх викликів національній безпеці, констатується, що "латентність" подібної інформації не сприяє консолідації суспільства, не мобілізує його на вирішення необхідних завдань і є ознакою низького рівня демократії в державі та правосвідомості її громадян, а також правової культури.*

Ключові слова: *валідність, демократія, достовірність, латентність, пропаганда, публічна інформація.*

Summary. *The article analyzes the issue of the existence of the phenomenon of "latent" public information in the information space of Ukraine, the term "latency of public information" is defined, its structure is revealed – internal and external validity, types of information validity and direction of action of the specified information; examples of the existence of this information as modern internal challenges to national security are given, it is stated that the "latency" of such information does not contribute to the consolidation of society, does not mobilize it to solve the necessary problems and is a sign of a low level of democracy in the state and the legal awareness of its citizens, as well as legal culture.*

Keywords: *validity, democracy, reliability, latency, propaganda, public information.*

Аннотация. *В статье исследуется вопрос существования феномена, каким является "латентная" публичная информация в информационном пространстве Украины, дается определение термина "латентность публичной информации", раскрывается ее структура – внутренняя и внешняя валидность, виды валидности информации и направленность действия указанной информации, приводятся примеры существования данной информации, как современных внутренних вызовов национальной безопасности, констатируется, что "латентность" подобной информации не способствует консолидации общества, не мобилизует его на решение необходимых задач и является признаком низкого уровня демократии в государстве и правосознания ее граждан, а также правовой культуры.*

Ключевые слова: *валидность, демократия, достоверность, латентность, пропаганда, публичная информация.*

Постановка проблеми. Відповідно до положень статті 34 Конституції України громадяни мають право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Зазначені положення Конституції України, а також прийнятого на виконання її положень Закону України "Про доступ до публічної інформації" [1], а також на реалізацію статей 18, 19 "Міжнародного пакту про громадянські і політичні права" від 16.12.66 р., Рекомендацій Ради Європи "Про доступ до інформації, що перебуває в розпорядженні органів влади" від 25.11.81 р. № R (81)19 та "Про доступ до офіційних документів від 21.02.02 р. № R (2008), а також Конвенції Ради Європи " Про доступ до офіційних документів" від 12.07.18 р., мають гарантувати право кожному, без дискримінації за будь-якою ознакою, на доступ, за вимогою, до офіційних документів, що знаходяться в розпорядженні державних органів. Саме в доступі до публічної інформації для суспільства відбувається реальне забезпечення прозорості в діяльності органів влади.

Результати аналізу наукових публікацій. Теоретичну базу порушеного питання становлять праці філософів, теоретиків права, політологів, соціологів, фахівців інших галузей права: Баймуратова М., Батанова О., Белякова К., Бисаги Ю., Бостана С., Брижко В., Гультая М., Гусарєва С., Довганя В., Золотар О., Жоля К., Калиновського Б., Камінської Н., Копейчикова В., Наливайко Л., Пилипчука В., Скрипнюка О., Тихомирова О., Швеця М., Шемшученка Ю. й ін.

Разом з цим у вивченні права особи на доступ до публічної інформації, залишається ряд питань, які не досліджені і потребують подальших розробок, формулювання теоретичних висновків і практичних рекомендацій щодо визначення поняття, змісту, гарантій реалізації даного права, удосконалення механізму його забезпечення. Саме в цьому і полягає дослідження питання латентності публічної інформації.

Метою статті є оцінка проблем щодо поняття "латентність публічної інформації", яку громадськість отримує від публічної влади, розкриття її змісту та наслідків впливу на поінформованість суспільства, стан правопорядку та правосвідомості громадян, розкриття викликів та ймовірних загроз від її дії на свідомість громадськості та на стан правопорядку в державі.

Виклад основного матеріалу. Реалізація права людини на доступ до публічної інформації завжди пов'язано з обставинами, які можуть визначатися маніпулюванням свідомістю людини з метою інформаційно-психологічного на неї впливу. По-суті, маніпуляція (від лат. "manipulus" – сучасне переносне значення слова – спритне поводження з людьми як з об'єктами, речами) – це цензура, яка є засобом інформаційної боротьби, що не лише обмежує свободу слова але й порушує складні інформаційно-когнітивні процеси, пов'язані з розумово-інтелектуальною діяльністю людини, розвитком громадянського суспільства та держави. У зв'язку з розвитком електронно-інформаційного середовища вже активно застосовуються таки поняття, як "електронна боротьба", "електронно-інформаційне протиборство" та узагальнюючий термін "інформаційна війна", про деяких принципових аспектах якої детально мова йде в [2].

Публічна влада будь-якої сучасної економічно і демократично розвинутої держави прагне забезпечити всебічний і рівний доступ всіх до інформації, спираючись на міжнародне визнані стандарти відкритості і прозорості в роботі органів публічної влади. В Україні важливим кроком у вирішенні даної проблеми стало прийняття вищевказаного Закону України [1]. Відповідно до його положень, публічною інформацією є відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, яка була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим законом (ст. 1). Зазначена інформація є відкритою, за виключенням випадків, встановлених законом.

Не звертаючись до публічної інформації з обмеженим доступом, зазначимо, що згідно з доповненою статтею 10-1 згаданого Закону України [1] публічна інформація може існувати у формі відкритих даних. Публічна інформація у формі відкритих даних – це публічна інформація у форматі, що дозволяє її автоматизовану обробку електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних [3] та на своїх веб-сайтах.

Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення. Будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації.

Зазначимо, що держава гарантує доступ до публічної інформації. Гарантія досягається шляхом:

– обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

– визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

– максимальним спрощенням процедури подання запиту та отримання інформації;

– доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

– здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

– юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Зазначена гарантія доступу до публічної інформації має відповідати наступним принципам:

– систематичного та оперативного оприлюднення публічної інформації, що здійснюється: в офіційних друкованих виданнях; на офіційних веб-сайтах в Інтернеті; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом;

– надання публічної інформації за інформаційними запитами.

Публічна інформація, яка є відкритою, має бути доступною для кожного громадянина держави і відповідати певним критеріям. Можна виділити наступні основні критерії:

– достовірність (англ. – credibility) інформації. Достовірність включає в себе об'єктивні та суб'єктивні компоненти правдоподібності джерела або повідомлення.

Достовірність сходить до арістотелівської теорії риторики. Аристотель визначає риторику як здатність бачити те, що можливо переконливо в будь-якій ситуації [4]. Він розділив засоби переконання на три категорії, а саме: "Етос" (достовірність джерела), "Патос" (емоційні чи мотиваційні заклики) та "Логос" (логіка, яка використовується для підтвердження претензії), які, на його думку, здатні впливати на приймача повідомлення.

Надійність має два ключові компоненти: надійність та досвід, які мають як об'єктивні, так і суб'єктивні компоненти. Достовірність базується більше на суб'єктивних факторах, але може включати об'єктивні вимірювання, такі як встановлена надійність

джерела чи повідомлення (наприклад, облікові дані, сертифікація чи якість інформації). Вторинні компоненти достовірності включають динамізм джерела (харизму) та фізичну привабливість.

Достовірність означає її повноту і загальну точність. В ній мають бути: відсутні помилкові або перекручені відомості; наявність розбірливої мови (як усної, так і письмової); низька ймовірність помилкового вживання одиниць інформації (літери, цифри, символу, біта). Достовірність може оцінюватися за шкалами, так само як і джерело цієї інформації (повністю надійне, частіше всього надійне, досить надійне і так далі до абсолютно надійного і того, чий статус не визначений);

– своєчасність інформації (англ. – timely information). Це означає, що вона є саме тією, яка потрібна на даний момент, суттєвою, важливою на цей час. Цю властивість інформації називають також актуальністю (від англ. “actual”, що означає існуючий у дійсності, дійовий). Актуальність інформації визначається тим, наскільки важливі для людини або суспільства відомості, чи можуть вони бути використані в конкретній ситуації для вирішення проблеми. Це властивість багато в чому залежить від інтервалу часу, що пройшов з моменту появи цієї інформації, а також від того, наскільки швидко змінюється ситуація.

Таким чином, своєчасність інформації передбачає її надходження не пізніше заздалегідь призначеного моменту часу, узгодженого з часом вирішення поставленого завдання. Лише актуальна, вчасно отримана інформація може принести користь людям. Недарма прогноз погоди повідомляють напередодні, а не в той же день. Відповідно до цього ж правила вчені намагаються знайти більш надійні способи попередження про землетруси, урагани та інші стихійні лиха;

– повнота і точність інформації. Інформацію можна назвати повною, якщо її достатньо для розуміння ситуації і прийняття рішення. Наприклад, мрія історика – мати повну інформацію про минулі епохи. Але історична інформація ніколи не буває повною, і повнота інформації зменшується при віддаленні від нас історичної епохи. Навіть події, що відбувалися на наших очах, і повністю документуються, багато забувається, і спогади піддаються перекручуванню. Неповна інформація може принести до помилкового висновку або рішення.

У свою чергу, точність інформації – це ступінь близькості відображуваного інформацією значення і справжнього значення цього параметра.

Не будемо розглядати інші властивості інформації, оскільки згаданих достатньо для аналізу латентності інформації. У довідковій літературі зазначено, що термін латентність походить від латинського “latens” – прихований, невидимий, тобто це здатність об’єктів або процесів перебувати в прихованому стані, не проявляючи себе [5]. Таким чином, під “латентною інформацією” можна розуміти таку інформацію, внутрішні властивості якої, тобто реальні зміст і призначення, перебувають у прихованому стані і явно не проявляють себе.

Як правило, поняття “латентність” використовується в кримінології, психології, в техніко-технологічних процесах тощо. В інформаційній сфері згадане поняття відкрито не вживається. Однак, процеси, що відбуваються у даній сфері дають підстави для того, щоб приділити цьому відповідну увагу. Такі властивості інформації використовуються в дипломатичній, політичній, розвідувальній діяльності, при веденні воєнних та інформаційних спецоперацій тощо, і призначена вона для приховування істинних намірів її власника, введення в оману (відволікання) опонента (супротивника) і досягнення необхідного для себе результату. Тобто, внутрішня валідність (дійсність, надійність) інформації кардинально відрізняється від формальної зовнішньої валідності

(показової дійсності чи надійності) інформації. Тим самим можна говорити про внутрішню (конструктну) і зовнішню (критеріальну) валідність інформації.

Існують різні види валідності інформації: валідність за критерієм; змістовна; конструктна. Валідність за критерієм можемо отримати під час здійснення аналізу інформації шляхом зіставляння із критерієм, тобто з безпосередньою і незалежною мірою того, що повинен передбачити результат застосування інформації. Валідність інформації за критерієм може бути прогнозуючою і конкурентною. Прогнозуюча валідність вказує на реальність, очікуваність отримання належного, запрограмованого результату. У свою чергу, валідність інформації за конкурентністю показує вірогідність отримання результату в різних варіаціях.

Конструктна валідність показує, наскільки результати аналізу інформації можуть розглядатися в контексті очікуваного результату застосування інформації, як міра певного теоретичного конструкта, або властивості.

Змістовна валідність (внутрішня, логічна) показує результати аналізу інформації за її відповідними властивостями і особливостями та репрезентативність даної інформації, тобто відповідність надійності її.

В сучасних умовах ведення гібридних війн, у процесі проведення інформаційних спецоперацій, широко використовується критерій “латентності” інформації для різнобічного впливу (психологічного, морального, духовного, культурного тощо) на визначений об’єкт (держава, влада, суспільство, особа тощо) з метою зміни їхнього сприйняття (уявлення) про ті чи інші національні цінності і, тим самим, досягнення відповідних преференцій чи мети на тому чи іншому напрямку протистояння із відповідним об’єктом. Під інформаційними спецопераціями можна розуміти інтегроване використання інформаційно-комунікаційних технологій, інформації з метою впливу на людську свідомість для руйнування, розкладання, або й взагалі перехоплення впливу на прийняття рішень супротивника, при цьому захищаючи своє власне (рішення).

Такими, наприклад, є інформаційні спецоперації Російської Федерації проти України, країн Прибалтики, Молдови, Грузії тощо. Поряд із внутрішньою пропагандою стосовно власного народу, включивши пропагандистську машину і передаючи пропагандистську інформацію каналами лінійного радіо, телебачення, в мережі Інтернет, влада Російської Федерації здійснює проти України цілеспрямовану інформаційну пропаганду всього російського під ідеологічною назвою “руський мір” в усі сфери українського суспільного життя. Особливий вплив можна відзначити на Сході України і в Криму, через що соціокультурно некерована Україною частина населення навіть після початку війни недружньо, навіть з ненавистю, по-нацистськи ставиться до всього українського [6].

Російська пропаганда або кремлівська пропаганда – це російська державна інформаційна політика, спеціальні інформаційні заходи (“спецоперації”, “політичні технології”) та конгломерат відповідних державних органів та установ, які під виглядом “суспільного інформування” займаються психологічною обробкою населення Російської Федерації, а також населення інших країн – в першу чергу країн пострадянського російськомовного простору та російської діаспори. Також об’єктом російської пропаганди є іншомовне населення у США, ЄС, арабських країнах, тощо. Загалом російська пропаганда розповсюджується щонайменше 40 мовами світу у 160 країнах [7].

Російська державна пропаганда є тотальною, цинічною, брехливою і має прямим попередником радянську пропаганду, але також активно використовує досвід інших історичних авторитарних та тоталітарних режимів. Пропаганда в Росії завжди застосовується в тандемі з цензурою: цензура відсікає будь-яке інакомислення,

пропаганда змушує думати відповідно до інтересів і цілей владної верхівки. Її мета – не переконати, як у класичній пропаганді, а зробити інформаційне поле "брудним", щоб ніхто нікому не довіряв. Коли "інформаційне поле" вбито, все, що лишається – страхи, паніка та апатія.

Це – наочний приклад латентності публічної інформації держави в контексті ідеологічної пропаганди, оскільки здійснюється усім механізмом публічної влади. Пропагандуючи в інформаційні сфері одне, пропагандистська (т. зв. "інформаційна") обробка свідомості значної кількості російських громадян досягла такої глибини і деталізації, таких масштабів і такої витонченості, що режиму вдалося домогтися створення у багатьох людей системи сприйняття навколишнього світу, значною мірою не лише відірваної від його реальної картини, але і такої, що не має нічого з нею спільного. Іншими словами, інформаційному спецназу путінського режиму вдалося домогтися набагато більш вражаючої перемоги, ніж спецназу ГРУ, що окупував Крим. Той зміг захопити півострів з двома з гаком мільйонами жителів, а цей – свідомість 123 мільйонів (86 %) жителів Росії.

Однак, наведені приклади є зовнішнім фактором латентності публічної інформації. Не меншої шкоди національним інтересам може завдати і внутрішній фактор, тобто подання населенню публічної інформації формально достовірної, але за якою може переслідуватися інша мета. Такими, на жаль, непоодинокими є публічна інформація, поширена представниками публічної влади України на різних рівнях. Наведемо декілька прикладів такої інформації.

Так навесні 2020 року Україну сколихнула публічна інформація про висування пропозиції, шляхом внесення законопроекту України № 3300, в якому пропонується перенести місце знаходження Конституційного Суду України із міста-столиці Києва до міста Харків. Аргументація такої пропозиції, на думку його розробника, полягала в спроможності таким чином підвищити рівень незалежності Суду і покращити суспільно-політичний статус обраного міста, оскільки в ньому перебуває Президія Національної академії правових наук України.

Однак, за такою шляхетною, на перший погляд, метою в дійсності криється інша, більш негативна мета. Відповідну думку із зазначеного питання висловили представники Центру політико-правових реформ, авторитетного в Україні аналітичного центру, неурядової неприбуткової організації, створеної у 1996 році для сприяння проведення реформ у політичній та правовій сферах з метою утвердження в Україні верховенства права та належного урядування. Вони зазначили, що більшість ініціатив розробників законопроекту є недоцільними та неконституційними, а за бажанням підвищити незалежність Суду криється можливість прояву непрямого політичного тиску на суддів [8].

Дійсно, можна погодитися із таким висновком, а також додати у питанні щодо підвищення суспільно-політичного статусу міста наступні історичні факти.

Харків у грудні 1917 році став містом, в якому більшовики-колабораціоністи, всупереч існуючої УНР і її столиці Київ, проголосили Українську Народну Республіку Рад зі столицею Харків. Після цього підтримані ними війська Радянської Росії вторглися в Україну, а проведений більшовиками Перший Всеукраїнський з'їзд рад оголосив створення Республіки Рад робітничих, солдатських і селянських депутатів. Почалася перша російсько-українська війна, яка закінчилася втратою Україною своєї незалежності.

Щось подібне відбулося у лютому 2014 року, коли у Харкові відбувся з'їзд депутатів південно-східних областей і Криму, ініційований рухом "Український фронт" на чолі з губернатором Харківщини Михайлом Добкіним, які оголосили, що південно-

східні області України, Крим і Севастополь готові взяти на себе всю повноту влади до забезпечення порядку в Києві. У свою чергу, Верховна Рада України ухвалила постанову про запобігання сепаратизму. Проти губернатора Харківської області Михайла Добкіна та мера Харкова Геннадія Кернеса через їхні сепаратистські заяви СБУ порушила кримінальні справи. Однак, як показав час, ніхто не поніс покарання.

Місто Харків в історичному вимірі показало себе більш знакове як столиця українського сепаратизму. А тому твердження розробників законопроекту про можливість покращити суспільно-політичний статус Харкова не може відповідати дійсності. Це – латентність публічної інформації. Зазначене можна сприймати як спробу в майбутньому реалізувати те, що не вдалося раніше – розколоти Україну, як це було в її історії.

Таким чином в запропонованих намірах перенесення місцезнаходження Суду до Харкова, цілковито реально криються наміри підвищити спроможність регіону у реалізації негативного сценарію подальшого розвитку держави. А це вже – відкриті загрози національній безпеці. Тим паче, наведена аргументація розробників законопроекту щодо забезпечення незалежності Суду в сучасних умовах, коли "телефонне право" активно діє – не витримує ніякої критики. Незалежність Суду можна досягти лише правовими механізмами шляхом правової мінімізації політичного впливу на Суд при його формуванні та функціонуванні.

Інший факт – у березні 2020 року мас-медіа України оприлюднили копії протоколів засідання тристоронньої контактної групи (далі – ТКГ) у Мінську, в яких передбачалося створення Консультативної ради. До складу Ради мали входити ***по 10 представників від України та ОРДЛО*** та ***по одному з правом дорадчого голосу від ОБСЄ, Росії, Німеччини та Франції.*** ТРК в Мінську розглядає можливість створення консультативної ради для обговорення питань, передбачених у пакеті Мінських домовленостей, заявив голова Офісу президента України Андрій Єрмак на брифінгу Ради національної безпеки та оборони. Він наголосив, що це рішення ще не ухвалене, але сторони ТКГ "зафіксували необхідність прийняття такого рішення". Єрмак не дав чіткої відповіді на те, за яким критерієм до такої ради будуть відбирати людей з окупованих територій [9; 10].

Не вдаючись до розкриття деталей цієї історії, зазначимо, що суспільством було неоднозначно сприйнято офіційну інформацію Офісу Президента України, і лише висока і принципова позиція громадянського суспільства не дала змоги керівництву держави фактично здійснити національну зраду, оскільки протоколом згаданого дійства так звані представники окупованих Росією територій України переводилися у статус їх офіційних представників, а Росія – зі статусу агресора в статус посередника. Як писали мас-медіа, в нинішній переговорній команді з Банкової Росія знайшла вдячних слухачів і реалізаторів своїх ідей, які, можливо, розраховують на те, що в умовах хайпу навколо наростання небезпеки епідемії коронавіруса "мінська зрада" пройде непоміченою" [10].

Під "хайпом" (англ. hype – "обман, збудження, настирлива реклама") розуміється розкрутка, роздування інформації, галас, ажіотаж, бурхлива дискусія, хвиля статей в ЗМІ.

Таким чином, зазначена державною владою України публічна інформація щодо Мінської позиції стосовно Ради є латентною, тобто, внутрішня (конструктна) валідність поданої нею інформації відрізняється від зовнішньої (критеріальної) валідності. Було це зроблено умисно, чи це є проявом непрофесіоналізму представників державної влади – покаже час, оскільки про здійснення аналізу та перевірки цього факту з боку СБУ поки що невідомо.

Наступний приклад – результати подання громадянином Г.М. Учайкіним від ГО "Українська асоціація власників зброї" електронної петиції Президенту України В. Зеленському від 22.05.19 р. № 22/053416-еп, яка набрала необхідну кількість голосів.

Основна мета цієї петиції – законодавче унормування обігу в Україні зброї та права на її застосування з метою захисту життя, здоров'я людини і громадянина та їх приватної власності, як це передбачено частиною другою статті 27 Конституції України : "Кожен має право захищати своє життя і здоров'я, життя і здоров'я інших людей від протиправних посягань". Тим паче, що відповідно до положень статті 3 Конституції "Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю", а "Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави".

Зазначена петиція була подана повторно в умовах тривалого проведення Російською Федерацією воєнної агресивної політики щодо України, великої кількості зброї, що знаходиться в неврегульованому обігу в державі у зв'язку із проведенням бойових дій на Сході країни, гострою криміногенною ситуацією у державі, що вже є об'єктивними підставами для створення умов максимального насичення громадянського суспільства зброєю для самозахисту. Дане твердження підкріплюється фактом, що саме завдяки тому, що добровільний порив патріотично налаштованих громадян, які, насамперед, зі своєю особистою зброєю, в 2014 році стали на захист своєї Вітчизни, Україна змогла стримати агресію проти нею з боку Російської Федерації. Ця загроза не усунута, оскільки агресор сконцентрував біля кордонів України більш як 70 тис. озброєних до зубів вояк, які доповнюються найманцями приватних військових компаній та колабораціоністами, і створив загрозу нової агресії, насамперед на Півдні України.

Саме для реалізації зазначеного права громадянину необхідно мати відповідні засоби захисту, застосування яких має регулюватися законом. Однак відповідь головної посадової особи країни на зазначену петицію щодо передчасності його вирішення і відмова його підтримки, викликає подив, здивування і нерозуміння з боку значної кількості громадян України, а також породжує нові питання до Президента України. Чого тут більше – нерозуміння цією посадовою особою реальної ситуації, що склалася навколо України та всередині держави, чи особиста недосвідченість у вирішенні подібних питань, чи умисел щодо сприяння ускладненню самої ситуації – покаже час, як це було визначено відносно злочинної бездіяльності та щодо злочинних намірів колишнього Президента України В. Януковича.

Наведений приклад "латентності" публічної інформації, наданої Президентом України В. Зеленським на відповідну електронну петицію громадян України, так само, як і подібні заяви представників влади про намір скоротити чисельність Збройних Сил України більш ніж на 10 тис. осіб, Повітряних Сил, Морської піхоти та Десантно-штурмових військ – по декілька тисяч осіб, ряду підрозділів – в нинішніх умовах сприймається неоднозначно і викликає нерозуміння у суспільстві.

Подібних фактів можна навести ще багато, однак формальні вимоги до обсягу статті не дають можливості цього зробити. Зазначимо, на нашу думку, головне: наявність латентної публічної інформації, її обсяг і частота вказують на існування невисоких рівнів демократії та стану правової культури в державі, правової освіченості та правосвідомості громадян, насамперед представників публічної влади держави.

Висновки.

В сучасному світі факти латентності публічної інформації не рідкість, і навіть в останні роки динаміка її зростає. Окремі держави світу на латентності своєї публічної інформації навіть сформували свою як внутрішню, так і міжнародно-правову політику, що знайшло своє відображення в діяльності багатьох відомих міжнародних організацій таких, як: ООН, Рада безпеки ООН, ЄС, ПАРЄ тощо.

Аналогічним поширенням латентної публічної влади всередині держави, користуються майже усі політичні сили після їхнього приходу до влади. На переконання керівників відповідних політичних сил в Україні, публічна інформація має подаватися громадянському суспільству не вся, а дозовано, тобто так, щоб вона не нашкодила іміджу політичної сили і сприяла вирішенню політичних питань партією. Водночас, такого роду інформація є внутрішніми викликами національній безпеці, оскільки вона не сприяє консолідації суспільства і не налаштовує його на вирішення виникаючих перед ним завдань.

Зазначене вказує на те, що в Україні правосвідомість і правова культура осіб, які очолюють політичні сили і які беруть безпосередню участь у формуванні публічної влади, далека від того, щоб стверджувати, що в Україні сформовано правове суспільство. Принцип "верховенство права" лише задекларовано в правових документах України, а для його реального впровадження і домінування в суспільному житті потрібно ще прикласти значних зусиль, так само як і для формування громадянського суспільства.

Використана література

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

2. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с. С. 11-27, 43-82.

3. Єдиний державний веб-портал відкритих даних. URL: https://data.gov.ua (дата звернення: 16.06.2020).

4. Credibility. URL: https://en.wikipedia.org/wiki/Credibility (дата звернення: 19.06.2020).

5. Латентність. URL: http://esu.com.ua/search_articles.php?id=53398 (дата звернення: 20.06.2020).

6. Нерсесян Г.А. Інформаційні спецоперації в умовах війни в історії. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2018/1_2018/42.pdf (дата звернення: 20.06.2020).

7. Російська пропаганда. Вікіпедія. URL: https://uk.wikipedia.org/wiki (дата звернення: 20.06.2020).

8. Перенесення Конституційного Суду є проявом непрямого політичного тиску на суддів – ЦППР. URL: https://lexinform.com.ua/v-ukraini/perenesennya-konstytutsijnogo-sudu-ye-proyavom-nepryamogo-politychnogo-tysku-na-suddiv-tsppr (дата звернення: 20.06.2020).

9. "Новий Мінськ": початок прямих переговорів із бойовиками? URL: https://www.radiosvoboda.org/a/30485608.html (дата звернення: 21.06.2020).

10. Єрмак анонсує "консультативну раду" з жителів окупованих та підконтрольних територій для обговорення "Мінська". URL: https://www.radiosvoboda.org/a/news-yermak-konsultatyvna-rada/30485915.html

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

УДК 341:316.774

СОЛОДКА О.М., *кандидат юридичних наук, с.н.с.*,
докторант НА СБ України.
ORCID: https://orcid.org/0000-0002-1799-0712.

СВОБОДА ІНФОРМАЦІЇ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

Анотація. *У статті досліджено поняття "інформаційна свобода", "інформаційний суверенітет", їх співвідношення та сучасні підходи до забезпечення. За результатами проведеного дослідження встановлено, що реалізація інформаційного суверенітету держави передбачає забезпечення прав і свобод людини в інформаційній сфері; визначення виключних підстав для обмежень доступу до інформації, що встановлюються при забезпеченні інформаційного суверенітету держави; пошук балансу між правами людини і необхідністю реалізації цілей держави в інформаційній сфері. Основоположними началами забезпечення інформаційного суверенітету держави є: презумпція інформаційної свободи як базисний принцип реалізації інформаційного суверенітету; захищеність інформаційної приватності людини; забезпечення права на інформацію як обов'язок держави.*

Ключові слова: *інформаційна свобода, інформаційний суверенітет, інформаційні права і свободи.*

Summary. *The article examines the notions of "information freedom", "information sovereignty", their relationship and modern approaches to their assurance. According to the results of the study, it is established that the implementation of the information sovereignty of the state involves ensuring human rights and freedoms in the information sphere; determination of exclusive grounds for restrictions of information access established in ensuring the information sovereignty of the state; finding a balance between human rights and the need to achieve the goals of the state in the information sphere.*

Keywords: *information freedom, information sovereignty, information rights and freedoms.*

Аннотация. *В статье исследованы понятия "информационная свобода", "информационный суверенитет", их соотношение и современные подходы к обеспечению. По результатам проведенного исследования установлено, что реализация информационного суверенитета государства предусматривает обеспечение прав и свобод человека в информационной сфере; определение исключительных оснований для ограничений в сфере доступа к информации, устанавливаемых при обеспечении информационного суверенитета государства; поиск баланса между правами человека и необходимостью реализации целей государства в информационной сфере.*

Ключевые слова: *информационная свобода, информационный суверенитет, информационные права и свободы.*

Постановка проблеми. Свобода у правовому контексті – це об'єктивна можливість людини і громадянина здійснювати або не здійснювати певні дії, що ґрунтуються на його конституційних правах і свободах. Основні постулати вчення про свободу: усі люди вільні від народження і ніхто немає права відчужувати їхні природні права [1, с. 441].

Інформаційна свобода є однією з найважливіших гарантій розвитку, дотримання і захисту будь-яких універсальних прав людини, що особливо відчутно на етапі розвитку інформаційного суспільства. Попри це, особливістю вказаного періоду є раніше невідома активізація двох діалектично пов'язаних тенденцій: необмежені можливості у

доступі до інформації та їх використання у протиправних цілях. В зазначених умовах держава відчуває нагальну потребу у забезпеченні інформаційної безпеки, що неможливо реалізувати за відсутності інформаційного суверенітету. Хоча остання категорія здебільшого негативно сприймається представниками ліберальних режимів як така, що суперечить теорії свободи інформації та зводиться до контролю за інформаційними потоками.

Результати аналізу наукових публікацій. Досліджуючи проблематику інформаційних правовідносин, вітчизняні та зарубіжні науковці неодноразово зверталися у своїх працях до питань з'ясування змісту та ознак поняття "свобода інформації", "інформаційні права людини", "доступ до інформації", "інформаційний суверенітет" тощо. Зазначених і суміжних питань торкаються наукові розробки О. Баранова, К. Бєлякова, В. Брижка, О. Данильяна, О. Дзьобаня, О. Довганя, І. Забари, О. Золотар, Б. Кормича, А. Марущака, О. Олійника, О. Радутного та інших. Водночас, незважаючи на те, що проблематиці свободи інформації в юридичній науці присвячено достатньо уваги, необхідно зауважити, що питання інформаційного суверенітету держави є вельми дискусійними, а в поєднанні зі свободою інформації взагалі такими, що взаємовиключають один одного.

Метою статті є з'ясування змісту термінів "свобода інформації", "інформаційний суверенітет" та визначення їх співвідношення.

Виклад основного матеріалу. Свобода інформації – поняття, що використовується для позначення групи прав і свобод людини, включаючи право на інформацію (право вільно збирати, зберігати, використовувати і поширювати інформацію), свободу вираження поглядів і переконань, свободу думки і слова, свободу обміну інформацією.

Ретроспективний аналіз інформаційного законодавства свідчить про те, що питання свободи інформації актуалізувались ще близько 250 років тому у Швеції з прийняттям шведським парламентом Закону про свободу преси (друку) від 2 грудня 1766 року, що був результатом роботи Андерса Чайденіуса, священика, мислителя, політика. "Свобода, – зазначав він, – це повна протилежність обмеженню, вона має багато значень; слово це слід вживати обережно, адже воно може принести як користь, так і збитки. Під свободою я розумію право кожного громадянина, надане йому законодавством і конституцією, задовольняти власні запити, що не повинні шкодити іншим громадянам країни та всьому суспільству" [2, с. 35].

Широкого розповсюдження ця теорія набула лише в кінці XX століття, коли вперше була запропонована Концепція свободи інформації на Міжамериканській конференції 1945 р. у Мехіко як свобода шукати, отримувати та поширювати інформацію будь-якими засобами й незалежно від державних кордонів. У 1946 р. свобода інформації як фундаментальне право людини було проголошено на першій сесії Генеральної асамблеї ООН у Резолюції 59 (I) "Скликання міжнародної конференції з питань свободи інформації". Згодом ця концепція знайшла своє втілення в Загальній декларації з прав людини, Міжнародному пакті про громадянські та політичні права та інших міжнародних документах, що стосуються прав і свобод людини і громадянина. Зокрема, у Резолюції 59 (1) Генеральної Асамблеї ООН зазначено, що "свобода інформації є основним правом людини і критерієм усіх інших свобод" [3].

Вище викладене підтверджує те, що гарантії інформаційних прав і свобод людини належать до найважливіших засад формування правової держави та громадянського суспільства і на сьогодні набувають особливого значення, оскільки в умовах прискореного розвитку інформаційного суспільства інформаційна свобода визнана найвищою цінністю. Ці права включені і до дієвого державного механізму в

демократичному суспільстві, що визначає забезпечення захисту прав і свобод людини в інформаційній сфері однією з найважливіших цілей інформаційної безпеки, а власне людину – найголовнішим її об'єктом.

Реалізація свободи інформації та встановлення меж її здійснення, хоча і є, складовою свободи в цілому, проте відзначається певною специфікою. Це пояснюється тим, що для здійснення цього виду свободи характерним є: властивості феномену інформації; специфічні механізми реалізації права на свободу інформації; методи правового регулювання у цій сфері; визначене коло суб'єктів інформаційних відносин; специфіка обігу інформації [4].

Інформація та свобода становлять основу інформаційних прав і свобод, під якими розуміють комплекс прав, похідних від свободи інформації, як фундаментального права людини, до яких віднесено: 1) інформаційні права, що пов'язані з особою (особистістю) людини; 2) право власності на інформацію; 3) право на доступ до інформації; 4) свободу поширення інформації будь-яким законним способом; 5) право на безпечне інформаційне середовище [5].

Право на свободу інформації гарантується Конституцією України, що закріплено в наступних положеннях [6]:

- гарантія права на свободу думки і слова, на вільне вираження своїх поглядів і переконань (частина 1 ст. 34);

- право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (частина 2 ст. 34);

- гарантія права вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (частина 2 ст. 50).

Зв'язок природного права та інформаційної свободи полягає в тому, що інформаційна свобода надає людині низку можливостей, які продиктовані природним станом людини – станом свободи. Ці можливості не залежать від волі держави, не державою вони встановлені, а самою природою людини. Держава не має права дарувати можливість реалізації інформаційної свободи, як і не має права позбавляти їх. Держава зобов'язана за допомогою правових норм створити умови, за яких людина зможе реалізувати належну їй інформаційну свободу [7]. Забезпечення та охорона цих прав – головне призначення держави. Свобода не може бути абсолютною, вона обмежена правами та свободою інших людей, принципами моралі, інтересами загального добробуту. Демократичне суспільство ґрунтується не на вільному балансі між свободою та соціальною справедливістю, свободою та державним інтересом. Межі свободи можуть бути визначені тільки правовим законом, який і є її мірою" [1]. Цю рису свободи людини помітив ще І. Кант, який проголосив, що свобода кожного повинна бути сумісна зі свободою всіх інших [8, с. 94-95]. Правова держава визнає основою свого існування свободу.

Саме держава є ключовим суб'єктом у врегулюванні правовідносин в інформаційній сфері та захисті інформаційних прав і свобод людини та громадянина, адже власне вона виступає законодавцем, що формує правові засади розвитку інформаційних відносин, юридичним гарантом реалізації права на інформацію, здатним захистити суб'єктів права від несанкціонованого доступу до інформації, забезпечити недоторканність приватного життя людини.

Отже, на державу з однієї сторони покладається завдання захисту інформаційних прав і свобод громадян, а з іншої постає вимога забезпечення інформаційної безпеки людини, суспільства, держави.

О. Довгань, вибудовуючи модель системи забезпечення інформаційної безпеки, яка утворюється об'єктами інформаційної безпеки та суб'єктами інформаційної безпеки, серед іншого, відносить до об'єктів інформаційної безпеки інформаційний суверенітет, безпеку національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції та послуг [9].

Суверенітет – це верховенство влади всередині країни та її незалежність і рівноправність у зовнішніх зносинах. Поняття інформаційного суверенітету держави відображає верховенство державної влади в національному інформаційному просторі та рівноправність у міжнародних відносинах в глобальному інформаційному просторі.

Як свідчить досвід країн з розвиненою демократією, інформаційна безпека людини не повинна протиставлятись інформаційній безпеці держави та суспільства. Адже саме людина визнається основною цінністю кожного суспільства і забезпечення її прав і свобод є кінцевою метою реалізації функцій держави. Проте, реалії інформаційного суспільства обумовлюють необхідність обмеження прав та законних інтересів людини з метою захисту національних інтересів держав, попередження міжнародних конфліктів чи/та терористичних актів, а також забезпечення безпеки національних інформаційних ресурсів. Таким чином, має місце конфлікт інтересів різних об'єктів інформаційної безпеки. Вирішення цього конфлікту демократичним шляхом є однією з первинних задач при створенні відповідних правових норм [5, с. 332]. Національні інтереси ж повинні бути обумовлені природними правами та свободами людини і громадянина, тобто похідними від індивідуальних. Окрім цього, інформаційний суверенітет розглядається як один з фундаментальних національних інтересів, і, водночас, реалізація національних інтересів визначена як спосіб забезпечення інформаційного суверенітету (серед іншого).

У цьому контексті, суттєвим аспектом свободи інформації у співвідношенні з інформаційним суверенітетом є двоєдина концепція, що лежить в основі цього права, основними елементами якої є "свобода доступу до держави" і "свобода від держави". Соціалістична концепція передбачає ж розглядати свободу як певний припис, вказівку або "директиву, що прописує свободу, спрямовану не стільки на попередження втручання держави в особисте життя індивідума, скільки на його соціальну інтеграцію у суспільне життя" [10].

"Свобода від держави" реалізується через гарантії права людини на невтручання в особисте життя. Зокрема, в ст. 32 Конституції визначено: "Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини". Ст. 31 Конституції України гарантує кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [6]. Ці положення знаходять своє відображення в намірах розвитку інституту захисту персональних даних в Україні відповідно до сучасних європейських правових стандартів та створення ефективної загальнодержавної системи забезпечення приватності персональних даних в умовах поширення можливостей Інтернет-середовища і складнощами застосування традиційних, "доцифрових" юридичних норм і практик [11].

“Свобода доступу до держави” основним чином реалізується через доступ до інформації, який у суб’єктивному розумінні визначається як гарантована державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. В об’єктивному розумінні доступ до інформації – це сукупність правових норм, що регламентують суспільні інформаційні відносини щодо одержання їх учасниками відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій [12].

В означеному контексті з правом інформаційної свободи, яке апріорі передбачає всю інформацію як загальнодоступну, перетинається інститут інформації з обмеженим доступом. Відсутність чітких критеріїв віднесення інформації до категорії з обмеженим доступом, а також конкретної процедури обмеження доступу до неї сприяють зловживанням органами державної влади шляхом ненадання інформації через неправомірне застосування грифів обмеження доступу до інформації.

Свобода інформації повинна обмежуватись в тій мірі, яка необхідна для досягнення однієї з визначених міжнародно-правовими актами цілей. Обмеження не повинно зводитись лише до заборони з будь-якого конкретного питання. Кожне з обмежень, сукупність яких визначена міжнародно-правовими актами повинно відповідати визначеним умовам, а саме повинно: бути встановлено законом, слугувати одній з перерахованих цілей і бути необхідним для досягнення такої цілі. Беззастережною є вимога у міжнародно-правових актах про те, що будь-які обмеження повинні бути офіційно закріплені в (національному) законі. І такий закон повинен містити конкретну вказівку на можливість втручання з боку правоохоронних органів. Важливе значення має характер нормативного акту [13].

Головним обмеженням свободи інформації є заборона будь-якої пропаганди й агітації, що породжують соціальну, національну, расову, релігійну ненависть і ворожнечу, а також пропаганди соціальної, расової, національної, релігійної або мовної переваги. Частина 3 статті 34 Конституції України формулює виключний перелік підстав для обмеження права на інформацію: в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [6]. Зазначені положення відповідають нормам міжнародного законодавства. Зокрема, ст. 29 Загальної декларації прав людини проголошує, що при здійсненні своїх прав і свобод кожною людиною до неї застосовуються тільки такі обмеження, які встановлені законом винятково з метою забезпечення гідного визнання та поваги до прав і свобод інших і задоволення справедливих вимог моралі суспільного порядку та загального благополуччя в демократичному суспільстві [14]. Відповідно до ст. 10 Європейської Конвенції з прав людини, яка встановлює обмеження щодо права на вираження своєї думки, такі обмеження мають бути [15]: 1) встановлені законом; 2) бути необхідними в демократичному суспільстві; здійснюватися в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших людей, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету та безсторонності суду. Слід зазначити, що наведені міжнародно-правові вимоги з незначними відмінностями втілені у частині 3 ст. 34 Конституції України, яка

встановлює право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань та право на інформацію [6].

Сучасне суспільство є інформаційним та відповідно інформатизованим, що обумовлює віртуалізацію інформаційних відносин, і в першу чергу, це стосується обігу персональних даних. Ідея про забезпечення прав людини он-лайн знайшла відображення у багатьох актах і рішеннях. У 2013 році Генеральна Асамблея ООН прийняла резолюцію "Право на приватність у цифрову епоху", де вказано, що "права, які належать людям у середовищі офф-лайн, також повинні "бути захищені он-лайн", а усі держави "поважати та захищати право на приватність в цифровій комунікації". Керівні принципи ЄС щодо свободи вираження он-лайн та офф-лайн сфокусувалися на забезпеченні права на інформацію, свободи вираження та права на приватність.

У Рекомендаціях Комітету Міністрів Ради Європи наголошується на тому, що права людини повинні однаковою мірою забезпечуватися офф-лайн та он-лайн і вказано, що таким чином не запроваджуються нові види прав, а доступ до Інтернету розглядається як "важливий спосіб реалізації прав, свобод та участі в демократії". Разом з тим, у багатьох країнах широко використовують термін "цифрові права" (digital rights) як умовну категорію, яка визначає особливості реалізації та гарантії захисту прав людини в Інтернеті, зокрема в контексті права на доступ до Інтернету, свободи вираження поглядів та приватності он-лайн. Як зазначають науковці, обізнаність щодо можливостей використання Інтернету – це передумова здатності здійснювати свободу вираження поглядів он-лайн [16].

Закріплення зазначених прав ускладнюється тим, що Інтернет-відносини виходять поза межі юрисдикції конкретної держави, а це породжує невирішеність питань щодо уніфікації підходу до їх юридичного визначення, процедури оскарження та відновлення у разі порушення. Інформаційний суверенітет у даному контексті є засобом досягнення он-лайн свободи інформації громадян конкретної держави через забезпечення т.зв. цифрових прав.

Висновки.

Інформаційні права і свободи людини і громадянина у демократичному суспільстві виступають основним критерієм, що характеризує наявність інформаційного суверенітету держави, оскільки одним із основних пріоритетів інформаційної політики будь-якої країни є дотримання балансу відповідних інтересів особистості, суспільства і держави в інформаційній сфері. Проте, на сучасному етапі еволюція свободи інформації в теоріях інформаційного суспільства здебільшого розглядається у двох ракурсах: без урахування обмежень, коли утверджуються ідеї свободи, але більшою мірою ігноруються вимоги інформаційної безпеки (демократичний режим) та з тотальними обмеженнями, коли принципи інформаційної безпеки держави превалюють над інформаційними правами (недемократичний режим).

Інформаційний суверенітет держави полягає в її здатності проводити незалежну інформаційну політику і забезпечувати верховенство національного законодавства в інформаційному просторі. Принципове значення для забезпечення інформаційного суверенітету має визначення та реалізація національних інтересів держави в інформаційній сфері, які в свою чергу, повинні бути обумовлені природними правами та свободами людини, серед яких основоположним вбачаємо право на свободу інформації.

Відтак, реалізація інформаційного суверенітету держави передбачає забезпечення прав і свобод людини в інформаційній сфері; визначення виключних підстав для обмежень доступу до інформації, що встановлюються при забезпеченні інформаційного

суверенітету держави; пошук балансу між правами людини і необхідністю реалізації цілей держави в інформаційній сфері, а також створення умов для формування інформаційного суспільства та забезпечення доступу до його надбань (цифрові права).

Основоположними началами забезпечення інформаційного суверенітету держави є: презумпція інформаційної свободи як базисний принцип реалізації інформаційного суверенітету; захищеність інформаційної приватності людини; забезпечення права на інформацію як обов'язок держави.

Загалом вище викладена збалансованість, що виражена у пріоритетності свободи інформації та необхідності забезпечення інформаційного суверенітету характеризується тим, що: по-перше, чинне законодавство не лише надає громадянам право доступу до інформації та суспільно важливої інформації, але й гарантує відповідний захист цього права та передбачає відповідальність за порушення такого права. Завдяки цьому громадяни мають можливість використовувати інформацію в особистих інтересах для забезпечення власної життєдіяльності, а також впливати на державу з метою підвищення рівня її прозорості та демократичності; по-друге, обмежуючи доступ до персональних даних та до окремих категорій інформації, держава забезпечує невтручання в особисте життя, попереджує потенційні можливості завдання шкоди особистій безпеці громадян, інформаційній та національній безпеці.

Використана література

1. Юридична енциклопедія: в 6 т. Т. 5 / ред. кол.: Ю.С. Шемшученко (голова ред. кол.) та ін. Київ: Українська енциклопедія, 1998, 2004. С. 441.

2. The World's First Freedom of Information Act / Anders Chydenius' Legacy Today. Kokkola: Anders Chydenius Foundation, 2006. 103 p.

3. Созыв международной конференции по вопросу о свободе информации : Резолюция ГА ООН 59 (I) от 14.12.46 г. URL: www.daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG /NR003310.pdf?OpenElement

4. Письменицький А.А., Слинько Д.В. Теорія держави і права: навч. посіб. Харків: ХНУ ім. В.Н. Каразіна, 2007. 252с.

5. Золотар О.О. Правові основи інформаційної безпеки людини: дис. д-ра юр. наук.: 12.00.07. Київ, Харків, 2018. 479 с.

6. Конституція України: Закон України від 28.06.96 р. *Відомості Верховної Ради України.* 1996. № 30. Ст.141.

7. Данильян О.Г., Дзьобань О.П. Інформаційна свобода: деякі штрихи до усвідомлення сутності. *Стратегічна панорама*. 2016. № 2. С. 73-77.

8. Кант И. Соч.: в 6 т. Москва: Мысль, 1964. Т. 3, 392 с.

9. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3 (19). С. 6-17.

10. Поощрение и защита права на свободу убеждений и их свободное выражение: Резолюция Комиссии по правам человека. – (Доклад специального докладчика г-на Абида Хуссейна, подготовленный в соответствии с резолюцией 1993/45 Комиссии по правам человека. 19 декабря 1994 г. E/CN.4/1995/32). URL: http://www.daccess-ods.un.org/TMP/7821679.71134186.html

11. Брижко В.М. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ Видавничий дім "АртЕК", 2017. 226 с. С. 114; Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних: / [І. Майстренко – переклад з англ.; В. Брижко – редагування тексту]. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.

12. Марущак А.І. Визначення поняття “доступ до інформації”. *Правова інформатика.* № 3(11)/2006. С. 69-74.

13. Забара І.М. Свобода інформації: сучасний концептуальний підхід у науці міжнародного права. *Правова інформатика*. № 1(45)/2015. С. 48-57.

14. Загальна Декларація прав людини від 10 грудня 1948 року: ООН. URL: http://zakon2.rada. gov.ua

15. Європейська Конвенція з прав людини від 04 листопада.1950 року: Рада Європи. URL: http://zakon2.rada.gov.ua

16. Бенедек Ф., Кеттеман М. Свобода вираження поглядів та Інтернет. П.: Видавництво Ради Європи, 2013. 204 с.

17. Брижко В.М. Права і свободи людини і громадянина. – (Кн.: *Основи систематизації інформаційного законодавства: теоретичні та правові засади*: монографія. Київ: ТОВ “ПанТот”, 2012 р. 304 с. С. 16-57); Брижко В.М., Фурашев В.М. *Джерела знань філософії права. “Людина”, “громадянин” і “особа” та “права” і “свободи”.* – (Кн.: *Інформаційне право та інформаційне законодавство*: наукове видання. Київ: Видавничий дім “АртЕК”, 2020. 288 с. С. 10-62, 81-84).

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

УДК 342.7

КОСІЛОВА О.І., *кандидат політичних наук, доцент,*
науковий співробітник юридичного факультету
Київського національного університету ім. Тараса Шевченка.
ORCID: https://orcid.org/0000-0002-5574-3771.

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ОБМЕЖЕННЯ ПРАВ І СВОБОД: ВІТЧИЗНЯНИЙ ТА ЗАРУБІЖНИЙ ДОСВІД

Анотація. *В статті аналізуються актуальні питання обмеження прав і свобод людини і громадянина в Україні, розглядаються теоретичні питання обмеження прав і свобод у практиці Конституційного Суду України та Федерального конституційного суду Німеччини, ЄСПЛ, нормах вітчизняного законодавства та міжнародно-правових актів. Наводяться приклади обмеження політичних прав і свобод в Україні.*

Ключові слова: *права і свободи, обмеження прав та свобод, заборона, втручання, виправдання втручання, "обмеження обмежень" (нім. - "Schranken-Schranken").*

Summary. *The article analyzes topical issues of restriction of human and civil rights and freedoms in Ukraine, theoretical aspects of restriction of rights and freedoms in the practice of the Constitutional Court of Ukraine and the Federal Constitutional Court of Germany, the European Court of Human Rights, norms of domestic law and international legal acts are analyzed. Examples of restrictions on political rights and freedoms in Ukraine are given.*

Keywords: *rights and freedoms, restrictions of rights and freedoms, prohibition, interference, justification of interference, restrictions on restrictions (ger. - "Schranken-Schranken").*

Аннотация. *В статье анализируются актуальные вопросы ограничения прав и свобод человека и гражданина в Украине, анализируются теоретические вопросы ограничения прав и свобод на практике Конституционного Суда Украины и Федерального конституционного суда Германии, ЕСПЧ, в нормах отечественного законодательства и международно-правовых актов. Приводятся примеры ограничения политических прав и свобод в Украине.*

Ключевые слова: *права и свободы, ограничения прав и свобод, запрет, вмешательства, оправдание вмешательства, "ограничения ограничений" (нем. - "Schranken-Schranken").*

Постановка проблеми. Одним із найскладніших питань реалізації прав та свобод людини і громадянина є їх обмеження. Про це свідчать численні рішення суб'єктів публічної адміністрації, судів загальної юрисдикції, Конституційного Суду України та справи, які були направлені на розгляд до Європейського Суду з прав людини (далі – ЄСПЛ).

В Основному Законі України говориться про те, що конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України (частина перша статті 64 Основного Закону України) [1].

У теорії права, обмеження прав людини з одного боку може тлумачитися як порушення прав та їх звуження. З іншого боку, обмеження прав та свобод однієї особи на користь іншої за певних передумов є запобіжником свавілля однієї особи над іншою, або групою осіб, забезпечує принцип верховенства права, принцип рівності та законності, й тлумачитися як складова механізму захисту прав та свобод.

Таким чином, обмеження прав та свобод є актуальним та важливим питанням, що стосується їх реалізації та забезпечення, як у публічно-правовому, так і приватно-правовому просторі.

Результати аналізу наукових публікацій. Проблема обмеження прав і свобод є актуальним напрямком дослідження, як для вітчизняних, так і зарубіжних дослідників. Зокрема, серед українських науковців цією проблемою займалися Мельник Р., Поєдинок В., Римаренко Ю., Савчин М., Федоренко В. та інші дослідники.

Серед зарубіжних, зокрема німецьких дослідників слід згадати праці Ліндера Дж., Єппіга В., Шлоєра Б. та інших.

Метою статті є визначення сутності та змісту поняття "обмеження прав", підстав та меж обмеження шляхом аналізу норм вітчизняного законодавства, практики Конституційного Суду України та міжнародних нормативно-правових актів.

Виклад основного матеріалу. За загальноприйнятою юридичною практикою, що закріплена в нормах Основного Закону та деталізована у конституційних законах, конституційні права та свободи гарантуються та не можуть бути скасовані (відповідно до ч. 2 ст. 22 Основного Закону). Відповідно до ч. 3 ст. 22, при прийнятті нових законів, або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих прав та свобод. Водночас, у Конституції України, у ст. 64 зазначається, що в умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень. Відповідно до частини другої ст. 64 Конституції України не можуть бути обмежені права і свободи, передбачені статтями 24, 25, 27 – 29, 40, 47, 51, 52, 55 – 63 [1].

Для цілісного та об'єктивного дослідження окресленої проблеми слід спочатку визначити зміст самого терміну "обмеження прав та свобод", а також визначити критерії та підстави обмеження, межі обмеження.

У практиці Конституційного Суду України, зокрема у рішенні № 5-рп/2005, визначено, що: "Скасування конституційних прав і свобод – це їх офіційна (юридична або фактична) ліквідація. Звуження змісту та обсягу прав і свобод є їх обмеженням" [2]. У цьому ж рішенні визначається, що "обсяг прав людини – це їх сутнісна властивість, виражена кількісними показниками можливостей людини, які відображені відповідними правами, що не є однорідним і загальним".

ЄСПЛ у рішенні у справі "Евелін проти Франції" наголосив, що під категорією "обмеження", зафіксованою у п. 2 ст. 11 Конвенції Ради Європи "Про захист прав людини і основоположних свобод" 1950 р. (далі – Конвенція РЄ) [7], необхідно розуміти заходи, які застосовуються як до, так і під час зібрання, а також заходи покарання, що реалізуються після зібрання [3, с. 37].

На думку українського дослідника Савчина М., сутність обмежень фундаментальних прав людини відповідно до принципу верховенства права полягає у забезпеченні легітимного втручання держави у приватну автономію індивіда з метою забезпечення загального блага [4, с. 151-152].

При цьому, під межами обмежень прав людини науковець визначає "…сукупність усіх явищ, які окреслюють зміст та обсяг прав людини. До складу цих явищ можуть входити, зокрема, юридичні норми, встановлені міжнародним чи національним правом. У такому разі певні обмеження (межі) прав людини є наслідком нормотворчої діяльності відповідно міжнародних чи державних органів" [4, с. 151].

Римаренко Ю. під обмеженням прав людини розуміє діяльність владних суб'єктів, насамперед, компетентних державних органів, по встановленню меж (обмежень) щодо здійснення прав людини [5].

Мельник Р., аналізуючи види обмежень права на мирні зібрання, виділяє такі можливі форми: повну заборону проведення запланованого зібрання; обмежувальні заходи; примусове припинення (розпуск) зібрання, що триває [6, с. 147].

Критерії обмеження основних прав і свобод.

У теорії прав людини, зарубіжній практиці та діяльності ЄСПЛ вироблені такі критерії обмеження основних прав і свобод, які закріплені у положеннях Конвенції РЄ: необхідність у демократичному суспільстві; національна безпека; громадський порядок і безпека; права і свободи інших людей; моральність населення [7].

На думку Савчина М., основними критеріями, яким повинні відповідати обмеження конституційних прав та свобод є наступні:

1. Обмеження на основі закону. Допускається обмеження фундаментальних прав виключно на основі закону, оскільки таке повноваження народ делегує виключно парламентові як вищому представницькому органові влади. Делегування законодавцем повноважень урядові стосовно обмеження фундаментальних прав людини у невизначеній формі, без вказівки його адресата, строків та засобів контролю є неправомірним.

2. Відповідність легітимній меті. Правовою основою обмеження прав людини є загальне визнання його суспільної необхідності, існування нагальної потреби визначення меж здійснення суб'єктивного права з урахуванням інтересів інших осіб [4, с. 152].

Відповідно до німецької правової доктрини, при встановленні обмежень прав і свобод людини і громадянина важливо встановлювати "Schranken" ("обмеження"), та "обмеження-обмежень" ("Schranken-Schranken"), тобто межі, яких слід дотримуватися при обмеженні основних прав [8]. При цьому, сам термін "втручання" ("Eingriff"), що широко використовується у німецькій правовій доктрини, відповідає терміну "обмеження" у вітчизняній юриспруденції. Саме втручання, на наш погляд можна визначити як цілеспрямовану (імперативну) діяльність органів державної влади, спрямовану на забезпечення громадського інтересу, захисту державного ладу, громадського порядку, прав та свобод громадян [9, с. 51].

"Schranken" ("обмеження") означає втручання в основні права людини на підставі нормативно-правового акту, прийнятого парламентом або адміністративного акту органів державної влади. Втручання в основні права повинно здійснюватися виключно на підставі закону (діє так зване "законодавче застереження" (нім. "Gesetzesvorbehalt") або легітимного адміністративного акту. При цьому, сам нормативно-правий акт повинен бути конституційним у формальному та матеріальному відношенні [10, с. 18]. Наприклад, втручанням у право асоціацій, закріпленому у ст. 9 п. 1 Основного закону ФРН є всі норми, що перешкоджають здійсненню свободи асоціацій. Найважчою формою втручання є заборона. Таким чином, у німецькій правовій доктрині втручання в основні права визначається як законне, за умови, що воно конституційно виправдане.

Виправдання втручання та визначення міри втручання у приватну автономію:

Конституційна юриспруденція України стоїть на наступній позиції: "Таке обмеження має встановлюватися виключно Конституцією та законами України; переслідувати легітимну мету; бути обумовленим суспільною необхідністю досягнення цієї мети, пропорційним та обґрунтованим. У разі обмеження права на оскарження судових рішень законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію права… і не порушувати сутнісний зміст такого права" [11].

Окрім того, Конституційний Суд України вважає, що обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими, вони мають встановлюватися виключно Конституцією і законами України; у разі обмеження конституційного права або свободи законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з

мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права [12].

Відповідно до Рішення Конституційного Суду України від 29 червня 2010 року № 17-рп/2010, обмеження основних прав людини та громадянина і втілення цих обмежень на практиці, відповідно до принципу правової визначеності (який є одним із елементів верховенства права), допустиме лише за умови забезпечення передбачуваності застосування правових норм, встановлюваних такими обмеженнями. Тобто обмеження будь-якого права повинне базуватися на критеріях, які дадуть змогу особі відокремлювати правомірну поведінку від протиправної, передбачати юридичні наслідки своєї поведінки [13].

Нормативне забезпечення захисту прав та свобод людини і громадянина в Україні здійснює Верховна Рада України, яка повноважна ухвалювати закони, що встановлюють обмеження, відповідно до таких критеріїв: "обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими, вони мають встановлюватися виключно Конституцією і законами України, переслідувати легітимну мету, бути обумовленими суспільною необхідністю досягнення цієї мети, пропорційними та обґрунтованими, у разі обмеження конституційного права або свободи законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права" [12].

У рішенні Федерального конституційного суду Німеччини визначено, що при обмеженні прав та свобод має бути забезпечений принцип пропорційності, який полягає у забороні надмірного впливу**,** вимагає, щоб втручання в основне право переслідувало легітимну мету і виступало відповідним, необхідним і пропорційним засобом досягнення цієї мети: a) мета, яку переслідує обмеження, повинна бути легітимною, тобто, мати конституційно-правові підстави; b) втручання повинно виступати засобом досягнення цієї мети; aa) відповідний – такий, що слугує досягненню мети; bb) необхідний – потрібний (найм'якший засіб); cc) співрозмірний – пропорційний: балансування тягаря втручання та переслідуваної мети. Вимога пропорційності вимагає, щоб тягар втручання в загальний баланс не був непропорційним до ваги причин, що виправдовують його [14; 15].

Підстави для запровадження обмежень прав людини й основоположних свобод.

Відповідно до легітимної мети підстави для обмеження прав людини мають ґрунтуватися на засадах сприяння у їх здійсненні. Таким чином, запровадження певних заходів мають передбачати мінімально достатні та доречні засоби щодо охорони певних конституційних благ, яким існує невідворотна загроза при здійсненні певних прав.

Конституція ФРН [16] визначає можливості виправдання втручань, якщо було виконано наступні умови:

1. Належне прийняття: компетенція, процедура, форма, ст. 70 і наступні статті Основного Закону.

2. Вимога цитування (нім. "Zitiergebot"), реч. 2 ч. 1 ст. 19: обов'язок законодавця при обмеженні основного права законом або на підставі закону зазначати статтю Основного Закону, яка стосується цього основного права, або стосується лише основних прав, для яких прямо передбачена можливість обмеження законом або на підставі закону (вузьке тлумачення); зокрема, не стосується ч. 1 ст. 2, ст. 3, 5, 12 і 14.

3. Заборона обмежуючих законів індивідуальної дії, реч. 1 ч. 1 ст. 19.

4. Гарантія збереження сутності, ч. 2 ст. 19 вимагає недоторканності сутності основних прав.

5. Визначеність та нормативна ясність, ст. 20, ч. 1 ст. 28.

Таким чином, термін "втручання", що широко використовується у німецькій правовій доктрині, відповідає терміну "обмеження" у вітчизняній юриспруденції. Відповідно до проведеного аналізу, термін "втручання" на наш погляд можна визначити як: цілеспрямовану (імперативну) діяльність органів державної влади, спрямовану на забезпечення громадського інтересу, захисту державного ладу, громадського порядку, прав та свобод громадян.

Приклади обмежень окремих прав та свобод у політичній сфері.

Переважна більшість політичних прав та свобод громадян відповідно до Конституції України не є абсолютними та можуть обмежуватися за певних умов. Зокрема, може бути обмежене право на об'єднання у політичні партії. Так, відповідно до змісту ст. 37 Конституції України та ст. 5 Закону України "Про політичні партії в Україні" [17], утворення і діяльність політичних партій забороняється, якщо їх програмні цілі або дії спрямовані на: ліквідацію незалежності України; зміну конституційного ладу насильницьким шляхом; порушення суверенітету і територіальної цілісності України; підрив безпеки держави; незаконне захоплення державної влади; пропаганду війни, насильства, розпалювання міжетнічної, расової чи релігійної ворожнечі; посягання на права і свободи людини; посягання на здоров'я населення; пропаганду комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їх символіки. Політичні партії не можуть мати воєнізованих формувань [17].

Обмеження права на свободу об'єднання у політичні партії пов'язано із добровільною відмовою від реалізації цього конституційного права у зв'язку із вступом на державну службу. Зокрема, йдеться про вимоги щодо позапартійності державної служби, яка випливає із приписів п. 1 ч. 3 ст. 10 Закону України "Про державну службу" [18]; ч. 3 ст. 18 Закону України "Про прокуратуру" [19]; ч. 4 ст. 61 Закону України "Про Національну поліцію" [20]; п. 1 ч. 2 ст. 13 Закону України "Про Національне антикорупційне бюро України" [21] тощо.

Тоді як у ФРН обмеженням (втручанням) у право асоціацій, закріпленому у ст. 9 п. 1 Основного закону є всі норми, що перешкоджають здійсненню свободи асоціацій. Найважчою формою втручання є заборона. Зокрема, у ст. 9 п. 2 Конституції ФРН зазначено, що: "Асоціації, цілі чи діяльність яких суперечать кримінальним законам або спрямовані проти конституційного порядку або проти ідеї міжнародного порозуміння, заборонені".

Щодо втручання безпосередньо у право на об'єднання у політичні партії, то слід зазначити, що втручання у це право здійснюється відповідно до положень Основного Закону (ст. 9 п. 2) [16] та Закону "Про політичні партії" [22]. Згідно з формулюванням статті 21 Конституції ФРН, заборона партії може бути розглянута лише в тому випадку, якщо партія, виходячи зі своїх цілей або поведінки своїх прихильників, має на меті зміну або ліквідацію вільного демократичного конституційного ладу ФРН. Якщо партія визнана антиконституційною рішенням Федерального конституційного суду, вона виключаються з державного фінансування.

Особливістю правового регулювання права на об'єднання у політичні партії у Німеччині у порівнянні з Україною є, зокрема, відсутність заборони для держслужбовців та військовослужбовців мати членство у партіях, а також право іноземців набувати членство у партіях.

Суб'єктивне виборче право громадян України вільно обирати і бути обраним насамперед передбачено ст. 38 Конституції України, а також у спеціально присвяченому

цьому питанню третьому розділі (статті 69-71) обмеженим шляхом встановлення так званих "виборчих цензів", таких як вік та інші умови, за яких громадянин України набуває право у повному обсязі здійснювати свої виборчі права [23, с. 363].

Зокрема, право голосу на виборах мають громадяни України, які досягли на день їх проведення вісімнадцяти років, за винятком громадян, яких визнано судом недієздатними. У Конституції України закріплено, що недієздатні особи не мають права голосу на виборах і референдумах (ст. 70). У зв'язку з цим до зазначених осіб застосовуються обмеження, передбачені у ст. 72, 76, 81, 103 Основного Закону України. На думку Конституційного Суду України, визнання особи недієздатною не може позбавляти її інших конституційних прав і свобод чи обмежувати їх у спосіб, що нівелює їхню сутність [12].

Право на свободу зібрань може обмежуватися лише судом відповідно до закону і лише в інтересах національної безпеки та громадського порядку (з метою запобігання злочинів чи заворушень, для захисту прав і свобод інших людей або для охорони здоров'я населення). Основою обмежень свободи зібрань є конституційна вимога їх мирного і беззбройного характеру [23, с. 368]. Таким чином, Конституційний Суд України визначив критерії правомірності проведення зібрань: зібрання можна проводити "за умови обов'язкового завчасного сповіщення про це органи виконавчої влади чи органи місцевого самоврядування"; таке сповіщення слід проводити "через організаторів масових зібрань"; завчасне сповіщення повинно носити попередній характер тощо [24]. Як зазначає Р. Мельник, обмеження щодо права проведення мирних зібрань можуть стосуватися питань часу, місця, форми, способу проведення зібрання, висловлювань та лозунгів, що їх мають намір використовувати його учасники, допоміжних засобів (освітлювальної техніки, звукопідсилювальної техніки). Перелік можливих обмежень не є закритим, а відтак – судом можуть запроваджуватися й інші обмеження, що відповідають обставинам конкретного зібрання [6, с. 151].

Висновки.

1. Сутність обмежень фундаментальних прав людини відповідно до принципу верховенства права полягає у забезпеченні легітимного втручання держави у приватну автономію індивіда з метою забезпечення загального блага.

2. Конституційний Суд України тлумачить зміст терміну "обмеження прав і свобод" як звуження їх змісту та обсягу та наголошує, що встановлення обмежень прав і свобод людини і громадянина є допустимим виключно за умови, що таке обмеження є домірним (пропорційним) та суспільно необхідним.

3. Поняття "обмеження" прав і свобод, які застосовується в українській правовій доктрині відповідає терміну "втручання" у німецькій правовій доктрині, тому їх слід розглядати як синонімічні. Водночас, в Україні відповідно до практики Конституційного Суду України, обмеження прав і свобод не передбачає їх скасування, а лише звуження змісту та обсягу, тоді як у Німеччині найвищою формою втручання є заборона.

4. Конституційна юриспруденція України стоїть на наступній позиції щодо виправдання втручання та визначення міри втручання у приватну автономію: обмеження має встановлюватися виключно Конституцією та законами України; переслідувати легітимну мету; бути обумовленим суспільною необхідністю досягнення цієї мети, пропорційним та обґрунтованим, що повністю відповідає положенням Конвенції Ради Європи про захист прав людини і основоположних свобод.

5. Нормативне обмеження прав і свобод людини і громадянина може здійснюватися відповідно до чітко визначених критеріїв, які окрім вищенаведених включають: обмеження щодо реалізації конституційних прав і свобод не можуть бути

свавільними та несправедливими, мають бути пропорційними та обґрунтованими. При ухваленні нових законів або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих конституційних прав і свобод людини, якщо таке звуження призводить до порушення їх сутності. У разі обмеження конституційного права або свободи законодавець зобов'язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права.

Використана література

1. Конституція України: Закон України від 28.06.96 р. № 254/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
2. Рішення Конституційного суду України від 22.09.05 р. № 5-рп/2005. URL: http://www.ccu.gov.ua/docs/516 (дата звернення 05.06.20).
3. Решение Европейского суда по правам человека по делу "Эвелин против Франции" (Case of Ezelin v. France) от 26 апреля 1991 г. – (Дикман С.С., Терехов К.И. Свобода мирных собраний в практике Европейского Суда и Комиссии по правам человека: сб. решений и постановлений; под общ. ред. С.С. Дикмана. Москва: РИО "Новая юстиция", 2011. 360 с.).
4. Савчин М.В. Порівняльне конституційне право: навч. посібник. Київ: Юрінком Інтер, 2019. 328 с.
5. Римаренко Ю. Приватне життя і поліція. URL: https://westudents.com.ua/glavy/68495-52-klasifkatsya-ta-mej-zdysnennya-prav-lyudini.html (дата звернення: 05.07.20).
6. Мельник Р.С. Право на свободу мирних зібрань: теорія і практика. Київ, 2015. 168 с.
7. Про захист прав людини і основоположних свобод: Конвенція Ради Європи від 4 листопада 1950 року. URL: https://zakon. rada.gov.ua/laws/show/995_004#Text (дата звернення: 05.07.20).
8. Beck'scher Online-Kommentar GG. Retrieved June 12, 2020. URL: https://beck-online. beck.de/?vpath=bibdata/komm/BECKOK_29_BandVerfR/GG/cont/BECKOK.GG%2Ehtm (дата звернення: 05.07.20).
9. Косілова О.І., Поєдинок В.В. Втручання у права людини в німецькій та українській правових доктринах (2019). *Порівняльно-аналітичне право*. № 3, 50-56. URL: http://www.pap.in.ua/3_2019/13.pdf (дата звернення: 05.05.20).
10. Eppig V. Grundrechte (2010). Springer-Verlag Berlin Heidelberg. 471 с.
11. Рішення Конституційного Суду України від 22.05.18 р. № 5-р/2018. URL: https://zakon.rada.gov.ua/laws/show/v005p710-18#Text (дата звернення: 05.07.20).
12. Рішення Конституційного Суду України від 01.06.16 р. № 2-рп/2016. URL: https://zakon.rada.gov.ua/laws/show/v002p710-16#Text (дата звернення: 05.07.20).
13. Рішення Конституційного Суду України від 29.06.10 р. № 17-рп/2010 https://zakon.rada.gov.ua/laws/show/v017p710-10#Text (дата звернення: 05.07.20).
14. BVerfGE 118, 168. URL: https://www.servat.unibe.ch/dfr/bv118168.html (дата звернення: 05.07.20).
15. Gropl, Verfassungsrechtliche Rechtfertigung von Grundrechtseingriffen URL: https://www.uni-saarland.de/fileadm (дата звернення: 05.07.20).
16. Grundgesetz für die Bundesrepublik Deutschland (1949). URL: https://www.gesetze-im-internet.de/gg/BJNR000010949 (дата звернення: 07.07.20).
17. Про політичні партії в Україні: Закон України від 05.04.01 р. № 2365-III. URL: https://zakon.rada.gov.ua/laws/show/2365-14 (дата звернення: 25.05.2020).
18. Про державну службу: Закон України від 10.12.15 р. № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19 (дата звернення: 25.05.2020).
19. Про прокуратуру: Закон України від 14.10.14 р. № 1697-VII. URL: https://zakon.rada.gov.ua/laws/show/1697-18 (дата звернення: 25.05.2020).

20. Про Національну поліцію: Закон України від 02.07.15 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 25.05.2020).

21. Про Національне антикорупційне бюро України: Закон України від 14.10.14 р. № 1698-VII. URL: https://zakon.rada.gov.ua/laws/show/1698-18 (дата звернення: 25.05.2020).

22. Gesetz über die politischen Parteien.1967. URL: https://www.gesetze-im-internet.de/partg (дата звернення: 10.06.2020).

23. Савчин М.В. Конституційне право України: підручник / відп. ред. проф., д.ю.н. М.О. Баймуратов. Київ: Правова єдність, 2009. 1008 с.

24. Рішення Конституційного Суду України у справі щодо завчасного сповіщення про мирні зібрання від 19.04.01 р. № 4-рп/2001. URL: https://zakon.rada.gov.ua/laws/show/v004p710-01#Text (дата звернення: 05.07.20).

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

УДК 316(477)

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,* головний науковий співробітник НДІ інформатики і права Національної академії правових наук України.
ЖДАНЕНКО С.Б., *кандидат філософських наук, доцент*, доцент кафедри філософії Національного юридичного університету імені Ярослава Мудрого.

МНОЖИННА ІДЕНТИЧНІСТЬ ОСОБИСТОСТІ У МЕРЕЖЕВИХ УМОВАХ: ДО АНТРОПОЛОГІЧНИХ ЗАСАД ІНФОРМАЦІЙНОГО ПРАВА

Анотація. *У статті показано, що в умовах глобального інформаційного простору особистість під впливом мережевих взаємодій стикається з системою множинності ідентичності, з формуванням "мережевої ідентичності". Доводиться, що багатоваріантність сучасного культурного середовища породжує різноманітні форми самоідентифікації особистості. Мережева культура сприяє появі нового типу особистості – "мережево-інформаційної", яка включена в особливу сферу комунікацій.*

Ключові слова: *інформаційне суспільство, ідентичність, мережеві комунікації.*

Summary. *The article shows that in the conditions of the global information space, a person, under the influence of network interactions, collides with a system of identity plurality, with the formation of "network identity". It is proved that the multi-variability of the modern cultural environment gives rise to various forms of personality self-identification. Network culture contributes to the emergence of a new type of personality – "network-informational", included in a special sphere of communications.*

Keywords: *information society, identity, network communications.*

Аннотация. *В статье показано, что в условиях глобального информационного пространства личность под влиянием сетевых взаимодействий сталкивается с системой множественности идентичности, с формированием "сетевой идентичности". Доказывается, что многовариантность современной культурной среды порождает различные формы самоидентификации личности. Сетевая культура способствует появлению нового типа личности – "сете-информационной", включенной в особую сферу коммуникаций.*

Ключевые слова: *информационное общество, идентичность, сетевые коммуникации.*

Постановка проблеми. Особливістю сучасного суспільства є інтенсивна динаміка інформаційного простору. Остання інформаційна революція зумовила виникнення нової галузі – інформаційної індустрії, яка пов'язана із виробництвом технічних засобів, методів, технологій задля здобуття нових знань. Бурхливий розвиток комп'ютерної техніки та інформаційних технологій сприяв розвитку суспільства і обумовив антропологічну складову інформаційної революції [1, с. 34], що передбачає удосконалення не тільки техніки й технологій, але й людини, насамперед, механізмів її самоідентифікації.

Реальністю сучасної цивілізації Е. Тоффлер проголошує розпад універсальної картини світу, що супроводжується кризою індивідуальної та групової ідентичності. "Ті, кому доведеться жити на нашій планеті у цей вибуховий період, повною мірою відчують вплив Третьої хвилі на себе. Розрив сімейних зв'язків, коливання в економіці, параліч політичних систем, руйнування наших цінностей – на все це здійснює вплив Третя хвиля… Виникаюча цивілізація пише для нас нові правила поведінки і веде нас за межі стандартизації, синхронізації і централізації, за межі уявлень до накопичення енергії, грошей чи влади", – зазначає Е. Тоффлер [2, с. 33].

В умовах глобалізації, націленої не лише на всесвітню інтеграцію, а й на уніфікацію майже всіх сфер людської діяльності, як справедливо зазначає Л. Прокопович, спостерігається і зворотній процес, обумовлений розумінням важливості (і необхідності) культурного різноманіття. У цьому процесі набуває актуальності питання ідентичності – культурної, національної, релігійної, соціально-статусної тощо [3, с. 58].

Під впливом наростаючого процесу інформатизації усіх сторін життєдіяльності індивіда відбувається переакцентуація ціннісної, морально-духовної складових світоглядного поля людини, трансформуються традиційні форми комунікації, ускладнюються системні зв'язки соціальних суб'єктів. Як наслідок, по-новому постає проблема ідентифікації, яка являє собою багатовекторний філософський феномен, що визначає особливу роботу самосвідомості й дозволяє індивіду визначити свою ідентичність і соціально-особистісний ареал. У особистості з'являється альтернатива: або незалежно встановити свою життєву позицію, або погодитися з тими готовими приписами, які пропонуються їй інформаційним простором з його мережевою різноманітністю і множинною ідентичністю.

Важливою проблемою сучасного філософського знання є питання динаміки особистості у межах історичного процесу, особливо в сучасних умовах глобальних змін її ціннісних орієнтирів, що визначають змістовну спрямованість особистості.

Результати аналізу наукових публікацій свідчать, що незважаючи на величезну кількість наукових публікацій проблема людини в умовах становлення інформаційного суспільства ще недостатньо повно досліджена. Проблема трансформації особистісних орієнтирів стала предметом пильного вивчення з початку XX ст. у великих промислових європейських і американських центрах у зв'язку з нестримним зростанням побічних продуктів промисловості, що загрожують здоров'ю людей.

Власне виникнення проблематики ідентифікації та ідентичності традиційно пов'язують з психологічними вченнями. У 40-і роки минулого століття Е. Еріксон пропонує у своїх концепціях терміни "ідентичність", "криза ідентичності". У 1950-ті роки виникають різні інтерпретації цих понять. Подальша еволюція проблеми ідентичності від появи перших зародкових теоретичних форм до самостійного теоретичного знання простежується в роботах класиків зарубіжної філософії, психології та соціології У. Джеймса, З. Фрейда, К. Юнга, Ж. Піаже, Е. Фромма, Дж. Міда, Ч. Кулі, Е. Еріксона, А. Маслоу, Р. Мейлі, Ю. Хабермаса, К. Хорні та багатьох інших дослідників.

Філософські концепції людини і суспільства мислителів усіх часів є тим підґрунтям, на базі якого сформувалися сучасні теорії особистості й суспільства. Разом з тим, стрімка динаміка інформаційних процесів у сучасному суспільстві відкриває все нові й нові сторони проблеми буття особистості в інформаційному суспільстві. За останні кілька років під впливом розвитку віртуальних засобів взаємодії сталася серйозна трансформація суспільних відносин, що вимагає адекватного наукового опису і пояснення нового контексту соціальної взаємодії в інформаційному суспільстві. Є потреба у філософському аналізі змін умов соціальної взаємодії, оскільки є деяка неадекватність наукового опису комунікації як форми соціальних відносин в умовах віртуальної реальності при наявності глобальної комунікаційної системи.

Незважаючи на те, що інтереси наукової спільноти спрямовані на розгляд цієї проблеми, ми змушені відзначити, що найчастіше вона осмислюється односторонньо, без урахування багатьох важливих аспектів.

Метою статті є визначення ключових аспектів взаємодії особистості з сучасним суспільством крізь призму проблеми збереження її ідентичності у нових мережевих умовах.

Виклад основного матеріалу. Як справедливо зазначає С. Ганаба, в умовах інформаційно-комунікативного способу розвитку суспільства сучасна людина опиняється й перебуває у просторі небезпеки, безпорядку та потенційних ризиків, з якими до цих пір не зустрічалася. Вона стає заручником світу, який сама створила, щосекунди зустрічаючись з реаліями майбутнього та виявляючи недостатню здатність адаптуватися до швидкоплинного життя. Такі обставини спонукають до пошуків нових життєвих смислів, що покликані подолати всеохоплюючий стан ситуативної тривожності, задовольнити вітальні та духовні потреби людини, окреслити шляхи її самовираження та самовдосконалення, культивувати здатність збагнути та розкрити світ власної унікальності та духовно-культурної самобутності [4, с. 326].

Динаміка соціального простору і часу завжди відкриває перед особистістю можливість розкритися найбільш рельєфно, оскільки всі епохи ставлять перед людиною свої завдання. Особистість активно включається у соціально-культурний простір, одним з аспектів якого є багатовимірність, що дозволяє їй як соціальному суб'єктові займати в ньому різноманітні позиції.

Сутнісні зміни в соціальних пріоритетах та суперечливі ціннісні орієнтації сучасного суспільства змушують людину знаходитись у стані постійного пошуку та вибору життєвої стратегії, розуміння своєї професійної, культурної позиції по відношенню до соціального життя [5, с. 84].

Факт, що сучасна світова система переживає на даний момент період перетворень у бік глобалізації соціального життя, є очевидним. Як зазначалося раніше, переважно це проявляється в економічній сфері, оскільки розвиток економіки є одним з істотних факторів структуризації соціального простору [6 – 9]. У контексті цього П. Бурдьє зазначив: "Соціальний простір – абстрактний простір, конституйований комплексом підпросторів або сфер (економічна сфера, інтелектуальна сфера тощо, які зобов'язані своєю структурою нерівноправному поділу окремих видів капіталу); він, може сприйматися у вигляді структури поділу різних форм капіталу, що функціонує синхронно як засіб і мета боротьби в різноманітних полях... Створений фізично соціальний простір – це розподіл у фізичному просторі всіляких різновидів благ і послуг, а також персональних агентів і груп, зосереджених фізично... і таких, які мають потенціал привласнення цих почасти істотних благ і послуг" [10].

У зв'язку з цим зміна соціального і економічного укладу суспільства, розширення життєвих горизонтів особистості в результаті глобалізаційних процесів веде до соціальних територіальних змін, а також до переструктуризації особистісних орієнтирів, як на життєво-особистісному, так і на соціокультурному рівні. У результаті глобалізація призводить не лише до соціальних змін, але й до трансформації особистісних установок, розширення суспільного поля особистості. Більш чітко це відображається у взаєминах людей усієї світової спільноти і вносить свої корективи у стратегію поведінки країн, континентів і пересічних обивателів, які (взаємини), як би парадоксально це не звучало, стали можливими у зв'язку з впровадженням у соціальне життя принципу загальнодоступності інформації.

Одним із способів вирішення екологічної проблеми стала пропозиція щодо використання нових видів палива і зміна існуючих технологій.

Інформаційна революція, що відбулася в третій чверті XX ст., внесла оптимістичний настрій в особистісні орієнтири жителів планети. З одного боку, важка промисловість і металургія фактично втратили своє провідне значення, з іншого – підвищення наукоємності виробництва знизило матеріаломісткість і енерговитрати на одиницю продукції.

Суспільство дійшло висновку, що технічні засоби створюють певні незручності й підсилюють соціальні складності й перешкоди. За справедливою заявою Ж. Бодрійяра, "техніка є нам вже не як річ, пристрій або засіб у діяльності. І не як учасник соціального процесу, який впливає на ті чи інші його параметри. Новий контекст технічної присутності виникає в рамках феноменологічного підходу до інтерсуб'єктивності життєвого світу. Немає сумніву у тому, що процеси впливу техніки на життєвий світ здатні виявити латентні фактори впливу на системні джерела суспільної інтеграції" [11, с. 171]. Інакше кажучи, технічний прогрес свого часу виступив як фактор особистісного розвитку.

У процесі еволюції людини її простір життєдіяльності завжди був комбінованим, як природним, так і неприродним, тут об'єкти природи існували по сусідству з артефактами, тобто з продуктами людської діяльності. Переконливими є висновки дослідників про існування техносфери, яка виникла й існує на основі науково-технічної революції [12 – 14]. Деякі дослідники навіть ведуть мову про віртосферу – сферу соціального буття людини, опосередковану символічною реальністю віртуального комп'ютерного дискурсу [15].

Очевидно, що обсяг і масштаби індустріального суспільства кардинально відрізняються від традиційних, які створені й детермінують природні можливості простої людини. Чітко вимальовується й те, що світоглядні горизонти значно розширюються і доленосно змінюються одні ціннісні орієнтири на інші: що є цінним для представників індустріального суспільства, вже не має такої цінності для представників суспільства інформаційного.

У контексті даної статті інформаційне суспільство будемо розглядати як сучасний щабель формування культури з переважаючою значущістю інформації і знання, тотальним впровадженням інформаційно-комунікаційних технологій (далі – ІКТ) у всю виробничо-господарську діяльність, як людини, так і суспільства в цілому. В основі діяльності сучасної людини лежать інформатизаційні процеси, спрямовані на формування телекомунікаційної інфраструктури, що пов'язує територіально розділені інформаційні фонди та можливості. Процедура інформатизації – це природний результат і процес формування інформаційно-комп'ютерних технологій та їх трансформації. Як справедливо стверджує О. Алтинкович, сьогодні основу інформатизаційних процесів складають кібернетичні способи й технології управління, а також механізми ІКТ [16, с. 50].

Однак було б невірним розглядати інформатизаційні процеси виключно у технологічній сфері, випускаючи з уваги соціальні та культурологічні аспекти, пов'язані з істотними модифікаціями у стилі життя сучасної людини. Ці модифікації охоплюють практично весь спектр діяльнісних процедур від ліквідації комп'ютерної неграмотності до формування інформаційної культури.

Очевидним є те, що в ході інформатизації, з'являється можливість вирішити широке коло завдань, таких, як зміна підходів до виробництва, модернізація укладу життя, формування системи цінностей. У цій ситуації особливо цінним є вільний час, оскільки відтворюються й споживаються розумові здібності, досвід, де превалює частка інтелектуальної праці. Від суб'єктів інформаційної спільноти усе частіше вимагається творчий підхід до праці і зростають цілком обґрунтовані претензії до знань. Значною мірою модифікується матеріальна й технологічна складова суспільства, першорядне значення надається різним аналітичним, інноваційним, інформаційним системам менеджменту, що виникли на основі інформаційно-обчислювальних технологій, включаючи комп'ютерні мережі й телекомунікаційні зв'язки. Безсумнівно, що основним завданням інформатизації є модифікація рушійних важелів суспільства, яке повинно переорієнтуватися на виробництво не матеріального продукту, а інформаційного

продукту і послуг, пов'язаних з ним. Очевидно, що в ході інформатизації виникають цілком реальні можливості для вирішення широкого кола завдань, таких як зміна підходів до виробництва, модернізація укладу життя, формування системи цінностей.

З упровадженням інформаційних технологій в усі сфери виробничо-господарської діяльності з'являється можливість управляти великими організаціями і виробничими системами, яким необхідна скоординована діяльність величезної кількості людей. У зв'язку з цим йде активне вивчення і впровадження нововведень у сфері інформаційних теорій, інформатики, кібернетики, у системі прийняття рішень, теоріях ігор, тобто в таких напрямках, де існує прямий зв'язок з питаннями організаційних множин.

Тотальність індустріального суспільства призводить до знеособлення особистості до надзвичайного стану, коли вона стає частиною механізму державної машини. З цього приводу О. Алтинкович, вслід за З. Бауманом цілком справедливо підкреслює, що "суспільство перетворюється на ієрархічну піраміду безперервно примножуваних всеосяжних "місцевостей", на вершині яких стоїть загальнодержавна влада, яка стежить за всіма, у той час як сама не піддається постійному контролю. Глобальна інформаційна павутина, яка з'явилась над цією територіальною (урбаністичною) архітектурою, формує новий, кібернетичний простір" [16, с. 52]. У результаті ми виявляємо нове розширення обстежуваних горизонтів суспільної реальності, тому знову здійснюється переоцінка цінностей і виникнення нових світоглядних смислів. Інформаційний простір стає одним з факторів, який духовно готує людей до осмислення глобалізації всіх суспільних відносин.

Спільна діяльність людей спрямована не лише на фізичний вплив на природу і суспільство, також тут активно обмінюються інформацією люди різних поколінь, забезпечуючи міжпоколінну спадкоємність. Подібний обмін і зберігання інформації забезпечує знаково-символічна система, що символізує як суспільні значення, так і їх мовне втілення. У зв'язку з цим, усі символічні, знакові засоби і форми вираження формують своєрідне семіотичне поле, що є необхідним для осмисленої діяльності людей, їх подальшої взаємодії та комунікації. На цій основі виникають зосередження, збереження і трансляція загальнолюдських цінностей і положень, які у подальшому виступають як умови конкретної діяльності людей, як на рівні свідомості, так і на рівні практичного застосування. У зв'язку з цим у загально-філософському ракурсі набирає популярності наукова дискусія про семіосферу [17 – 19], аналогічно дискусіям про ноосферу, біосферу тощо.

У цьому контексті Ю. Лотман вважав, що простір семіосфери носить абстрактний характер [20, с. 12]. Він розглядає семіотичний універсум як "сукупність окремих текстів і мов, замкнутих у відношенні одна до одної" [20, с. 13], причому "мова" в цьому контексті набуває значення "мови культури", а сукупність текстів являє семіосферу. Ю. Лотман характеризує семіосферу як певну семіотичну однорідність і індивідуальність. Законом організації семіосфери, вважає Ю. Лотман, є внутрішня нерівномірність, яка характеризується "наявністю ядерних структур (частіше декількох), що тяжіє до периферії більш аморфного семіотичного світу, в який ядерні структури занурені". Ці рівні знаходяться в стані активної взаємодії, що є "одним із джерел динамічних процесів всередині семіосфери" [20, с. 17]. Неоднорідність семіосферного простору, за Лотманом, є основою формування динамічних процесів як одного з механізмів вироблення нової інформації. Тому є всі підстави вважати, що в наш час семіосфера стає необхідною умовою виникнення кіберпростору, при цьому саме вона виступає соціокультурним гарантом існування інформаційного простору.

Соціокультурне поле інформаційного суспільства та інформаційний простір – цілісна система: за розвитком економічних відносин йде масштабне впровадження комп'ютерних технологій і розширення зв'язків між ними, створення мереж. Глобальна мережа Інтернет виробляє нові форми фінансових операцій, торгових угод, створюються досі не звідані ринки і форми послуг, що надаються. Сприяючи солідарності користувачів, інформаційний простір виступає як певне уособлення свободи.

Парадокс формування інформаційного простору полягає в тому, що при всій своїй формальності свободи, він виступає для особистості не автономно, а лише як один із способів здійснення її комунікації. Тобто, інформаційний простір існує поряд з природним та індустріальним і гарантом цього виступає особистість як суб'єкт інтелектуальний, соціальний і біологічний. Тому інформаційний простір самостійно не забезпечує людської свободи, незважаючи на те, що сучасна особистість прагне бачити в існуванні інформаційного простору саме її (свободи) забезпечення.

Важливим фактом є те, що в інформаційному суспільстві зростає значення інформації як соціального джерела й особистого надбання. Інформаційний простір фігурує як масив інформації, без якого сучасна особистість не може існувати тією ж мірою, як рослина не може вирости без води. У зв'язку з цим зміна структури світоглядних орієнтацій особистості, а разом з ними і суспільних засад її існування, є проекцією інформаційного простору на соціальну реальність і особистість.

Таким чином, трансформації в екологічному мисленні, поширення техносфери, поява інформаційного простору значним чином модифікують світоглядні цілі сучасної особистості, переструктуровуються її цінності, а також розширюється її соціально-культурний простір [21].

Специфіка людської життєдіяльності в інформаційному суспільстві проявляється у кризовому стані ідентичності [22], тому необхідним є розгляд основних проблем ідентифікації, які з'являються в результаті втрати особистістю своїх колишніх смисложиттєвих орієнтирів і ціннісних установок [23 – 26].

В інформаційному суспільстві немає стандартних мислень, і це призводить до зміни уявлень про цілісну ідентичність особистості. Проте, особистість, як би вона не втрачала стабільність свого почуття ідентичності, все одно намагається цю стабільність отримати, принаймні у новій якості. В її прагненні до соціальної взаємодії спостерігаються зусилля виходу з "кризи ідентичності" і пошук ліній подолання розпаду, породженого втратою колишніх орієнтирів.

Щодо зміни природи людини і спрямованості цінностей, які пов'язані зі зміною історичних періодів, переконливо говорив М. Вебер, що прогнозував настання епохи "ціннісного політеїзму" [27]. Проблеми цінностей розглядалися і в дослідженнях Ж. Бодрійяра, де він вибудовував їх за рівнем розвитку суспільства і кваліфікував нинішню епоху як етап дроблення, "дифузії цінностей" [28].

Людина знаходиться в залежності від тих комунікаційних зв'язків, які пов'язують її у соціальну єдність, і які панують у різні періоди системи знань і цінностей. Власне під впливом цих комунікаційних зв'язків формується ідентичність особистості. Як результат узгодженості "людина і зовнішнє середовище" ідентичність сприяє осягненню навколишнього світу, відображаючись у свідомості особистості.

Культурна основа інформаційного суспільства М. Кастельсом розглядається як культура "реальної віртуальності", що здійснюється у мережевому просторі, у спеціальному "кіберпросторі" і "позачасовому часі" [29 – 30]. Реальність даної сфери обумовлюється її повсюдним розширенням, а віртуальність визначається тим, що під впливом мультимедіа в ході формування особистості змінюються її картина світу,

ціннісна система, уявлення про світ, які є стрижневими, більш істотними, аніж вплив живих, навіть найближчих людей.

Упровадження у віртуальну реальність наштовхує до перевороту всієї реальності, яка набуває невластивих їй рис. Спілкування через Інтернет стало звичним явищем, тому люди віддають більшу перевагу мережевому спілкуванню за допомогою комп'ютера, аніж реальному, якщо навіть знаходяться на одній території одного приміщення. Йому ставлять запитання і викладають проблеми, іноді й особистісного характеру. Проте, спілкування з комп'ютером призводить і до серйозних позитивних ефектів, це: безперервна робота з програмами і бажання їх удосконалювати; час від часу оновлення програм зі встановленням їх останніх версій і посилення оперативної пам'яті – все це дає особистості почуття впевненості у своїх якостях "суб'єктності". У такі моменти людина відчуває себе творцем світу, у якому знаходиться, через створювані нею артефакти й програмні продукти. Ці особливості культури, які обумовлюють збільшення значущості окремої особистості, не вбудованої у всілякі спільноти, безпосередньо пов'язані з розвитком інформаційного суспільства. У суспільстві такого типу перетворюється як спрямованість праці та джерела фінансової спроможності, яким стає інформація, так і самі суспільні відносини. У високоіндустріальному суспільстві надіндустріальної культури практично всі процеси формування особистості здійснюються за активною участю інформаційно-комунікаційних технологій. Отже, культура домагається високого ступеня "інноватівності", характеризується демасифікацією і дестандартизацією політико-економічного життя; "персоналізацією" – орієнтацією культури і суспільства на кожну особу, при цьому втрачаються контури "масовізованої особистості", що мешкає в "масовому суспільстві"; трансформацією всього арсеналу засобів міжособистісних відносин, що змінюють усю систему цінностей і спрямованість особистості в бік психологічної, соціальної та етичної цілей.

Тривале спілкування з комп'ютером призводить як до віртуалізації розуму, що є побічним результатом інформатизації, так і до значного підйому значущості індивідуальності. Розробка всіляких програм, їх вдосконалення дає відчуття особистої сили, коли світ відчувається створеним так само, як і наступне мережеве творіння.

Поняття "віртуальна культура" міцно закріпилося у свідомості людей, а Інтернет стрімко увірвався у професійну й побутову сфери їх життя, урізноманітнивши її і зробивши більш інформативною. Вона демонструє нові досягнення і межі нової культури, оригінальним різновидом якої виступає кіберкультура [31]. Віртуальна культура відрізняється від культури як такої, оскільки культура складається з об'єктивних і суб'єктивних факторів і представляється як цілісна система, а віртуальна культура є частиною даної системи, один з видів сучасної культури.

Культура є невід'ємною якістю кожного суспільства на будь-якому рівні його формування. Однак кожна епоха висуває перед нею свої запити і завдання, заохочуючи її подолання утворених розбіжностей. Винятковістю віртуальної культури є заснована з позиції організації мультимедійного гіпертексту віртуальна зона, що представляє собою специфічне об'єднання інформаційних масивів, модулі яких міцно об'єднані один з одним системою взаємозалежних відносин. Через своєрідності просторової будови віртуальної реальності у віртуальній культурі створюється абсолютно оригінальна логіка мислення: нелінійна, асоціативна, позбавлена традиційної логіки, недетерміністська, а іноді й суперечлива. Дані особливості утворюються внаслідок моделювання та утворення абсолютно іншого соціуму, іншого простору, іншої особистості і зовсім іншого часу: багатовимірного, неконкретного, перетворюваного, пізнаваного, різноспрямованого й безмірного.

Існує світ природи, де особистість залежить від об'єктивно сформованих закономірностей, але ще існує світ свободи й культури, там особистість визначає своє розуміння реальності, поведінки і діяльності рівнем духовності, яка об'єднує всі якісні характеристики, а саме: морально-етичні, естетичні, цивілізовані, інтелектуально-комунікативні та інші якісні характеристики. У світі культури особистістю, перш за все, формуються думки про себе і навколишній реальний світ для збереження своєї індивідуальності й відповідності нормам суспільства.

Віртуальна культура представляє оригінальні межі сучасної віртуальної цивілізації, ознаками якої є кіберкультура. Одна з найбільш істотних для сучасної особистості граней віртуальної культури полягає в тому, що вона формує потенціал для безперешкодного пошуку особистістю встановлення своєї ідентичності у мережевому взаємозв'язку, який забезпечує функціонування інформаційного простору.

Створення інформаційних глобальних просторів гостро змінює духовну обстановку сьогоднішнього світоустрою. Для особистості мова, культура, етнічна приналежність не є перешкодою для її самовизначення і вона встановлює свою духовну тотожність з Іншим, за образом цього спільного простору, де вона знаходиться. На цьому місці на передній позиції виступає культурний компонент мережевих зв'язків.

Зміна ідентичностей є закономірним процесом, оскільки вони організовуються соціальними процесами [22]. Дані ідентичності з'являються і формуються при взаємодії індивідуальної свідомості кожної особистості з основними принципами розумової діяльності цілої соціальної конструкції, до чого вона має безпосереднє відношення. Тут особистість звертає увагу на всі зміни суспільства в цілому – допомагає, модифікує і бере участь в ході його реорганізації. Власне молоде покоління можна віднести до наймасовіших учасників течії "хакерів" у сучасному світі, саме вони з наростаючою швидкістю "ховаються" від проблем нещадного і байдужого зовнішнього світу.

Інтернет-середовище є простором мережевої культури, де відбувається реалізація можливостей віртуальних спільнот; воно не може бути територією "загальної рівності" і необмежених можливостей. Пробудження особливих ефектів у деяких особистостей і соціальних груп, що утворюють субкультури, пов'язані з прагненнями переміщення в мережу закономірних принципів реального світу, що, природно не залишиться без відгуку, формує "мережеву ідентичність". Дане поняття характеризує складову соціально-культурної ідентичності.

Мережева ідентичність – наслідок складного пізнавально-емоційного процесу роздроблення особистості, що визначає рівень ідентифікації з "людьми мережі", які мають високий рівень знань, володіють сучасними комп'ютерними технологіями, стильовими і лінгвістичними характеристиками комунікації. Вона ж встановлює і рівень ізольованості особистості від інших членів соціуму, є причиною комунікативної незручності, або, навпаки, основою для комунікації (субкультура "хакерів", "субкультура завзятих інтернетників") [15; 22; 31; 32]. Мережева ідентичність – це певною мірою наслідок формування субкультури хакерів, в її межах вона відкристалізовується.

Мережева ідентичність як складна, публічна і доступна ідентичність дає можливість особистості увійти в мережу, "представляючись" по-своєму, і здійснювати свої задуми не традиційним чином, а згідно із загальновизнаними принципами і нормами у віртуальному просторі. При цьому вона не відмовляється від своєї рідної мови і культури. Отже, можна стверджувати, що "мережева культура" впливає на

формування незвичайного типу особистості, на становлення і дозрівання якого істотно впливають системи мережевих взаємодій.

Основою функціонування Інтернет є принцип мережевої самоорганізації, яка не схожа на звичні всім "системні" закономірності, тобто на структурні принципи взаємодії; на комунікації центру і периферії; "ядерних" схем. Сьогоднішнє комп'ютерне підростаюче покоління виявляє для себе цю територію і вважає, що стоїть на порозі відкриття цілого світу інноваційної культури. Але цей незвичайний віртуальний простір є тільки невеликим фрагментом типізованої культури. Даний світ високих технологій і розумних дій, сконцентрований інформацією і знаннями, не в змозі дати для формування особистості найважливішого – людинолюбства, благородної духовності і соціального досвіду, придбаного культурою повсякденності. З цього випливає, що виховання і формування розумових здібностей дитини повинні починатися не з комп'ютера і електронних і комп'ютерних ігор, а з істинного, традиційного культивування соціальних комунікацій і знань.

Он-лайнові ідентифікаційні відомості виражають соціальну ідентичність, які користувач Інтернет формує в он-лайн спільнотах і веб-сайтах. Мережева ідентичність є однією з систем організації самопрезентації у мережевому просторі. Найчастіше ідентичності зупиняють свій вибір на використанні в он-лайн справжніх імен, іноді віддають перевагу анонімності, використовуючи псевдоніми, що містять ідентифікуючу персональну інформацію.

Таким чином, у культурі інформаційного суспільства, представленій як у реальній, так і у віртуальній реальності, починає лідирувати віртуальна культура. Вона представлена як спільність культурних цінностей і смислів, які формуються в ході абсолютно нового спілкування між індивідами у віртуальному просторі і відображає не тільки дійсність, а й перспективні бажання, які є зручними особистості для їх виконання. Як зазначалося вище, Інтернет-простір дає особистості незалежність у конструюванні власного образу в кіберпросторі і як наслідок – свою ідентичність.

З позиції М. Кастельса, мовний фактор стає підставою безлічі сучасних видів націоналізму, які організовуються за межами державних кордонів і в більшості випадків є більше культурними, аніж політичними, і тому здебільшого орієнтованими виступити на захист уже сформованих традицій культури, аніж на формування і захист держави [28 – 29]. Користувачі глобальної мережі в пошуку необхідної інформації стикаються з необхідністю володіння тією мовою, якою створено потрібний контент. Наприклад, уся свіжа інформація про світові події, сучасні технології доступна в основному англійською мовою. У пошуках потрібних матеріалів, відсутніх рідною мовою, людина для задоволення своїх культурних і інформаційних потреб змушена звертатися до зовнішніх джерел, тобто до закордонних інформаційних потоків. Інтернет є тією сферою, де є можливість знайти всю або майже всю бажану інформацію і мультимедійні джерела.

Постійне звернення до зовнішніх Інтернет-ресурсів у комплексі з вимогами знання іноземної мови відчужують особистість від вітчизняного сегменту глобальної мережі. Постійне звернення до Інтернет-простору несе і свої позитивні моменти: особистість наближається до світового інформаційного і культурного простору, має можливість занурення в "Інше", у якому пізнає відтінки свого "Я" [15, с. 64]. Особливість "комп'ютерної особистості" полягає в тому, що вона дивиться на навколишній світ крізь комп'ютерні та телекомунікаційні системи.

У світовій практиці існує чимало моделей, які можна застосувати для того, щоб врятувати етнокультурну мережеву ідентичність:

- модель ізольованості кіберпростору (дана модель властива Північній Кореї і Китаю). Модель характеризується цензурою, обмеженням доступу, жорстким контролем;

- модель "інтенсивного контенту" характеризується залученням користувачів Інтернет на внутрішні Інтернет-ресурси завдяки створенню високоякісного і затребуваного контенту. Ця модель актуальна для Південної Кореї і Японії;

- переважна модель, характеризується превалюванням певного контенту в глобальній інформаційній зоні. До них відносяться країни Європи і США;

- підпорядкована модель, характеризується потраплянням під вплив країн з домінуючою моделлю і моделлю "інтенсивного контенту". До них відносяться країни з економікою, що розвивається.

Битва за кіберпростір і сферу впливу у всесвітній павутині здійснюється в тому числі і через конкуренцію з формування більш злободенного, рідкісного і бажаного контенту: текстового і мультимедійного. Це боротьба за свідомість споживачів мережі Інтернет, значна частина з них виступають як мережеві космополіти, значить, усі прагнення уряду в сфері національної політики, можливо, виявляться безуспішними без адекватної відповіді на загрози, що йдуть з кіберпростору. По-перше, комп'ютерна особистість має можливість виходу до колосальних масивів інформації і застосовує їх у своїй життєдіяльності; по-друге, вона одержима цією інформацією, впадає в повну залежність від неї, усувається від дійсного зовнішнього світу і тому втрачає здатність до самостійного синтезу і прийняття рішень. У зв'язку з цим, абсолютно логічним є те, що ймовірність здійснення прагнень особистості обумовлюється діяльністю соціальних мереж в інформаційному просторі, там людина знаходить шанс самоідентифікації своєї особистості, відновлення втрачених нею усталених традиційних зв'язків у певній соціальній спільності, в реальному світі.

Мережева ідентичність відрізняється від реально-буденної ідентичності, оскільки відтворює не тільки комплекс символів, які вже є в багажі особистості, а й може формулювати готовність особистості відчувати себе в новій якості. Мережева ідентичність, узагальнюючи реальне і віртуальне середовище, виявляє потенціал для пошуку альтернатив формування суспільства, напрямку на взаємну узгодженість міжособистісних і міжнародних взаємин. У ситуації кризи ідентичності мережевий простір дає можливість для його подолання через пошук інших сторін і, в першу чергу, в царині культурної ідентичності.

Беручи до уваги значні масштаби розвитку комп'ютерних технологій, цілком обґрунтовано припустити, що недалеке майбутнє принесе кардинально нові проблеми і рішення у відносинах "людина – Інтернет". Посилиться вплив культурно-ціннісних спрямувань особистості на самовдосконалення. Крім того, зміниться і вплив мережі Інтернет на ідентичність, причому, важко спрогнозувати спрямованість цього впливу.

Безсумнівним є лиш те, що багато принципів соціально-культурної взаємодії, властиві інформаційному суспільству, особистості доведеться засвоювати в майбутньому досить тривалий час. Усі технології, комунікації, ідентифікації, ранжування ціннісно-смислових систем, формування адаптаційних механізмів до швидких змін зовнішнього середовища стають основними характерними властивостями всієї культури актуального на сьогоднішній день інформаційного суспільства.

Висновки.

Відзначимо, що створення глобального інформаційного простору гостро змінює духовну обстановку сьогоднішнього світоустрою. Головним джерелом розвитку інформаційного суспільства стає інтелектуальний капітал і творчі ідеї особистості, які під впливом інформаційно-комунікаційних технологій набувають інноваційного характеру і

народжують мережеві моделі динамічного поширення знання. У даній ситуації особистість стикається з системою множинності ідентичності. При цьому субкультури, пов'язані з прагненнями переміщення в мережу закономірних принципів реального світу, формують феномен "мережевої ідентичності", на формування і становлення якої суттєво впливають системи мережевих взаємодій.

Багатоваріантність сучасного культурного середовища породжує різноманітні форми для фактично будь-якої самоідентифікації – від вершин творчості власного буття до повної деградації людини. Тому саме від самоідентифікації людини, від того, які саме цінності вона спроможна генерувати у своєму житті залежить її розвиток та самореалізація в сучасному світі.

Поступове впровадження в реальне життя сучасної людини інформаційно-комунікаційних технологій у процесі віртуальної соціалізації сучасної особистості приховує у собі небезпеку модифікації етнокультурної ідентичності. Мережева культура змінює не тільки ціннісні орієнтири, але й наповнює новим комунікативним змістом картину світу, що сприяє появі нового типу особистості, не просто "людини інформаційної" (homo informaticus), а "мережево-інформаційної", яка включена в особливу сферу комунікацій, глобальні й ускладнені соціальні взаємозв'язки.

Використана література

1. Архіпова Є.О., Ковалевська О.В. Критичне мислення як необхідна складова розумової діяльності людини в межах сучасного інформаційного суспільства. *Гуманітарний часопис*. 2012. № 2. С. 34-38.

2. Тоффлер Э. Третья волна / пер. с англ. Москва: Новый мир, 2004. 781 с.

3. Прокопович Л.В. Соціально-філософський аналіз візуалізації культурної ідентичності в "театрі" повсякдення. *Грані*. 2019. Т. 22. № 1. С. 57-67.

4. Ганаба С. "Homo comlexus" як образ людини інформаціонального суспільства. *Наукові записки Національного університету "Острозька академія". Серія: Культурологія*. 2012. Вип. 9. С. 325-329.

5. Автомонова Т.І. Соціальне самовизначення людини в інформаційному суспільстві. *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія.* 2011. № 2. С. 84-88.

6. Дзьобань О.П. До питання про інституціоналізацію комунікаційного простору. *Інформація і право*. № 1(4)/2012. С. 81-89.

7. Дзьобань О.П., Жданенко С.Б. Соціокультурний простір інформаційного суспільства як середовище буття сучасної людини. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2014. № 2 (21). С. 12-21.

8. Дзьобань О.П., Левада О.В. Самоорганізація в соціальному просторі: філософський аспект. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2011. Вип. 8. С. 3-11.

9. Дзьобань О.П. Діалектика глобалізації віртуальної реальності й суспільного розвитку. *Гілея: науковий вісник:* зб. наук. праць. 2012. Вип. 63 (№ 8). С. 254-260.

10. Пьер Бурдьё. Физическое и социальное пространства: проникновение и присвоение. URL: https://gtmarket.ru/laboratory/expertize/3053 (дата звернення 11.09.2020).

11. Бодрийяр Ж.Д. Система вещей. Москва: Рудомино, 1994. 272 с.

12. Булат Е.А., Дырда В.И. Некоторые проблемы взаимосвязи науки, эволюции техносферы и устойчивого развития. *Геотехнічна механіка*. 2019. Вип. 144. С. 31-46.

13. Буравльов Є. Як запобігти небезпечним ситуаціям у техносфері? *Вісник Національної академії наук України*. 2010. № 4. С. 30-40.

14. Алієва О. Погляд на процес формування техносфери крізь призму еволюційної теорії Чарльза Дарвіна. *Схід*. 2014. № 5. С. 91-96.

15. Фандєєва Г.К. Віртосфера – новий простір формування соціальних ідентичностей. *Гілея: науковий вісник:* зб. наук. праць. 2019. Вип. 141 (№ 2). С. 169-173.

16. Алтынкович Е.Е. Динамика культурных ценностей личности в информационном обществе: дис. …канд. филос. наук. Москва, 2016. 184 с.

17. Чуркіна В.Г. Трансформація семіосфери культури в умовах глобальної комунікації. *Вісник Харківської державної академії дизайну і мистецтв.* 2012. № 3. С. 152-155.

18. Козакова О.М. Семіосфера як антропокультурний феномен. *Філософські обрії*. 2013. Вип. 30. С. 126-132.

19. Полулях Ю.Ю. Модерн, Постмодерн, Другий Модерн: варіації семіосфери життєсвіту. *Вісник Луганського національного університету імені Тараса Шевченка. Соціологічні науки.* 2010. № 12. Т. 2 (2). С. 204-212.

20. Лотман Ю.М. О семиосфере. Избранные статьи в 3-х т. Таллин: Александра, 1992. Т. 1. С. 11-24.

21. Dzeban O., Aleksandrova O., Vinnikova N. Axiological portrait of information society. *Схід:* аналітично-інформаційний журнал. 2019. № 5 (163). С. 13-19.

22. Степико М.Т. Українська ідентичність у глобалізованому світі: монографія. Харків: Майдан, 2020. 258 с.

23. Дзьобань О.П., Жданенко С.Б. Соціокультурний простір інформаційного суспільства як середовище буття сучасної людини. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2014. № 2 (21). С. 12-21.

24. Дзьобань О.П., Соснін О.В. Віртуальна реальність суспільства постмодерну як соціокультурне тло соціалізації "людини інформаційної". *Гуманітарний вісник Запорізької державної інженерної академії:* зб. наук. праць. 2017. Випуск 69 (1). С. 69-76.

25. Данильян О.Г., Дзьобань О.П. Людина в інформаційному суспільстві: проблема моральної ідентифікації. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія*. 2019. № 1 (40). С. 8-20.

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

27. Вебер М. Избранное. Образ общества. Москва: Юрист, 1994. 702 с.

28. Бодрийяр Ж.Д. Общество потребления. Москва: Республика, 2006. 272 с.

29. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. под науч. ред. О.И. Шкаратана. Москва: ГУ ВШЭ, 2000. 608 с.

30. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-ФАКТОРИЯ, 2004. 328 с.

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

32. Ганаба С. Ідентичність у мережевому суспільстві: постановка проблеми. *Наукові записки Національного університету "Острозька академія". Серія: Культурологія*. 2016. Вип. 17. С. 304-306.

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

УДК 340:1+347.9

СОЛОНЧУК І.В., старший викладач кафедри інформаційного права та права інтелектуальної власності Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".
ORCID: https://orcid.org/0000-0001-6447-246x.

ІНФОРМАЦІЙНЕ СУДОЧИНСТВО ЯК ЗАКОНОМІРНІСТЬ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Анотація. *У статті розглядаються методологічні проблеми змісту понять "інформаційне суспільство", "інформаційні правовідносини", "інформаційне судочинство". аналізуються висновки наукових розвідок з даної проблематики та обґрунтовуються категорії "інформаційні правовідносини" та "інформаційне судочинство", визначаються тенденції та значення інформаційного судочинства як об'єктивної закономірності інформаційного суспільства, окреслюється коло дискусійних питань сфери судочинства, які ще не врегульовані законодавцем.*

Ключові слова: *інформація, інформаційне суспільство, інформаційні правовідносини, інформаційна діяльність, інформаційне судочинство.*

Summary. *The article is devoted to methodological problems of the concepts "information society", "information legal relations", "information court proceedings", analyzes the conclusions of scientific research on this issue and substantiates the categories of "information law" and "information court proceedings", identifies trends and values of information court proceedings, outlines the range of issues in the field of justice.*

Keywords: *information, information society, information legal relations, information activity, information court proceedings.*

Аннотация. *В статье рассматриваются методологические проблемы содержания понятий "информационное общество", "информационные правоотношения", "информационное судопроизводство", анализируются выводы научных исследований данной проблематики, обосновываются категории "информационные правоотношения" и "информационное судопроизводство", определяются тенденции и значение информационного судопроизводства как объективной закономерности информационного общества, указываются дискуссионные вопросы в судопроизводстве, которые еще юридически не урегулированы.*

Ключевые слова: *информация, информационное общество, информационные правоотношения, информационная деятельность, информационное судопроизводство.*

Постановка проблеми. Інформаційна діяльність й інформація притаманні сучасному суспільству як невід'ємна складова відносин. Особливої уваги вимагають суспільні відносини, які регулюються нормами права та виникають у різноманітних сферах діяльності. Темпи розвитку інформаційних технологій та переваги щодо передачі, обробки та збереження інформації, що надають ці технології, вимагають від законодавця своєчасного реагування і, як наслідок, розроблення дієвих механізмів регулювання та захисту прав та обов'язків учасників інформаційних правовідносин.

Епоха інформаційного суспільства – нова стадія розвитку людства, започаткована в другій половині XX сторіччя [1, с. 76]. Як зазначає Згуровський М.З., Інтернет-технології та інтелектуальні комп'ютерні системи відкрили захоплюючі перспективи для прийдешніх поколінь, оскільки надають доступ до глобальних знань, які перебувають

поза межами локальних й споконвічних контекстів, характеризуються розмаїттям джерел та базуються на глобальній інформаційній інфраструктурі [2].

Прискорені автоматизація, роботизація і комп'ютеризація спричинили корінні зміни соціально-економічних структур, а також відбувся перехід працівників в інформаційну галузь діяльності й в сферу послуг. Сьогодні в суспільстві інформаційному економіка, політика та культура залежать від створення, збереження і доступності інформації не тільки в національному, але і в світовому масштабах [1, с. 77] .

В науковому обігу термін "інформаційне суспільство" використовується вже понад 50 років, проте до сьогодні ще не вироблено уніфікованого розуміння даного поняття, що, в свою чергу, становить методологічну проблему, адже така неоднозначність трактування породжує термінологію, яка не має достатнього наукового підґрунтя і, зокрема, застосовується в сфері судочинства.

Результати аналізу наукових публікацій. Вивчення природи інформаційного суспільства вимагає комплексного підходу, тому наукові дослідження даного питання виконуються в різних напрямах, зокрема з позицій філософії, соціології, політології, економіки та юриспруденції. Останніми роками спостерігаємо підвищений науковий інтерес до поняття інформаційного суспільства, закономірностей та перспектив його розвитку. Дослідженню інформаційного суспільства приділяли увагу Арістова О.В., Баранов О.А., Боер В.М., Брижко В.М., Бордюгова Т.Г., Виноградова Г.В., Даніл`ян В.О., Данько Ю.А., Згуровський М.З., Кізляр В.Б., Коваленко Л.П., Копилов В.А., Кормич Б.А., Кохановська О.В., Маріц Д.О., Ліпкан В.А., Павельєва О.Г., Пилипчук В.Г., Скалацький В.М., Сидоренко О.П., Синєокий О.В., Тарасенко Р.В., Фурашев В.М., Штанько В.І.та інші шановні вчені.

Окремо заслуговують на увагу розвідки застосування електронних засобів у судочинстві таких науковців: Білоус В.В., Бринцев О.В., Ємельянов С.В., Заплотинський Б.А., Квасневська Н.Д., Клюцевський В.І., Кушакова-Костицька Н.В., Логинова Н.М., Пчелін В.Б., Сердюк І.В., Сердюк Л.Р., Середницька І.А., Ульяник М.М., Якутко В.Ф..

Проте на сьогодні відсутні комплексні дослідження інформаційних відносин у контексті інформаційного судочинства. Тому, як вважаємо, правове регулювання судочинства в інформаційному суспільстві, а також механізми забезпечення права на інформацію при зверненні до суду, потребують подальшого наукового опрацювання.

Матеріал статті є продовженням попередніх розвідок, присвячених особливостям судочинства в інформаційному суспільстві [3 – 7]. Її емпіричною базою є міжнародні та національні нормативно-правові акти. Заслуговують окремої уваги Міжнародні стандарти правосуддя, зокрема інформаційному забезпеченню судочинства присвячені Висновок № 14 (2011) Консультативної ради європейських суддів "Судочинство та інформаційні технології", прийнятий на дванадцятому пленарному засіданні у Страсбурзі 7 – 9 листопада 2011 р. [8] та Рекомендація № R (81) 7 Комітету Міністрів Ради Європи державам-членам щодо заходів, що полегшують доступ до правосуддя, ухвалена Комітетом Міністрів Ради Європи на 68 засіданні заступників міністрів 14 травня 1981 року [9].

Метою статті є оцінка наукових підходів до розуміння інформаційного суспільства, обґрунтування понять "інформаційні правовідносини" та "інформаційне судочинство", представлення пропозиції щодо удосконалення судочинства в інформаційній сфері.

Виклад основного матеріалу. Відповідно до ст. 3 Закону України "Про інформацію", одним із напрямів державної інформаційної політики України є створення умов для формування інформаційного суспільства [10]. Можемо зробити висновок, що даною

правовою нормою законодавець акцентує увагу на значенні інформаційного суспільства та чітко окреслює пріоритетний напрямок державної діяльності щодо його розбудови. Наукова думка останніх років приділяє все більше уваги інформаційному суспільству: поняттю, етапам формування, ознакам, властивостям, принципам тощо. Сьогодні інформаційне суспільство дедалі активніше досліджується в наукових працях, адже в сучасному розумінні це вже не абстрактне явище, а наше сьогодення. Коли в 60-х рр. XX ст. американський економіст Фріц Махлуп використав термін "інформаційне суспільство", він говорив не про юриспруденцію, а досліджував інформаційний сектор економіки на прикладі США [11, с. 140]. У 1961 р. японський журналіст Тадао Умесао застосував даний термін під час розмови з архітектором Кисьо Курокавою, а пізніше відобразив у статті "Теорія інформаційної індустрії", де представлене дослідження теорії еволюції, що ґрунтується на перетворенні інформації [12, с. 129]. Але слід зазначити, що з того часу термін "інформаційне суспільство" зазнав трансформації щодо розширення сфери використання у різноманітних галузях життєдіяльності людини. Японський вчений Кохіяма Кенічі у праці "Введення в теорію інформаційного суспільства" (1968 р.) звернув увагу на виникнення телематичного суспільства, тобто суспільства ери інформації. Пізніше японський професор Хаяші Юдзіро у дослідженні "Інформаційне суспільство: від індустріального суспільства до інтелектуального" (1969 р.) пов'язав перехід суспільних відносин до інформаційного суспільства зі збільшенням об'ємів інформації та її обміном за посередництвом інформаційних технологій [12, с. 129-131]. Вагоме місце в обґрунтуванні категорії "інформаційне суспільство" посідають праці відомого японського вченого, директора Інституту інформаційного суспільства Йонезі Масуди, який є родоначальником однієї з концепцій інформаційного права. В роботі "Інформаційне суспільство як постіндустріальне" Масуда ще у 1983 році стверджував, що основою суспільства майбутнього будуть комп'ютерні технології з їх функцією підсилення інтелектуальної праці. На думку Масуди інформаційно-комп'ютерна техніка та технології швидко перетворюватимуться на нову виробничу силу та зроблять можливим масове виробництво когнітивної, систематизованої інформації, технології і знань, а провідною галуззю економіки стане інтелектуальне виробництво, продукція якого накопичуватиметься й розповсюджуватиметься через синергетичне виробництво та дольове використання [13, с. 14].

Суспільство XXI сторіччя сміливо можемо називати інформаційним, адже завдяки технічному прогресу широко використовуються інформаційні технології у всіх сферах життєдіяльності людини. Інформаційне суспільство часто називають суспільством нового типу, що сформувалося внаслідок переходу від індустріального до інформаційного устрою. Колодюк А.В. характеризує інформаційне суспільство як сучасний стан розвитку, який базується на цивілізаційних здобутках: новітніх соціальних, політичних, технологічних та інформаційних передумовах [14, с. 4]. Завдяки активним дослідженням інформаційного суспільства як явища, сформувалися різні підходи до його розуміння. У загальному розумінні інформаційне суспільство визначається як таке, що має розвинуту індустрію інформаційних технологій, високий рівень інформаційної культури, в якому більшість працівників зайняті виробництвом, збереженням, опрацюванням і реалізацією інформації і, особливо, знань як вищої її форми [15, с. 151]. Даніл'ян В.О. пропонує, з позиції соціально-філософського аналізу, розглядати інформаційне суспільство як якісно новий етап соціотехнологічної еволюції суспільства, що формується в результаті довгострокових тенденцій попереднього соціально-економічного розвитку, який передбачає збільшення ролі інформації, знань та формування, споживання інформаційних ресурсів у всіх системах життєдіяльності суспільства за допомогою розвитку

інформаційно-комунікаційних технологій, які існують у глобальних масштабах [16, с. 22]. Арістова І.В. розглядає поняття інформаційного суспільства як суспільства нового типу, що формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвертацією інформаційних та комунікаційних технологій [17, с. 89]. Цю позицію підтримує Ліпкан В.А. і також характеризує інформаційне суспільство як суспільство нового типу, що формується внаслідок глобальної соціальної революції [18, с. 102]. За висловом Данька Ю.А., інформаційне суспільство – це соціальна й футурологічна концепція, де основним фактором суспільного розвитку є виробництво й використання науково-технічної та іншої інформації; це одна з теоретичних моделей, що використовуються для опису якісно нового етапу суспільного розвитку, в який вступили розвинені країни з початком інформаційно-комп'ютерної революції, а технологічною основою суспільства стають не індустріальні, а інформаційно-комунікаційні технології [1, с. 79]. Баранов О.А.визначає інформаційне суспільство як таке, в якому вся сукупність суспільних відносин з метою підвищення ефективності людської діяльності в різних сферах (політиці, економіці, публічному управлінні, військовій справі, освіті, культурі, розвагах, особистому житті тощо) реалізується на основі максимального використання інформаційних комп'ютерних технологій [19, с. 33]. Неоднозначність наукової думки щодо поняття інформаційного суспільства можемо пояснити еволюцією інформаційного права, а також стрімким розвитком інформаційних технологій, які передають, обробляють або ж зберігають інформацію.

Сучасні відносини, безумовно, мають інформаційне забарвлення. Виник новий напрям життєдіяльності суспільства – інформаційна діяльність, основними видами якої є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації [10]. Як слушно наголошує Кізляр В.Б., сьогодні інформаційна діяльність поширюється на всі сфери суспільної діяльності: політичну, економічну, соціальну, науково-технічну, міжнародну тощо. Водночас, інформаційна діяльність присутня і в тих сферах, які виникли внаслідок даної діяльності, а саме у сфері інформаційних технологій та у кіберсфері [20, с. 114]. Важко уявити відносини, які не породжують інформацію, в яких не присутня інформація чи взагалі не стосуються інформації. А тому значення інформації важко переоцінити, адже вона становить сутність життєдіяльності суспільства. Отже, вироблення єдиного поняття даної категорії є надзвичайно важливим для ефективного регулювання інформаційної діяльності.

За статтею 1 Закону України "Про інформацію", інформацією є будь-які відомості, дані, які відповідають одному із двох критеріїв: 1) можуть зберігатися на матеріальних носіях; 2) є відображеними в електронному вигляді [10].

У ч. 1 ст. 1 Закону України "Про телекомунікації" спостерігаємо більш просторове розуміння інформації, до якої відносять відомості, які подаються у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [21].

Як вже зазначалося в попередніх дослідженнях, наразі існує складність щодо єдності розуміння терміну "інформація", що спричиняє використання даного терміну в різних значеннях [4, с. 28-29]. Пилипчук В.Г. стверджує, що інформація є ключовою складовою інформаційного суспільства та світового інформаційного простору, а тому відсутність єдності в розумінні сутності інформації становить системну проблему [22, с. 17]. Зважаючи на стрімкий розвиток інформаційного суспільства, активізацію інформаційної діяльності в життєдіяльності суспільства, особливого значення набуває нормативне закріплення поняття інформації як юридичної категорії з метою уніфікації розрізнених визначень, які спостерігаємо в сучасних нормативно-правових актах України.

Відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації (інформаційні відносини) регулюються державою. Оскільки дані відносини врегульовані юридично, то, на наш погляд, є доцільним використання в даному контексті терміну "інформаційні правовідносини". На підставі раніше виконаного наукового дослідження пропонуємо узагальнене визначення інформаційних правовідносин як суспільних відносин, що врегульовані нормами права, які виникають між різними суб'єктами щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та охороняються державою від порушень [4, с. 35].

Державна інформаційна політика є структурованою та охоплює чітко визначені напрями: 1) забезпечення кожному доступу до інформації; 2) забезпечення кожному рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; 3) створення умов для формування в Україні інформаційного суспільства; 4) забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; 5) створення інформаційних систем і мереж інформації, розвиток електронного урядування; 6) постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; 7) забезпечення інформаційної безпеки України; 8) сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору. Право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів, є правом кожного. Держава встановлює гарантії забезпечення права на інформацію, створенням механізму реалізації права на інформацію, до яких належать: 1) створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів; 2) обов'язок суб'єкта владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення; 3) обов'язок суб'єкта владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації; 4) здійсненням державного і громадського контролю за додержанням законодавства про інформацію; 5) встановленням відповідальності за порушення законодавства про інформацію. Водночас, законодавець вимагає, щоб реалізація права на інформацію не порушувала громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. До того ж, нормативно закріплена можливість обмеження права на інформацію, але виключно законом та з наступних підстав: 1) в інтересах національної безпеки, територіальної цілісності або громадського порядку; 2) з метою запобігання заворушенням чи кримінальним правопорушенням; 3) для охорони здоров'я населення; 4) для захисту репутації або прав інших людей; 5) для запобігання розголошенню інформації, одержаної конфіденційно; 6) для підтримання авторитету і неупередженості правосуддя [10].

Серед ознак інформаційного суспільства Бринцев О.В. називає переведення максимальної кількості комунікацій звичайної життєдіяльності людини в електронну, інформаційну форму. Однією із таких сфер, де спостерігаємо вказані переведення, є судочинство [23, с. 4]. Як вже зазначалося у попередніх дослідженнях, застосування інформаційних комп'ютерних технологій при здійсненні правосуддя надає можливість підвищити його ефективність, впорядкувати організацію органів судової влади та покращити комунікаційні процеси між судами, учасниками справи та державними інституціями [5, с. 248]. Зважаючи на надшвидкісні темпи інтеграції інформаційних

правовідносин у всі сфери життєдіяльності людини та суспільства, виконавши дослідження, узагальнення та аналіз наукових публікацій, присвячених інформаційним правовідносинам в судочинстві, маємо намір окреслити коло певних проблем, які потребують методологічного розроблення та нормативного закріплення з метою врегулювання суспільних відносин.

В даному контексті видається слушною думка Баранова О.А.. який вважає, що певна неоднозначність щодо визначення дефініції "інформаційне суспільство", яка все ще існує на сьогодні, спровокувала поширення низки недостатньо обґрунтованих термінів (зокрема, терміну "електронний суд"). В цьому аспекті виникає нагальна потреба у подальшому чіткому визначенні основоположних понять, якими оперують дослідники [19, с. 32].

Оскільки інформаційна діяльність є предметом регулювання різних галузей права, в даному дослідженні, ґрунтуючись на узагальненні наукової думки, хочемо звернути увагу на методологічну невизначеність термінології в сфері судочинства. Останнім часом спостерігаємо широке використання терміну "електронний суд". В зазначеному дослідженні представлена спроба, не претендуючи на однозначність, окреслити проблему доцільності використання даного терміну в інформаційній діяльності у сфері судочинства.

Кушакова-Костицька Н.В. говорить про новий варіант правосуддя – "електронне правосуддя", яке виникає внаслідок подальшого розвитку сучасної техногенної цивілізації, зокрема, у формі інформаційного суспільства. Електронне правосуддя – це правосуддя майбутнього, яке функціонуватиме на базі інформаційних технологій, але вже сьогодні існує автоматизація певних судових процедур, спрощення інформування зацікавлених осіб через інтернет, засоби мобільного зв'язку тощо. Система електронного судочинства як один з елементів електронного урядування, що розглядається як спосіб організації державної влади за допомогою інформаційних мереж з метою забезпечення функціонування органів влади в режимі реального часу та максимального спрощення і доступності щоденного спілкування з ними громадян, юридичних осіб, неурядових організацій. У даному контексті електронне судочинство автор визначає як використання у судочинстві сучасних інформаційних технологій. [24, с. 104]. Клюцевський В.І. говорить про електронне судочинство та електронну систему судочинства [25]. Середницька І.А. та Ульяник М.М. досліджують "віртуальне судочинство", ототожнюючи дане поняття з поняттям "електронне судочинство" [26, с. 66]. Сердюк Л.Р. наголошує на електронному форматуванні судочинства, яке, порівняно із традиційним, матиме ряд очевидних переваг: покращить гарантії доступу до правосуддя, забезпечить швидкість розгляду судами справ, сприятиме якості судових рішень, забезпечить контроль сторін за розглядом справи та економію судових витрат, посилить змагальність і публічність судових процесів тощо [27, с. 129]. Більшість наукових досліджень з цього питання вивчають можливості застосування та значення для правосуддя інформаційно-комунікаційних досягнень науки та техніки.

На наш погляд, на сьогодні доцільно розглядати інформаційні правовідносини в судочинстві в ширшому контексті, адже складну процедуру формування судів, діяльності суддів та здійснення правосуддя не можна зводити лише до використання електронних технологій. Комітет Міністрів Ради Європи у Додатку до Рекомендації R (81) 7 серед принципів, яких рекомендовано додержувати державам-членам у сфері правосуддя, називає захід, який полегшує доступ до правосуддя – інформування громадськості, що передбачає надання громадськості інформації про місцезнаходження і компетенцію судів, про порядок звернення до суду, про процедуру захисту своїх інтересів у судовому порядку. Інформація

загального характеру має бути одержана або безпосередньо в судах, або в іншій компетентній службі чи органі. До інформації загального характеру відноситься: 1) процесуальні норми (за умови, що така інформація не містить юридичних порад по суті справи); 2) порядок звернення до суду та строки, впродовж яких таке звернення є можливим, а також процесуальні вимоги й необхідні в зв'язку із цим документи; 3) засоби виконання рішення суду та, за можливості, про супутні його виконанню витрати [8]. Враховуючи ці положення, на наше переконання сьогодні слід говорити про інформаційне судочинство як якісно новий етап судочинства, який охоплює всі інформаційні відносини у сфері судочинства, зокрема як такі, об'єктом яких є інформація, так і ті, які містять чи породжують інформацію. У попередній розвідці запропоновано в поняття "інформаційне судочинство" включати весь комплекс процесуальних дій, а саме подання заяв, скарг учасниками процесуальних дій, прийняття ними рішень, перегляд рішень судами, порядок виявлення, розслідування злочинів, передання матеріалів кримінальних справ до суду тощо, пов'язаних з порядком розгляду та вирішення судом справ щодо спорів, які виникають з інформаційних правовідносин та правовідносин, обумовлених процесами забезпечення обороту інформації [5, с. 249].

Отже, вважаємо оперування терміном "електронний суд" не виправданим, адже в судочинстві важливим чинником, який забезпечує досягнення мети правосуддя, є людський фактор, а саме – суддя як головний учасник судового процесу. Згідно з Міжнародним стандартам правосуддя, судочинство не повинно сприйматися користувачами як суто технічний процес, без його фундаментальної функції, а тому здійснення правосуддя не може бути повністю автоматизованим і є неможливим без участі людини. Судочинство має включати людський фактор, що і становить складову роботи судді, оскільки мова йде про реальних людей та про вирішення їхніх спорів, адже в оцінці поведінки сторін та їх свідків в судовому засіданні найвагоміше значення має саме людський фактор [9]. Саме тому, на наше переконання, в даному контексті доцільно говорити про інформаційне судочинство, в якому є місце і електронним технологіям, і людському фактору.

Висновки.

Підводячи підсумки, зазначимо, що в правовій державі, якою згідно з Конституцією України є наша держава, право на інформацію має бути забезпечене в усіх сферах, а сфера судочинства не може бути виключенням. Кожному при зверненні до суду в порядку статті 55 Конституції України гарантується реалізація права на інформацію [28].

При розгляді та вирішенні справи в суді мають місце інформаційні правовідносини, при чому у будь-якому випадку, а не тільки тоді, коли предметом судового розгляду є інформація. Нормативне врегулювання прав та обов'язків учасників судового процесу, безперечно, має бути. Тому, на наш погляд, доцільно оперувати терміном "інформаційні правовідносини", що позначатиме закріплення на законодавчому рівні прав та обов'язків учасників цих відносин, а отже, існуватиме можливість застосування заходів державного примусу у випадку невиконання обов'язків чи порушення прав.

Враховуючи стрімкий розвиток інформаційного суспільства, на наше переконання, на сучасному етапі розвитку суспільних відносин, вже слід говорити про інформаційне судочинство як якісно новий етап судового реформування, що передбачає комплексний підхід науковців різних галузей знань. Як слушно зауважує М.З. Згуровський, одним із характерних явищ, притаманних сучасному суспільству, є "інформаційний вибух", що постійно наростає. Сучасні бази даних, бази знань у різних розділах науки є гігантськими "сховищами" для нескінченних фактів та базових істин, а глобальні

комп'ютерні мережі стали потужним інструментом для високошвидкісного доступу до них з будь-якого куточку світу [2]. Якщо законодавець не враховуватиме темпи розвитку інформаційних технологій та їх можливості, реформування судової системи України ризикує стати "хронічним" процесом без досягнення очікуваних позитивних результатів.

Використана література

1. Данько Ю.А. Теорії інформаційного суспільства в сучасному науковому дискурсі. *Сучасне суспільство*. 2013. Вип. 1. С. 76-84.

2. Згуровський М.З. Шлях до інформаційного суспільства – від Женеви і Тунісу. *ZN.UA*. 2005. № 34. 2 – 9 верес. URL: https://zn.ua/ukr/EDUCATION/shlyah_do_informatsiynogo _suspilstva _ id_ zhenevi_do_tunisu.html (дата звернення: 19.08.2020).

3. Солончук І.В. Інформаційні правовідносини в контексті цивільного судочинства. *Інформація і право.* № 1(24)/2018. С. 164-173.

4. Солончук І.В. Інформаційні правовідносини: поняття та охорона. *Інформація і право*. № 4(31)/2019. С. 28-36.

5. Фурашев В.М., Солончук І.В. Інформаційне право: інформаційне судочинство. *Право та державне управління.* 2019. № 3 (36). Том 1. С. 241-251.

6. Фурашев В.М., Солончук І.В. Інформаційні правовідносини в судочинстві України у сучасності. *Інформація і право.* № 3(30)/2019. С. 55-64.

7. Солончук І.В. Інформаційне судочинство як елемент державної інформаційної політики та її складової – інформаційної безпеки: мат. І міжнарод. наук.-практич. конференції *Інформаційна безпека: сучасний стан, проблеми та перспективи,* м. Київ, 20 верес. 2019 р. Київ: КПІ імені Ігоря Сікорського, 2019. С. 20-23.

8. Щодо заходів, що полегшують доступ до правосуддя: Рекомендації № R (81) 7 Комітету Міністрів Ради Європи державам-членам, ухвалений Комітетом Міністрів Ради Європи на 68 засіданні заступників міністрів 14 травня 1981 року. – (Міжнародний стандарт судочинства). URL: https://court.gov.ua/userfiles/08.pdf (дата звернення: 18.08.2020).

9. Судочинство та інформаційні технології: Висновок № 14 (2011) Консультативної ради європейських суддів, прийнятий КРЄС на 12-ому пленарному засіданні (Страсбург, 7 – 9 листопада 2011 року). – (Міжнародний стандарт судочинства). URL: http://court.gov.ua/inshe/mss (дата звернення: 18.08.2020).

10. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

11. Кушакова-Костицька Н.В., Сердюк І.В. Інформаційне суспільство: сутність та основні концептуальні підходи. *Філософські та методологічні проблеми права*. 2016. № 1. С. 139-153.

12. Япония: 2008. Москва: Аиро-XXI, 2008. 312 с.

13. Штанько В.І., Бордюгова Т.Г. Інформаційне суспільство: соціально філософські проблеми становлення: навч. посібник. Харків: ХНУРЕ, 2012. 172 с.

14. Колодюк А.В. Інформаційне суспільство: сучасний стан та перспективи розвитку в Україні: автореф. дис. на здобуття наук. ступеня к-та політ. наук: 23.00.03. НАН України. Ін-т держави і права ім. В.М.Корецького. Київ, 2005. 20 с.

15. Информатизация: понятийный словарь терминов и аббревиатур / под ред. Л.С. Винарика, М.И. Крулькевича. Донецк: ИЭП НАН Украины, 2006. 208 с.

16. Даніл`ян В.О. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз): монографія. Харків: Право, 2008. 184 с.

17. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / за заг. ред. О.М. Бандурки: монографія. Харків: Ун-т внутрішніх справ, 2000. 368 с.

18. Ліпкан В.А., Залізняк В.А. Систематизація інформаційного законодавства України: монографія / за заг. ред. В.А. Ліпкана. Київ: ФОП О. С. Ліпкан, 2012. 304 с.

19. Баранов О.А. Правові проблеми “електронної демократії”. *Інформація і право*. № 1(20)/2017. С. 28-38.

20. Кізляр В.Б. До питання визначення змісту поняття “інформаційні відносини”. *Університетські наукові записки*. 2019. № 69-70. С. 114-123.

21. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

22. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері. *Вісник Академії правових наук України*. 2011. № 3. С. 16-27.

23. Бринцев О.В. “Електронний суд” в Україні. Досвід та перспективи: монографія. Харків: Право, 2016. 72 с.

24. Кушакова-Костицька Н.В. Електронне правосуддя: українські реалії та зарубіжний досвід. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 103-109.

25. Клюцевський В.І. Електронне судочинство: шляхи впровадження та зарубіжний досвід. *Теорія та практика державного управління і місцевого самоврядування*. 2020. № 1. URL: http://el-zbirn-du.at.ua/2020_1/16.pdf (дата звернення: 17.08.2020).

26. Середницька І.А., Ульяник М.М. Право на суд у “розумні строки” або віртуальне судочинство: майбутнє чи реалії сьогодення? *Південноукраїнський правничий часопис*. 2014. № 2. С. 66-68.

27. Сердюк Л.Р. Електронне судочинство через призму верховенства права: окремі питання теорії й практики. *Науковий вісник Херсонського державного університету*. *Сер. Юридичні науки.* 2016. Вип. 1(4). С. 126-129.

28. Конституція України: Закон України від 28.06.6 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

29. Брижко В.М. Основи систематизації інформаційного законодавства: теоретичні та правові засади: монографія. Київ: ТОВ “ПанТот”, 2012 р. 304 с.

30. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДІІП НАПрН України). Київ: Видавничий дім “АртЕК”, 2020. 288 с.

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

Інформаційна і національна безпека

УДК 343.14:004

СВІНЦИЦЬКИЙ А.В., директор Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
СТЕПАНОВ В.А., *кандидат технічних наук,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,* головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ЩОДО ТЕРМІНОЛОГІЇ У СФЕРІ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ЗНЯТТЯ ІНФОРМАЦІЇ З КАНАЛІВ ЗВ'ЯЗКУ ТА ІНШИХ ТЕХНІЧНИХ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Анотація. *Стаття присвячена аналізу проблем термінології у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації.*

Ключові слова: *спеціальні технічні засоби для зняття інформації з каналів зв'язку, інші технічні засоби негласного отримання інформації, технічна забезпеченість, придатність, скритний спосіб.*

Summary. *The article is devoted to the analysis of problems in terminology in the field of special technical means for interception of the information from communication channels and other technical means for surreptitious obtaining of information.*

Keywords: *special technical means for interception of the information from communication channels, other technical means for surreptitious obtaining of information, technical support, aptitude, covert way.*

Аннотация. *Статья посвящена анализу проблем терминологии в области специальных технических средств для снятия информации с каналов связи и других технических средств негласного получения информации.*

Ключові слова: *специальные технические средства для снятия информации с каналов связи, другие технические средства негласного получения информации, техническая обеспеченность, пригодность, скрытный способ.*

Постановка проблеми. Конституцією України кожному громадянину гарантується захист від втручання у приватне життя та таємницю приватного спілкування. Тимчасове обмеження цього права, різновидом якого є право на територіальну, комунікаційну та інформаційну приватність [1, с. 303], допускається в разі застосування спеціальних технічних засобів для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації (далі – СТЗ) на підставах і за умови, визначених законодавством, і лише в інтересах національної безпеки, економічного добробуту та захисту людини.

Застосування зазначених засобів дозволяється тільки відповідним оперативним підрозділам уповноважених органів під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій. Законодавство визначає межі, особливості ринку [2], обігу СТЗ [3],

а також повноваження з технічного регулювання у сфері СТЗ [4]. Належність продукції (виробів) до СТЗ визначає Служба безпеки України за результатами проведення судових експертиз і експертних досліджень та/або оцінки супутніх до неї відомостей.

Термін СТЗ не має свого визначення в законі. Основними формулюваннями, що "представляють" продукцію (вироби), яка застосовується для негласного отримання інформації у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій, є:

1) "спеціальні технічні засоби" [5];
2) "спеціальна техніка" [6];
3) "технічні засоби" [7];
4) "оперативно-технічні засоби" [8; 9];
5) "спеціальні технічні засоби негласного отримання інформації" [10 – 12];
6) "спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації " [2 – 4, 13 – 15].

Необхідно зазначити, що така багатоманітність формулювань СТЗ є одним із недоліків законодавства України, який призводить до помилкових висновків про віднесення продукції побутового та відомчого промислового призначення до СТЗ і техніки подвійного використання, наслідком якого, на думку окремих народних депутатів і журналістів, є: демотивація технічно освіченої частини населення професійно займатися в Україні наукомісткими технічними розробками; уповільнення розвитку інформаційно-комунікаційних технологій; плутанина під час підготовки нових та внесення змін в існуючі нормативно-правові акти та нормативні документи.

Результати аналізу наукових публікацій. Дослідженням проблемних питань у сфері СТЗ займалися такі науковці, як Бєгишев І. [16], Галстян Г. [8], Допілка В. [10], Логінов І. [17], Пасєка О. [11], Петрочєнков С. [18], Черних А. [19] та інші.

Праці зазначених науковців, безсумнівно, є вагомим внеском в дослідження зазначеної проблеми. Однак її розв'язання залишається досі не завершеним, а одержані наукові результати потребують поглибленого осмислення та узагальнення науковцями як технічного, так і гуманітарного напрямку, у тому числі юридичного.

Метою статті є удосконалення на базі аналізу чинного законодавства термінології у сфері спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації.

Виклад основного матеріалу. Роздуми щодо застосування саме такої термінології у сфері СТЗ виникли не випадково. Постановою Кабінету Міністрів України "Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації" від 22.09.16 р. № 669 визначено види СТЗ [2].

Окремим видом СТЗ є технічні засоби для зняття інформації з каналів зв'язку (транспортних телекомунікаційних мереж). Слід зауважити, що цей вид СТЗ згадується в актах Європейського Союзу, а саме: в резолюції Ради Європи ЄС COM 96/C329/01 "Про законне перехоплення телекомунікацій" [20] та ENFOPOL 55 "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг зв'язку" [21], Директиві Європейського Парламенту та Ради 2006/24/ЄС "Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку" [22]. З метою реалізації цих актів в Європейському інституті телекомунікаційних стандартів – ETSI створено та працює технічний комітет "Lawful Interception" зі стандартизації технічних засобів

законного перехоплення інформації з телекомунікаційних мереж.

Тому згадування в назві терміну СТЗ його окремого виду – технічних засобів для зняття інформації з каналів зв'язку – є логічно обґрунтованим й таким, що відповідає європейським стандартам. Саме це зумовлює застосування зазначеної вище назви терміну СТЗ.

Зміст продукції (виробів), яка застосовується для негласного отримання інформації у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій, має відображати її унікальні ознаки та особливості функціональних можливостей з метою її відмежування від:

продукції побутового, у тому числі прикладного та відомчого промислового призначення, у визначенні якої згадуються терміни "спеціальні технічні засоби", "спеціальна техніка", "технічні засоби";

продукції, яка охоплюється терміном "оперативно-технічні засоби", яка застосовується у широкому контексті в оперативно-розшуковій діяльності та гласних слідчих (розшукових) діях;

продукції побутового, у тому числі прикладного та відомчого промислового призначення, у визначенні якої згадується термін "спеціальні технічні засоби негласного отримання інформації", яка застосовується для отримання контрольної інформації щодо окремих технологічних процесів без відома операторів цієї інформації та сторонніх осіб;

виробів, які охоплюються терміном "технічні засоби розвідки" та застосовуються в розвідувальній діяльності;

продукції, яка охоплюється терміном "військова та спеціальна техніка" та застосовується у військовій справі.

Вбачається, що СТЗ є найбільш відповідним та змістовним терміном для позначення продукції (виробів), яка застосовується для негласного отримання інформації у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій.

СТЗ характеризується такими ознаками, як "доступ до інформації" "негласне отримання інформації", "конструктивні особливості", "параметри", "придатність", "скритний спосіб", "технічна забезпеченість", "технічні характеристики", "функціональні можливості", частина яких відтворена у визначенні терміну СТЗ, яке міститься у Постанові Кабінету Міністрів України "Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації" від 22.09.16 р. № 669 [2]. В цьому акті під терміном СТЗ розуміють "технічні, апаратно-програмні, програмні та інші засоби, які відповідають критеріям належності технічних засобів негласного отримання інформації, що мають технічну забезпеченість для негласного отримання (прийому, обробки, реєстрації та/або передачі) інформації, призначені для використання у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності".

Вважаємо, що наведене визначення СТЗ потребує удосконалення з урахуванням нижче означеного:

1) обладнання, інструменти та препарати, що відносяться до СТЗ, взагалі не згадані у визначенні цього терміну. Відкритим для обговорення залишається питання віднесення спеціалізованого обладнання випробування СТЗ, у тому числі імітаторів технологічних процесів формування та передачі інформації, до категорії СТЗ;

2) частина продукції (виробів), яка на даний час належить до СТЗ за ознаками технічної забезпеченості, з початку створення не мала призначеності на використання для

негласного отримання інформації у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності, а розроблялася з іншою метою (безпосередньою обумовленістю їх застосування). Тому у вказаному визначенні СТЗ слово "призначені" слід замінити словом "придатні";

3) функціональні можливості частини СТЗ спрямовані не на отримання інформації, а на забезпечення доступу до неї;

4) з лінгвістичної точки зору, невдалим у визначенні СТЗ є фразеологічний зворот "у спосіб, характерний для …діяльності";

5) запропоноване визначення не містить згадки про те, що СТЗ застосовують також при проведенні негласних слідчих (розшукових) дій.

Потребує удосконалення й визначення "спеціальні технічні засоби", яке міститься у наказі Служби безпеки України "Про затвердження Зводу відомостей, що становлять державну таємницю" від 12.08.05 р. № 440 [12]. Під цими засобами розуміються технічні засоби, устаткування, апаратура, прилади, пристрої, програмне забезпечення, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації. По-перше, за межами дефініції залишилися такі ознаки віднесення продукції (виробів) до СТЗ, як "придатність" та "технічна забезпеченість". По-друге, "негласне отримання інформації" не охоплює за змістом "отримання доступу до інформації", що є невід'ємною характеристикою частини СТЗ. По-третє, відсутність ознаки "у скритний спосіб" у процесі негласного отримання інформації значно ускладнює ідентифікацію СТЗ.

У спеціальній літературі також немає єдності поглядів щодо визначення терміну СТЗ. Незважаючи на важливість цього терміну, в багатьох наукових працях воно дається неповно або суперечливо.

Наприклад, Бєгишев І.розуміє під СТЗ програмний або апаратний прилад, який створений або призначений виключно для перехоплення, обробки та аналізу інформації [16, с. 4]. У цьому визначенні підкреслено лише технічні види приладів, але не відображено суті поняття СТЗ. По-перше, "перехоплення, обробка та аналіз інформації" значно звужує зміст ознаки "отримання інформації", що не є виправданим. По-друге, за межами дефініції залишилися такі ознаки віднесення продукції (виробів) до СТЗ, як "придатність" та "технічна забезпеченість". По-третє, потребує уточнення й формат процесу "перехоплення, інформації" з урахуванням "негласного отримання інформації у скритний спосіб".

Не відображено суті поняття СТЗ у визначенні, яке запропонував В. Допілка. Згідно з його позицією під терміном СТЗ необхідно розуміти пристрої, обладнання, апаратуру тощо, які були спеціально пристосовані (сконструйовані) для негласного отримання інформації [10, с. 47]. У цьому визначенні наведені не всі технічні ознаки СТЗ, зокрема, не згадані такі як "придатність" та "технічна забезпеченість". Як зазначалося раніше, "негласне отримання інформації" не охоплює "отримання доступу до інформації", що визначає частину СТЗ.

У більшості джерел визначення СТЗ взагалі не дається або перераховуються лише його ознаки. Так, С. Петрочєнков, аналізуючи кримінальну відповідальність за СТЗ, згадує лише окремі ознаки СТЗ: апаратура, що володіє здатністю скритного отримання інформації; засоби, що порушують таємницю листування, телефонних переговорів, поштових, телеграфних або інших повідомлень громадян [18]. Слабким місцем цієї позиції, як і попередньої, є брак ознак, які характеризують СТЗ.

Деякі вчені, як це і належить робити, визначали термін СТЗ відповідно до його змісту. З точки зору Логінова І., СТЗ – це різновид спеціальної техніки, тобто засоби, спеціально створені, розроблені, запрограмовані або модернізовані для негласного

пошуку та фіксації фактичних даних про готування або вчинення злочину в інтересах кримінального судочинства [17, с. 101]. До речі, схожий підхід міститься у законопроєкті "Про внесення змін до статті 201 Кримінального кодексу України (щодо відповідальності за незаконне ввезення, придбання, збут або використання спеціальних технічних засобів негласного отримання інформації)" від 12.02.15 р., реєстр. № 2125 [23], де під терміном СТЗ пропонується розуміти технічні засоби, устаткування, апаратуру, прилади, пристрої, обладнання та інші вироби, виготовлені для виконання завдань з негласного отримання інформації під час здійснення оперативно-розшукової діяльності і заборонені у вільному обігу, перелік яких встановлюється Кабінетом Міністрів України. Проте ці визначення також здаються небездоганними. Словосполучення "пошук та фіксація фактичних даних" або "виконання завдань з негласного отримання інформації" не виправдано звужують зміст "негласного отримання інформації або доступу до неї у скритний спосіб". Як і в проаналізованих нормативно-правових актах та інших джерелах, за межами дефініції залишаються такі технічні ознаки віднесення продукції (виробів) до СТЗ, як "придатність" та "технічна забезпеченість". Крім цього, наведені визначення не містять згадку про препарати, що відносяться до СТЗ.

Оригінальна думка була висловлена Черних А., який запропонував таке визначення: СТЗ – прилади, системи, пристрої, спеціальний інструмент та програмне забезпечення для електронних обчислювальних машин та інших електронних пристроїв незалежно від їх зовнішнього вигляду, технічних характеристик, а також принципів роботи, яким навмисно додані якості і властивості для забезпечення скритного (таємного, неочевидного) отримання інформації або доступу до неї (без відома власника) [19, с. 3]. Але й це визначення не є бездоганним. В цьому визначенні більше уваги приділялося продукції, що відноситься до СТЗ, хоча поза увагою автора залишилися обладнання та препарати. Вади цієї позиції, як і попередньої, зумовлені тим, що характеристика "незалежно від їх зовнішнього вигляду та технічних характеристик" надто загальна. Такі ознаки віднесення продукції (виробів) до СТЗ, як "придатність" та "технічна забезпеченість" відсутні у дефініції. Так само у наведеному визначенні бракує посилання на термін "негласність" щодо процесу отримання інформації.

Висновки.

На підставі аналізу законодавства у цій сфері та висловлених вище аргументів є підстави надати таке визначення: *СТЗ – створені або модернізовані та пристосовані з наданням нової якості та властивості технічні засоби, обладнання, інструменти, програмне забезпечення, препарати та інші вироби, які за своєю технічною забезпеченістю або за безпосередньою обумовленістю їх застосування придатні для негласного отримання інформації або доступу до неї у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій*.

Наведене визначення містить низку унікальних ознак, серед яких виділяються:

"Технічна забезпеченість" – сукупність технічних характеристик, параметрів, функціональних можливостей та конструктивних особливостей технічного засобу або обладнання, інструменту та іншого виробу, технічних характеристик, параметрів та функціональних можливостей програмного забезпечення та препарату, необхідна та достатня для забезпечення його застосування для здійснення заздалегідь визначених дій.

"Технічні характеристики" – складова технічної забезпеченості, яка кількісно та якісно характеризує сукупність основних розпізнавальних властивостей технічного засобу, обладнання, інструменту, програмного забезпечення, препарату та іншого виробу, спрямованих на виконання його функцій впродовж життєвого циклу.

“Параметри” – складова технічної забезпеченості, яка кількісно характеризує фізичними та/або хімічними величинами основні властивості технічного засобу, обладнання, інструменту, програмного забезпечення, препарату та іншого виробу та наведена в паспорті або формулярі на нього.

“Функціональні можливості” – складова технічної забезпеченості, яка характеризує спосіб використання технічного засобу, обладнання, інструменту, програмного забезпечення, препарату та іншого виробу для негласного отримання інформації у скритний спосіб.

“Конструктивні особливості” – складова технічної забезпеченості, яка характеризує виготовлення, виконання, побудову тощо технічного засобу, обладнання, інструменту та іншого виробу.

“Придатність” – оцінка технічної забезпеченості технічного засобу або обладнання, інструменту, програмного забезпечення, препарату та іншого виробу на предмет можливого застосування для здійснення заздалегідь визначених дій.

“Негласне отримання інформації” – заходи або дії, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених законодавством, та здійснюються для отримання інформації (спостереження, прийому, зняття, відбору, перехоплення, передачі та/або фіксування, оброблення) без відома суб’єкта цієї інформації (її володаря) та сторонніх осіб.

“Скритний спосіб” – метод отримання інформації або доступу до неї, що забезпечує мінімальну ймовірність виявлення ознак встановлення та застосування технічного засобу, обладнання, інструменту, програмного забезпечення, препарату та ін. виробу.

На нашу думку, реалізація на законодавчому рівні запропонованого підходу з приведенням у відповідність до нього інших подібних формулювань, сприятиме з’ясуванню суті СТЗ, зменшенню похибок у віднесенні до СТЗ і техніки подвійного використання продукції побутового та відомчого промислового призначення, зміцненню мотивації підприємців у впровадженні інноваційних технологій у зазначену сферу діяльності, розвиток якої є в інтересах національної безпеки та економічного державного добробуту.

Використана література

1. Соколан Т.С. Право на недоторканність приватного життя та основи його дотримання під час здійснення відео спостереження. *Вісник ХНУВС*. 2011. № 2. С. 301-307.

2. Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації: Постанова Кабінету Міністрів України від 22.09.16 р. № 669. *Офіційний Вісник України*. 2016. № 79. Ст. 2640.

3. Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв’язку: Указ Президента України від 13.04.01 р. № 256. *Офіційний Вісник України*. 2001. № 16. Ст. 697.

4. Про визначення сфер діяльності, в яких центральні органи виконавчої влади та Служба безпеки України здійснюють функції технічного регулювання: Постанова Кабінету Міністрів України від 16.12.15 р. №1057. *Офіційний Вісник України*. 2015. № 102. Ст. 3519.

5. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Служби безпеки України від 12.08.05 р. № 440. URL: http://zakon4.rada.gov.ua/laws/showz090205/print1414494494558707 (дата звернення: 25.05.2020).

6. Про затвердження Порядку складання єдиного наскрізного плану створення зразка (системи, комплексу) озброєння, військової і спеціальної техніки: Постанова Кабінету Міністрів України від 26.06.13 р. № 449. *Офіційний Вісник України*. 2013. № 50. Ст. 1793.

7. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10, 11-12, 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17

8. Галстян Г.Г. Зарубіжний досвід використання оперативно-технічних засобів. *Науковий вісник Херсонського державного університету. Сер. Юридичні науки*. 2018. Т. 2. С. 78-81.

9. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.

10. Допілка В.О. Контрабанда спеціальних технічних засобів негласного отримання інформації. *Митна справа*. 2012. № 2. С. 45-49.

11. Пасека О.Ф. Окремі проблемні аспекти кримінальної відповідальності за незаконне придбання, збут або використання спеціальних технічних засобів негласного отримання інформації за КК України. *Науковий вісник Львівського державного університету внутрішніх справ*. 2016. Вип. 2. С. 301-310.

12. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/ 2341-14.

13. Про Службу безпеки України: Закон України від 25.03.92 р. № 2230-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 38.

14. Про ліцензування видів господарської діяльності: Закон України від 02.03.15 р. № 222-VIII. *Відомості Верховної Ради України*. 2015. № 23. Ст. 158.

15. Про внесення змін до деяких законодавчих актів України щодо імплементації актів законодавства Європейського Союзу у сфері технічного регулювання: Закон України від 06.06.19 р. № 2740-VIII. *Відомості Верховної Ради України*. 2019. № 28. Ст. 116.

16. Бегишев И.Р. Уголовно-правовая характеристика специальных технических средств, предназначенных для негласного получения информации. *Следователь.* 2010. № 5. С. 2-4.

17. Логінов І.В. Визначення терміну “спеціально технічні засоби”: мат. міжвід. наук.-практ. конф. *Актуальні проблеми оперативно-розшукової діяльності в сучасних умовах,* м. Київ, 19 трав. 2011 р. Київ: Наук. вид. відділ Нац. акад. СБУ, 2011. С. 98-103.

18. Петроченков С.Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: дис. …канд. юрид. наук: спец. 12.00.08. Москва, 2013.

19. Черных А.А. Правовое регулирование оборота специальных технических средств, предназначенных для негласного получения информации. *Юридические науки*. 2018. № 16. С. 2-4.

20. Council Resolution of 17 January 1995 on the Lawful interception of telecommunications. *Offical Journal*. C. 329. 04/11/1996. P. 0001-0006. URL: http://eurlex. europa.eu/LexUriServ/Lex UriServ.do?uriCELEX:31996P1104:EN:HTML (дата звернення: 25.05.2020).

21. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг зв’язку: Резолюція Ради Європи. – (Брюссель, 20.06.2001). URL: http://zakon.rada.gov.ua/laws/show/994_234 (дата звернення: 25.05.2020).

22. On the retention of data generated or processed in connection with the provision of public available electronic communications services or of public communications networks and amending Directive 2002/58/EC: Directive 2006/24/EC of European Parliament and of the Council of 15 March 2006. URL: http://eur-lex.europa.eu/legal-content/GA/TXT/?uriCELEX:32006L0024 (дата звернення: 25.05.2020).

23. Про внесення змін до статті 201 Кримінального кодексу України (щодо відповідальності за незаконне ввезення, придбання, збут або використання спеціальних технічних засобів негласного отримання інформації): проєкт Закону України від 12.02.15 р. (реєстр. № 2125). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2 (дата звернення: 25.05.2020).

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

УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук.*
ORCID: https://orcid.org/0000-0001-7786-4657.

ЗАХИСТ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Анотація. *У статті здійснено аналіз напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів. Запропоновано внести зміни у кримінальне процесуальне законодавство України та Закон України "Про телекомунікації" задля імплементації положень Конвенції про кіберзлочинність, ввести кримінальну відповідальність за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Сформульовано низку пропозицій щодо удосконалення адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів, зокрема запропоновано запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси та переглянути нормативні документи у сфері технічного і криптографічного захисту інформації.*

Ключові слова*: державні електронні інформаційні ресурси, кібербезпека, кіберзахист, удосконалення законодавства, інформаційно-телекомунікаційні системи.*

Summary. *The article deals with the issues of the directions for improvement of the current legislation of Ukraine with the purpose of the state electronic information resources protection. It is proposed to amend the criminal procedural legislation of Ukraine and the Law of Ukraine "On Telecommunications" in order to implement the provisions of the Convention on Cybercrime, to introduce criminal liability for unauthorized interference with the work of information and telecommunication systems in which state electronic information resources are processed. A number of proposals have been formulated to improve the administrative and legal procedures related to the protection of state electronic information resources, in particular, it is proposed to introduce licensing of activities of Internet service providers for public authorities in which state electronic information resources are processed and review technical and cryptographic information security regulations.*

Keywords*: state electronic information resources, cybersecurity, cyber defence, legislative improvements, information and telecommunication systems.*

Аннотация. *В статье осуществлен анализ направлений совершенствования действующего законодательства Украины с целью защиты государственных электронных информационных ресурсов. Предложено внести изменения в уголовное процессуальное законодательство Украины и Закон Украины "О телекоммуникациях" для имплементации положений Конвенции о киберпреступности, ввести уголовную ответственность за несанкционированное вмешательство в работу информационно-телекоммуникационных систем, в которых обрабатываются государственные электронные информационные ресурсы. Сформулирован ряд предложений по совершенствованию административно-правовых процедур, связанных с защитой государственных электронных информационных ресурсов, в частности предложено ввести лицензирование деятельности провайдеров Интернет-услуг для органов государственной власти, в которых обрабатываются государственные электронные информационные ресурсы и пересмотреть нормативные документы в сфере технической и криптографической защиты информации.*

Ключевые слова: *государственные электронные информационные ресурсы, кибербезопасность, киберзащита, совершенствование законодательства, информационно-телекоммуникационные системы.*

Постановка проблеми. Визначення шляхів формування безпечного функціонування електронних інформаційних ресурсів вищих органів державної влади, державних підприємств, установ та організацій є одним із пріоритетів для розвитку систем електронного урядування, реалізації концепції "держава у смартфоні" тощо. В Україні існує низка чинників, що впливають на регулювання, захист та розвиток системи обігу державних електронних інформаційних ресурсів. Поряд з безумовною відкритістю інформаційної сфери України загалом, досить часто нормативно-правові акти, що регулюють функціонування державних електронних інформаційних ресурсів, не враховують стратегічних орієнтирів, об'єктивних українських реалій, а також загроз, що виникають у зв'язку з протиправними посяганнями на електронні інформаційні ресурси і на державні зокрема. Виникають випадки, коли частина інформаційних відносин регулюється підзаконними нормативно-правовими актами, що не завжди узгоджуються із чинними законами України, зокрема Законом України "Про основні засади забезпечення кібербезпеки України", а також концептуальними документами, наприклад, "Стратегією кібербезпеки України".

Результати аналізу наукових публікацій свідчать про те, що питання забезпечення кібернетичної і інформаційної безпеки держави були предметом досліджень багатьох українських учених, а саме Довганя О.Д., Климчука О.О., Марущака А.І., Остроухова В.В., Панченко В.М., Пилипчука В.Г., Польового В.І., Розвадовського О.Б., Хлевицького В.Б., Юрченка О.М.та інших.

У попередніх дослідженнях [1] автор частково розкриває організаційні питання діалогу суб'єктів Національної системи кібербезпеки і представників ІТ-бізнесу з метою підвищення довіри між приватними суб'єктами та державними органами, а відповідну платформу для обговорення пропонує організувати на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Частково питання методології побудови класифікатора загроз для державних інформаційних ресурсів розкривають дослідники технічних наук Юдін О.К.та Бучик С.С. [2]; у контексті електронного урядування принципи організації національних електронних інформаційних ресурсів, зокрема у частині державних електронних інформаційних ресурсів аналізує Приймак Ю. [3, с. 130]. Стратегічну проблему забезпечення інформаційної безпеки в контексті глобалізації у своїй монографії розкриває Довгань О.Д. [4].

Однак у цілому питання удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів було предметом наукових досліджень лише фрагментарно. Саме тому у сучасний період у системі функціонування електронних інформаційних ресурсів держави свого вирішення потребують науково-теоретичні проблеми удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Метою статті є визначення окремих напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Виклад основного матеріалу. Насамперед, звернемо увагу на відсутність Державної цільової програми, яка б передбачала заходи із забезпечення кіберзахисту України, зокрема і в частині захисту державних електронних інформаційних ресурсів. У цьому контексті підтримуємо позиції експертів щодо необхідності передбачення у програмі першочергових заходів: запровадження міжнародних стандартів безпеки, підвищення рівня обізнаності населення з загрозами кібербезпеки, впровадження системи навчання з кібербезпеки і визнання міжнародної сертифікації з кібербезпеки ІТ-аудиту [5]. Дійсно, Закон України "Про основні засади забезпечення кібербезпеки України"

передбачає, що функціонування національної системи кібербезпеки забезпечується зокрема шляхом програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту [6, ст. 8]. Відповідно, правові передумови для прийняття Державної цільової програми кіберзахисту України існують і вони актуалізуються сучасними загрозами кібербезпеці держави. Існують також приклади прийняття і реалізації подібних програм в провідних іноземних країнах, зокрема у Сінгапурі, де впроваджено Національну програму з кібербезпеки [7]. Тому вважаємо за необхідне прийняти Державну цільову програму кіберзахисту України.

У розвиток позиції Марущака А.І. щодо імплементації у вітчизняне законодавство статей 16 – 18 Конвенції про кіберзлочинність [8] (далі – Конвенція) відзначимо також, що від належного нормативно-правового регулювання відносин щодо повноважень правоохоронних органів залежить ефективність їх діяльності щодо захисту державних електронних інформаційних ресурсів від кіберінцидентів та кібератак. Норми Конвенції мають імплементуватися у законодавство нашої держави, зокрема у частині доповнення Кримінального процесуального кодексу України статтями щодо електронних доказів у кримінальному провадженні у частині визначення поняття цифрових (електронних) доказів (ст. 14 Конвенції: "…кожна Сторона застосовує повноваження і процедури, передбачені до… збору доказів у електронній формі стосовно кримінального правопорушення" [9]), порядку обмеження (блокування) інформаційного ресурсу (інформаційного сервісу) і впровадження термінової фіксації інформації в цифровій (електронній) формі та її збереження (ст. 16 Конвенції: "1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати ордери або іншим подібним шляхом спричиняти термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації. 2. Якщо Сторона застосовує пункт 1 вище шляхом видачі ордеру особі, яким така особа зобов'язується зберігати визначені комп'ютерні дані, які зберігаються і знаходяться у власності або під контролем такої особи, вона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів [9]), специфіки проведення обшуку і арешту з метою розширення дії на цифрові (електронні) докази, в тому числі можливість копіювати необхідні дані (ст. 19 Конвенції "Обшук і арешт комп'ютерних даних, які зберігаються" [9]).

У зв'язку з викладеним та з урахуванням положень Конвенції необхідно також передбачити у Законі України "Про телекомунікації" (ст. 39) [10] обов'язок суб'єктів ринку телекомунікації, які надають послуги доступу до Інтернет, забезпечити ідентифікацію власних абонентів за ПІБ, IP-адресою, фізичною адресою надання послуг, а також зберігати дані щодо спожитих ними послуг, форм оплати та інформацію щодо з'єднань абонентів протягом 90 днів.

Наступна пропозиція удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів стосується врегулювання проблемних питань протидії кіберзлочинності, зокрема і спрямованої на такі державні ресурси. Так, кримінальне законодавство України не виокремлює злочини щодо державних електронних інформаційних ресурсів, що не дає змоги віднести їх досудове

розслідування до підслідності слідчих СБ України, хоча це передбачено положеннями Стратегії кібербезпеки України [11]. На нашу думку, необхідно ввести відповідальність за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Адже останнім часом фіксується збільшення кібератак, зорієнтованих на спричинення шкоди національним інтересам держави, на такі ресурси, відповідні інформаційно-телекомунікаційні системи, а також на об'єкти критичної інформаційної інфраструктури. Протидія ж органами СБ України зазначеним загрозам ускладнюється через відсутність належного кримінально-правового захисту інтересів держави. Адже на сьогодні предмет, об'єктивна та суб'єктивна сторони злочинів, передбачених статтями 361 та 362 КК України [12] не повною мірою охоплюють діяння, спрямовані на порушення сталої роботи державних електронних інформаційних ресурсів.

Наступні пропозиції для удосконалення законодавства України стосуються зміни адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів. Так, рішенням РНБО України від 29 грудня 2016 р. [13], Кабінету Міністрів України було доручено врегулювати питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації. Відповідне рішення до цього часу не втілилося в окремий нормативно-правовий акт, оскільки суб'єкти ринку Інтернет-послуг та їх об'єднання блокують його прийняття на стадії громадського обговорення. Однак, з 2018 року оператори (провайдери) телекомунікацій отримують в Держспецзв'язку України атестати відповідності щодо забезпечення захисту інформації згідно з вимогами нормативних документів системи технічного захисту інформації в Україні, які дозволяють їм надавати послуги з доступу до мережі Інтернет – "Захищений вузол Інтернет-доступу" – державним органам, підприємствам, установам і організаціям державної форми власності.

У цьому напрямі пропонуємо запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси.

На сьогодні законодавство України також не передбачає адміністративної відповідальності за невиконання законних вимог посадових осіб СБ України. У контексті наділення СБ України додатковими повноваженнями здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, протидіяти кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідувати кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечувати реагування на кіберінциденти у сфері державної безпеки [6]. За такого стану правового регулювання відсутність адміністративної відповідальності за невиконання законних вимог посадових осіб СБ України суттєво знижуватиме ефективність реалізації зазначених вище повноважень, передбачених Законом України "Про основні засади забезпечення кібербезпеки України".

Саме тому вважаємо, що пропозиція внести зміни до Кодексу України про адміністративні правопорушення шляхом включення статті 185-14 "Невиконання законних вимог посадових (службових) осіб Служби безпеки України або перешкоджання

здійсненню Службою безпеки України визначених законом функцій або повноважень" [14] є цілком обґрунтованою і сприятиме, серед іншого, належному виконанню органами СБ України повноважень щодо розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, боротьбу з кібертероризмом та кібершпигунством.

Потребують також перегляду нормативні документи у сфері технічного і криптографічного захисту інформації (НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі", НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"), відповідно до яких здійснюється побудова комплексних систем захисту інформації. Зокрема, згідно з чинним законодавством [15] при проведенні перевірки інформаційно-телекомунікаційних систем визначається відповідність комплексних систем захисту інформації вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації. Тобто, видається, що перевіряється виключно технічна документація з впровадження таких систем без вивчення реального стану справ із захисту державних електронних інформаційних ресурсів. Такий підхід вважаємо застарілим і таким, що не відповідає як провідним міжнародним практикам, так і реаліям сучасних загроз у кіберпросторі, а тому має бути переглянутий у напрямку запровадження міжнародних апробованих підходів щодо виявлення вразливостей для завантаження шкідливого програмного забезпечення, порядку проведення регулярного аудиту захисту державних електронних інформаційних ресурсів тощо.

Ще однією проблемою практичного характеру, яка негативно впливає на стан захищеності державних електронних інформаційних ресурсів, є використання співробітниками державних органів, в яких обробляються такі ресурси, джерел розважального характеру, сторонніх поштових сервісів, соцмереж тощо. Це призводить до формування додаткових вразливостей для державних електронних інформаційних ресурсів.

З метою зниження рівня відповідного ризику для державних електронних інформаційних ресурсів, пропонуємо передбачити розпорядчим документом Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, ведення Реєстру ресурсів, доступ до яких абонентів телекомунікаційних мереж – органів державної влади України обмежений. До такого реєстру доцільно включати ресурси розважального характеру, сторонні поштові сервіси, соцмережі, анонімайзери доступу, тор-браузери тощо.

Насамкінець відзначимо, що незважаючи на рішення Ради національної безпеки і оборони України "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" від 29 грудня 2016 р. введеного в дію Указом Президента України від 13.02.17 р. № 32 [16], на даний час не сформовано перелік інформаційно-телекомунікаційних систем об'єктів критичної інформаційної інфраструктури (відповідно до постанови Кабінету Міністрів України від 23.08.16 р. № 563 [17]), що суттєво ускладнює протидію загрозам безпечному функціонуванню інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Тому вважаємо, що є усі підстави для пришвидшення формування зазначеного переліку.

Висновки.

Підсумовуючи викладене, зазначимо, що здійснений аналіз дав підстави для формулювання напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Набули подальшого розвитку питання імплементації норм Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України у частині порядку обмеження (блокування) інформаційного ресурсу (інформаційного сервісу) і впровадження термінової фіксації інформації в цифровій (електронній) формі та її збереження, проведення обшуку і арешту з метою розширення дії на цифрові (електронні) докази. Відповідно, доцільно також передбачити у Законі України "Про телекомунікації" обов'язок суб'єктів ринку телекомунікації, які надають послуги доступу до Інтернет, забезпечити ідентифікацію власних абонентів, а також зберігати дані щодо спожитих ними послуг протягом 90 днів.

Обґрунтовано необхідність введення відповідальності за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси, з метою кримінально-правового захисту інтересів держави.

Сформульовано низку пропозицій щодо удосконалення адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів, а саме запропоновано:

прийняти Державну цільову програму кіберзахисту України;

запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси;

внести зміни до Кодексу України про адміністративні правопорушення шляхом включення статті щодо відповідальності за невиконання законних вимог посадових (службових) осіб Служби безпеки України або перешкоджання здійсненню Службою безпеки України визначених законом функцій або повноважень;

переглянути нормативні документи у сфері технічного і криптографічного захисту інформації у напрямку запровадження міжнародних апробованих підходів щодо виявлення вразливостей для завантаження шкідливого програмного забезпечення, порядку проведення регулярного аудиту захисту державних електронних інформаційних ресурсів тощо;

передбачити розпорядчим документом Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації ведення Реєстру ресурсів, доступ до яких абонентів телекомунікаційних мереж – органів державної влади України обмежений.

Перспективами подальших наукових пошуків визначаємо питання правових механізмів для розбудови мережі ситуаційних центрів кібербезпеки в Україні.

Використана література

1. Петров С.Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право*. № 4(31)/2019. С. 107-112.

2. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. Київ: НАУ, 2015. 214 с.

3. Приймак Ю. Розвиток електронного урядування в Україні: організація національних електронних інформаційних ресурсів. URL: http://www.visnyk.academy.gov.ua/wp-content-/upload/2013/11/2011-4-18.pdf

4. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ: Видавничий дім "АртЕк", 2015. 386 с.

5. Котвицкий І. Що потрібно зробити Україні для власної кібербезпеки. URL: https://www.glavnoe.ua/articles/a12228-scho-potribno-zrobiti-ukraini-dlja-vlasnoi-kiberbezpeki

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

7. The National Cybersecurity R&D Programme. URL: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

8. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. № 1(24)/2018. С. 127-132.

9. Про кіберзлочинність: Конвенція РЄ від 23 листопада 2001 року. *Офіційний вісник України*. 2007. № 65. Ст. 253.

10. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

12. Кримінальний кодекс України: Закон України від 05.04.01 р. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

13. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації": Указ Президента України від 13.02.17 р. № 32. URL: https://www.president.gov.ua/documents/322017-21282

14. Про внесення змін до Закону України "Про Службу безпеки України": проект закону щодо удосконалення організаційно-правових засад діяльності Служби безпеки України від 10.03.20 р. № 3196. URL: https://www.http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

15. Про затвердження Положення про державний контроль за станом технічного захисту інформації: Наказ Адміністрації Держспецзв'язку України від 16.05.07 р. № 87. *Офіційний вісник України*. 2007. № 50. Ст. 2037.

16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації": Указ Президента України від 13.02.17 р. № 32/2017. *Офіційний вісник України*. 2017. № 16. Ст. 464.

17. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. *Офіційний вісник України*. 2016. № 69. Ст. 2332.

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

УДК 004.9:343.14

ГОВОРУХА В.І., начальник підрозділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
СТЕПАНОВ В.А., *кандидат технічних наук,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК РІЗНОВИД НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Анотація. *Стаття присвячена проблемі зняття інформації з електронних інформаційних систем як різновиду негласних слідчих (розшукових) дій.*
Ключові слова: *негласні слідчі (розшукові) дії, зняття інформації, електронна інформаційна система, спеціальні технічні засоби для зняття інформації з каналів зв'язку, технічні засоби негласного отримання інформації.*

Summary. *The article is devoted to the problem of interception of information from electronic information system as form of covert investigative (search) actions.*
Keywords: *covert investigative (search) actions, interception of information, electronic information system, special technical means for interception of the information from communication channels, technical means for private obtaining of information.*

Аннотация. *Статья посвящена проблеме снятия информации с электронных информационных систем как разновидности негласных следственных (розыскных) действий.*
Ключевые слова*: негласные следственные (розыскные) действия, снятие информации, электронная информационная система, специальные технические средства для снятия информации с каналов связи, технические средства негласного получения информации.*

Постановка проблеми. З метою отримання (збирання) доказів або перевірки вже отриманих доказів у конкретному кримінальному провадженні проводяться слідчі (розшукові) дії.

Різновидом слідчих (розшукових) дій відповідно до ст. 246 Кримінального процесуального кодексу України (далі – КПК України) є негласні слідчі (розшукові) дії, відомості про факт та методи проведення яких не підлягають розголошенню за винятком випадків, передбачених зазначеним кодексом України [1].

До негласних слідчих (розшукових) дій, які передбачають втручання у приватне спілкування, віднесені заходи зі зняття інформації з електронних інформаційних систем (ст. 264 КПК України). Такі дії проводять у разі, якщо відомості про злочин і особу, яка його вчинила, неможливо отримати іншим способом. Вони проводяться на підставі ухвали слідчого судді виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів (ст. 246 КПК України). Водночас, закон не містить визначення заходів зі зняття інформації з електронних інформаційних систем. Тому існує нагальна потреба їх конкретизації, розкриття змістовних ознак цих заходів з урахуванням меж втручання правоохоронних органів у приватне життя.

Результати аналізу наукових публікацій. Після прийняття КПК України 2012 року вивченням різних аспектів інституту негласних слідчих (розшукових) дій займалися такі науковці, як Бандурко О. [2], Галстян Г. [3], Допілка В. [4], Луцик В. [5], Манжай О. [2], Перепелиця М. [2], Тертишник В. [6], Уваров В. [7] та інші.

Праці зазначених науковців, безсумнівно, є вагомим внеском в дослідження цього інституту. Проте, аспекти негласної розшукової дії (далі – НСРД), пов'язаної зі зняттям інформації з електронних інформаційних систем, залишаються не повною мірою висвітленими, а тому потребують додаткового дослідження.

Метою статті є визначення на основі аналізу та узагальнення поняття НСРД "зняття інформації з електронних інформаційних систем".

Виклад основного матеріалу. Таємниця приватного спілкування як частина приватного життя, визнана та гарантована міжнародним законодавством, яке регулює суспільні відносини у галузі прав людини, як невід'ємна складова будь-якого сучасного правового, демократичного суспільства, а також передбачена національним законодавством багатьох країн, у тому числі і України. Під спілкуванням розуміють передавання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб (ч. 3 ст. 258 КПК України) [1].

У ст. 32 Конституції України передбачено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання і використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Втручання у таємницю спілкування можливе лише на підставі судового рішення, у випадках, передбачених КПК України, з метою виявити та запобігти тяжкому чи особливо тяжкому злочину, встановити його обставини, особу, яка вчинила злочин, якщо іншими способами неможливо досягти мети.

Втручання у приватне спілкування полягає в отриманні доступу до нього та змісту інформації приватного спілкування однієї особи з іншою без відома цих осіб.

Дослідження НСРД "зняття інформації з електронних інформаційних систем" ускладнюється тим, що на даний час в законодавстві України відсутнє визначення самого поняття "електронні інформаційні системи".

Під електронною інформаційною системою слід розуміти взаємозв'язок технічних засобів (комп'ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп'ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному вигляді. В той же час, під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту.

Сутність НСРД "зняття інформації з електронних інформаційних систем" полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частинах, без відома власника, володільця або утримувача системи. Зазначена НСРД проводиться, у разі якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися, як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного

проникнення. Негласне зняття інформації з засобів електронно-обчислювальної техніки полягає у застосуванні технічних засобів із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диску (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого. Програмне проникнення до електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують подолання системи захисту і копіювання інформації, що обробляється в зазначених системах (їх частинах), на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю НСРД.

Сукупність таких технічних та програмних засобів для проведення зазначеної НСРД складає окремий вид спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації (далі – СТЗ). Під СТЗ автори розуміють створені або модернізовані та пристосовані з наданням нової якості та властивості технічні засоби, обладнання, інструменти, програмне забезпечення, препарати та інші вироби, які за своєю технічною забезпеченістю або за безпосередньою обумовленістю їх застосування придатні для негласного отримання інформації або доступу до неї у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій.

Саме застосування СТЗ, на нашу думку, зумовлює уточнення деяких ознак поняття "зняття інформації з електронних інформаційних систем" в контексті НСРД.

Умовно в згаданій НСРД можливо виділити дві функціональні площини:

1) отримання доступу до інформації електронних інформаційних систем шляхом установлення їх логічного або фізичного місцезнаходження, програмного проникнення та/або безпосереднього фізичного (технічного) доступу до них;

2) відбір інформації за визначеними ознаками з електронних інформаційних систем або їх частин шляхом її копіювання, зняття, передачі, фіксації та обробки.

Луцик В.В. всі способи зняття інформації з електронних інформаційних систем об'єднує в дві основні групи: перша – це способи безпосереднього доступу, друга – способи опосередкованого (віддаленого) доступу до комп'ютерної інформації шляхом підключення до лінії телекомунікацій користувача з проникненням в комп'ютерну систему за допомогою підбору паролів або перехоплення імен та паролів користувачів [5, с. 283].

Також до другої групи належить спосіб електромагнітного перехоплення, який дозволяє отримати інформацію без підключення до електронної інформаційної системи, за рахунок перехоплення випромінювань центрального процесора, комунікаційних каналів та інших, а також – знімати і розшифрувати випромінювання працюючого принтера на відстані до 150 м, а випромінювання моніторів – до 500 м [8, с. 161].

Сучасні технології дозволяють оперативно відстежувати діяльність злочинних співтовариств принципово на іншому рівні. Представляє значний інтерес досвід спецслужб США в розробці і застосуванні систем "Oasis" (ЦРУ) і "Magic Lantern" (ФБР), які уможливлюють не тільки контролювати інформаційний обмін злочинних співтовариств, але і "зламувати" комп'ютери підозрюваних, упроваджувати в них "трояни" (програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері) тощо [7, с. 940].

Отже, враховуючи функціональні особливості та методи отримання інформації з електронних інформаційних систем, автори виділяють наступні типи СТЗ:

1) засоби для зняття (шляхом фізичного/технічного доступу) інформації з електронних інформаційних систем або з їх частин;

2) спеціалізовані програми для зняття (шляхом програмного проникнення), порушення цілісності, знищення, блокування та/або копіювання інформації з електронних інформаційних систем або з їх частин;

3) закладні пристрої, що розміщують безпосередньо в засобах обчислювальної техніки (USB-портах, системних платах, клавіатурах тощо) або в периферійному обладнанні (модемах, принтерах та інших пристроях);

4) засоби зняття, фіксації та аналізу побічних електромагнітних випромінювань від електронних інформаційних систем;

5) спеціальні засоби для експрес копіювання, руйнування (знищення) інформації з технічних носіїв.

Серед інших особливостей застосування таких СТЗ слід виділити:

- подолання системи логічного захисту електронних інформаційних систем;
- пошук, виявлення, обстеження, відбір, фіксація/копіювання інформації;
- передачу інформації третій стороні (при цьому можуть застосовуватись методи кодування чи шифрування інформації, передача за прискореними алгоритмами, активація за розкладом або за допомогою дистанційного керування, використання радіотехнологій);
- інші дії з інформацією в електронних інформаційних системах (порушення цілісності, знищення, блокування).

Як видно із наведених ознак СТЗ, крім зняття інформації з електронних інформаційних систем, такі засоби дозволяють здійснювати інші дії з інформацією, а саме: порушення цілісності, знищення та блокування.

Ці особливості функціонування СТЗ дають підстави для опису дій із отримання доступу до інформації електронних інформаційних систем в контексті пояснення ознаки “отримання інформації”.

Поняття “знищення інформації”, “блокування інформації”, “порушення цілісності інформації” наведені в Законі України “Про захист інформації в інформаційно-телекомунікаційних системах” [9].

Крім КПК України, визначення поняття “зняття інформації з електронних інформаційних систем” міститься в Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні. Згідно з цією Інструкцією “зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача” полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп’ютерах), автоматичних системах, комп’ютерній мережі [10].

Тертишник В.М., аналізуючи поняття “зняття інформації з електронних інформаційних систем”, виділяє наступні ознаки цього заходу [6]:

1) за своєю архітектурою електронні інформаційні системи можуть бути як локальними, в яких всі їх компоненти (база даних, система управління базою, клієнтське програмне забезпечення) знаходяться на одному комп'ютері, так і розподіленими, в яких компоненти розподілені по кількох комп'ютерах; розподілені даних електронні інформаційні системи, у свою чергу, розділяють на файл-серверні інформаційні системи (в них база даних знаходиться на файловому сервері, а система управління базою даних та клієнтське програмне забезпечення знаходяться на робочих станціях) та клієнт-серверні інформаційні системи (в них база даних та система управління базою даних

знаходяться на сервері, а на робочих станціях знаходиться клієнтське програмне забезпечення);

2) як локальні, так і розподілені електронні інформаційні системи можуть бути відкритими і закритими для громадян, тобто доступ до яких обмежений їх власником, володільцем або утримувачем шляхом розміщення файлових серверів та робочих станцій інформаційної системи у публічно недоступних місцях, житлі чи іншому володінні особи та встановленням систем логічного захисту доступу до електронної інформаційної системи з робочих станцій локальної мережі підприємства, установи, організації тощо, або з робочих станцій, зв'язаних з файловим сервером через мережу Інтернет [6].

У клопотанні слідчого, узгодженому з прокурором, про дозвіл на зняття інформації з електронних інформаційних систем повинні бути вказані ідентифікаційні ознаки електронної інформаційної системи (найменування електронної інформаційної системи, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець або утримувач) та спосіб, яким обмежений доступ до неї [6].

В проекті Закону України "Про оперативно-розшукову діяльність" передбачено, що зняття інформації з електронних інформаційних систем є оперативно-розшуковим заходом, який полягає у негласному пошуку, виявленні шляхом програмного та/або технічного доступу, відборі, фіксації відомостей, що містяться в електронних інформаційних системах або їх частинах, доступ до яких обмежується їх власником, володільцем або утримувачем, чи пов'язаний із подоланням системи логічного захисту [11].

На наш погляд, у цих визначеннях наведені не всі ознаки "зняття інформації з електронних інформаційних систем", зокрема, не згадані такі, як спосіб "негласного отримання інформації"; дія з "доступу до інформації"; дії з отримання інформації "копіювання, зняття, передача, обробка, порушення цілісності, знищення та блокування інформації"; "використання СТЗ".

Висновки.

За результатами аналізу законодавства та інших джерел, вважаємо за доцільне запропонувати таке визначення заходів із зняття інформації з електронних інформаційних систем: *"зняття інформації з електронних інформаційних систем" – заходи, що полягають в негласному доступі до інформації електронних інформаційних систем (установленні їх логічного або фізичного місцезнаходження, програмному проникненні до них та/або встановленні безпосереднього фізичного/технічного контакту з ними та відборі інформації за визначеними ознаками), в отриманні інформації з електронних інформаційних систем або їх частин (копіюванні, знятті, передачі, фіксації та обробки), а також в інших діях з зазначеною інформацією (порушенні цілісності, знищенні або блокуванні), з використанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації.*

Уточнення в законодавстві України запропонованого поняття НСРД "зняття інформації з електронних інформаційних систем" сприятиме забезпеченню законності під час її проведення.

Перспективи подальших досліджень зазначеної НСРД вбачаються в удосконалені практичних рекомендацій щодо застосування окремих СТЗ під час її проведення.

Використана література

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. №№ 9-10, 11-12, 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 25.07.2020).

2. Оперативно-розшукова компаритівстика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. Харків: Золота миля, 2013. 352 с.

3. Галстян Г.Г. Зарубіжний досвід використання оперативно-технічних засобів. *Науковий вісник Херсонського державного університету. Серія Юридичні науки*. 2018. Т. 2. С. 78-81.

4. Допілка В.О. Контрабанда спеціальних технічних засобів негласного отримання інформації. *Митна справа*. 2012. № 2. С. 45-49.

5. Луцик В.В. Зняття інформації з електронних інформаційних систем. URL: http://www.pravoznavec.com.ua/period/article/3719/% (дата звернення: 21.01.2019).

6. Тертишник В.М. Коментар до Кримінального процесуального кодексу України. Вид. 16-е, доп. і перероб. Київ: Правова Єдність, 2020. 1070 с. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2 (дата звернення: 25.07.2020).

7. Уваров В.Г. Зняття інформації з електронних інформаційних систем: новели КПК України та євро стандарти. *Форум права*. 2012. № 4. С. 939-943. URL: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12uvgute.pdf (дата звернення: 25.07.2020).

8. Егорышев А.С. Криминалистический анализ неправомерного доступа к компьютерной информации. *Южно-уральские криминалистические чтения. Межвузовский сборник научных трудов*. 2001. № 9. С. 156-165. URL: http://ndki.narud.ru/library/articles/Egoryshev_AS-Krim_har1.html. (дата звернення: 25.07.2020).

9. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

10. Про затвердження Інструкції "Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні": наказ Генеральної прокуратури України, МВС, СБУ, Адміністрації ДПС, Мінфіну, Мінюсту України від 16.11.12 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 25.07.2020).

11. Про оперативно-розшукову діяльність: проект закону України від 04.04.17 р. № 6284. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1 (дата звернення: 25.07.2020).

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

УДК 343.98:004.056

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

ШЛЯХИ ПОСИЛЕННЯ СПРОМОЖНОСТЕЙ ПРАВООХОРОННИХ ТА ІНШИХ ДЕРЖАВНИХ ОРГАНІВ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Анотація. *У статті розглянуто проблеми боротьби з кіберзлочинністю та надаються рекомендації щодо посилення спроможностей правоохоронних та інших органів у цій сфері.*
Ключові слова: *Інтернет, кіберзлочинність, кібербезпека, електронна комерція.*

Summary*. The article considers issues of cybercrime fighting and provides recommendations with regard to strengthening the capacity of law enforcement and other government agencies in this sphere.*
Keywords*: Internet, cybercrime, cybersecurity, e-commerce*

Аннотация: *В статье рассматриваются проблемы борьбы с киберпреступностью и даются рекомендации по усилению правоохранительных и других органов в этой сфере.*
Ключевые слова*: Интернет, киберпреступность, кибербезопасность, электронная коммерция.*

Постановка проблеми. Наприкінці минулого століття проблема профілактики злочинності, пов'язаної із застосуванням комп'ютерів, та боротьби з нею набула міжнародних масштабів та вже досліджувалася на рівні ООН [1]. Подальше поширення доступу до Інтернету та кількості підключених до глобальної мережі різноманітних пристроїв продовжує надавати кіберзлочинцям дедалі більше можливих векторів атак для здійснення злочинів. Якщо у 2008 році по всьому світу було 1,5 млрд. користувачів Інтернету, то у 2019 році Міжнародний союз телекомунікацій (МСЕ) визначив це число у 4,1 млрд., що становить більше половини населення планети [2]. За інформацією Державної служби статистики України, станом на 1 січня 2020 року в Україні було зафіксовано 28 млн. 787 тисяч користувачів Інтернету, що перевищує половину населення держави [3].

Відповідно до звіту Cisco (Cisco Annual Internet Report) кількість пристроїв, підключених до мережі Інтернет, до 2023 року перевищить кількість населення у світі втричі та складе 3,6 мережевих пристроїв на душу населення [4]. Завдяки цьому слід очікувати подальшого збільшення кількості можливих кібератак.

Кіберзлочинці постійно застосовують нові технології та методи кібератак, з метою уникнення своєї ідентифікації, користуючись прогалинами в законодавствах країн щодо належної ідентифікації особи в Інтернет-просторі. Для цього, наприклад, використовують технологію VPN (Virtual Private Network) та TOR (The Onion Router). Дедалі більшого поширення в Україні набуває практика використання провайдерами телекомунікаційних послуг технології NAT (Network Address Translation), яка за відсутності належного обліку використання внутрішніх IP-адрес провайдера фактично унеможливлює ідентифікацію конкретного користувача, який вчинив протиправне діяння.

З огляду на вказані тенденції кіберзлочинність залишається постійною загрозою для приватних осіб, суб'єктів господарювання і держави, яка продовжує зростати в кількості і масштабах та різновидах. Особливістю поширення кіберзлочинності є її

транскордонний характер і її поширюваність як серед країн, що розвиваються, так і тих, хто має більш високий рівень розвитку. Широке використання технологій та зростаючі темпи підключення до Інтернету по всьому світу в поєднанні з постійним розвитком нових технологій, які забезпечують анонімність в Інтернеті, дають змогу кіберзлочинності бути низько ризиковою та високоприбутковою справою. Через це у два найближчі десятиліття кіберзлочинність залишатиметься однією з найбільших проблем для розвитку суспільства як в Україні, так і в більшості країн світу. Згідно з офіційним щорічним звітом про кіберзлочинність 2020 року компанії Cybersecurity Ventures, збитки від кіберзлочинності становитимуть понад 6 трильйонів доларів щорічно до 2021 року, що на 3 трильйони доларів перевищує збитки у 2015 році [5].

Результати аналізу наукових публікацій. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як Ахтирська Н.М., Бутузов В.М., Гавловський В.Д., Голубєв В.О., Демедюк С.В., Савченко А.В., Хахановський В.Г., Шеломенцев В.П. та ін. [6 – 11]. Проте багато питань потребують подальшого дослідження та вирішення у практичній площині.

Метою статті є надання рекомендацій щодо посилення спроможностей правоохоронних та інших органів у боротьбі з кіберзлочинністю.

Виклад основного матеріалу. В останні роки в Україні значно активізувався розвиток цифрової економіки. Цьому посприяв, зокрема, Закон України "Про електронну комерцію", який визначає організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та окреслює права і обов'язки учасників відносин у сфері електронної комерції. У січні 2018 року уряд ухвалив "Концепцію розвитку цифрової економіки та суспільства України на 2018 – 2020 роки", сред ключових напрямків якої – розвиток цифрової інфраструктури. Усю територію України заплановано покрити широкосмуговим Інтернетом, що дасть поштовх цифровим трансформаціям у системі освіти, медицини, екології, безготівкової економіки, інфраструктури, транспорту тощо. Діджиталізація (цифрові технології) приходить на заміну старим засобам електронної комунікації – телефону, факсу, телеграфу [12].

Також в Україні починаючи з вересня 2019 року, почало діяти Міністерство цифрової трансформації, яке реалізує державну політику у сферах цифрового розвитку, цифрової економіки, цифрових інновацій, розвитку цифрових навичок та цифрових прав громадян. Відповідно до Указу Президента України від 4.09.19 р. № 647/2019 передбачається переведення окремих публічних послуг в електронну форму [13].

У лютому 2020 року в Україні запустили мобільний додаток "Дія", завдяки якому можна отримати десятки публічних послуг он-лайн, зокрема, стати підприємцем, змінити вид діяльності чи припинити її тощо [14].

9 червня 2020 року Президент України подав на розгляд Верховної Ради України проект Закону "Про народовладдя через всеукраїнський референдум", який передбачає реалізацію права голосу виборця шляхом електронного голосування.

Разом з тим, в українському сегменті кіберпростору продовжують вчинятися кіберзлочини. З кожним роком кількість потерпілих від протиправних дій кіберзлочинців стає дедалі більше. Як уже зазначалося, самі правопорушення стають більш масштабними.

Найбільшу небезпеку становлять кібератаки на об'єкти критичної інформаційної інфраструктури, які за останні 5 років постійно здійснюються різноманітними кіберугрупованнями. Деякі з них завдали значних матеріальних збитків – зокрема сумновідомий вірус Petya Ransomware, через який постраждало понад 60 країн світу, а збитки від нього сягають 8 млрд. доларів США [15].

На важливості питання забезпечення кібербезпеки у процесі цифрової трансформації держави та кіберзахисті державних електронних інформаційних ресурсів наголосив Секретар Ради національної безпеки і оборони України Олексій Данілов під час 14-го засідання Національного координаційного центру кібербезпеки, яке відбулося 22 травня 2020 року.

Під час засідання Координаційного центру Секретар РНБО України звернув увагу представників органів влади на незадовільний стан захищеності державних електронних інформаційних ресурсів, реєстрів, баз даних та інших інформаційних масивів та наголосив на необхідності удосконалення практичної взаємодії між суб'єктами забезпечення кібербезпеки.

Наприклад, у травні 2020 року в месенджері Telegram з'явився бот, який видавав персональні дані громадян та іншу інформацію, зокрема було надано 4,5 млрд. логінів і паролів. За фактом розповсюдження персональної інформації громадян розпочато розслідування кримінального провадження за ч. 2 ст. 361 Кримінального кодексу України (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації) [16]. Під час проведення операції під умовною назвою "ДАТА", спрямованої на протидію несанкціонованим діям з інформацією та незаконному розповсюдженню чи збуту даних з обмеженим доступом, кіберполіція спільно зі слідчими підрозділами НП України, Міністерством цифрової трансформації України та Службою безпеки України, під процесуальним керівництвом прокуратури провели 36 обшуків у різних областях України. За результатами виявлено велику кількість файлів, що містять персональні дані громадян України, фрагменти баз даних державних, банківських та комерційних установ. Наразі встановлено 25 причетних до правопорушень осіб. Такі злочини підривають довіру суспільства до впроваджених Урядом цифрових ініціатив, відтак потребують значної уваги та інтенсивної роз'яснювальної роботи з громадськістю. Важливим напрямком є також відслідковування та впровадження прогресивних рішень захисту персональних даних громадян країни проти можливого втручання з боку третіх країн, і в цьому зв'язку подальше вдосконалення законодавства України і приведення його у відповідність до відповідних Директив Європейського Союзу (зокрема про електронну комерцію, про захист персональних даних тощо).

Поглиблення міжнародної співпраці є також на часі, оскільки завдяки розвитку ІТ-індустрії України та значному авторитету українських фахівців цієї галузі, на жаль дедалі частішими стають явища виявлення недобросовісних суб'єктів, які вчиняють злочини в цій сфері як на території України так і поза її кордонами. Так в липні 2020 року Секретна служба США і Держдепартамент оголосили про винагороду у 2 млн. доларів за інформацію, яка допоможе арештувати або засудити двох громадян України.

У США їх звинувачують у кібершахрайстві, зламі комп'ютерних систем і незаконних операціях з цінними паперами. На кібершахрайстві хакери незаконно заробили понад 4,5 млн. доларів, стверджує відомство. Секретна служба США наголошує, що це перший випадок, коли федеральна служба звертається за допомогою до громадськості у всьому світі.

В цьому ж місяці українські правоохоронці виявили та затримали відомого хакера під ніком "Sanix", який проживав в Івано-Франківську. У прес-службі СБУ повідомили, що саме цей хакер у минулому році звернув на себе увагу світових фахівців з

кібербезпеки після того, як виклав на одному з форумів оголошення про продаж бази із 773 млн. адресів поштових скриньок та 21 млн. унікальних паролів [17].

Слід також зауважити, що несанкціоновані дії з інформацією на інформаційних ресурсах здійснюють не тільки хакери чи спецслужби інших країн, але й адміністратори та інші особи, які мають право доступу до неї. Наприклад, у травні 2020 року Служба безпеки України викрила факт втручання в електронну систему Державного земельного кадастру, який здійснив посадовець Держслужби України з геодезії, картографії та кадастру. За версією слідства, чиновник на замовлення "клієнтів" безпідставно видалив відомості щодо прав власності на земельну ділянку загальною площею 5 гектарів на території Ірпінської міської ради [18].

Також набувають поширення кіберзлочини, які не пов'язані безпосередньо з несанкціонованим доступом до інформації, але відповідають визначенню, наданому в Законі України "Про основні засади забезпечення кібербезпеки України" від 5.10.17 р. № 2163-VIII, – кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Серед таких кіберзлочинів найбільш поширеними є шахрайство (чч. 3 і 4 ст. 190 КК України).

Наприклад, у червні 2020 року співробітники кіберполіції в Дніпропетровській області із залученням полку поліції особливого призначення та працівників виправної установи припинили злочинну діяльність групи осіб, які під виглядом продажу товарів заволоділи грошима громадян. Кіберполіція встановила, що до такої діяльності причетні четверо мешканців Дніпропетровської області. Фігуранти створили власний веб-сайт, за допомогою якого під виглядом продажу побутових товарів відомих брендів ошукували громадян. Своїми протиправними діями вони завдали збитків на загальну суму два мільйони гривень. Від їхніх дій постраждало близько 200 громадян України. Зазначимо, що організатор групи раніше неодноразово засуджений та відбуває покарання за вчинення злочину, передбаченого ст. 190 (Шахрайство) Кримінального кодексу України [19].

Посилене використання Інтернету під час пандемії надає кіберзлочинцям більше можливостей для реалізації шахрайських схем для інфікування шкідливими програмами або продажу лікарських, зачасти фальсифікованих товарів. З початку спалаху COVID-19 кіберзлочинці активно експлуатують цю проблему, створюючи сайти, заражені зловмисним програмним забезпеченням, та спонукаючи людей купувати підроблені ліки, добавки та вакцини. За даними, зібраними та проаналізованими Atlas VPN, ***кількість фішингових веб-сайтів під час карантину COVID-19 зросла на 350 %*** [20].

За кордоном вказаним видам злочинів приділяється значна увага з огляду на їх велику кількість та зростаючу динаміку шахрайських діянь. Наприклад, компанія з кібербезпеки RiskIQ (https://www.riskiq.com) почала сканувати нові домени, пов'язані з коронавірусом, відстежуючи такі ключові слова, як ковід, вірус, вакцина чи пандемія, та виявила понад 300 тисяч підозрілих веб-сайтів.

Як відповідь на подібні виклики, у Великобританії реєстратори доменних імен веб-сайтів активізують свої зусилля для боротьби з аферистами, і це починається ще до того, як їх веб-сайти з'являться в реальному часі.

Реєстратори перевіряють відповідність назв сайтів їх змісту та вимогам щодо їх утворення та наявність прав у замовника реєстрації оперувати відповідною назвою сайту. При виявленні невідповідності законодавчо визначеним вимогам такі сайти не

реєструють. Даний метод застосовується для попередження різних видів шахрайств, наприклад, пов'язаних із банківською діяльністю або сплатою податків, щоб зменшити діяльність шахрайських веб-сайтів, на етапі їх реєстрації. Спеціальні алгоритми підбирають спроби реєстрації доменів імен, які містять ключові слова, та оцінюють їх. Реєстратори доменних імен вже призупинили 600 підозрілих веб-сайтів, пов'язаних з темою коронавірусу.

Промисловий масштаб, в якому шахраї встановлюють веб-домени, змусив урядовців і інших країн закликати реєстраторів доменних імен посилити боротьбу з шахрайськими сайтами. Так, Генпрокурор Нью-Йорка Летітія Джеймс нещодавно надіслала відкриті листи шести найбільшим реєстраторам домену в Інтернеті з проханням посилити свої контрзаходи [21]. Об'єднання зусиль всіх реєстраторів і опрацювання проблеми з боку представників профільної галузі є важливою запорукою отримання позитивного ефекту в боротьбі з окресленою проблемою та створення інструментів відповідного саморегулювання з боку бізнесу.

Вчиненню подібних правопорушень в Україні сприяє наявність прогалини у чинному вітчизняному законодавстві.

Так Законом України "Про електронну комерцію" визначено організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлено порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та визначено права й обов'язки учасників відносин у сфері електронної комерції. Зокрема частиною 1 статті 7 передбачено обов'язок продавця товарів забезпечити прямий, простий, стабільний доступ інших учасників відносин у сфері електронної комерції до такої інформації:

повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи-підприємця;

місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи-підприємця;

адреса електронної пошти та/або адреса Інтернет-магазину;

ідентифікаційний код для юридичної особи або реєстраційний номер облікової картки платника податків для фізичної особи.

Наведена норма повною мірою відповідає положенням Директиви ЄС "Про захист прав споживачів та щодо електронної комерції" (Directive 2011/83/EU), проте, на відміну від законодавства ЄС, Закон України "Про електронну комерцію" ***не визначає*** відповідальність суб'єкта електронної комерції за невиконання обов'язків, встановлених Законом, а також не визначений контролюючий орган, який зобов'язаний моніторити виконання зазначених положень закону.

Це надає можливість недобросовісним учасникам відносин у сфері електронної комерції ***уникати сплати податків, продавати фальсифіковані товари, реалізовувати контрабандний товар*** – адже юридична особа не вказана і відсутні державні органи, які повинні контролювати зазначену сферу.

Наприклад, у липні 2020 року кіберполіція викрила осіб, які під виглядом продажу товарів та послуг "заробили" майже 1,5 млн. гривень. Члени групи створили 14 веб-сайтів, де продавали неіснуючі товари. У результаті від дій зловмисників постраждало понад дві сотні громадян. Правопорушникам загрожує до дванадцяти років ув'язнення з конфіскацією майна [22].

У результаті споживачі таких товарів можуть зазнавати загрози життю та здоров'ю, матеріальних збитків. Бюджет держави недоотримує відповідних надходжень, а шахраї

продовжують користуватися недоліками законодавства. Це є однією з причин, що надає можливість понад половині бізнесу перебувати в тіні.

На нашу думку, слід чітко визначити відповідальність за невиконання статті 7 Закону України "Про електронну комерцію" та державні органи, які уповноважені здійснювати контроль у зазначеній сфері. За аналогією з законодавством Європейського Союзу відповідними контролюючими органами можуть бути підрозділи податкової служби або кіберполіції та Державної служби України з питань безпечності харчових продуктів та захисту споживачів.

Так *Державна служба України з питань безпечності харчових продуктів та захисту споживачів* відповідно до Положення про службу перевіряє додержання суб'єктами господарювання, що провадять діяльність у сфері торгівлі і послуг, вимог законодавства про захист прав споживачів, а також правил торгівлі та надання послуг. До правил надання послуг в електронній комерції належить зокрема дотримання суб'єктами господарювання вимог щодо електронної комерції, зокрема в частині ідентифікації суб'єкта господарювання.

Також, безперечно, зазначену роботу можуть проводити співробітники *Департаменту кіберполіції НП України*, який спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних Інтернет-мереж і систем.

У зв'язку з тим, що власники зазначених сайтів, як правило, ухиляються від сплати податків, доцільною видається перевірка таких підприємців співробітниками регіональних підрозділів податкової служби.

Вирішення зазначених вище проблемних питань потребує здійснення системних заходів із створення відповідної законодавчої бази. Зокрема необхідно внести зміни до Податкового кодексу України, Кодексу України про адміністративні правопорушення, Кодексу адміністративного судочинства України, Закону України "Про захист прав споживачів", Закону України "Про авторське право та суміжні права" тощо. Вирішення зазначеного питання потребує оперативного опрацювання фахівцями профільних відомств.

Певна робота у цьому напрямі вже проводиться. Зокрема, зареєстровані законопроекти № 3860 та № 3861 щодо присвоєння та використання офіційної електронної адреси для юридичних та фізичних осіб. На нашу думку, необхідно впровадити реєстрацію офіційних сайтів на основі системи ID-Web. Реєстрація та адміністрування таких сайтів повинно здійснюватися за допомогою електронних ID-документів, що забезпечило б повну ідентифікацію власників сайтів, які займаються підприємницькою діяльністю, та значно зменшило б кількість шахрайських сайтів [23].

Окремо хочемо торкнутись питання щодо розподілу відповідальності та удосконалення законодавчого врегулювання діяльності правоохоронних органів у сфері кіберпростору, зокрема, СБУ та НП України. Адже фахівці Служби безпеки України регулярно нейтралізують сотні кібератак на інформаційні ресурси державних органів влади, протидіють поширенню шкідливих програм у банківському секторі, витоку інформації з обмеженим доступом. При цьому особливу увагу слід приділити питанням розслідування кіберзлочинів на об'єктах критичної інфраструктури. Такі об'єкти знаходяться під постійною увагою хакерів та спецслужб іноземних держав. Безумовно, необхідно в найкоротші строки створити реєстр як об'єктів критичної інфраструктури, так і реєстр об'єктів критичної інформаційної інфраструктури як необхідного елементу забезпечення відповідного рівня кіберзахисту.

Наприклад, у липні 2020 року за повідомленням прес-служби концерну "Укроборонпром" було здійснено чергову кібератаку на інформаційно-телекомунікаційну систему концерну. На корпоративні електронні поштові скриньки працівників концерну розсилалися електронні повідомлення, інфіковані вірусом типу "троян". Атака відбувалася з електронної адреси, розміщеної на серверах одного американського телекомунікаційного провайдера.

Для забезпечення кібербезпеки національного сегменту Інтернет задіяні і інші суб'єкти національної системи кібербезпеки.

У липні 2020 року фахівці Національного координаційного центру кібербезпеки при РНБО України виявили в DarkNet перелік з майже 3 млн. сайтів, які використовують сервіс Cloudflare для захисту від DDoS і низки інших кібератак. Опублікований перелік містить реальні IP-адреси сайтів українського сегменту Інтернет, що створює загрози спрямованих на них атак. Серед 6500 записів з доменом "ua" є адреси 45 записів з доменом "gov.ua" та ресурси, що належать об'єктам критичної інфраструктури.

Слід зазначити, що під час розслідування кібератак необхідно тісно співпрацювати з провайдерами комунікаційних послуг. Вони першими можуть виявляти такі атаки та зберігати шкідливий мережевий трафік для подальшого його аналізу. Водночас існує серйозна проблема отримання інформації від приватного сектору, оскільки на законодавчому рівні не встановлені вимоги щодо обов'язкового зберігання провайдерами інформації, наявність "сірої" адресації NAT, що призводить до унеможливлення отримання необхідної інформації або взагалі до її відсутності. У більшості випадків інформація надається виключно на підставі рішення суду, що призводить до отримання неактуальної або застарілої інформації. Також, при відсутності в Україні судової практики винесення судами ухвал за пришвидшеною процедурою про вжиття запобіжних заходів, правовласник, або особа, чиї права були порушені неправомірними діями власника веб-сайту, є фактично позбавленим можливості ефективного правового захисту.

Позитивний ефект роботи мають норми статті 52-1 Закону України "Про авторські та суміжні права" щодо залучення провайдера комунікаційних послуг до врегулювання відносин з власником веб-сайту у зацікавленої сторони, в разі, якщо власник веб-сайту всупереч законодавству не розголошує свої дані на створеній ним сторінці. Зазначений механізм повною мірою відповідає практикам взаємодії між провайдерами телекомунікаційних послуг та зацікавленими суб'єктами господарювання або державними органами країн в питаннях захисту авторських прав, наявній в судовій системі ЄС. Доцільним є подальше законодавче удосконалення ролі провайдера комунікаційних послуг, підвищення його відповідальності перед зацікавленими сторонами в разі якщо веб-сайт, розміщений на ресурсі, що ним обслуговується, порушує права третіх осіб.

Для протидії кібератакам важливого значення набуває обізнаність користувачів інформаційних систем щодо правил кібергігієни. Адже більшість кібератак розпочинаються за допомогою простого електронного листа. Більше 90 відсотків успішних атак та порушення даних відбуваються шляхом використання фішингових електронних листів, створених для того, щоб спровокувати своїх одержувачів натиснути посилання, відкрити документ або кому-небудь пересилати певну інформацію. За словами Кеті Х'юз – директора з інформаційної безпеки Northwell Health (найбільший приватний роботодавець США – 68000 осіб), люди – найслабша ланка в ланцюжку безпеки [24]. Наприклад, проведене у червні 2020 року масштабне дослідження

кіпрського студента щодо використання паролів показало, що кожен 142-ий пароль із мільярда облікових записів був “123456” [25], який легко визначається зловмисниками.

Тому важливе значення для посилення кібербезпеки, а отже й запобігання кіберзлочинності має впровадження у навчальний процес як цивільних, так і навчальних закладів правоохоронних органів спеціалізованих предметів із захисту інформації та систематичне проведення тренінгів і навчань з кібербезпеки.

Цікавим у цьому аспекті є досвід Національної академії внутрішніх справ, де у 2019 – 2020 навчальному році запроваджено вивчення особливостей пошуку й аналізу криміналістичної інформації під час здійснення досудового розслідування у відкритій (“поверхневій”, Surface Web) і прихованій (“темній”, Dark Web) частинах мережі Інтернет, застосування програмних засобів Microsoft Office, Power BI та IBM i2 Analyst’s Notebook як сучасного інструментарію для обробки й аналізу: телефонного трафіку; даних із відповідних реєстрів, баз даних та інформаційно-довідкових систем; даних про банківські транзакції та рух матеріальних цінностей; даних, отриманих з електронних платіжних систем і систем он-лайн банкінгу, тощо.

Корисною також є започаткована Національним банком України у липні 2020 року Всеукраїнська інформаційна кампанія з протидії платіжному шахрайству, у рамках якої громадян навчатимуть основним правилам безпеки безготівкових та он-лайн-платежів. Адже минулого року в Україні зафіксували майже 72 тисячі випадків незаконних дій із платіжними картами. 58 % із них сталися в Інтернеті. Найпопулярніший метод шахрайства – соціальна інженерія, коли люди самі переказують гроші аферистам або розкривають їм дані. У 2020 році через карантинні заходи в шахраїв з’явилися й нові сценарії – під виглядом державних органів обіцяють грошову допомогу через карантин і у такий спосіб виманюють інформацію з платіжних карток.

Оскільки для поширення атак кіберзлочинці використовують засоби автоматизації і алгоритми машинного навчання, правоохоронцям необхідно використовувати ті ж інструменти для протидії сучасним і витонченим методам атак. Зокрема небезпечними є кібератаки, які вчиняються через пристрої Інтернету речей, які в переважній більшості випадків ніяк не захищені. Доступ до цих пристроїв дозволяє кіберзлочинцям стежити за приватним життям, планувати протиправну діяльність на фізичному об’єкті, отримувати доступ до мережевих систем для запуску DDoS атак або атак з метою вимагання викупу. Корисним у цьому сенсі є нещодавно підписаний Меморандум між Департаментом кіберполіції НП України та Національним технічним університетом України “Київський політехнічний інститут імені Ігоря Сікорського”, відповідно до якого фахівці технічного вузу будуть ділитися з правоохоронцями технічними особливостями роботи комп’ютерних систем.

За дослідженнями кримінологів кіберзлочини вчиняються широким спектром дійових осіб з різноманітними мотиваціями. Загрози кіберзлочинності можуть надходити від організованих злочинних угруповань, терористів, суб’єктів, що безпосередньо працюють або наймаються суб’єктами ворожих держав, одиноких хакерів та інших осіб, які можуть бути мотивовані фінансовими, ідеологічними, політичними чи іншими причинами.

Особливо слід зазначити, що, незважаючи на відмінності в профілях злочинців та їх мотивації, більшість діянь, пов’язаних із кіберзлочинністю, за оцінками експертів, мають транснаціональний характер. Транскордонний характер Інтернету дає змогу легко створювати абсолютно нові категорії кіберзлочинів. Один кіберінцидент може вразити значну кількість об’єктів у багатьох країнах, незалежно від місцезнаходження кіберзлочинців, а це означає, що до розслідування кіберзлочинів та притягнення до

відповідальності лише деяких злочинців необхідно залучати представників різноманітних правоохоронних органів, прокурорів та суддів у різних юрисдикціях, що значно ускладнює розслідування кіберзлочинів, включаючи вирішення питання щодо екстериторіальної юрисдикції та ефективності механізмів міжнародного співробітництва у транснаціональному розслідуванні. І хоча для комунікації та обміну оперативною інформацією з правоохоронними органами іноземних держав і міжнародними компаніями Департамент кіберполіції Національної поліції України активно використовує канали захищеного зв'язку NCP (National Contact Point) та Siena (Secure Information Exchange Network Application), проте більшість країн та компаній відмовляють у наданні інформації на відповідний запит, регламентуючи це необхідністю направлення на правоохоронні органи іноземних держав MLAT (доручення про міжнародну правову допомогу). А це, у свою чергу, призводить до незначної кількості засуджених за вчинення кіберзлочинів (не тільки в Україні).

Наприклад, в Англії та Уельсі за законом про комп'ютерне зловживання у 2017 році було винесено менше 50-ти вироків, незважаючи на повідомлення Бюро національної статистики Великобританії про те, що з квітня 2017 по березень 2018 року було вчинено понад 1,2 млн. правопорушень [26].

Згідно із судовою статистикою в Україні у 2019 році за вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку розглянуто 101 провадження (кількість засуджених осіб – 66; осіб, щодо яких кримінальне провадження закрито, – 27; примусові заходи виховного характеру застосовано до 1 особи).

Відсутність правоохоронного потенціалу та спроможності розслідувати кіберзлочини дозволяє кіберзлочинцям бути досить впевненими щодо низьких шансів, що вони коли-небудь будуть виявлені, заарештовані та будуть нести покарання.

У зв'язку з постійним збільшенням кількості кібератак, вчиненням інших кіберзлочинів постає питання посилення спроможностей як безпосередньо правоохоронних підрозділів, так й інших державних органів, які протидіють кіберзлочинності.

Підтримка потенціалу для зміцнення знань, умінь та навичок суб'єктів кримінального правосуддя для подолання загрози кіберзлочинності та посилення верховенства закону й поваги до прав людини та громадянських свобод – це підхід, який користується широкою міжнародною підтримкою, зокрема ООН.

У травні 2019 року Комісія ООН з питань запобігання злочинності та кримінального правосуддя рекомендувала Генеральній Асамблеї прийняти проект резолюції, яка закликає держави-члени забезпечувати сталу розбудову потенціалу в галузі кіберзлочинності по всьому світу. Хоча певні країни вкладають значні кошти в нарощування потенціалу для власних систем кримінального правосуддя, глобальне посилення спроможностей щодо кіберзлочинності часто передбачає певну форму взаємовідносин донор – реципієнт, тобто такі відносини, коли країна, яка має певні знання, навички, технології тощо щодо протидії кіберзлочинності, допомагає або підтримує в розвитку інші країни.

Такий підхід використовує і Рада Європи, яка оцінила переваги розбудови потенціалу як одного з підходів до боротьби з кіберзлочинністю та класифікувала типи програм для нарощування спроможностей, які впроваджуються у всьому світі. Заходи такого програмування розбудови потенціалу можуть включати підтримку розробки стратегій боротьби з кіберзлочинністю; створення нової та/або оновлення законодавчої бази із гарантіями верховенства права; створення систем звітності про кіберзлочинність; створення або зміцнення спеціалізованих підрозділів з питань кіберзлочинності поліції чи прокуратури; розширення криміналістичних можливостей; проведення

правоохоронних, прокурорських та судових тренінгів; створення механізмів державно-приватного співробітництва для забезпечення успішних розслідувань кіберзлочинності.

У рамках проекту "Розбудова спроможностей кіберполіції" представники Координації проектів ОБСЄ в Україні передали підрозділам кіберполіції Національної поліції України 194 одиниці спеціалізованої техніки [27].

Разом з тим потребує свого подальшого розвитку спеціалізація слідчих та прокурорів, які задіяні у розслідуванні кіберзлочинів. Зокрема у структурі Головного слідчого управління Національної поліції України у 2017 році був створений відділ, який спеціалізуються на розслідуванні кіберзлочинів. Водночас після збільшення кількості оперативних працівників кіберполіції збільшилася кількість виявлених кіберзлочинів та навантаження на слідчих, кількість яких не змінилася. Збільшення кількості слідчих, які спеціалізуються на розслідуванні кіберзлочинів, надасть можливість належним чином проводити досудове розслідування.

Також проблемним питанням у проведенні досудового розслідування є існуюча процедура звернення до місцевих судів із клопотаннями про надання тимчасових доступів, обшуків, арештів тощо. Відсутність повноцінного електронного документообігу і зокрема не визначеність його використання під час проведення досудових розслідувань, існуюча процедура звернення до місцевих судів з клопотаннями про надання тимчасових доступів, обшуків, арештів тощо яка передбачає здійснення цих дій лише з використанням документів в паперовій формі створює перешкоди ефективному здійсненню відповідних процесуальних дій, значно відстає від сучасних практик електронного документообігу країн Євросоюзу.

Зокрема, для підготовки додатків до клопотань витрачається багато часу, паперу, витратних матеріалів, оскільки відсутній механізм звернення до суду з такими клопотаннями, додатками, у яких є відскановані матеріали (в електронному варіанті). Крім того, процесуальні документи, наприклад, ухвали слідчого судді, передаються в правоохоронні підрозділи тривалий час (за наявності засобів комунікації та Інтернет-зв'язку). Відсутність електронного документообігу між органом досудового розслідування та судами значно збільшує строк досудового розслідування. Тому вкрай необхідно Міністерству цифрової трансформації долучитися до впровадження в Україні електронного судочинства, зокрема організувати оперативну передачу електронних доказів та процесуальних документів мережами передачі даних.

Серед ***основних напрямів підвищення рівня спроможності правоохоронних органів*** у сфері боротьби з кіберзлочинністю слід виокремити такі:

нарощування спроможності спеціалізованих підрозділів правоохоронних органів щодо аналізу електронних доказів з метою забезпечення прийнятності їх в суді;

розробка нормативно-правової бази у сфері кіберзлочинності та імплементація міжнародних конвенцій і договорів, включаючи необхідні зміни до кримінального та кримінально-процесуального законодавства, узгодження їх з чинними глобальними конвенціями;

розробка методик розслідування кіберзлочинів, забезпечення належного використання нових технологій та обмін інформацією з приватним сектором;

поширення позитивного досвіду у сфері протидії кіберзлочинності для працівників правоохоронних органів та належне укомплектування відповідних підрозділів, які протидіють кіберзлочинності, кваліфікованими спеціалістами;

забезпечення обміну інформацією між правоохоронними органами та іншими державними органами, які протидіють кіберзлочинності на всіх рівнях, включаючи органи прокуратури та спецслужби;

налагодження механізмів обміну інформацією та співпраці між правоохоронними органами, приватним сектором;

удосконалення процесу звітування правоохоронних органів, задіяних у боротьбі з кіберзлочинністю, перед громадськістю;

повна імплементація положень Конвенції про кіберзлочинність, зокрема статей, які стосуються збереження електронних даних.

Як уже зазначалося вище, ефективне розслідування кіберзлочинів потребує чіткого законодавчого розмежування підслідності кіберзлочинів у контексті повноважень Національної поліції України та Служби безпеки України.

Висновки.

В Україні, як і у всьому світі кіберзлочинність продовжує поширюватися, завдаючи значних економічних збитків. Водночас існують певні проблеми щодо виявлення кіберзлочинів та притягнення винних осіб до кримінальної відповідальності.

Очевидно, що одним із найважливіших шляхів протидії кіберзлочинності є стимулювання глобальної співпраці у розслідуванні кіберзлочинів як між правоохоронними органами різних країн, так і приватним сектором. Транснаціональний характер загроз кіберзлочинності потребує посилених та розширених зусиль, спрямованих на подолання перешкод, які гальмують таку співпрацю.

Іншою необхідною умовою успішної боротьби з кіберзлочинністю є вдосконалення механізмів обробки електронних доказів для проведення експертизи та передачі їх до суду.

Враховуючи зазначене, для посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю пропонується:

1. Забезпечити імплементацію положень статей 16 і 17 Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних та часткового розкриття їх трафіку.

2. Сприяти посиленню ідентифікації суб'єктів кіберпростору та зокрема суб'єктів електронної комерції шляхом внесення змін до Закону України "Про електронну комерцію", Податкового кодексу України, Кодексу України про адміністративні правопорушення, Кодексу адміністративного судочинства України щодо відповідальності за ненадання інформації про продавця товарів на веб-сайтах, які здійснюють електронну комерцію.

3. Посилити кримінальну відповідальність за вчинення кіберзлочинів на об'єктах критичної інфраструктури та критичної інформаційної інфраструктури.

4. Внести зміни до Кримінального процесуального кодексу України щодо розмежування повноважень розслідування кіберзлочинів Національної поліції України та Служби безпеки України.

5. Внести до Кримінального процесуального кодексу України зміни у частині визначення поняття "електронні докази", а також нормативно визначити положення щодо особливостей їх отримання, зберігання та подання до суду, засвідчення факту їх існування органами нотаріату.

6. Посилити міжнародну співпрацю правоохоронних органів шляхом участі у спільних слідчих групах та обміну, у тому числі, оперативною інформацією каналами Європолу та Інтерполу.

7. Сприяти постійно діючому процесу навчання та перепідготовки слідчих Національної поліції України методикам розслідування кіберзлочинів, у тому числі на основі аналізу інформації з Інтернет.

8. У зв'язку з тим, що Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.16 р. № 96/2016, спрямована на реалізацію заходів кібербезпеки до 2020 року, а План заходів з її реалізації виконаний не повністю, необхідно розробити та затвердити нову Стратегію кібербезпеки на 2020 – 2025 роки.

Використана література

1. United Nations Manual on the Prevention and Control of Computer-related Crime, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, No. E.94.IV.5). URL: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_ Guide.pdf

2. Скільки людей у світі користуються Інтернетом – ООН. URL: https://www.the-village.com.ua/village/city/city-news/290933

3. Держстат порахував, скільки закарпатців користуються Інтернетом і телебаченням. URL: https://zakarpattya.net.ua/News/199742

4. Cisco Annual Internet Report (2018–2023) White Paper URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

5. Cybercrime Damages $6 Trillion By. 2021. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

6. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. Київ: ВПЦ "Київський університет", 2018. 229 с

7. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов та ін. – (Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з проблем боротьби з організованою злочинністю, Служба безпеки України, Нац. акад. СБУ). Київ, 2011. 404 с.

8. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний ун-т "ЗІДМУ", 2003. 296 с.

9. Klymenko, Olga A.; Gutsaliuk, Mykhailo V.; Savchenko, Andrii V. Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digita. JANUS.NET e-journal of International Relations, Vol. 11, N.º 1, Maio-Outubro 2020. Consultado [em linha] em data da última consulta, https://doi.org/10.26619/1647-7251.11.1.2

10. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов. Київ: Вид. ПАЛИВОДА А.В., 2004. 144 с.

11. Демедюк С.В., Марков В.В. Кіберполіція України. *Наше право*. 2015. № 6. С. 87-93. URL: http:// nbuv.gov.ua/UJRN/Nashp_ 2015_6_15

12. Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки: Розпорядження Кабінету Міністрів України від 17.01.18 р. № 67-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi

13. Про деякі заходи із забезпечення надання якісних публічних послуг: Указ Президента України № 647/2019. URL: https://www.president.gov.ua/documents/6472019-29441

14. В Україні запустили мобільний додаток "Дія". URL: https://www.unian.ua/science/10862255-v-ukrajini-zapustili-mobilniy-dodatok-diya.html

15. Збитки від атаки вірусу Petya.A у світі сягають 8 мільярдів доларів – експерт. URL: https://www.unian.ua/science/2003241

16. Витік персональних даних українців: Що сталося і хто за цим стоїть. URL: https://ua.112.ua/golovni-novyni/vytik-personalnykh-danykh-ukraintsiv-shcho-stalosia-i-khto-za-tsym-stoit-535795.html

17. СБУ затримали відомого хакера з Івано-Франківська. URL: https://frankivsk.znaj.ua/311983-haker-z-frankivska-postaviv-na-vuha-ves-svit-prodavshi-naybilshu-bazu-danih-v-istoriji-bond-nervovo-kurit

18. СБУ викрила протиправне втручання в електронну систему Державного земельного кадастру для зміни інформації. URL: https://ssu.gov.ua/ua/news/1/category/21/view/7641#.sq7YnPH7.dpbs

19. Кіберполіція викрила шахраїв, які ошукали близько 200 громадян. URL: https://stopcor.org/kiberpolicziya-vykryla-shahrayiv-yaki-oshukaly-blyzko-200-gromadyan

20. Google Registers a 350 % Increase in Phishing Websites Amid Quarantine. URL: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine

21. Domain name registry suspends 600 suspicious coronavirus websites. URL: https://www.zdnet.com/article/domain-name-registrar-suspends-600-suspicious-coronavirus-websites/

22. Кіберполіція викрила осіб, які під виглядом продажу товарів та послуг "заробили" майже 1,5 мільйони гривень. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-osib-yaki-pid-vyglyadom-prodazhu-tovariv-ta-poslug-zarobyly-majzhe--miljony-gryven-7838

23. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2008. № 18. С. 265-269.

24. 2019 Official Annual Cybercrime Report. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

25. One out of every 142 passwords is '123456'. URL: https://www.zdnet.com/article/one-out-of-every-142-passwords-is-123456/?ftag=CAD-03-10abf6j

26. Crime in England and Wales: year ending March 2018, United Kingdom Office for National Statistics (19 July 2018). URL: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018

27. Кіберполіція отримала 194 одиниці спеціального обладнання для протидії кіберзагрозам. URL: http://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm

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

УДК 354:340.133:340.134

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID:https://orcid.org/0000-0002-2488-7377.
ШОСТАК Р.М., *кандидат технічних наук,* старший науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

РОЗВИТОК МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ АНТИТЕРОРИСТИЧНОЇ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (НА ПРИКЛАДІ США)

Анотація. *Стаття присвячена аналізу проблем антитерористичної захищеності об'єктів критичної інфраструктури. Досліджуються проблемні питання методичного забезпечення цієї діяльності. Описані сучасні тенденції дослідження критичної інфраструктури в США. На базі аналізу позитивного американського досвіду запропоновані заходи з удосконалення методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури України.*

Ключові слова: *антитерористична захищеність, об'єкти критичної інфраструктури, методичне забезпечення, терористичні акти, методологія прогнозування.*

Summary. *The article is dedicated to the analysis of the problems of antiterrorist protection of the objects of critical infrastructure. The article provides research of the problematic questions of the methodical support of this activity. Recent trends in the research of critical infrastructure in the United States are described. On the basis of the analysis of positive American experience, measures are proposed to improve methodical support of the protection the objects of critical infrastructure of Ukraine.*

Keywords*: antiterrorist protection, objects of critical infrastructure, methodical support, terrorist acts, forecasting methodology.*

Аннотация*. Статья посвящена анализу проблем антитеррористической защищенности объектов критической инфраструктуры. Исследуются проблемные вопросы методического обеспечения этой деятельности. Описаны современные тенденции исследования критической инфраструктуры в США. На основании анализа позитивного американского опыта предложены меры по совершенствованию методического обеспечения антитеррористической защищенности объектов критической инфраструктуры Украины.*

Ключевые слова*: антитеррористическая защищенность, объекты критической инфраструктуры, методическое обеспечение, террористические акты, методология прогнозирования.*

Постановка проблеми. Проблематика захисту критичної інфраструктури пов'язана із бурхливим розвитком нових підходів до забезпечення національної безпеки в розвинених країнах світу, що зумовлено швидкими змінами, які відбуваються у безпековому середовищі у глобальному, регіональному та національному вимірах [1].

Відповідно до Стратегії національної безпеки України [2] серед основних напрямів державної політики в сфері національної безпеки виділяється забезпечення безпеки та необхідного рівня захищеності об'єктів критичної інфраструктури України, насамперед від загроз терористичного та диверсійного характеру.

Одним із завдань запобігання терористичній діяльності є підвищення ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, у тому числі шляхом розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів. Водночас, усунення та мінімізація наслідків терористичної діяльності передбачає вирішення завдань опрацювання комплексу заходів щодо забезпечення якнайшвидшого відновлення штатного режиму функціонування об'єктів, передусім об'єктів критичної інфраструктури, щодо яких вчинено терористичний акт (розд. IV Концепції боротьби з тероризмом) [3].

Результати аналізу наукових публікацій. Дослідженням проблемних питань захищеності об'єктів критичної інфраструктури займалися такі вітчизняні науковці, як Алексеєв О. [4], Антипенко В. [5], Кондратов С., Крутов В. [6], Кудінов С. [7], Рижов І. [8] та інші. Вагомий внесок у розроблення методів, засобів і технологій ідентифікації об'єктів критичної інфраструктури внесено дослідженнями, проведеними зарубіжними вченими. Це, зокрема, праці Дуденхофера Д., Педерсена П., Пермана М., Маніка М. [1], Дженкінса Р.та Хантера Р.

Незважаючи на те, що останнім часом з'явилася значна кількість публікацій, присвячених проблемам антитерористичної захищеності об'єктів критичної інфраструктури, залишається недостатньо дослідженим питання методології забезпечення антитерористичної захищеності таких об'єктів, на підставі якої впроваджується методологічний апарат для аналізу критичної інфраструктури та оцінки захищеності об'єктів критичної інфраструктури. Ця проблема набуває особливого значення в умовах зростання рівня терористичної загрози.

Мета статті полягає у проведенні аналізу досвіду антитерористичного забезпечення захисту об'єктів критичної інфраструктури США для удосконалення методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури України.

Виклад основного матеріалу. Дослідження критичної інфраструктури є надзвичайно актуальними в багатьох країнах світу, і, в першу чергу, в США у зв'язку з суттєвим підвищенням рівня терористичних загроз на початку XXI ст. Що стосується антитерористичного забезпечення захисту критичної інфраструктури, і визначення його напрямів в основних стратегічних документах у даній галузі, то попередньо доцільно охарактеризувати напрями антитерористичного забезпечення захисту критичної інфраструктури на прикладі США, оскільки ця країна має значний досвід розв'язання цієї проблеми.

Відповідно до директиви Президента США № 63 "Стратегія спільних зусиль адміністрації США і приватного сектору у сфері захисту критичної інфраструктури" головне завдання досліджень у цій сфері полягає у виявленні ключових об'єктів (або їх сукупності), вплив на які може спричинити найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці прогнозованих наслідків подібного впливу й розробці механізмів зниження таких ризиків [9].

Першим результатом цієї роботи було впровадження методики визначення пріоритетності об'єктів ключових фондів військово-промислової бази (The Asset Prioritization Model – APM) з використанням якої розроблена фахівцями міністерства

внутрішньої безпеки (МВБ) і міністерства оборони США модель загальної структури об'єкта. Методика регламентувала визначення індексу ризикованості об'єкта, що залежить від рейтингу об'єкта по шкалі категорії факторів і значимості даного фактора [10].

Згідно з чинним законодавством США, під критичною інфраструктурою розуміються: "системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище" [11].

Водночас, створення моделі саме критичної інфраструктури держави зумовило потребу визначення та врахування взаємного зв'язку вхідних у неї об'єктів, їх характеру та взаємозалежності.

Без вирішення цих питань, в тому числі обліку й аналізу мережевої складової кожного сектору критичної інфраструктури (економічного, фінансового, енергетичного і т.д.), вбачається проблематичним забезпечення достатньої адекватності моделі та об'єкту дослідження [10].

Для усунення виявлених недоліків у США розпочався етап формування цілого кластера науково-дослідних організацій, які займаються розробкою імітаційних математичних моделей для дослідження критичної інфраструктури. За результатами наукових досліджень у цій сфері були вироблені методичні підходи для аналізу критичної інфраструктури та з'ясовані особливості її функціонування.

На думку зарубіжних експертів [12; 13], критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об'єктів та параметрів системи; 2) важко прогнозована поведінка об'єктів, для яких характерна велика кількість взаємозв'язків, які класифіковано по різних секторах [14].

У роботі "Розкриття, розуміння й аналіз взаємозв'язків об'єктів критичної інфраструктури" [15] представлена класифікація взаємозв'язків між об'єктами критичної інфраструктури, зміст якої складають: фізичний, кібернетичний, географічний (топологічний), логічний.

У роботах інших зарубіжних дослідників [1] зустрічається більш уточнена класифікація взаємозв'язків за характером:

фізичний – визначає інженерну взаємозалежність між об'єктами;

інформаційний – залежність від інформаційного обміну (потоку інформації) між об'єктами;

геопросторовий – взаємозалежність виникає в результаті спільного розташування компонентів інфраструктури на місцевості. Наприклад, повінь або пожежа виводить з ладу всі розміщені на площі стихійного лиха об'єкти мережі;

процедурний (політичний) – подібна взаємозалежність виникає при будь-якій зміні (події) в одному з компонентів сектору інфраструктури й спричиняє вплив на об'єкти інших секторів;

соціальний – така взаємозалежність може виражатися через соціальні фактори: суспільна думка, суспільна довіра, страх тощо.

З наведеної класифікації випливає, що критична інфраструктура будь-якої держави є не що інше, як велика складна система стратегічного масштабу (ВССМ), що представляє собою сукупність значної кількості елементів різного типу, об'єднаних зв'язками різної природи, для яких характерна загальна властивість (призначення, функція), яка відмінна від властивостей окремих елементів усієї сукупності, що й вимагає розробки спеціальних методів дослідження [10].

Цілком очевидно, що структура критичної інфраструктури має містити величезну кількість різнотипних об'єктів та зв'язків між ними. Для оптимізації досліджень застосовуються методи групування об'єктів критичної інфраструктури відповідно до їх взаємозалежності за секторами різного рівня з урахуванням їх важливості, зміст якої відображений в Національній стратегії з фізичного захисту критичної інфраструктури та ключових об'єктів (The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets) 2003 року [16].

За результатами такої оцінки найвищий рівень захисту в ієрархії ключових об'єктів отримали об'єкти військово-промислового комплексу, системи охорони здоров'я та попередження надзвичайної ситуації. Наступне місце в ієрархії посідають об'єкти фінансового та транспортного сектору. І, нарешті, найнижчий рівень складають об'єкти інформаційно-телекомунікаційного та енергетичного сектору, а також сектору водозабезпечення. При цьому сектори вищого рівня взаємозалежать від секторів нижчого рівня. Зауважимо, що у США критичну інфраструктуру розглядають у більш широкому розумінні, включаючи до неї національні символи (пам'ятки культурної спадщини).

Слід зазначити, що складність повного врахування всіх взаємозв'язків і взаємозалежностей між об'єктами інфраструктури не дозволяла об'єктивно досліджувати критичну інфраструктуру [17].

Тому основні напрямки наукових досліджень критичної інфраструктури спрямовані на створення моделей, що точно імітують функціонування критичної інфраструктури, в тому числі під час реалізації загроз терористичного або диверсійного характеру. Таке моделювання дозволяє визначати взаємозв'язки між її об'єктами, за результатами якого виявляти найбільш уразливі з них. Таким чином, імітаційне моделювання як один з видів математичного моделювання стає реальним інструментом для аналізу й повноцінного дослідження критичної інфраструктури, що являє собою ВСССМ [18, с. 29].

Одним з найбільш яскравих прикладів сучасних імітаційних моделей є "Система моделювання критичних інфраструктур" (Critical Infrastructure Interdependency Modeling (CIMS), яка розроблена національною лабораторією Айдахо. Модель CIMS являє собою систему імітаційного моделювання, що поєднує дані геопросторової інформації та чотиривимірний (просторово-тимчасовий) ефект. Це дозволяє імітувати певні сценарії різних подій з відображенням каскадних ефектів [18, с. 29]. В залежності від обраних сценаріїв модель може відображати наслідки аварійних подій (імітаційне моделювання), наслідки вчинених терактів (ситуаційне моделювання), а також може слугувати інструментом для планування спеціальних операцій та диверсій (стратегічне моделювання).

Пошуком ключових об'єктів, вплив на які може визначити найбільш негативний ефект, дослідження критичної інфраструктури не обмежується. Це тільки перший крок, за результатами якого, як правило, проводиться оцінка уразливості розкритих "центрів ваги" за допомогою інженерного методу побудови дерева відмов, яке трансформується в дерево подій. Це дозволяє визначити можливі наслідки уразливості інфраструктури, а також їх варіації. Дерево відмов являє собою бінарне дерево з усіма можливими логічними подіями для кожної потенційної відмови. Саме дерево відмов і подій дозволяє сформулювати й розробити можливі заходи щодо захисту критично важливих і вразливих об'єктів інфраструктури. У випадку прогнозування наслідків аварійних подій, результатом формування дерева події є перелік уразливостей об'єктів, який

використовується для розрахунків ймовірності їх виникнення, а також формування гістограми ймовірності відмов [10].

На наступному етапі розроблюються алгоритми оцінки ризиків, зміст яких полягає у визначенні ресурсів, необхідних для забезпечення безпеки (впливу) найбільш важливих з виявлених об'єктів критичної інфраструктури. При цьому однією з головних умов залишається дотримання критерію "вартість – ефективність", а ключова проблема полягає в тому, щоб правильно вибрати способи й засоби для організації захисту таких об'єктів [10].

Таким чином, на сьогодні в США функціонує збалансована система забезпечення захисту критичної інфраструктури держави, зміст якої охоплює:

– визначений уповноважений орган (МВБ) для організації, координації та здійснення контрольно-наглядових функцій щодо заходів безпекового напряму;

– методичний апарат для аналізу та прогнозування наслідків як подій техногенного характеру, так і диверсій чи терористичних актів;

– систему науково-дослідних установ, які забезпечують науково-технічне супроводження функціонування системи аналізу стану критичної інфраструктури та експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури.

В Україні ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, в основу якої покладено методологічний підхід аналізу ризиків, які обумовлювалися надійністю функціонування елементів, складових, об'єктів тощо. Іншими словами, ризик виникнення надзвичайної ситуації визначався вірогідністю відмов природнього характеру, аварій, інших надзвичайних подій (ймовірність виникнення та розвитку подій внаслідок умисного пошкодження елементів не враховувався та не розглядався взагалі).

Проте, антитерористичне забезпечення передбачає інший підхід, в основу якого покладено оцінку можливих сценаріїв вчинення терористичних актів (та їх прогнозованих наслідків), спрямованих в найбільш уразливе місце об'єкта (що призводить до максимально можливих втрат з мінімальними витратами ресурсів), в найбільш незручний час з точки зору функціонування (виробничого циклу) об'єкта і стану його системи фізичного захисту. Оцінка можливих сценаріїв вчинення терористичних актів потребує, в свою чергу, отримання результатів розрахунку прогнозованих людських, економічних, екологічних, суспільно-політичних, культурних та інших втрат внаслідок події можливих впливів на об'єкт терористичного чи диверсійного характеру.

На наш погляд, створення системи антитерористичного забезпечення захисту критичної інфраструктури держави зумовлює:

– законодавче визначення повноважень Служби безпеки України з науково-технічного забезпечення процедур захисту об'єктів критичної інфраструктури (у т.ч. реалізації функцій з координації, здійснення контролю та нагляду, експертної оцінки, організації заходів компенсаційного та превентивного характеру тощо);

– створення в системі СБУ науково-дослідних установ, які будуть забезпечувати науково-технічне супроводження функціонування системи аналізу стану критичної інфраструктури та здійснювати експертизу з оцінки прогнозування наслідків впливів на стійкість об'єктів критичної інфраструктури;

– розробку та впровадження необхідного методичного та нормативного забезпечення аналізу та прогнозування наслідків диверсії або терористичних актів.

Одним з важливих елементів цієї системи є створення та впровадження єдиного методичного апарату для проведення технічної та судової експертизи у даній галузі, який має враховувати взаємозв'язки різного рівня між елементами окремого об'єкта, об'єктів між собою, об'єкта та системи, а також різних систем.

Для вирішення цього завдання в Українському науково-дослідному інституті спеціальної техніки та судових експертиз СБУ впроваджено нові експертні спеціальності.

Зокрема, до основних завдань експертизи за спеціальністю 5.3 "Оцінка можливих наслідків застосування вибухового пристрою (вибуху)" належать:

– надання висновку щодо здатності досліджуваного вибухового пристрою (вибухової системи) до вибуху;

– надання оцінки щодо потужності вибуху, наслідків дії вибуху (у т.ч. параметрів вибухової хвилі, фугасної та бризантної дії, радіусу та ступеня осколкових уражень, термічної дії);

– оцінка ступеня ураження факторами вибуху існуючих (розташованих) в межах дії безпосередніх факторів вибуху об'єктів (в т.ч. будівель, споруд, машин, механізмів, транспортних засобів, обладнання тощо), а також людей та інших об'єктів, а за наявності, негативних наслідків іншого характеру;

– оцінка достатності існуючого рівня захищеності об'єктів дослідження до впливу безпосередніх факторів вибуху;

– у разі необхідності обґрунтування рекомендацій з підвищення рівня живучості (стійкості) об'єктів дослідження та систем в цілому;

– встановлення причинових зв'язків між існуючим станом захисту об'єктів дослідження та настанням наслідків в результаті впливу факторів прогнозованого вибуху;

– встановлення причинових зв'язків між діями (бездіяльністю) певних відповідальних осіб та настанням негативних наслідків в результаті застосування вибухових пристроїв (вибуху).

До основних завдань судової експертизи за спеціальністю 5.5 "Оцінка наслідків впливу технічних факторів диверсії (терористичного акту) іншої надзвичайної ситуації" належать:

визначення ступеня впливу на об'єкт дослідження (систему) технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації з оцінкою можливості їх подальшого функціонування;

надання прогнозу розвитку та наслідків каскадної аварії в результаті взаємозалежності суміжних систем об'єктів та впливу на них технічних факторів диверсії, терористичного акту чи іншої надзвичайної ситуації;

визначення необхідних та достатніх вимог забезпечення функціонування об'єкта (системи в цілому) з урахуванням прогнозованого рівня загроз, а також відповідності існуючого стану захисту об'єктів вимогам діючих нормативних актів;

за потреби надання рекомендацій з підвищення рівня захисту об'єктів дослідження та систем в цілому;

встановлення причинових зв'язків між діями чи бездіяльністю певних відповідальних осіб та настанням негативних наслідків в результаті можливої реалізації диверсії чи терористичного акту.

Впровадження зазначених експертних спеціальностей спрямоване на всебічне експертне дослідження аспектів захисту об'єктів критичної інфраструктури, яке передбачає врахування взаємозв'язків різного рівня та різного характеру взаємозалежностей об'єктів та систем.

Для вирішення широкого кола різнопланових завдань з оцінки (прогнозування) наслідків системного характеру (диверсій, терористичних актів чи інших надзвичайних ситуацій) в рамках експертних спеціальностей 5.3 та 5.5 розробляється проект методики, який містить загальний методичний підхід, зміст якого передбачає системне врахування причинових зв'язків різного рівня та характеру.

Такий підхід базується на структуризації наслідків події різного характеру, а саме:

– наслідків І роду – наслідків безпосередньо фізичного впливу на об'єкт дослідження факторів диверсії або терористичного акту;

– наслідків ІІ роду – наслідки, що настають для інших пов'язаних елементів об'єкта в межах однієї системи, і є результатом опосередкованого впливу наслідків І роду на інший його елемент;

– наслідки ІІІ роду – наслідки, що настають для суміжних систем, що пов'язані зв'язками різного характеру (фізичні, інформаційні, геопросторові, процедурні (політичні), соціальні), і є результатом впливу наслідків І та ІІ роду.

Цей системний підхід може слугувати базисом для подальшого удосконалення методичного забезпечення експертних досліджень з оцінки (прогнозування) наслідків диверсії або терористичного акту та аналізу ступеня захисту об'єктів критичної інфраструктури.

Проблема запровадження системного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише понятійного та методологічного апарату. На перше місце висувається завдання створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди ключовим (вузловим) елементам критичної інфраструктури внаслідок дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа [19, с. 3].

Висновки.

На базі аналізу позитивного досвіду США у сфері антитерористичного захисту об'єктів критичної інфраструктури можна дійти висновку, що методичне забезпечення таких об'єктів в Україні потребує вдосконалення за напрямами:

– ідентифікації та градації об'єктів критичної інфраструктури;

– проведення аналізу ризиків та узагальнення вимог до рівнів захищеності (обґрунтування рівнів проектних загроз) об'єктів в залежності від вразливості об'єкта та масштабів його впливу на інші об'єкти та системи;

– аналізу та визначення найбільш ймовірних сценаріїв терористичних актів та диверсій на об'єктах критичної інфраструктури;

– розробки правил антитерористичної безпеки для об'єктів різного функціонального призначення;

– нормативної регламентації діяльності органів і підрозділів СБУ із захисту об'єктів критичної інфраструктури.

Використана література

1. Dudenhoeffer D.D., Permann M.R. and Manic M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. Submitted to Proceedings of the 2006. Conference: Proceedings of the Winter Simulation Conference WSC 2006, Monterey, California, USA, December 3-6. 2006. URL: https://www.researchgate.net/publication/221527820_CIMS_A_Framework_for_ Infrastructure_ Interdependency_Modeling_and_Analysis (дата звернення: 19.06.2020).

2. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287. *Офіційний вісник України*. 2015. № 43. Ст. 1353.

3. Концепція боротьби з тероризмом: Указ Президента України від 5.03.19 р. № 53. *Офіційний вісник України*. 2019. № 21. Ст. 710.

4. Алексеев О.Н. Противодействие терроризму в США: опыт и проблемы. *Теория и практика общественного развития.* 2012. № 7. С. 201-203. URL: https://cyberleninka.ru/article/n /protivodeystvie-terrorizmu-v-ssha-opyt-i-problemy (дата звернення: 19.06.2020).

5. Антипенко А.Ф. Міжнародна кримінологія: досвід дослідження тероризму : монографія. Одеса. Фенікс, 2011. 317 с.

6. Крутов В.В., Форноляк В.М. Система суб'єктів боротьби з тероризмом, їх адміністративно-правовий статус. *Інформаційна безпека людини, суспільства, держави*. 2019. Вип. 2. С. 56-64. URL: http://academy.ssu. gov.ua/ua/page/page_1581342762.htm (дата звернення: 19.06.2020).

7. Кудінов С.С. Міжнародний досвід протидії тероризму та його значення для України. *Вчені записки ТНУ імені В.І.Вернадського*. *Серія: юридичні науки*. 2019. № 1. Т. 30. С. 117-123.

8. Рижов І.М. Базові концепти антитерористичної безпеки: монографія. Київ. Нац. акад. СБУ, 2016. 327 с.

9. Executive Order. 13010. Critical Infrastructure Protection. *Federal Register*. Vol. 61, № 138. July 17. 1996. P. 3747-3750.

10. Кондратьев А. Современные тенденции в исследовании критической инфраструктуры в зарубежных странах. *Зарубежное военное обозрение*. 2012. № 1. С. 19-30. URL: http://pentagon us.ru/publ/sovremennye_tendencii_v_issledovanii_kriticheskoj_infrastruktury_v_zarubezhnoj_stranak h_2012/19-1-0-2082 (дата звернення: 19.06.2020).

11. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT). 2001. URL:http://frwebgate.access.gpo.gov (дата звернення: 19.06.2020)

12. Keating C, Rogers, R., Dryer D., Sousa-Poza A., Safford R., Peterson W., Rabadi G. System of Systems Engineering. *Engineering Management Journal*. 2003. Vol. 15. № 3.

13. Jackson, M. Systems Methodology for the Management Sciences. New York. Plenum, 1991. 298 p.

14. Congressional Research Service Report for Congress. Critical Infrastructures: Background, Policy and Implementation. 2002. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата звернення: 19.06.2020).

15. Rinaldi S., Peerenboom J. and T. Kelly. Idenlifying, Understanding and Analyzing Critical Infrastructure lnterdependencies. IEEE Control Systems Magazine, IEEE, December 2001. P. 11-25.

16. Ted G. Lewis Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation. Naval Postgraduate School Monterey. California. 2006.

17. Pederson P., Dudenhoeffer D. Hartley S., Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research., M. Permann, August 2006. URL: http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20 Modeling.pdf (дата звернення: 19.06.2020).

18. Mussington D. Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development. RAND: Science and Technology Institute, Santa Monica, CA. 2002.

19. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Аналітична доповідь. 2012. 57 с.

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

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

УДК 342.743:347.948+342.9

СВІНЦИЦЬКИЙ А.В., директор Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ПАДАЛКА А.М., *кандидат юридичних наук,* головний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

ПОНЯТТЯ ТА ЗНАЧЕННЯ СУДОВИХ ЕКСПЕРТИЗ У РОЗКРИТТІ Й РОЗСЛІДУВАННІ ОРГАНІЗОВАНОЇ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ У СФЕРІ ОПОДАТКУВАННЯ

Анотація. *У статті розглядаються завдання і предмет судово-економічних експертиз, висвітлюються їх можливості в практиці з розкриття й розслідування організованої злочинної діяльності у сфері оподаткування.*

Ключові слова*: податкові злочини, організована злочинність, судова експертиза, судово-економічна експертиза, податкова експертиза.*

Summary*. The article considers the tasks and subject of forensic economic expertise, highlights its capabilities in practice for the disclosure and investigation of organized crime in the field of taxation.*

Keywords*: tax crime, organized crime, forensic expertise, forensic economic expertise, tax expertise.*

Аннотация. *В статье рассматриваются задачи и предмет судебно-экономических экспертиз, освещаются их возможности в практике раскрытия и расследования организованной преступной деятельности в области налогообложения.*

Ключевые слова*: налоговые преступления, организованная преступность, судебная экспертиза, судебно-экономическая экспертиза, налоговая экспертиза.*

Постановка проблеми. Як відомо, податкові злочини вчиняються суб'єктами у процесі здійснення ними професійної управлінської або фінансово-господарської діяльності й мають вираз в недотриманні норм і правил, що їх регламентують. У зв'язку із цим сліди злочинної діяльності знаходять своє відображення у відповідних документах, котрими ця діяльність оформлюється й супроводжується. Податкові злочини відносяться до групи латентних, доволі часто вони маскуються зовнішньо звичайними і на перший погляд законними господарськими угодами. Зокрема, однією зі специфічних властивостей зазначеної діяльності є функціональне розмежування, тобто виділення у ній певних видів діяльності та виконання її окремими особами чи групами осіб. У свою чергу ця властивість зумовлюється своєрідністю даного виду злочинної діяльності як такої, що розрахована на тривалий період і виявляється у неодноразовості вчинення злочинів, причому вчиненні їх колективно, відносно стабільним складом учасників.

При розслідуванні організованої злочинної діяльності у сфері оподаткування особливе значення мають судово-економічні експертизи, що дозволяють встановити на основі документів бухгалтерського обліку фактичні дані про вчинені фінансово-господарські операції, економічні показники, наявність або відсутність грошових коштів.

В зв'язку з цим неабияке місце в кримінальних провадженнях про податкові злочини, вчинені організованими злочинними групами, мають експертні дослідження, що засновані на використанні прийомів та методів діагностики фінансово-господарського стану підприємства.

Результати аналізу наукових публікацій. Різні аспекти призначення судових експертиз досліджували такі вчені, як Бахін В.П., Бірюков В.В., Волобуєв А.Ф., Галаган В.І., Гора І.В., Іщенко А.В., Карпов Н.С., Клименко Н.І., Лисенко В.В., Лукашевич В.Г., Є.Д. Лук'янчиков, Пиріг І.В., Салтевський М.В., Федчишина В.В., Чернявський С.С., Чеберяк П.П., Чорноус Ю.М., Шепітько В.Ю., Шрамко О.М., Щербаковський М.Г.та ін. Однак питання щодо значення судових експертиз та використання спеціальних економічних знань під час розслідування організованої злочинної діяльності у сфері оподаткування ґрунтовно розглянуто не було.

Метою статті є визначення завдань і предмета судово-економічних експертиз й висвітлення їх можливостей в практиці з розкриття й розслідування організованої злочинної діяльності у сфері оподаткування.

Виклад основного матеріалу. З криміналістичної точки зору, спеціальні економічні знання слід вважати засобом виявлення та розпізнавання ознак взаємодії осіб, що вчиняють злочин з економічною системою та її окремими ланками. Адаптація окремих положень конкретних економічних галузей знань, таких як бухгалтерський облік, банківська справа, ревізія, аудит до потреб розслідування злочинів, а також інтеграція економічних та криміналістичних знань є обов'язковою передумовою підвищення ефективності боротьби з організованою злочинною діяльністю у сфері оподаткування. З цього приводу Чернявський С.С. цілком слушно зазначає, що, наприклад, спеціальні економічні знання експерта, які використовують для вирішення ключових питань у справах про злочини у сфері банківського кредитування, не можуть бути зведені виняткова до бухгалтерських, а вимагають застосування можливостей усього класу економічних експертиз [1, с. 15].

Своєрідність податкових злочинів полягає в тому, що їх виявлення можливе за допомогою податкових перевірок, проте розслідування механізму скоєння цих злочинів, встановлення винних осіб та обсягів завданої шкоди вимагають використання спеціальних знань, зокрема у сфері судово-економічної експертизи.

При розслідуванні організованої злочинної діяльності у сфері оподаткування слідчим, прокурором, судом використовується допомога як спеціаліста, так і експерта, до того ж, і спеціалісти, і експерти можуть бути фахівцями, що обізнані в тій самій галузі економічних знань. Зокрема, експертом можна залучати ту саму особу, що брала участь в провадженні як спеціаліст, оскільки вітчизняне кримінально-процесуальне законодавство не містить будь-якої заборони. Відмінності між спеціалістом і експертом можуть розглядатись в різній площині вирішуваних завдань. Це може стосуватися мети залучення спеціаліста або експерта до досудового розслідування чи судового розгляду кримінального провадження; кола завдань, які ними розв'язуються; форм участі в кримінальному процесі; застосованих методів досліджень; фактичних підстав для прийняття рішення; процесуального статусу результатів роботи спеціаліста чи експерта.

Відповідно до п. 1 ст. 242 КПК України експертиза проводиться експертом за зверненням сторони кримінального провадження або за дорученням слідчого судді чи суду, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання [2].

Ключовим завданням судово-економічної експертизи при розслідуванні організованої злочинної діяльності у сфері оподаткування є встановлення фактичних обставин фінансово-господарської діяльності, а саме:

- виконання (невиконання) вимог законодавства про бухгалтерський облік при відображенні фінансово-господарської діяльності або окремих фінансово-господарських операцій в бухгалтерському обліку і звітності підприємств і організацій;

- відображення (невідображення) в бухгалтерському обліку і звітності підприємств і організацій фінансово-господарської діяльності або окремих фінансово-господарських операцій;

- виконання (невиконання) вимог законодавства про податки і збори щодо обчислення підприємствами і організаціями податків та інших обов'язкових платежів;

- цільовий характер використання коштів, тощо.

Судово-економічна експертиза, як і будь-яка інша судова експертиза, призначається органами досудового розслідування чи судом для вирішення завдань, які пов'язані з предметом доказування. Експертні завдання, що витікають з завдань кожного конкретного злочину, перебувають у певній безпосередній або опосередкованій залежності від сукупності ознак, які характеризують злочин [3, с. 162].

Питання класифікації судово-економічних експертиз є доволі актуальним, оскільки має не лише теоретичне значення для розроблення і вдосконалення теорії судової експертизи, але й слугує основою для розроблення експертних методик, робить об'єктивним процес експертного дослідження і слугує основою для формулювання висновку експерта та його оцінки органами розслідування й судом як джерела доказів. Практика розслідування та розгляду судами податкових злочинів вказує на те, що слідчі, а в багатьох випадках і судді не достатньо інформовані щодо класів, родів судово-економічної експертизи. Доволі часто питання, які ставлять на її вирішення, виходять за межі спеціальних знань експерта, що вказує на проблемність визначення особою, яка призначає експертизу, роду та виду судово-економічної експертизи [4, с. 83]. Немає єдності в підходах до визначення роду судово- економічної експертизи і серед науковців, що зумовлено відсутністю єдиного науково-обґрунтованого підходу до класифікації експертиз, наявністю розбіжностей у формулюванні предмета та об'єкта судової економічної експертизи.

На нашу думку, критерієм класифікації судово-економічних експертиз є галузь економічних знань. Залежно від цього критерію економічні експертизи можна розділити на наступні види:

а) судово-бухгалтерська експертиза, предметом якої є операції фінансово-господарської діяльності, що відображаються в документах бухгалтерського обліку та звітності;

Судово-бухгалтерську експертизу, наприклад, за кримінальними провадженнями про злочини, пов'язані з розкраданням грошових коштів під час розрахунково-касових операцій призначають з метою не лише підтвердити або спростувати обґрунтованість висновків ревізії чи аудиторської перевірки, але й для визначення розміру фактично завданих матеріальних збитків, кола осіб, що причетні до їх завдання, недоліків в організації бухгалтерського обліку і контролю, які мали місце в діяльності підприємства чи установи і сприяли вчиненню злочину. Експертному дослідженню підлягають бухгалтерські документи, які були джерелом аудиторської перевірки чи ревізії, а також встановлені після їх проведення факти і записи в обліку, що мають значення для кримінального провадження. Експерт-бухгалтер використовує формальну, нормативну, арифметичну перевірку, взаємний контроль, зустрічні перевірки взаємопов'язаних

касових операцій. Зустрічною перевіркою прибуткових касових ордерів і квитанцій до них досліджують записи за конкретними фізичними чи юридичними особами, датами, сумами, підписами, штампами з надписами “отримано” або “погашено”, звертаючи при цьому увагу на наявність підписок, дописок або виправлень [4, с. 84].

Залежно від конкретної ситуації і сутності обставин, що досліджуються під час кримінального провадження, на вирішення експерту-бухгалтеру можуть бути поставлені різноманітні питання, наприклад: чи правильно відображені касові операції з формування засновниками статутного капіталу; чи мали місце в діяльності організації порушення порядку ведення касових операцій з приймання і повернення грошових коштів; чи правильно відображені в касових документах операції з обліку і реалізації акцій; чи правильними є висновки ревізії щодо суми виявленої в касі підприємства нестачі або надлишків і щодо винних у їх завданні особах; які недоліки в організації бухгалтерського обліку, звітності, контролю сприяли утворенню і приховуванню збитків і заважали їх своєчасному виявленню тощо [5, с. 39].

В такому випадку для комплексного дослідження зазначених документів і встановлення фактів зловживання, розкрадання та винних осіб, а також встановлення точної суми викрадених грошей доцільно призначати ревізії, а після їх проведення судово-бухгалтерські і почеркознавчі експертизи. На важливість своєчасного призначення зазначених ревізій та експертиз і використання спеціальних бухгалтерських знань вказує і Федчишина В.В., звертаючи увагу на ймовірність втрати можливості з’ясування певного або іншого питання [5, с. 40].

б) фінансово-економічна експертиза, що включає:

- дослідження ознак і способів спотворення даних про фінансові показники, що впливають на фінансовий результат і розрахунки за зобов’язаннями господарюючого суб’єкта;

- розрахунок пайової участі засновників (акціонерів) в майні і розподіленого прибутку господарюючого суб’єкта;

Чеберяк П.П. вважає, що предмет фінансово-економічної експертизи – це відображена в документах інформація щодо фінансово- економічних показників діяльності підприємства, акціонування, банкрутства, орендних відносин, цільового використання бюджетних коштів, які стали об’єктом розгляду судово-слідчими органами і відносно яких поставлені питання на вирішення експерта. Предметом фінансово-кредитної експертизи є відображені в документах господарські операції банків і підприємств при взаємовідносинах з банками, що стали об’єктом розгляду судово- слідчими органами, відносно яких поставлені питання на вирішення експерта. Від правильного визначення предмета експертизи залежить практична діяльність експерта, межі його компетенції в аспекті визначення кола питань, які він може вирішувати. Предмет експертизи – її суттєва ознака, котрою визначаються природа та джерела знань експерта будь-якої спеціальності [4, с. 85].

На нашу думку, всі різновиди судово-економічних експертиз досліджують один об’єкт – обліково-економічні операції. За такої ознаки судово-економічні експертизи можна класифікувати на експертизу облікового процесу та експертизу економічних операцій. Предметом експертизи облікового процесу виступають закономірності інформаційного відображення економічної діяльності в системі бухгалтерського обліку фактів господарської діяльності суб’єктів господарювання, котрі досліджуються для вирішення завдань, які виникають при розслідуванні злочинів економічної спрямованості. Об’єктами такої експертизи виступають факти господарської діяльності та облікова процедура. Предметом експертизи економічних операцій виступають

закономірності інформаційного відображення економічної діяльності в системі економічних показників та іншої обліково-економічної інформації, яка розкриває зміст економічних операцій, що досліджуються для вирішення завдань з розкриття й розслідування економічних злочинів. Об'єктами такої експертизи є економічні операції [6, с. 181].

в) фінансово-кредитна експертиза, в ході якої проводиться дослідження ознак і способів спотворення даних про фінансові показники, що характеризують платоспроможність, кредитоспроможність, використання і повернення кредитів господарюючого суб'єкта.

З урахуванням зазначених видів економіко-експертних досліджень, всі питання, які вирішує експерт-економіст, можна розділити на наступні групи:

- питання, пов'язані з відображенням або невідображенням в бухгалтерському обліку господарських операцій;
- питання, пов'язані з правильністю відображення в бухгалтерському обліку господарських операцій;
- питання, пов'язані з повнотою і правильністю обчислення податків;
- питання, пов'язані з розрахунком грошових потоків;
- питання, пов'язані з розрахунком товарних потоків;
- питання, пов'язані з правильністю витрачання отриманих коштів.

Також ключовими обставинами доказування в розслідуванні організованої злочинної діяльності у сфері оподаткування є використання незаконних схем та методів, встановлення сум ухилення, виявлення організаторів, пособників, виконавців. Більшість схем ухилення від оподаткування всередині країни існують завдяки розвинутій індустрії "конвертаційних центрів", підґрунтям для яких є фіктивне підприємництво. Фіктивним підприємництвом у розумінні сфери податків є використання контролю над суб'єктом підприємництва з метою приховування незаконної діяльності, зокрема для вчинення дій, спрямованих на уникнення або ухиляння від сплати податків. Функціонування подібних підприємств, як правило, добре продумано, а мережа клієнтів територіально розгалужена, вони можуть співпрацювати з десятками реальних суб'єктів господарювання.

Відповідно, щоб дослідити ці схеми з економічної позиції, необхідно залучати висококваліфікованих, добре підготовлених фахівців (експертів) у сфері економіки, навіть у тих ситуаціях, якщо слідчий володіє спеціальними навичками на рівні експерта-економіста. Адже він не має права суміщати в одній особі функції органу розслідування та експерта. Схема функціонування "конвертаційного центру" з використанням фіктивних підприємств з метою ухилення від сплати податків полягає в наданні послуги реально діючим суб'єктам господарювання у формуванні безпідставного та незаконного податкового кредиту та витрат, переведення податкових зобов'язань з ПДВ на фіктивні підприємства, отримання готівкових коштів й використання їх у нелегальному бізнесі або на власні потреби. Штучне нарощування податкового кредиту відбувається шляхом здійснення безтоварних операцій, які присутні в офіційному бухгалтерському, податковому обліку та звітності фіктивного підприємства, а також відповідні податкові зобов'язання з ПДВ. У подальшому такий податковий кредит "продається" реально діючим підприємствам з метою зменшення сплати ПДВ, при цьому самі операції існують лише на папері.

Розслідування діяльності організованої злочинності характеризується багатоепізодністю, великим обсягом матеріалів, які охоплюють значні звітні періоди, тому потребує ретельної побудови доказової бази у доведенні як незаконної діяльності

фіктивних підприємств, що входять до його складу, так і протиправних дій клієнтів – реальних суб'єктів підприємницької діяльності. Отримання таких доказів неможливе без документального підтвердження цих фактів, основою чого є висновок, підготовлений відповідним фахівцем-експертом. Специфіка податкових розслідувань злочинів з використанням фіктивного підприємництва визначає особливості проведення судово-економічної експертизи. Зокрема, це стосується визначення пріоритетних напрямів дослідження, встановлення предмета, об'єктів та завдань експертизи. Для підтвердження фактів ухилення від оподаткування недостатньо проводити дослідження документів бухгалтерського, податкового обліку та звітності з метою встановлення інтелектуальних підробок, тобто неправильного відображення в документах руху матеріальних цінностей, грошових коштів, порушення правил обліку, оскільки фіктивне підприємство надає документи клієнту (для незаконного збільшення ПДВ та витрат), які за формальними ознаками не містять слідів фальсифікацій і повністю відповідають вимогам законодавства. Тому необхідним є використання фінансово-економічного напряму дослідження, який ґрунтується на застосуванні прийомів і методів діагностики фінансово-господарської діяльності суб'єкта господарювання.

Дослідження за цим напрямом передбачає встановлення документальної обґрунтованості даних про спроможність суб'єктів господарювання фактично здійснювати операції, які відображені в бухгалтерському, податковому обліку, звітності та утворюють підстави для формування незаконного податкового кредиту та витрат. Такі дослідження дають можливість, з одного боку, отримати додаткові докази удаваності операцій підприємств, що входять до складу організованої злочинності, а з іншого – підтвердити умисне ухилення від сплати податків його клієнтами.

Звертаючи увагу на те, що предметом конкретного експертного дослідження є фактичні дані, які необхідно встановити щодо конкретного розслідуваного злочину, предметом судово-економічної експертизи з питань ухилення від сплати податків організованою злочинною групою є факти безпідставного і незаконного формування податкового кредиту та витрат внаслідок проведення безтоварних операцій, які відображені в первинних документах бухгалтерського обліку та стали об'єктом розгляду слідчими органами ДФС і стосовно яких поставлені питання на вирішення експерта. При цьому головним завданням є документальне підтвердження фактів, які формують предметну сферу експертного дослідження. Вирішення завдання потребує оцінки показників структури майна та джерел його придбання, наявності та інтенсивності використання необоротних та оборотних активів і джерел їх формування, джерел власних коштів, реальності розрахунків із дебіторами і кредиторами, аналізу економічної доцільності проведення окремих господарських операцій та аналізу інших питань, пов'язаних із предметом дослідження.

Отже можемо стверджувати, що судові експертизи є специфічним засобом встановлення доказів у кримінальному судочинстві. Вони характеризуються такими основними ознаками: використання спеціальних знань; проведення дослідження з метою встановлення обставин, які мають важливе значення для вирішення провадження; процесуальна форма призначення та проведення експертизи; оформлення результатів у спеціальному процесуальному документі; безпосереднє дослідження об'єктів експертизи [7, с. 517].

Якщо в обґрунтуванні поділу судової експертизи на різні види можна визначити певні критерії (вид спеціальних знань, предмет, об'єкти і методи), то поділ щодо економічної експертизи має іншу природу. Судово-економічна експертиза, як підкреслюється в літературі, з одного боку, виступає як спеціальна наука, а з іншого –

як загальна наука (щодо галузевих економічних дисциплін). При цьому, по суті, відіграє роль загальнотеоретичної методологічної науки, виступає як засіб, інструмент пізнання конкретних економічних дисциплін, їх інститутів, окремих норм права. Теорія судово-економічної експертизи не повинна давати готових рецептів щодо окремих економічних дисциплін. Вона має розробляти методику вирішення окремих проблем і, у свою чергу, вирішувати загальні для ряду економічних наук питання, зокрема про критерії їх розмежування. При цьому, беручи до уваги специфіку окресленої проблеми та появу нових схем злочинності у сфері оподаткування і трансфертного ціноутворення, потрібно враховувати, що вирішення питань з оподаткування зумовлює необхідність у виділенні податкової експертизи у самостійний вид експертиз.

І тому на сьогодні для України значимим є вирішення питань, безпосередньо пов'язаних із судовою податковою експертизою та використанням спеціальних знань з питань правильності нарахування і сплати податків. Визнаючи самостійне існування судової податкової експертизи як виду, необхідно встановити її предмет, об'єкти, відмежувавши її від судово-економічних експертиз. Хоча нормами Податкового кодексу України (далі – ПК України) визначено порядок узгодження термінології та правил податкового обліку із правилами бухгалтерського обліку та документування операцій відповідно до правил бухгалтерського обліку та фінансової звітності, однак, під впливом багатьох факторів, перш за все появи нових ускладнених схем злочинів у сфері оподаткування, вирішувати питання оподаткування в межах судово-економічних експертиз стає дедалі важче. І саме такі обставини суттєво обмежують можливості проведення економічних експертиз і дають поштовх до проведення самостійного виду економічних експертиз – податкової експертизи, яка передбачає потребу в отриманні експертом широких знань у сфері оподаткування як самостійного напряму економічної науки. Тобто необхідно розглядати питання застосування спеціальних знань експерта в оподаткуванні, а не в економічній науці взагалі.

Судово-податкова експертиза, досліджуючи первинні облікові документи, реєстри бухгалтерського обліку і фінансової звітності, проводитиме дослідження щодо підтвердження або не підтвердження повноти і правильності нарахування податків і зборів, порушення вимог податкового законодавства. На нашу думку, виділення окремого виду податкової експертизи процесуального значення не має, проте має велике практичне значення.

Висновки.

З вище викладеного можемо стверджувати, що судово-економічна експертиза є одним із засобів доказування у кримінальних провадженнях з питань ухилення від сплати податків. Основне призначення експертних досліджень полягає у формуванні повної доказової бази, що надає сторонам кримінального провадження значно ширших можливостей у доказуванні. Проведення експертизи в процесі розслідування схем ухилення від оподаткування повинно враховувати їх розмаїття та наявність особливостей у механізмі їх вчинення.

У теорії судово-економічної експертизи є багато напрямів, які, гарантуючи кваліфіковане, науково і методично забезпечене дослідження об'єктів, мають значення для встановлення обставин злочину. У більшості з них уже є своя історія, наукова основа та емпірична база. Тому при розслідуванні організованої злочинної діяльності у сфері оподаткування нами пропонується виділити самостійний вид судових експертиз – "податкова експертиза". Виконуючи поставлені завдання, податкова експертиза могла б більш точно досліджувати питання, пов'язані з дослідженням об'єктів –

первинних бухгалтерських документів, реєстрів бухгалтерського обліку і фінансової звітності, встановлюючи обґрунтованість застосування норм податкового права суб'єктами господарювання, виконання ними зобов'язань, підтверджуючи факти ухилення від сплати податків.

Використана література

1. Чернявський С.С. Методика розслідування злочинів у сфері банківського кредитування: автореф. дис. …канд. юрид. наук: спец. 12.00.09. Київ, 2002. 20 с.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 27.07.2020).

3. Шрамко О.М. Можливості судово-економічних експертиз при розслідуванні окремих корупційних злочинів. *Актуальні проблеми правознавства.* 2019. Вип. 1. С. 162-165.

4. Чеберяк П.П. Завдання судових експертиз при розкритті й розслідуванні злочинів, вчинених в економічній сфері України. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 10. С. 83-88.

5. Федчишина В.В. Щодо окремих аспектів податкової експертизи. *Фінансове право.* 2016. № 1 (35). С. 38-42.

6. Давиденко В.С. Спеціальні знання в розслідуванні економічних злочинів. *Юридичний часопис Національної академії внутрішніх справ.* 2016. № 2. С. 178-188.

7. Федчишина В.В. Місце спеціальних економічних знань в інституті судової експертизи України. *Управління публічними фінансами та проблеми забезпечення національної економічної безпеки*: зб. тез Податкового конгресу, м. Ірпінь, 12 грудня 2019 р.. Ірпінь: Університет ДФС України, 2019. С. 517-520.

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

УДК 343.14

КРИВЕНКО А.Л., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ.

ШЛЯХИ ПРОТИДІЇ КОРУПЦІЇ У СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ

Анотація. *У статті здійснено аналіз та запропоновано шляхи протидії явищу корупції у сфері державних закупівель. Зазначається, що феномен корупції універсальний для будь-якого суспільства, який відрізняється лише масштабом і формами його прояву. Аналізується державна політика протидії корупції в країнах ЄС в контексті запозичення позитивного зарубіжного досвіду для України та удосконалення національного законодавства у сфері державних закупівель.*

Ключові слова: *державні закупівлі**,** державна політика, протидія корупції, феномен корупції, антикорупційні заходи, державні закупівлі.*

Summary. *The article analyzes and suggests ways to combat corruption in public procurement. It is noted that the phenomenon of corruption is universal for any society, which differs only in the scale and forms of its manifestation. Article analyzes the state policy of anti-corruption in the EU countries in the context of borrowing positive foreign experience for Ukraine and improving national legislation in the field of public procurement.*

Keywords: *public procurement, state policy, combat corruption, phenomenon of corruption, anti-corruption measures, public procurement.*

Аннотация. *В статье осуществлен анализ и предложены пути противодействия явлению коррупции в области государственных закупок**.** Отмечается, что феномен коррупции универсален для любого общества, отличается только масштабом и формами его проявления. Анализируется государственная политика противодействия коррупции в странах ЕС в контексте заимствования положительного зарубежного опыта для Украины и усовершенствования национального законодательства в государствнных закупок.*

Ключевые слова: *государственные закупки, государственная политика, противодействия коррупции, феномен коррупции, антикоррупционные меры, государственные закупки.*

Постановка проблеми. Державні закупівлі як засіб державного регулювання економіки забезпечують розвиток і функціонування всіх сфер економіки країни. За допомогою державних закупівель держава задовольняє свої потреби в тих чи інших товарах, роботах чи послугах, забезпечує і фінансує бюджетні та позабюджетні державні заклади.

Незважаючи на досить ефективну систему правового регулювання державних закупівель і детально вибудувану систему державного контролю в даній сфері, викорінити корупцію в держзакупівлях не вдалося жодній державі.

Корупція в системі держзакупівель призводить до колосальних втрат для будь-якої країни, причому не тільки фінансових.

Результати аналізу наукових публікацій. Серед українських та зарубіжних науковців, у працях яких досліджувалася окреслена проблематика, варто назвати таких, як Закалюк А., Кузьмін А., Супрун Т. [1], Трепак В., Чебоксаров П., Фрідріх К., Д. Саймон, Д. Ейтцен, Дж. Най, С. Роуз-Аккерман, Гаращук В., Мухатаєв А., Пархоменко-Куцевіл О. [2], Шестопалова Л. [3].

Ці вчені зробили вагомий внесок у розробку теоретичної моделі запобігання та протидії корупції та вдосконалення практичних аспектів діяльності з цих питань. Однак швидке оновлення антикорупційного законодавства потребує постійного перегляду існуючих підходів до розуміння окреслених питань.

Проте, незважаючи на те, що проблематика протидії корупційним проявам знайшла своє часткове висвітлення в певних наукових працях, окремі її аспекти стосовно протидії корупції у сфері державних закупівель є актуальними і залишаються ще недостатньо вивченими.

Метою статті є визначення на підставі аналізу вітчизняного антикорупційного законодавства та зарубіжного досвіду шляхів протидії корупції у сфері державних закупівель.

Виклад основного матеріалу. Зародження і еволюція корупційних відносин як в Україні, так і в інших країнах світу відбувалося паралельно розвитку і становленню державних інститутів, влади. Поява і зростання "попиту" і "пропозиції" на ринку корупційних послуг були обумовлені наявністю в системі державних інститутів осіб, наділених правом прийняття рішень, владними повноваженнями, в тому числі в частині розподілу та перерозподілу фінансових і матеріальних ресурсів.

Розвиток економічних відносин, економічних взаємозв'язків, міжнародних ринкових відносин, процеси глобалізації, науково-технічний прогрес привели до еволюції корупції і корупційних оборудок, способів і характеру їх здійснення. Корупція як складне явище піддається різним формам інтерпретації в економічній теорії.

Відповідно до положення Закону України "Про засади запобігання та протидії корупції" від 07.0411 р. № 3206-УІ [4] під корупцією розуміється використання особою наданих їй службових повноважень та пов'язаних із цим можливостей з метою одержання неправомірної вигоди або прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди такій особі або на її вимогу іншим фізичним та юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень та пов'язаних з цим можливостей.

Сучасна корупція несе в собі загрозу для економічної та соціальної безпеки України, її наслідки виражаються в зниженні інвестиційної привабливості економіки України, ухиленні від сплати податків, неправомірне звільнення від сплати обов'язкових платежів, зниження фінансової захищеності країни. Все це диктує необхідність вироблення ефективних механізмів протидії виникненню і поширенню корупції, які також схильні до еволюції внаслідок розвитку корупційних процесів.

З огляду на те, що "корупційні" угоди найчастіше вигідні з фінансово-економічної точки зору всіх учасників корупційних процесів, то створення державою системи боротьби з корупцією, яка зачіпає її інтереси, як правило, натрапляє на активну протидію з боку корумпованих представників владних структур, що обумовлено зрощенням бюрократії і бізнесу. Одним з основних сегментів економічної безпеки держави, якому корупція завдає відчутної шкоди, є фінансово-бюджетна безпека, що є основоположною умовою здатності держави проводити політику щодо захисту національних інтересів. Таким чином, саме вироблення механізмів боротьби з корупцією, що забезпечують бюджетну безпеку нашої країни, буде сприяти появі можливості зміцнення безпеки країни.

Ефективна протидія корупції в системі державних закупівель неможлива без розробки і впровадження надійних механізмів, інструментів і технологій боротьби з корупцією.

Існують питання ефективного запобігання та протидії корупції як однієї з найважливіших проблем, яку намагається вирішити сучасне українське законодавство. Актуальність цієї проблеми полягає в тому, що корупція провокує і посилює соціальні кризи, підриває імідж України на світовій арені, негативно впливає на мікро- та макроекономічні процеси, перешкоджає встановленню конструктивного діалогу між владою та громадськістю, руйнує принципи побудови верховенства права та громадянського суспільства. Звідси розвиток і реалізація антикорупційних заходів є головним пріоритетом і завданням державної влади.

Дослідники приділяють велику увагу запобіганню та боротьбі з корупцією у сферах забезпечення прозорості державної служби та законодавства. Можна вважати, що такий підхід до цього питання був продиктований особливостями соціально-економічних, політичних, законодавчих процесів та умов, які визначають фокус антикорупційних заходів.

Як зазначає Молдован Е., найбільша кількість антикорупційних заходів на державній службі поєднують у собі організаційні та управлінські напрями (скорочення кількості функцій державних служб із реалізації застосування неправомірної вигоди; чітке законодавче визначення порядку прийняття управлінських рішень; оптимізація кількості станів, які мають структуруватися з метою уникнення паралелізму на роботі, зменшення кількості контрольних та моніторингових інстанцій) [5, с. 2-15].

Деякі проекти створюються спеціально для того, щоб певні групи отримували ренту (“державну” або “адміністративну”) від осіб, які є виконавцями проекту. Державні закупівлі, як правило, припускають вибір об’єктивно кращої пропозиції з декількох на основі конкурсу, проте іноді чиновник може забезпечити перемогу продавця, який пообіцяв найбільші “комісійні” (“відкат”) з операції. Для цього обмежується участь у конкурсі, його правила повністю не оголошуються. Як наслідок, закупівлі здійснюються за завищеною ціною. Позабюджетні рахунки часто створюються з легітимною метою (пенсійні, дорожні фонди тощо). Проте в деяких фондах, наприклад для допомоги інвалідам, доходи можуть значно перевищувати реальні витрати, що стимулює бажання деяких чиновників привласнити “надлишки”. Навпаки, у разі дефіциту чиновники часто вирішують на власний розсуд, хто в результаті отримає гроші. У деяких країнах кошти, отримані через іноземну допомогу або від продажу природних ресурсів, надходять до спеціальних фондів, які менш прозорі й гірше контролюються, ніж бюджетні гроші. Через часті коливання цін на товари визначити дійсну суму транзакції і величину відрахувань до цих фондів непросто, що дозволяє частину грошей перенаправляти в кишені чиновників [2].

Також громадяни України вказують, що тендери на державні закупівлі виграють зазвичай ті, хто надав керівництву підприємства від 10 до 30 % грошей від суми закупівлі. Відсутність контролю за такими правопорушеннями з боку уповноважених органів пояснюється, насамперед, низьким професіоналізмом кадрів, недосконалим здійсненням оперативно-розшукової діяльності та небажанням втручатися у справи, в яких задіяні їх родичі чи знайомі.

Український парламентарій Стретович В.свого часу навів реальний приклад дії корупційних схем: “Зі слів директора Інституту серцево-судинної хірургії ім. М. Амосова, ціна одного й того ж клапана для серця за тендером становить 29 тис. грн., а без тендера – 20 тис. грн. Таким чином, замість прооперованих двох можна було б прооперувати трьох осіб. Так корупція відображається на здоров’ї та стані нашого суспільства” [5; 6].

Протидію корупції можна розглядати в якості найважливішої мети державних закупівель, оскільки без чесної і сумлінної поведінки фахівців із закупівель неможливо придбати товари, роботи і послуги за найкращою ціною і кращої якості, а отже, і реалізувати інші цілі державних закупівель. У такому випадку для протидії корупції в сфері державних закупівель, слід запропонувати активну роботу з мінімізації корупційних відносин методами кадрового та адміністративного характеру. Так як основна частка порушень – результат усвідомлених і цілеспрямованих дій з боку осіб, які оголосили торги, зважаючи на наявність у них неправомірних інтересів з приводу предмета аукціону або конкурсу [1].

Корупційні правопорушення в сфері держзакупівель відбуваються завжди навмисне, бо неможливо уявити собі отримання посадовцем корисливої вигоди випадково, "з необережності".

У наукових дослідженнях, присвячених аналізу проблем державних закупівель, виявлено залежність ефективності функціонування системи держзакупівель від ефективності адміністративно-правового регулювання кадрового забезпечення управління в даній сфері, в тому числі від кількості зайнятих фахівців, рівня їх підготовки, кваліфікації та правової культури, матеріального забезпечення [2].

Недостатня кваліфікація відповідних фахівців, в тому числі юристів, є серйозною проблемою господарської діяльності державних (муніципальних) організацій щодо укладення договорів [5]. Антикорупційні кадрові технології в сфері державних закупівель можна визначити як сукупність прийомів і засобів, пов'язаних з підбором, розстановкою, навчанням, вихованням, професійною перепідготовкою та підвищенням кваліфікації, а також здійсненням контролю за діяльністю працівників державних органів та організацій, в чиї трудові (службові) обов'язки входить виконання окремих функцій щодо здійснення державних закупівель товарів, робіт і послуг [6].

Отже, антикорупційні кадрові технології в сфері державних закупівель являють собою певну систему, основними елементами якої є:

- пред'явлення відповідних кваліфікаційних вимог до персоналу організації-закупника, членам конкурсних (аукціонних) комісій, експертам;
- професійна підготовка, перепідготовка, підвищення кваліфікації працівників органів і організацій, що здійснюють закупівлю;
- антикорупційне навчання і виховання зазначених осіб;
- вжиття заходів щодо запобігання та врегулювання конфлікту інтересів у сфері закупівель товарів, робіт і послуг;
- здійснення контролю за доходами та витратами осіб, які здійснюють діяльність в сфері державних закупівель.

До методів боротьби з проявом корупції в сфері держзамовлення, застосовуваних безпосередньо стосовно службовця, зайнятого в сфері закупівель, можна віднести:

- перевірку анкетних даних, біографії кандидата та відгуків з попередніх місць роботи;
- спеціальні глибинні тестування кандидатів при прийомі на роботу, що дозволить отримати досить чіткий психологічний портрет, в тому числі, з точки зору потенційної схильності до незаконного збагачення за рахунок роботодавця;
- ефективну мотивацію співробітників. У європейських країнах чиновники, що відповідають за державні закупівлі, виділені в окрему категорію державних службовців і отримують більш високу винагороду за свою роботу в порівнянні з іншими своїми колегами – своєрідну "доплату за чесність". Це підтримує престиж професії;

- ротація співробітників, зайнятих в сфері держзакупівель, що дозволяє зруйнувати наявні у недобросовісних чиновників домовленості з постачальниками (виконавцями) – формування корпоративної етики нетерпимості до корупції [7].

Ще одним методом боротьби з проявом корупції в сфері держзамовлення є впровадження в практику проведення антикорупційної експертизи документації про закупівлі.

Об'єктом даної експертизи є такі документи:

1) повідомлення про закупівлю;

2) інструкції учасникам;

3) форми заявок та інших документів, які подаються претендентами на участь в конкурентних процедурах;

4) технічне завдання;

5) проект контракту;

6) інші документи в залежності від форми конкурентної процедури [7].

Метою антикорупційної експертизи документації щодо закупівлі є виявлення корупціогенних чинників, тобто таких положень (невідповідність початкової (максимальної) ціни товарів, що закуповуються, робіт, послуг за середньоринковими цінами на даний тип і чи вид товарів, робіт, послуг; нереальні терміни виконання контракту, "заточування" під певний вид товару, завищені вимоги до учасника процедури закупівлі та інше), які можуть створити умови для виникнення корупційних відносин, і вироблення пропозицій щодо їх усунення.

Частково цю проблему законодавець намагається вирішити впровадженням уніфікованих типових документів, що застосовуються в закупках: типові контракти, каталог товарів, робіт, послуг, граничні терміни оплати. Але держзакупівлі поширюються на різні сфери діяльності замовників, тому дані типові форми не враховують всієї специфіки та складності окремих закупівель. Даний вид антикорупційної експертизи документації слід розглядати як контроль, що проводиться до розміщення замовлення, що запобігатиме саме прояву корупції. При цьому слід враховувати особливості і специфіку діяльності замовника (охорона здоров'я, будівництво, НДР і т. д.), так як експерт по виявленню корупціогенних чинників повинен володіти спеціальними знаннями не тільки в області договірних правовідносин, а й знати предмет замовлення, умови виконання контракту в умовах діяльності замовника [3].

Висновки.

Усунення корупції можна розглядати в якості найважливішої мети державних закупівель, оскільки без чесної і сумлінної поведінки фахівців із закупівель неможливо придбати товари, роботи і послуги за найкращою ціною і кращої якості, а отже, і реалізувати інші цілі державних закупівель. У такому випадку для усунення корупції в сфері державних закупівель ми пропонуємо активну роботу з мінімізації корупційних відносин методами кадрового та адміністративного характеру, так як основна частка порушень – результат усвідомлених і цілеспрямованих дій з боку осіб, які оголосили торги, зважаючи на наявність у них неправомірних інтересів з приводу предмета аукціону або конкурсу. Корупційні правопорушення в сфері держзакупівель є завжди навмисними, бо неможливо уявити собі отримання чиновником корисливої вигоди випадково, "з необережності".

Повністю викорінити корупційні прояви в державних закупівлях, на жаль, не вдалося жодній країні, проте це зовсім не означає, що немає ефективних заходів щодо її зниження. Справа в тому, що в даний час основні зусилля контролюючих

органів спрямовані на усунення наслідків вже скоєних правопорушень та злочинів у сфері державних закупівель, а не на профілактику та запобігання корупції та інших порушень.

Використана література

1. Супрун Т. Зарубіжний досвід запобігання та протидії корупції. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2017. № 2. С. 199-204.

2. Пархоменко-Куцевіл О. Теоретико-методологічні підходи до класифікації корупційних відносин в Україні. *Підприємництво, господарство і право*. 2018. № 9. С. 138-142.

3. Шестопалова Л. Відмежування корупційних правопорушень від правопорушень, пов'язаних із корупцією. *Підприємництво, господарство і право.* 2017. № 5. С. 193-197.

4. Про засади запобігання та протидії корупції: Закон України від 7.04.11р. № 3206-VI. URL:www.rada.gov.ua

5. Доненко В. Правові та організаційні засади протидії корупції: конспект лекцій. 2019. 123 с. (ДДУВС).

6. Ржеутська Л. Які органи в Україні борються з корупцією. *Made for minds*. 2019. URL: https://www.dw.com/uk.

7. Шапка Б.В. Удосконалення антикорупційного законодавства на засадах світових стандартів. URL: https://minjust.gov.ua/m/str_31896

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

УДК 34-058.87:340.13:316.64:007

РОМАНІВ Х.Б., *кандидат юридичних наук,* доцент кафедри цивільно-правових дисциплін, Львівський державний університет внутрішніх справ.

РОЛЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ФОРМУВАННІ ПРОФЕСІЙНОЇ ПРАВОСВІДОМОСТІ СТУДЕНТІВ-ЮРИСТІВ

Анотація. *У процесі набуття правових знань з використанням інформаційно-комунікаційних технологій відбуваються найбільш прогресивні форми впливу на свідомість індивіда, тому головною ознакою інформаційно-комунікаційних технологій у правовій освіті є формування професійної правосвідомості. Підкреслено, що інформатизація правової освіти повинна здійснюватися в межах двох основних цілей: 1) забезпечення випускників вищого юридичного навчального закладу рівнем професійних знань та навичками їх умілого застосування у процесі практичної діяльності; 2) підвищення рівня інформаційної компетентності у майбутнього фахівця з галузі права через інтегрування інформаційно-комунікаційних технологій у навчальну діяльність.*

Ключові слова: *інформаційно-комунікаційні технології, правова освіта, правосвідомість, компетентність, правова інформація, правові знання.*

Summary. *In the process of acquiring legal knowledge using information and communication technologies, the most progressive forms of influence on the individual's consciousness occur; therefore, the main feature of information and communication technologies in legal education is the formation of professional legal consciousness. It was emphasized that informatization of legal education should be carried out within two main objectives: 1) provision of graduates of a higher educational law establishment with the level of professional knowledge and skills for their proficient application in the process of practical activity; 2) raising the level of information competence of a future expert in the field of law through the integration of information and communication technologies into educational activities.*

Keywords: *information and communication technologie, legal education, legal consciousness, competence, legal information, legal knowledge.*

Аннотация. *В процессе приобретения правовых знаний с использованием информационно-коммуникационных технологий происходят наиболее прогрессивные формы воздействия на сознание индивида, так главным признаком информационно-коммуникационных технологий в правовом образовании является формирование профессионального правосознания. Подчеркнуто, что информатизация правового образования должна осуществляться в пределах двух основных целей: 1) обеспечение выпускников высшего юридического учебного заведения уровнем профессиональных знаний и навыками их умелого применения в процессе практической деятельности; 2) повышение уровня информационной компетентности у будущего специалиста в области права через интегрирование информационно-коммуникационных технологий в учебную деятельность.*

Ключевые слова: *информационно-коммуникационные технологии, правовое образование, правосознание, компетентность, правовая информация, правовые знания.*

Постановка проблеми. З винаходом комп’ютера, а згодом із створенням всесвітньої комп’ютерної мережі Інтернет змінилося людське життя і ці зміни також торкаються системи освіти. Інформаційно-комунікаційні технології (далі – ІКТ) стали основою кожного суспільного сектору, без ІКТ не може обійтися й освіта. Тому, комп’ютери та пов’язані з ними інформаційно-комунікаційні технології є основою інформатизації освіти.

Інтеграція ІКТ в освіту є важливою умовою для вдосконалення процесу навчання, що зумовлено необхідністю розробки нової моделі системи освіти. Сучасне інформаційне суспільство вимагає нових технологій роботи з навчальною інформацією, оскільки тенденція розвитку суспільства XXI ст. мотивує розширення напрямів використання ІКТ у освітній сфері. На сьогодні, використання ІКТ є обов'язковим атрибутом професійної діяльності чи не для всіх суспільствознавчих дисциплін, не винятком у цьому правилі є і правознавство.

Сучасна юридична діяльність нерозривно пов'язана з ІКТ, а тому інформаційна культура, як складова професійної правосвідомості студента-юриста є не менш актуальною, адже фахівець-юрист нового покоління має ефективно застосовувати отримані знання, впливати на розвиток демократичної, правової держави і громадянського суспільства.

ІКТ сприяє утворенню єдиного європейського освітянського простору та фаховому зростанню майбутніх юристів. Окрім того, прискорення темпів створення і поширення інформації дозволяє розширювати правнику-студенту свій інтелектуальний потенціал. Адже у своїй професійній діяльності юрист зіштовхується з опрацюванням великих обсягів правової інформації, яка пов'язана з різними юридичними фактами, правопорушеннями та їх подоланням, різноманітними правовідносинами і правопорядком. Для оперативного вирішення правових ситуацій юрист повинен застосовувати ІКТ, які мають допомогти систематизувати та забезпечити швидкий доступ до правової інформації. Відповідно, на сьогодні, важливо навчити студента-юриста не лише базовим правовим знанням, але й вмінню оперативно реагувати та находити вирішення різноманітних правових ситуацій.

Результати аналізу наукових публікацій. Проблема формування професійної правосвідомості студента-правника за допомогою ІКТ у науковій літературі не розроблялася. Однак, окремі автори розкривають наближені до обраної нами теми, а саме: використання ІКТ у освіті, зокрема у правовій. До таких дослідників відносимо: Гершунского Б.С., Гуревич Р.С., Зелінську В.А., Кадемію М.Ю., Козер М.М., Луппу В.А., Логінову Н.І., Нетьосова С.І., Русіну Н.Г., Савченко І., Федорчук О.С., Шермана М.І., Шийку С.В., Шмирова О.В. та ін.

Широке розповсюдження комп'ютерних технологій вимагає розроблення якісно нових підходів до підготовки фахівців, у тому числі юристів. Відповідно навчання повинне передбачати не лише володіння знаннями у різних галузях права, але й з знаннями, пов'язаними з ІКТ, тобто сучасне суспільство вимагає вміння залучати комп'ютерні технології у своїй професійній діяльності.

За допомогою методів і засобів навчання, студент-юрист має навчитися одержувати відповіді на питання про те, які є інформаційні ресурси у галузі права, де вони розміщені, як можна одержати доступ до них і як вони допоможуть при підвищенні ефективності юридичної діяльності.

Водночас однією з актуальних проблем є готовність викладача до впровадження ІКТ у навчальний процес для вирішення педагогічних завдань. Для забезпечення якісної підготовки студентів-юристів необхідно готувати викладача нової формації, здатного ефективно впроваджувати правові знання з допомогою ІКТ. Використання педагогом ІКТ в процесі навчання дозволяє виявити зв'язок навчання з практикою та наводити приклади з практичного застосування правових знань.

Втім, ще досі у навчальному процесі ми стикаємось з проблемами інформатизації правової освіти, до яких відносять: формування інформаційно-правової культури викладача; створення електронних посібників та навчальної літератури на електронних

носіях; розробка нових інформаційних технологій, їх психолого-педагогічних і психолого-фізіологічних засад; розбудова науково-освітніх інформаційно-правових мереж і бібліотек та розвиток інформаційно-правового середовища в Україні; впровадження дистанційного навчання; підготовка педагогічних кадрів до застосування комп'ютерної техніки у професійній діяльності. [1, с. 455].

Однією з важливих умов підвищення якості підготовки фахівців у галузі права є формування високих професійних та моральних якостей у студентів. Це завдання є особливо актуальним, оскільки завдяки ІКТ, які допомагають студентам-юристам розв'язати різноманітні правові задачі, підвищується якість професійної підготовки випускників.

Метою статті є визначення проблем у формуванні правосвідомості студента-правника за допомогою ІКТ.

Виклад основного матеріалу. Якщо для більшості індивідів правосвідомість є чинником, що детермінує ефективність задоволення їх власних потреб, то від правосвідомості людей, чия професійна діяльність має юридичний характер безпосередньо залежить ефективність реалізації інтересів інших суб'єктів. Це пояснюється тим, що від розвиненості та сформованості елементів професійної правосвідомості залежить спрямованість усієї правової діяльності, вибір правових засобів, якість взаємодії та дієвість правового регулювання в цілому [2, с. 307]. Під професійною правосвідомістю, у широкому аспекті, слід розуміти правову свідомість, суб'єктом якої виступають юристи, для яких професійна діяльність здійснюється у правовій сфері з використанням правових знань та засобів.

На сьогодні, ми можемо стверджувати, що роль права і значення правових знань в українському суспільстві змінилася докорінно. Якщо раніше право було лише засобом за допомогою якого державі вдавалося контролювати людей, то тепер право, набуваючи практичного значення для кожного з нас, веде до правової держави та громадянського суспільства. Такий перехід неможливий без формування у майбутніх спеціалістів відповідних правових знань. Саме тому тематика статті стосується не професійної правосвідомості вже сформованого юриста, а студента нової генерації, який би сприяв нормальному функціонуванню держави і гарантував захист прав людини і громадянина.

Правосвідомість юристів у літературі визначається як одна з колективних форм правової свідомості, що виступає системою правових поглядів, знань, почуттів, ціннісних орієнтацій і інших структурних утворень правової свідомості спільності людей, які професійно займаються юридичною діяльністю, що потребує спеціальної освітньої і практичної підготовки. [3, с. 11].

Мухін В.В. пропонує під професійною правосвідомістю розуміти "цілісний, системний, практично спрямований, нормативно детермінований спосіб пізнання правової дійсності і активного впливу на неї, що забезпечує функціонування і розвиток правопорядку, суб'єктом якого виступають особи, що мають спеціальну юридичну освіту та професійно займаються юридичною практикою" [4, с. 14].

В свою чергу, під професійною правосвідомістю студентів слід розуміти відношення до права і готовність застосувати систему правових знань та уміння для вирішення професійних і соціально-побутових проблем, які формуються в процесі професійної підготовки. [5, с. 18]. Така професійна підготовка має бути спрямована на кількісні, якісні і структурні перетворення, що зумовлюються умовами розвитку правосвідомості майбутніх юристів. Під такими умовами у літературі розуміють сукупність усіх тих явищ, від яких залежить виникнення, існування, функціонування та розвиток цього феномену [6]. Формування правосвідомості юристів здійснюється під впливом

соціального середовища (об’єктивних умов і суб’єктивних факторів, що пронизують всі сфери суспільного життя), особливо під впливом права, його формування та реалізації. До основних засобів формування правосвідомості юристів необхідно віднести правове виховання та правову освіту як первинні (базові) елементи механізму, дія яких спрямована на розвиток правової компетентності, що передбачає інтегровану здатність особистості цілісно реалізовувати на практиці знання, способи діяльності, досвід правомірної поведінки, правові ціннісні орієнтації в конкретних моделях поведінки у правовому контексті, підвищення рівня правової культури, правової активності [7].

Під правовим вихованням розуміють цілеспрямовану систематичну діяльність держави, її органів та посадових осіб, громадських об'єднань і трудових колективів з метою формування і підвищення правосвідомості та правової культури. [8, с. 396] У свою чергу, правове виховання майбутнього юриста – це систематичне опанування необхідного мінімуму як загальнотеоретичних, так і спеціальних практичних юридичних знань. Через правове виховання студентів найбільш повно сприймаються моральні цілі суспільства, які впливають на внутрішній імператив службового обов’язку, суттєво знижують рівень соціального конформізму, підвищують інформаційну культуру майбутнього фахівця [6].

Саме правова освіта у сучасних умовах модернізації системи української освіти в сторону її інтеграції у світовий освітній простір є віссю правового виховання та виховує в майбутніх юристів готовність до сумлінного виконання службових обов'язків і дотримання правової дисципліни, формує ціннісні установки, орієнтовані на правову поведінку.

Професіоналізм формується в першу чергу через освіту, тому професійний юрист – це утвердження себе в галузі права через знання та майстерність. Правова освіта повинна забезпечити ці знання та майстерність, розуміння прав і основних свобод людини, визнаних законодавством країни і міжнародним правом, своїх обов’язків та відповідальності перед державою та іншими громадянами, етичних та правових принципів, моральних ідеалів задля головної мети – додержання правового порядку.

Ставлення студентів до обраної спеціальності багато в чому визначається характером навчально-виховного процесу, який моделює майбутнє професійної діяльності. Для усвідомлення перспектив майбутньої фахової діяльності необхідне створення психолого-педагогічних умов, які зумовлюють специфічні особливості організації змісту професійного навчання [9, с. 100]. Психолого-педагогічні умови розвитку правосвідомості студентів-юристів – це сукупність заходів в освітньому процесі, що забезпечують досягнення майбутніми фахівцями необхідного рівня правосвідомості [6]. До таких педагогічних умов, які формують позитивну професійну правосвідомість у студентів-юристів та на які повинні бути спрямовані зусилля держави та вищого навчального закладу, слід віднести: спрямування освітнього процесу на формування у студентів-юристів цінності права та моральних орієнтирів; спеціальна підготовка педагогічного складу з відповідною правовою та інформаційною компетенцією; відповідне методичне забезпечення, яке б включало інформаційні технології; організація комунікації між студентом та викладачем, в тому числі з використанням ІКТ; забезпечення безперевності удосконалення своїх знань через самостійну роботу; створення єдиного інформаційно-освітнього середовища.

Педагогічні умови, що забезпечують ефективність виховання правової свідомості студентів, розкриваються через збагачення змісту правової інформації та посилення її ціннісно-смислових аспектів; використання ситуацій, максимально наближених до

реальності майбутньої професійної діяльності студентів; стимулювання розвитку у студентів активної правової позиції [10, с. 61].

Лише вдосконалення правової освіти, введення нових інформаційних технологій навчання зможе виховати юристів нового покоління з високою правовою активністю та правосвідомістю, що відповідають вимогам сучасного європейського співтовариства та очікуванням наших громадян. Сучасна система вітчизняної професійної освіти зазнала суттєвих змін. Це зумовлено наближенням відчизняної правової системи до європейської, де на перший план висуваються права і свободи людини і громадянина, правові цінності, засади справедливості, свободи та рівності. Наша держава прагне стати членом європейського співтовариства, тим самим розширюючи права громадян та громадянських об'єднань, створюючи рівні умови в ринковій економіці, забезпечуючи судовий захист прав і свобод громадян, підсилюючи захист підприємництва тощо. Однак це лише перші та "маленькі" кроки, оскільки наша держава перебуває у становищі, зумовленому сучасними економічними та соціальними умовами. Втім, "великим" кроком, що зумовив поштовх в освіті, стали останні тенденції світого розвитку, що зумовлені переходом до інформаційного суспільства.

Під інформаційним суспільством прийнято розуміти якісно новий етап розвитку людства, в якому будь-яка людина за допомогою інформаційно-комунікаційних технологій може отримувати, переробляти, розповсюджувати інформацію, а держава забезпечує високий рівень інформатизації всіх галузей [11, с. 129]. Інформаційне суспільство характеризується тим, що збільшується роль інформації і знань, стає безперешкодний доступ до інформації через збільшення інформаційних ресурсів, постійна поява нових та модифікація старих інформаційних та комунікаційних технологій у всіх галузях суспільства та науки.

Інформаційне суспільство – наступна стадія розвитку суспільного життя, основними ресурсами якої є інформація і знання. Інформація у сучасному суспільстві є однією із головних виробничих ресурсів, тому важливо щоб педагогічний працівник був професійно підготовлений до використання ІКТ та мав відповідну інформаційну культуру. Вища школа повинна ставити перед собою завдання, яке полягає у постійному підвищенні якості підготовки спеціалістів. Цьому сприяє, зокрема, висока інформаційна компетентність викладача-педагога, що полягає у розробці нових інформаційних технологій навчання та методик викладання. У свою чергу, професійна правосвідомість студента-юриста передбачає професійну інформованість, що прогнозує компетентність у сфері чинного законодавства і практики його реалізації, виражається у достатньо глибоких та професійно необхідних знаннях про право та закономірності його буття, що дозволяє займатися професійною юридичною діяльністю [2, с. 309].

Отже, одержання теоретичних правових знань, переконаність у соціальній корисності права, його цінності, розуміння застосування правової норми є головним завданням правової освіти. Через одержання, використання, поширення та зберігання правової інформації, її усвідомлення та перетворення на правові знання, які у свою чергу стають основою ціннісної орієнтації, морально-правової установки формується правосвідомість студента-правника. Тому ключовим є те, за допомогою яких методів та засобів можна донести правову інформацію до студента, так щоб це було якісно та швидко, а головне – запам'ятовувалося та перетворювалося на знання, які в подальшому будуть придатні для використання при вирішенні життєвих та практичних правових ситуацій та задач. Таким чином, правосвідомість ґрунтується на правовій інформації, яку студент повинен запам'ятати, усвідомити, зрозуміти та перетворити на власні переконання.

Суспільні зміни, розвиток системи правового забезпечення, підвищення якості суспільного життя висуває нові вимоги до правової освіти і до професії юриста, зокрема. Рівень підготовки юристів у вищих навчальних закладах вимагає пошуку нових інформаційних методів та засобів, які мають використовуватися як у процесі підготовки на рівні забезпечення відповідного методичного матеріалу, так і в процесі викладання правових наук, враховуючи в тому числі і забезпечення студента-юриста відповідною базою для самостійної підготовки. Новітні технології повинні сприяти творчому потенціалу студента, його фаховості та вмінню виконувати правові завдання, які моделюються у процесі навчання із якими студент безпосередньо матиме справу вже у своїй практичній діяльності. Тому, важливо знайти найбільш ефективні шляхи модернізації й підвищення якості сучасної правової освіти, які в подальшому методом снігової лавини зачепили б зміни у нормотворчій, правоохоронній та правозастосовчій діяльності нашої держави.

На сучасному етапі одним з головних завдань правової освіти "є побудова такого процесу навчання, який став би основою формування навчальної і професійної діяльності по підготовці і вихованню фахівців і сприяв би підвищенню рівня їх культури, розширенню кругозору, умінню творчо відноситися до своєї праці" [12, с. 326].

Інформатизація правової освіти повинна здійснюватися в двох основних напрямах:

1) забезпечення випускників вищого юридичного навчального закладу рівнем професійних знань та навичками їх умілого застосування у процесі практичної діяльності;

2) підвищення рівня інформаційної компетентності у майбутнього фахівця з галузі права через інтегрування інформаційно-комунікаційних технологій у навчальну діяльність.

Гіпершвидка трансформація постіндустріального суспільства в інформаційне співтовариство, де виробництво і споживання інформації є найважливішим видом діяльності, а інформація визнається найціннішим ресурсом, зумовило визнати найефективнішим засобом підвищення якості професійного навчання ІКТ [13, с. 68-69].

Щоб осягнути великий обсяг знань про право, правові явища, правові норми, їх усвідомити, проаналізувати, зрозуміти та освоїти, необхідні дієві методи. Від їх кількісної та якісної характеристики залежить процес передачі, накопичення та засвоєння правових знань. Правовий потенціал та правова підготовка, які є основою професійності, формуються через уміння наочно використовувати правові знання. Все це, як і наочність правових знань, здатні забезпечити інформаційно-комунікаційні технології.

Однією із актуальних проблем інформатизації юридичної освіти є формування навичок застосування ІКТ для фахової діяльності, що є важливою складовою правосвідомості майбутніх правознавців. Інформаційно-комунікаційні технології, які використовуються у навчальному процесі, сприймаються як один із інструментів пізнання навколишнього світу, набуття умінь і навичок вдосконалення професійної майстерності [9, с. 162].

Слід погодитись з Гершунським Б.С., що "в остаточному підсумку всі досягнення в галузі застосування інформаційних технологій у сфері освіти, створення мереж телекомунікацій і підтримка інформаційних потоків у них, створення і супровід банків даних і баз знань, експертних систем і інших видів ІКТ мають служити одній меті: розробці методологічної основи застосування інформаційних технологій у процесі освіти. Власне кажучи, в даний час суспільство стоїть перед завданням навчитися правильно, оптимально і нешкідливо застосовувати комп'ютер у всій системі освіти в цілому" [14, с. 33].

Інформаційно-комунікаційні технології, що використовуються у навчальному процесі, сприймаються як один з інструментів пізнання навколишнього світу, набуття

умінь і навичок вдосконалення професійної майстерності. Вони допомагають адаптуватися майбутнім фахівцям до життя у сучасному суспільстві та, як і будь-які інші педагогічні технології, інформаційні технології навчання ґрунтуються на високому професіоналізмі викладачів, співпраці та творчості між викладачем і студентом, атмосфері довіри, відповідній матеріальній та методологічній базі, відповідальному ставленню студентів до засвоєння теоретичного матеріалу й оволодіння відповідними уміннями та навичками. Ефективність прийняття рішень як запорука професійної діяльності можлива лише при використанні інформаційно-комунікаційних технологій за рахунок своєчасного отримання необхідної інформації. Здійснення майбутнім фахівцем фахової діяльності є опанування визначеним обсягом знань, умінь та навичок з ІКТ, які є достатніми для усвідомлення проблем і шляхів практичного застосування цих навичок у професійній діяльності [9, с. 14, 62]. Отже, особливе місце у правовій освіті займає потенціал ІКТ, в основі якого лежить розвиток пізнавальних навичок студентів, умінь самостійно структурувати і актуалізувати свої правові знання. Актуалізує дане питання і те, що аналіз сучасної ситуації у вищій професійній школі показав: в навчальному процесі переважають традиційні технології з низьким рівнем використання інноваційних технологій; відсутні технології, орієнтовані на систематичне використання інформаційних і комунікаційних технологій в юридичній підготовці майбутніх спеціалістів [5, с. 19].

Виходячи з вищезазначеного, вважаємо, що інформаційно-комунікаційні технології у формуванні професійної правосвідомості студента-юриста відповідають за такі компоненти:

1) професійний – формування навичок пошуково-дослідницької діяльності (обробка, передача, зберігання правової інформації з використанням ресурсів мережі Інтернет, електронні носії; можливість створювати власні бази даних);

2) мотиваційний – підвищують навчальну мотивацію;

3) світоглядний – розширюють світогляд студента-юриста;

4) інтелектуальний – дозволяють сформулювати новий стиль роботи, що розкриває у студентові-правникові інтелектуальний потенціал;

5) мовленнєвий – ІКТ сприяють збільшенню зацікавленості студентів до правових знань, а отже до покращення їхньої юридично-мовленнєвої складової конкурентоздатності;

6) аналітичний – формують уміння структурувати і аналізувати свої правові знання;

7) діяльнісно-практичний – здатність вирішувати професійні завдання з використанням ІКТ, формують уміння ухвалювати правильні та нестандартні правові рішення;

8) орієнтаційний – сприяють формуванню навичок орієнтації в інформаційно-правовому полі;

9) комунікаційний – відповідають за діалогізацію навчання та за прискорення передачі досвіду від викладача до студента, тобто сприяють розвитку правової комунікації;

10) культурний – формують інформаційну культуру, сприяють інформаційній грамотності;

11) прогностичний – передбачають прогнозування правових ситуацій за допомогою ІКТ;

12) ціннісний – формують ставлення до права і правових норм;

13) аналітичний – передбачають уміння аналізувати правові та неправові діяння, явища та співставляти їх із законом та правом;

14) адаптаційний – формують уміння студента-правника швидко адаптуватися у різних правових та неправових ситуаціях, а також надають студентові професійної впевненості;

15) пізнавальний – активізують пізнавальну здатність студента-правника;

16) рефлексивний – сприяють розвитку особистості, надають нові можливості для творчості, розвивають правове мислення.

Отже, ІКТ створюють необхідні умови для формування й розвитку рефлексії, самосвідомості особистості, а також правосвідомості студентів-юристів.

Висновки.

Нині суспільство вступило в таку стадію розвитку, що характеризується стрімким розвитком інформаційно-комунікаційних технологій, без яких неможливе ефективне вирішення професійних проблем. Відповідно, правовій сфері необхідні юристи, які володіють таким видом знань та вмінь.

Освіта, в тому числі правова, як і держава, прагнуть суттєвих змін, а тому інформатизація освіти є складовою цього процесу. Навчання у вищому навчальному закладі є досить складним процесом, адже щороку, і це особливо стосується галузі права, збільшується обсяг інформації, яку студент повинен засвоїти. Задля оптимізації його праці, швидкому пошуку її у навчальному процесі, впроваджується ІКТ. У зв'язку з цим студенти надають перевагу не лише змісту, але й формі подачі матеріалу, яка за допомогою ІКТ підвищує їхню зацікавленість, розвиває запам'ятовуваність, рівень наочності.

Мета нової гуманістично-комунікаційної освіти – виховання відповідальної особи, що здатна до саморозвитку і самоосвіти. Все це зумовлює гостру потребу у створенні і реалізації особистісного підходу до студента. Правова освіта повинна бути зацікавлена в особистостях-юристах, які здатні самостійно й активно діяти, приймати рішення, швидко адаптуватися до різних життєвих та правових ситуацій.

Вища юридична освіта повинна забезпечити державу такими фахівцями, які б сприяли нормальному функціонуванню держави і гарантували захист прав людини і громадянина.

Використана література

1. Шмирова О.В., Зелінська В.А. Роль інформаційно-комунікаційних технологій на сучасному етапі інформатизації освіти. *Молодий вчений*. 2017. № 5 (45). С. 455-458.

2. Жидовцева О.А. Структура та функції професійної правосвідомості. *Форум права*. 2012. № 1. С. 307-312.

3. Соколов Н.Я. Профессиональное сознание юристов. Москва: Наука, 1988. 224 с.

4. Мухін В.В. Професійна правосвідомість: поняття, особливості, функції: автореф. дис. ...канд. юрид. наук, Національна юридична академія України ім. Ярослава Мудрого. Харків, 2007. 20 с.

5. Кручинин М.В., Кручинина Г.А. Моделирование процесса формирования профессионального правосознания студентов неюридических специальностей в высшем образовании. *Вестник Нижегородского университета им. Н.И. Лобачевского*. 2012.№ 3 (1). С. 17-24.

6. Кононенко С. В. Теорія і практика формування правосвідомості у майбутніх юристів. *Вісник Національної академії Державної прикордонної служби України*. 2011. Вип. 4. URL: http://nbuv.gov.ua/UJRN/Vnadps_2011_4_33

7. Калюжний Р.А. Формування правосвідомості юристів в сучасних умовах освітніх змін: мат. науково-практичної конференції *Правова освіта в Україні: еволюція, сучасний стан, перспективи розвитку*, м. Київ, 27 квіт. 2017 р. URL: http://er.nau.edu.ua:8080/handle/NAU/32549

8. Нерсесянц В.С., Муромцев Г.И., Мальцев Г.В. и др. Право и культура / под ред. Соколовой Н.С. Москва: Изд-во РУДН, 2002. 423 с.

9. Федорчук О.С. Формування у майбутніх правознавців навичок професійного застосування інформаційно-комунікаційних технологій: дис. ...канд. наук. – (Інститут педагогічної освіти і освіти дорослих). Київ, 2009. 258 с.

10. Ніколаєнко С.І. Виховання професійної правосвідомості майбутнього юриста у процесі вивчення "Юридичної психології": матеріали Міжнародної науково-практичної конференції *Психологічна просвіта у сучасному суспільстві: методологія, досвід, перспективи*, 20-21 лист. 2014 року. С. 60-61.

11. Петрухно Ю.Є. Інформаційне суспільство: поняття, основні складові, характеристика. *Вісник Одеського національного університету*. *Сер. Бібліотекознавство. Бібліографознавство. Книгознавство*. Т. 19. Вип. 1. 2014. С. 127-133.

12. Савіцька В. Готовність майбутнього соціального працівника до професійної діяльності як запорука її ефективності: зб. наукових праць Уманського державного педагогічного університету. Ч. 2. 2013. С. 325-331.

13. Савченко І. Інформаційно-комунікаційні технології як ефективний інструмент реалізації інноваційних педагогічних ідей у практику навчально-виховного процесу ПТНЗ. *Педагогіка і психологія професійної освіти*. 2014. № 1. С. 68-79.

14. Гершунский Б.С. Компьютеризация в сфере образования: проблемы и перспективы. Москва: Педагогика, 1987. 264 с.

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

УДК 316.614.034:34.096

PETRIAIEV O., Postgraduate Student, National Institute for Strategic Studies.
ORCID: https://orcid.org/0000-0001-6561-2647.

CYBER SOCIALIZATION: INFORMATION-TECHNICAL, EDUCATIONAL AND LEGAL ASPECTS

Summary. *A new generation of young people, is our replacement. How it is today, socialized in the context of new social relations based on information technology. What role in these conditions of socialization was taken by the ruling state structures, to which their next reforms of education will lead? Based on this, what will humanity be like in the coming decades? Little doubt that it will be completely different from the usual generation that came from the second half of the last century. This article is devoted to these and other issues.*

Keywords: *socialization, cybersocialization, education, young generation.*

Петряєв О. Кіберсоціалізація: інформаційно-технічні, освітні та правові аспекти

Анотація. *У статті розкриваються проблеми соціалізації нового покоління молодих людей. Нове покоління молодих людей – наше прийдешнє, наша зміна. Яким воно є вже сьогодні, соціалізоване в умовах нових громадських стосунків на основі інформаційних технологій. Яку роль в цих умовах соціалізації відвели собі панівні державні структури, до чого призведуть їхні чергові реформи освіти. З огляду на зазначене, яким стане людство найближчими десятиліттями? Безсумнівно, воно буде зовсім іншим, ніж звичне нам покоління, що прийшло з 2-ої половини минулого століття. Цим та іншим питанням присвячена ця стаття.*

Ключові слова: *соціалізація, кіберсоціалізація, освіта, молоде покоління.*

Петряев О. Киберсоциализация: информационно-технические, образовательные и правовые аспекты.

Аннотация. *В статье раскрываются проблемы социализации нового поколения молодых людей. Автор ставит вопрос о коллизиях современной социализации в условиях новых общественных отношений на основе информационных технологий. Какую роль в этих условиях социализации отвели себе властвующие государственные структуры, к чему приведут их очередные реформы образования. Исходя из этого, каким станет человечество в ближайшие десятилетия? Мало кто сомневается, что оно будет совсем другим, чем привычное нам поколение, пришедшее из 2-й половины прошлого столетия. Этим и другим вопросам посвящена данная статья.*

Ключевые слова: *социализация, киберсоциализация, образование, молодое поколение.*

Problem statement. The development of modern civilization is constantly associated with the complication of the nature of social relations and their transformation. The most controversial social relations that require legal regulation are elevated to laws, ensuring public consent.

Today, information technology (hereinafter IT) is actively contributing to an increase in the amount of information that forms new types of social relations, ensuring the accelerated development of civilization. A variety of information content has formed an army of users of information networks, providing the society with new knowledge, new needs and interests. Like any new one, IT has led to the transformation of the established conditions and principles of socialization, breaking the stereotypes, rules, forms and harmony of the formation of young people who have been developed for centuries. In addition to breaking the traditional forms of upbringing of the young generation, IT, as an objective factor of the era, combined with fundamental reforms of secondary and higher education, backed by legislation, are used by

many developed countries as a new tool for socialization. Depending on which final human product the state wants to receive in the remainder – the essence of the tasks of the ruling structures. The final result of the first stage of socialization is the answer to the question that interests us, because the assessment of the quality of the products is determined by the efficiency of its operation. The level of intellectual development of society is the cornerstone of state security, which, in our opinion, needs legal regulation.

Analysis of recent research. The theory of cyber socialization was introduced by Russian scientist V.A. Pleshakov in 2005 and is further developed in his works and the works of his followers [1]. Today, many scientists in the field of pedagogy and psychology are studying this phenomenon, in particular O.V. Voznyuk [2]. However, among legal scholars, this issue has only just begun to be investigated.

The purpose of the article is to analyze the impact of IT and the modern education system on the socialization (or cyber socialization) of young people in Ukraine, as well as the search for ways to form a new balance of socialization in the context of changing social relations, which should be regulated by law.

Statement of the main material. In the scientific literature, socialization is considered as the assimilation and reproduction by an individual of social experience in the process of lif*e*, i.e. as a two-way process: on the one hand, the individual assimilation of social experience through entry into the social environment; on the other hand, the process of active reproduction by an individual of a system of social ties through his active activity [3]. In other words, socialization is the individualization of the social and the socially individual.

No one doubts that the process of socialization directly depends on a specific historical period, each of which is filled with its social, technical, cultural, moral, scientific and other living conditions. Thus, the process of personality development takes place in conjunction with its surrounding social environment. And since modern socialization is characterized by an accelerated pace of development of technical and technological, communication and information links that affect all spheres of a person's social life, the socialization process under these conditions cannot but affect the consciousness, especially of young people. As a unity of determinism and chaos, or patterns and randomness, socialization consists in the unity of a spontaneous and purposeful influence on the formation of personality, external and internal content. Targeted impact processes are implemented through a system of education and training; spontaneous – through mass communication [3].

Modern information technologies have fundamentally changed the process of socialization, partially replacing its traditional elements with social information networks, combining communication, educational and training functions. The information volumes of communication networks are many times greater than a decade ago and continue to grow rapidly. All this information and logistics system forms the information space of society and becomes dominant. There is a noticeable erosion of the influence of the family, pre-school and school educational institutions on the personality, first of all, of the first stage of socialization (childhood and youth periods). The author of the article "Evil in your pocket" M. Bokov notes that the family ceases to be interested in each other, talk, the tradition of gathering at the same table is completely gone – instead, everyone is absorbed in the virtual reality offered by the smartphone [4].

A significant part of this information in its content is considered to be "information garbage", which performs the functions of virtual entertainment and communication. Such information resources include modern clip-art films and computer games, constantly updating various news, advertisements, correspondence with friends online, descriptions of people's private lives in the field of show business, politics, sports, self-promotion and many other resources that create unique conditions of comfort. An overabundance of such information

does not bring a person anything other than "cluttering" consciousness. In the scientific world of this information, a softer name was invented – "white noise".

Earlier we wrote that the "white noise" absorbs more and more free time of the individual, and therefore the whole society, tearing them away from real life. The contemporary picture of social life is looming ever more clearly when the Internet does not serve the individual as an instrument for solving various social problems, and the individual (society) begins to obey the Internet, which, like an octopus, draws it into the abyss of informational rubbish from which it is no longer able to get out [5].

Memory is a complex cognitive process, thanks to which a person can memorize, save and reproduce his past experience. Loading the brain with "white noise", memory overload occurs, the brain quickly gets tired and a person begins physical fatigue, brain exhaustion. Immersion in the atmosphere of "white noise" leads to disorientation in time, which entails its wasting without any compensation. For the assimilation of useful, systemic information, a person no longer has the strength or time.

Young people staying in a constant "white" information space, in particular continuous "sticking" into a smartphone, brings them to a state of not only brain and physical fatigue, but also memory atrophy. The vast majority of young people today are not able to remember simple and concise information.

"Black noise," that is, populating the Internet space and the media with cruelty, promoting an unhealthy lifestyle and bad habits, does even more harm. In fact, both types of information ("white and black noise") harm the human psyche, especially the children's psyche. However, the legislation does not generally regulate the process of creating, placing (broadcasting), using and consuming ordinary information ("white noise"). The issue of handling information, objects of intellectual property rights that contain information with elements of cruelty, propaganda of war, national and religious hostility is partially regulated by the Law of Ukraine "On the Protection of Public Morality" of November 20, 2003 [6] (part 3 of article 2), [*Закон України "Про захист суспільної моралі" від 20.11.03 р. (ч. 3 ст. 2)*] as well as the Law of Ukraine "On Television and Radio Broadcasting" dated December 21, 1993 (part 7 of article 4) [*Закон України "Про телебачення і радіомовлення" від 21.12.93 р. (ч. 7 ст. 4)*] [7].

In general, the dissemination of such information is prohibited, but this prohibition does not apply to works of art, which include all films that promote violence and cripple the children's psyche, and often the psyche of an adult. Therefore, there are suggestions that the state should more influence through the state request and tax benefits on the creation and broadcast of video products, which are not only interesting, but also socially useful and bear an educational message [8].

One of the functions of the state is the formation of a mentally and physically healthy young generation of citizens, and the purpose of education in the Law of Ukraine "On Education" dated September 5, 2017 [*Закон України "Про освіту" від 05.09.17 р.*] [9] declared the formation of citizens who are capable, including of a conscious choice and direction of their activities for the benefit of other people and society. But for this purpose, the state should regulate the reduction of harmfulness of information posted on the Internet and in the media, as well as regulate the time of access to social networks and the Internet as a whole in the walls of educational institutions. This will help both for educational purposes and in order to maintain mental and physical health. G.O. Cirfa notes that the issue of regulating access and dissemination of information via the Internet should be a paramount task for the state [10].

World studies have shown that constant “freezing” in networks leads to mental dementia, back in 2007 in South Korea this phenomenon was given the name “digital dementia”. In particular, psychiatrist Yuna Sen-chang noted that “since today people are more dependent on digital devices for finding information than on remembering, the function of the search brain is improving, while the ability to remember on the contrary is rapidly declining. The result of this dependence is a form of digital dementia, which manifests itself in a decrease in memory performance [11].

The life circumstances of each of us are largely formed at the very beginning of our conscious life by external influence (upbringing), primarily of our close environment - parents, friends, preschool, school and higher educational institutions. The goals and objectives that they set for themselves in the formation of the future personality are the essence of the aggregate manifestation of the elements of influence. Hence, the path of development for each young person is formed in different ways, depending on the sources of influence.

Note that the modern young generation is physiologically no different from all previous generations. The only difference is in the new tools that affect all forms of socialization – study, communication, physical development, health, etc.

If we take into account the fact that children start using information computer technologies from the age of 2 to 3 years old (parents themselves uncontrollably put them on gadgets and enjoy their “creative” development without realizing what dangers they put their children into), then it becomes clear why by the school age (6-7 years) the child’s brain is already overloaded with “white noise”.

Along with an overabundance of information, computer addiction minimizes useful information before clip perception, developing the so-called “clip consciousness” (perceiving the world through short information images), which, accordingly, forms a “clip culture”.

Recently, quite a lot of research has been conducted on the subject of clip consciousness, which indicates a high speed of “searching” and “fixing” the necessary information and, at the same time, the inability to comprehend it. As a result, the process of memorization and assimilation of information is very minimized in young people, not only the nature of the origin of facts and phenomena is lost, but also the logical chain of their development and understanding, i.e. causal relationships of events. Therefore, in our opinion, the use of gadgets in the classroom should be prohibited at the legislative level, in addition to certain classes, which include training in information and communication technologies, solving problems that involve access to a legislative or other database, and similar things. Studies confirm that in people with clip consciousness, the brain processes pictures more efficiently than text, and does it at high speed [4]. In other words, thought in itself disappears, the image dominates knowledge [5].

Hence, young people massively stopped reading classical literature, textbooks, scientific primary sources, which form a person’s imaginative and logical thinking, speech culture, desire for knowledge and improvement. To the annual question to the students' audience what art books you have read in your life, with each subsequent year, the answers are getting closer to zero.

In addition to the above negative processes that affect the cognitive development of young people, the uncontrolled use of information technology actively affects the physical development of a person.

As a result, children's games and sports from the field of personal participation moved into the field of virtual experience. Only 10 % of children come to school relatively healthy. The reasons for the increased incidence of children are the violation of body functions with limited physical activity of “physical inactivity”. Modern children experience a “motor deficit” [12]. The many hours of absorption by gadgets has led to massive visual impairment in children. In percentage terms, the number of children suffering from visual impairment

today is about 9% of the total in the lower grades and about 30 % already in the senior graduation classes [13]. In addition, the abuse of electronic devices also leads to emotional breakdowns, depression and a decrease in empathy; indifference to the fate and security of his state is developing. As a result, young people who come to school and then to university are physically undeveloped, weak, quickly tired and do not cope with the curriculum.

In the future, many adults cannot even lead a relatively healthy social lifestyle. For example, gambling, as a form of dependence, has already been recognized as the basis for limiting legal capacity in accordance with clause 2 of Article 36 of the Civil Code of Ukraine [*п. 2 ст. 36 Цивільного кодексу України*] [14]. But, computer games can also involve large expenditures of money or simply take so much time from a person that he will not work and provide for his family, which, in our opinion, is essentially the same as gambling, should be the basis for limiting the capacity of such citizen. However, it is necessary to deal with such computer games and their addiction in childhood and adolescence. It is necessary to introduce mandatory testing of computer games regarding their harmfulness, semantic and developmental load. In the case of propaganda of violence, the absence of a developmental (instructive) load and the presence of an obsessive influence on the psyche, such games should be prohibited by law (in accordance with clause 2 of Article 288 of the Civil Code of Ukraine [*п. 2 ст. 288 Цивільного кодексу України*], any negative mental effect is prohibited).

Psychologists have long noted such a form of addiction as Internet addiction, i.e. gambling and Internet addiction, leading to social autism. Subsequently, people are unable to communicate live, to verbalize and deverbalize information, which means the inability to turn words into emotion, and emotion into a sign-shaped system [2]. And, this is an important component of emotional intelligence as the basis of human interaction. In addition to cyber addiction, children and young people cease to distinguish between the virtual world and the real world, which appears in deviant behavior and delinquent actions [15].

In general, any public relations should be regulated by law, the same applies to relations on the Internet to maintain public order and protect the rights of children. Many computer games induce children to certain types of behavior, in particular to bowling, which affects a significant part of children in schools. In addition, social networks and various Internet platforms can host extremely dangerous “games”, for example, “Blue Whale”, because of which many teenagers committed suicide. Also, new specially protected information transmission channels, for example, Tor, can serve as a means of drug trafficking, spreading extremist ideology and committing cyber diversions against individual institutions or even national security in general [16].

However, an overabundance of even “white information” along with physical underdevelopment does not allow young people to concentrate attention while studying. Digital autism on epidemic levels was announced by the famous psychiatrist A. Kurpatov, who also notes scientifically verified data that the constant perception of information (especially visual) makes it impossible to think, because different brain modes that cannot work simultaneously [17] (this can be compared with the process of food intake, which needs a break for its digestion). The same applies to the quality of information, toxic information kills the psyche in the same way as poor-quality food poisons a person.

The principles and forms of the educational process have also undergone major changes, which now must correspond to the modern level of information technology. Due to the clip consciousness, the traditional forms of conducting classes for modern schoolchildren and students are becoming ineffective, boring, difficult to tolerate. The brain’s inability to accumulate information (remembering) and hedonism developing in young people have led to the need to increase and expand interactive forms of conducting classes. The active process has begun of replacing the traditional form of lectures with vivid pictures – a slide show, i.e., a clip

form of perception of lecture material, where the listener's attention is directed not to the teacher, but to a colorful informational limited slide. Thereby, contact with the lecturer is lost, and the content is dissolved in a bright picture of the slide. Involuntarily, a situation arises when a student begins to "demand" spectacles not only on the street, but also within the walls of the alma mater, because his brain is no different from the level of "street masses". If previously a teacher kept the audience's attention with the depth of his knowledge and oratory, today the depth of knowledge has to be replaced by elements of the show.

This problem is typical not only for Ukraine, but also for all developed countries in which there is a high level of use of information technology. For example, in Italy, by the end of school, many children write poorly in Italian, do not read much, and have difficulty communicating. High schools have long been confronted with language gaps by their students who make mistakes that are permissible only in the third grade of primary school. Teachers of Italian universities urge to revise the school curriculum and introduce periodic certification throughout the course of training [18].

American scientists note that students leave colleges without the intellectual skills necessary to substantiate complex issues because of the low ability for critical thinking due to a lack of understanding of its essence and, accordingly, the lack of skills for the latter on the part of the teachers themselves. Only a small minority of college faculty (19 %) can give a clear explanation of what critical thinking is. Moreover, according to their answers, only 9 % of respondents taught their students critical thinking [19]. Indeed, among other things, information scattered on the Internet and partially read, ceases to exist in a holistic form, and is fragmented and these fragments often do not correlate directly with each other [20].

In the theses of the report "Acting Aspects of Special Features" A.M. Bezhevets compares the positive and negative properties of the virtual world with – "Medicines that themselves are called upon to treat a certain disease, but their overdose can cause not only the opposite effect, but even lethal outcome. At the same time, no one had the idea to assert that all medicines are evil, and it is necessary to abandon them" [21].

It is difficult to disagree with this judgment, especially if the medicine stimulates recovery, and an overdose is a random event. However, one should not forget that drugs that have a strong effect on the body, up to its destruction, translate into the status of strict medical control. The common sense of simple survival determined the rules of behavior not only in medicine, but also in other social relations. For example, even with such a social phenomenon as crime, for many centuries mankind has learned to fight.

If some thinkers consider digital dementia as a natural result of the formation of the consciousness of a "person of the future" based on information technology, then, in our opinion, the genocide of many peoples can be justified in the same way by the natural course of history in separate segments of their development. In content – blasphemous, but in form and our conviction is correct, because digital dementia is nothing but the intellectual genocide of young people.

Today, everyone already understands that the uncontrolled use of information technology affects the consciousness and subconscious of people, leading them to "dullness". Not taking any actions aimed at the "recovery" of society, it is the same as stopping the society from fighting crime, drug addiction and alcoholism, tuberculosis, AIDS and oncology. Therefore, legislation should still not lag behind the development of technology, but should regulate these processes by law.

Conclusions.

The reform of secondary and higher education set forth in the Law of Ukraine "On Education" [*Закон України* "*Про освіту*"] dated September 15, 2017, consolidated its new

standards, aimed not at the ability to think based on the knowledge gained, but at the development of reflex actions based on competencies. However, competencies do not fully reflect the essence of the concept of "education". Indeed, it also includes the ability to think critically, create new ideas, compare, systematize and verify the basic realities of life, to distinguish between "good" and "evil" and so on. In fact, the Law of Ukraine "On Education" did not remove the obligation for scientific and pedagogical workers to educate pupils (students), which is reinforced by Part 7, Clause 2, Article 54 [*ч. 7 п. 2 ст. 54*] of the same law. In the blurring of the truth of life principles, which is propagated by the worldwide network and some objects of intellectual property, the part of education that is responsible for the formation of a mentally healthy socialized person (and not a psychopath) is especially important. Therefore, the commercialization of education, which implies the provision of "educational services", does not fully comply with the concept of "education", which should include not only the formation of certain competencies among students, but also inculcate in them respect for public morality and social values, in particular , truth, justice, patriotism, humanism, tolerance, industriousness (Article 54 of the Law of Ukraine "On Education") [*ст. 54* Закона *України* "*Про освіту*"].

But for these purposes, the state should regulate the level of "toxicity" of information that is posted in the Ukrainian segment of the Internet, as well as video products that are broadcast in the media to form a mentally healthy young generation, and also regulate the time pupils (students) access gadgets, at least walls of educational institutions. Such content restrictions should not concern journalistic research and any factual evidence so as not to become censorship.

List of sources used

1. Плешаков О.В., Угольков Н.В. Интернет как фактор киберсоциализации молодежи. *Вестник КГУ им. Н.А. Некрасова. Сер. Педагогика. Психология. Социальная работа. Ювенология. Социокинетика*. Т. 13. 2013. № 3. С. 117-119.

2. Вознюк О.В. Негативні наслідки кіберсоціалізації: мат. Регіональної науково-практичної Інтернет-конференції *Інтернет-бум: психолого-педагогічні проблеми та наслідки агресивно-інформаційного впливу на психологічне здоров'я і розвиток дітей та учнів*, м. Житомир, лист. 2017 р. URL: https://dpszt.blogspot.com/2017/11/159_75.html

3. Андреева Г.М. Понятие социализации. URL: http://www.razlib.ru/psihologija/socialnaja_psihologija_shpargalka/p47.php (дата доступа: 25.04.2020).

4. Боков Павел. Зло в кармане. URL: http://rusplt.ru/society/zlo-v-karmane-18316.html (дата доступа: 23.04.18).

5. Петряев С.Ю. "Киберцивилизация": А ≠ А. *Інформація і право*. № 3(12)/2014. С. 25-30.

6. Про захист суспільної моралі: Закон України від 20.11.03 р. *Відомості Верховної Ради України.* 2004. № 14. Ст. 192.

7. Про телебачення і радіомовлення: Закон України від 21.12.93 р. *Відомості Верховної Ради України*. 1994. № 10. Ст. 43.

8. Когут Н.Д. Розповсюдження інформації в сучасному суспільстві. *Інформація і право*. № 3(12)/2014. С. 56-59.

9. Про освіту: Закон України від 5.09.17 р. *Відомості Верховної Ради України*. 2017. № 38-39. Ст. 380.

10. Цирфа Г.О. Феномен Інтернет і "феноменологія духу" або шляхи соціалізації і кіберсоціалізація. *Правова інформатика*. № 4(44)/2014. С. 15-21.

11. Цифровая деменция как новый вид слабоумия. URL: http://lechdok.ru/facts/cifrovaya-demenciya-kak-novyj-vid-slaboumiya/ (дата доступа: 15.05.18).

12. Мещерякова Е.А., Воронина Н.М. Проблемы физического воспитания дошкольников в условиях современного дошкольного образования. *Молодой ученый*. 2016. № 13.3. С. 60-62. URL https://moluch.ru/archive/117/32422 (дата доступа: 21.04.2018).

13. Профилактика нарушения зрения у детей младшего школьного возраста. URL: http://www.vashaibolit.ru/1429-profilaktika-narusheniya-zreniya-u-detey-mladshego-shkolnogo-vozrasta.html (дата доступа: 06.04.18).

14. Цивільний кодекс України: Закон України від 16.01.03 р. *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356.

15. Потьомкіна Н. Кіберсоціалізація юні: соціально-педагогічний підхід. *Social work and education*. 2019. Vol. 6, no 3. С. 269-284.

16. Стовпець О.В., Стовпець В.Г. Світлі й темні сторони нової інформаційної реальності (у контексті охорони прав інтелектуальної власності). *Часопис Київського університету права*. 2020. № 1. С. 229-233.

17. Психиатр Андрей Курпатов: "Идет эпидемия цифрового аутизма". *Православная жизнь*. 10 февраля 2020 г. URL: https://pravlife.org/ru/content/psihiatr-andrey-kurpatov-idyot-epidemiya-cifrovogo-autizma

18. Итальянские ученые и преподаватели пожаловались на безграмотность молодежи. URL: https://news.rambler.ru/world/36009194/?utm_content=news&utm_medium=read_more&utm_source=copylink (дата доступа: 23.09.2019).

19. The State of Critical Thinking Today. URL: http://www.criticalthinking.org/pages/the-state-of-critical-thinking-today/523 (дата доступа: 12.10.2019).

20. Ожеван М.А., Дубов Д.В. Философские, культурологические и политические предпосылки формирования конвергентного общества: монография. Київ: НИСИ, 2017. 272 с. С. 23.

21. Бежевець А.М. Деякі аспекти кіберсоціалізації особистості. *Інформація і право*. № 1(13)/2015. С. 140-144.

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

УДК 34.037

УХАНОВА Н.С., старший науковий співробітник
НДІІП НАПрН України.
ORCID: https://orcid.org/0000-0002-2366-5166.

ПОЛІТИЧНА СОЦІАЛІЗАЦІЯ МОЛОДІ ЯК ПЕРЕДУМОВА ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ

Анотація. *У статті здійснено аналіз теоретико-правових засад та проблемних аспектів політичної соціалізації молоді. Наведено основні наукові підходи до особливостей та специфіки процесу політичної соціалізації молоді в сучасних умовах розвитку українського інформаційного суспільства. Визначено теоретичне підґрунтя для характеристики основних передумов та принципів політичної соціалізації молоді в Україні. Обґрунтовано авторське бачення особливостей здійснення процесів політичної соціалізації молоді. Приділено значну увагу критичному аналізу різних наукових поглядів щодо засобів та інструментів політичної соціалізації молоді, зокрема розглянуто роль Інтернету як сучасного засобу комунікацій для активного та прискореного включення молоді у політичне життя. Проведено аналіз результатів соціологічного дослідження щодо інклюзії української молоді у політичні процеси. Зроблено висновки стосовно основних тенденцій та специфіки участі молоді у політичних процесах, що виражається через організацію різних громадських організацій та рухів.*

Ключові слова: *молодь, політика, політична соціалізація, передумови політичної активності, громадські організації, громадські рухи.*

Summary. *The article analyzes the theoretical and legal principles and problematic aspects of political socialization of youth. The main scientific approaches to the peculiarities and specifics of the process of political socialization of youth in modern conditions of development of Ukrainian information society are given. The theoretical basis for characterizing the basic preconditions and principles of political socialization of youth in Ukraine is determined. The author's vision of the features for the implementation of the processes of political socialization of youth is substantiated. Considerable attention is paid to the critical analysis of various scientific views on the means and tools of political socialization of youth, in particular, the role of the Internet as a modern means of communication for active and accelerated involvement of young people in political life. An analysis of the results of a sociological study on the inclusion of Ukrainian youth in political processes is carried out. Conclusions are made regarding the main trends and specifics of youth participation in political processes, which is expressed through the organization of various public organizations and movements.*

Keywords*: youth, politics, political socialization, preconditions of political activity, public organizations, social movements.*

Аннотация*. В статье осуществлен анализ теоретико-правовых основ и проблемных аспектов политической социализации молодежи. Приведены основные научные подходы к особенностям и специфике процесса политической социализации молодежи в современных условиях развития украинского информационного общества. Определены теоретические основы для характеристики основных предпосылок и принципов политической социализации молодежи в Украине. Обосновано авторское видение особенностей осуществления процессов политической социализации молодежи. Уделено значительное внимание критическому анализу различных научных взглядов относительно средств и инструментов политической социализации молодежи, в частности рассмотрена роль Интернета как современного средства коммуникаций для активного и ускоренного включения молодежи в политическую жизнь. Проведен анализ результатов социологического исследования по инклюзии украинской*

молодежи в политические процессы. Сделаны выводы относительно основных тенденций и специфики участия молодежи в политических процессах, выражается через организацию различных общественных организаций и движений.

***Ключевые слова**: молодежь, политика, политическая социализация, предпосылки политической активности, общественные организации, общественные движения.*

Постановка проблеми. Політична соціалізація молоді в процесі розвитку українського суспільства є важливою складовою реформування соціальної системи у напрямку забезпечення демократичних засад громадянського суспільства та формування інформаційної культури. Зважаючи на багатоаспектність та різновекторність досліджуваної проблематики нині досить актуальним є визначення передумов, принципів та особливостей включення української молоді до політичного життя країни. Це є дуже важливим з огляду на проблематику формування сучасних політичних еліт, які є базисом для майбутнього соціально-економічного розвитку держави та формування сучасного інформаційного суспільства.

Дослідженнями питань політичної соціалізації молоді займалися такі науковці як Акименко І.М. [1], Береза В.О. [2], Білецька Т. [3], Воронкова А.І. [4], Козьма В.В. [5], Ніколаєнко Н.О. [7], Цивін М.Н., Матвієнко О.В. [8] та ін. Праці наведених авторів містять обґрунтування теоретичних засад та практичної специфіки процесів участі української молоді у політичному житті. Проте, подальшого розвитку потребують питання, які стосуються основних передумов та принципів політичної соціалізації молоді на тлі сучасних політико-економічних перетворень в Україні.

Метою статті є визначення особливостей політичної соціалізації молоді в умовах формування сучасного інформаційного суспільства.

Виклад основного матеріалу. Політична соціалізація в сучасних умовах виступає доволі поширеним суспільним феноменом, що характеризується високою зацікавленістю з боку фахівців у сфері політичної психології, політології, соціології, тощо. Дослідження підходів різних авторів щодо вивчення цього питання дає можливість ідентифікувати політичну соціалізацію здебільшого з точки зору політико-правових процесів.

Ніколаєнко Н.О. та Годован Ю.В. відзначають, що дослідження феномену політичної соціалізації здійснюється у різних площинах науково-методичних підходів. Зокрема, вони звертають увагу на різні сфери дослідження політичної соціалізації молоді: соціально-політичний (характеризує фактори освітнього розвитку особистості), розвиток політичних здібностей особистості під впливом різних політичних інститутів, забезпечення національної автентичності у процесі реформування політичного устрою країни [7].

Цивін М.Н. та Матвієнко О.В. відзначають, що агентами соціалізації для молоді є засоби масової комунікації та міжособистісні контакти (сім'я, друзі, викладачі, стихійні контакти), які можуть вносити у соціалізацію особистості як спрямовані, так і стихійні імпульси. При цьому на думку авторів, провідну роль у процесі соціалізації молоді у сучасних умовах безперечно відіграють засоби масової комунікації, а у міжособистісних контактах (зокрема, стосовно студентської молоді) важливим чинником є трансляція з боку викладачів власних суспільно-політичних цінностей, установок, уподобань та міркувань, часто діаметрально протилежних залежно від політичних і наукових поглядів, позиції, ангажованості, національної та ідеологічної приналежності, вигоди, віку або інших чинників [8].

На наш погляд, засоби комунікацій хоча і є важливим інструментом системи політичного життя, однак значною мірою на процеси політичної соціалізації молоді

впливають також інші чинники: освіта, культура, система життєвих цінностей, правова система країни. У наведеному аспекті слушну думку наводить Воронкова А.І., яка стверджує, що політична соціалізація молоді є процесом, який базується на принципах системності, тобто зміни у будь-якій її складовій (від суб'єкта організації до одного із факторів впливу на процес її здійснення) викликають трансформацію в інших елементах, які становлять її цілісність [4]. Авторка апелює до певних постулатів, які, на її погляд, складають теоретичний базис сучасних концепцій політичної соціалізації. Основні ознаки політичної соціалізації молоді, виділені Воронковою А.І., наведено на Рис. 1 [4].

Як відзначає Воронкова А.І., процес політичної соціалізації молоді передбачає одночасне існування: цілеспрямованого впливу на індивіда з боку пануючої політико-ідеологічної системи (через різноманітні політичні інститути та процеси); стихійного (так званого "позасистемного") впливу на індивіда з боку інших систем (через різні неполітичні структури та чинники); певного рівня впливу з боку самого індивіда на оточуючий його політичний світ (через різні види соціальної активності) з метою його опанування; взаємодія особистості з політичною системою здійснюється в контексті виникнення двох процесів, кожен із яких постійно доповнює інший: а) один із цих процесів – процес самовідтворення політичної системи завдяки механізму рекрутування, збереження та передачі своїх політичних цінностей, цілей і традицій новому члену суспільства; б) другий – процес перетворення особистості в громадянина через формування її політичної свідомості та політичної поведінки в контексті функціонування певних вимог існуючої політичної системи (її цінностей, норм, правил і зразків поведінки) [4].

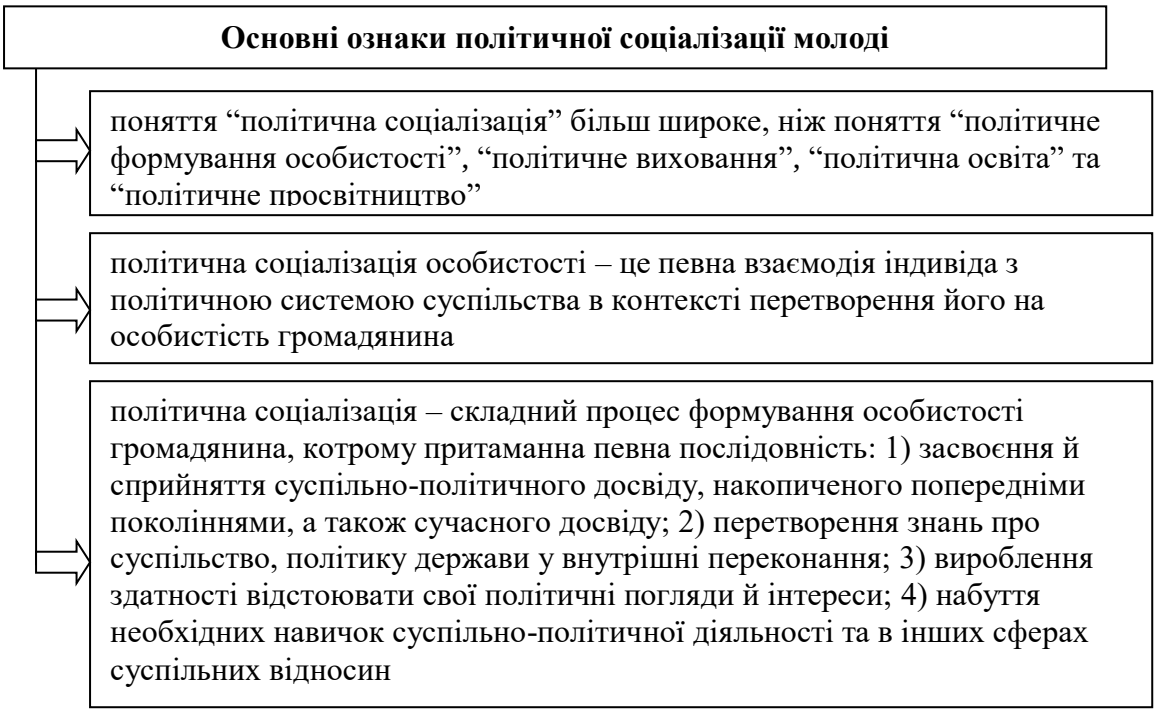

Рис. 1. Основні ознаки політичної соціалізації молоді [4].

Визначаючи сучасні аспекти соціалізації молоді у політичному житті, Акименко І.М. проводить аналіз політичного процесу та робить висновки про те, що українське сучасне суспільство пройшло шлях від монолітної політичної культури до плюралістичної, але ще не достатньо, тому як потрібно сформувати відчуття культурно-історичної єдності [1]. На думку автора, структурні елементи політичної культури, цінності, навички, орієнтації,

методи й прийоми політичної діяльності в Україні були оновлені через проведення реформ. Суспільство поступово звикло до політичного плюралізму, багатоманітності підходів до розв'язання нагальних проблем, відкритого висловлення свого ставлення до політичних і державних інститутів. Втім, стара тоталітарна політична культура, трансформуючись у нову систему цінностей, дає про себе знати у вигляді формального, відчуженого ставлення до офіційних норм, цінностей, традицій, поведінки. Типовими явищами є політична індиферентність громадян, соціальна апатія, рецидиви конфронтаційного мислення, ерозія моральних цінностей та ідеалів, дискредитація принципів демократії, деструктивна діяльність певних соціальних груп [1].

Доповнюючи вищесказане, Козьма В.В. звертає увагу на те, що відсутність конкурентної боротьби між механізмами політичної соціалізації створила сприятливі умови для того, щоб панівні позиції в боротьбі за "політичні умонастрої" українців зайняли різноманітні ЗМІ. На думку автора, для сучасної політичної науки осмислення феномену маніпулювання має важливе значення, оскільки дає змогу вести мову не просто про технології протидії маніпуляціям, а піднімати питання про державну політику інформаційної безпеки, а це, у свою чергу, дає можливість знову наголосити на важливості поширення базових політичних знань на ранніх етапах соціалізації індивіда [5].

Зважаючи на специфіку становлення сучасного українського суспільства, також варто зважати на такий важливий чинник політичної соціалізації молоді, як політична культура. Як відзначає Береза В.О., в результаті політичної соціалізації через формування політичної свідомості особистості, що включає політичні цінності, орієнтації, установки, норми, та засвоєння й наступного відтворення зразків політичної поведінки відбувається відтворення політичної культури [2].

На думку Білецької Т., особливу роль в процесах політичної соціалізації відіграють, як уже зазначалося нами вище, ЗМІ, а в останнє десятиріччя суттєву конкуренцію їм складає Інтернет [3]. Авторка вважає, що саме ці канали на сьогодні є ключовими в цих процесах, адже виступають головними джерелами інформації серед молоді, формують її політичні уподобання та пріоритети. Політичний вплив і маніпулювання з боку ЗМІ на громадян сьогодні, не піддаються сумніву і здійснюються як на індивідуальному, так і груповому, соціальному рівнях. При цьому Білецька Т. зауважує, що маніпулювання як засіб впливу на поведінку людей має низку переваг: воно здійснюється непомітно, не вимагає значної кількості матеріальних затрат для реалізації. Основними його прийомами є формування у масовій свідомості соціально-політичних міфів; підтасовування фактів, замовчування, дозування інформації, поширення неправдивих матеріалів [3].

Доповнюючи наведену вище думку, Ніколаєнко Н.О. та Годован Ю.В. головним недоліком "Інтернет-плюралізму" визначають анонімність і часто повну безвідповідальність. Інтернет відповідає основним вимогам інформаційного суспільства, але як тільки ми живемо в цифровому світі, ми не бачимо головного – неможливості бути політично активною в реальному житті, виражати це усно і не по відношенню до реального опонента, а не практично аргументувати невербальну комунікацію. ЗМІ часто є серед інноваційних інститутів політичної соціалізації. Незважаючи на те, що вони є формою комунікації як формою передачі інформації, засоби масової інформації розглядаються як засіб політичної соціалізації порівняно короткий час. ЗМІ є важливим інститутом політичної системи. Вони є установами, які були створені для публічної передачі різних інформаційних компонентів за допомогою спеціальних технологічних інструментів [7]. Під дією технологічних факторів в Україні формується конфліктний та кон'юнктурний типи політичної соціалізації. Безперечно, всі ці особливості політичної

соціалізації молоді є визначальними у відносно “спокійні” періоди суспільного розвитку. Утім, у періоди суспільно-політичних криз зростає політична активність молоді [8].

До основних компонентів процесу політичної соціалізації молоді в Україні часто відносять засоби масової інформації. Незважаючи на те, що вони як форма передачі інформації та забезпечення безперервних комунікацій у соціумі функціонують досить тривалий час, у якості інструменту політичної соціалізації ЗМІ почали розглядатися відносно недавно. Засоби масової інформації є важливим інститутом політичної системи. Вони передбачають собою установи, створені для публічної передачі різноманітних інформаційних компонентів за допомогою спеціального технологічного інструментарію [7].

Узагальнюючи наведені вище наукові погляди, було визначено ряд передумов, які впливають на специфіку процесів політичної соціалізації молоді в сучасному українському суспільстві (Рис. 2).

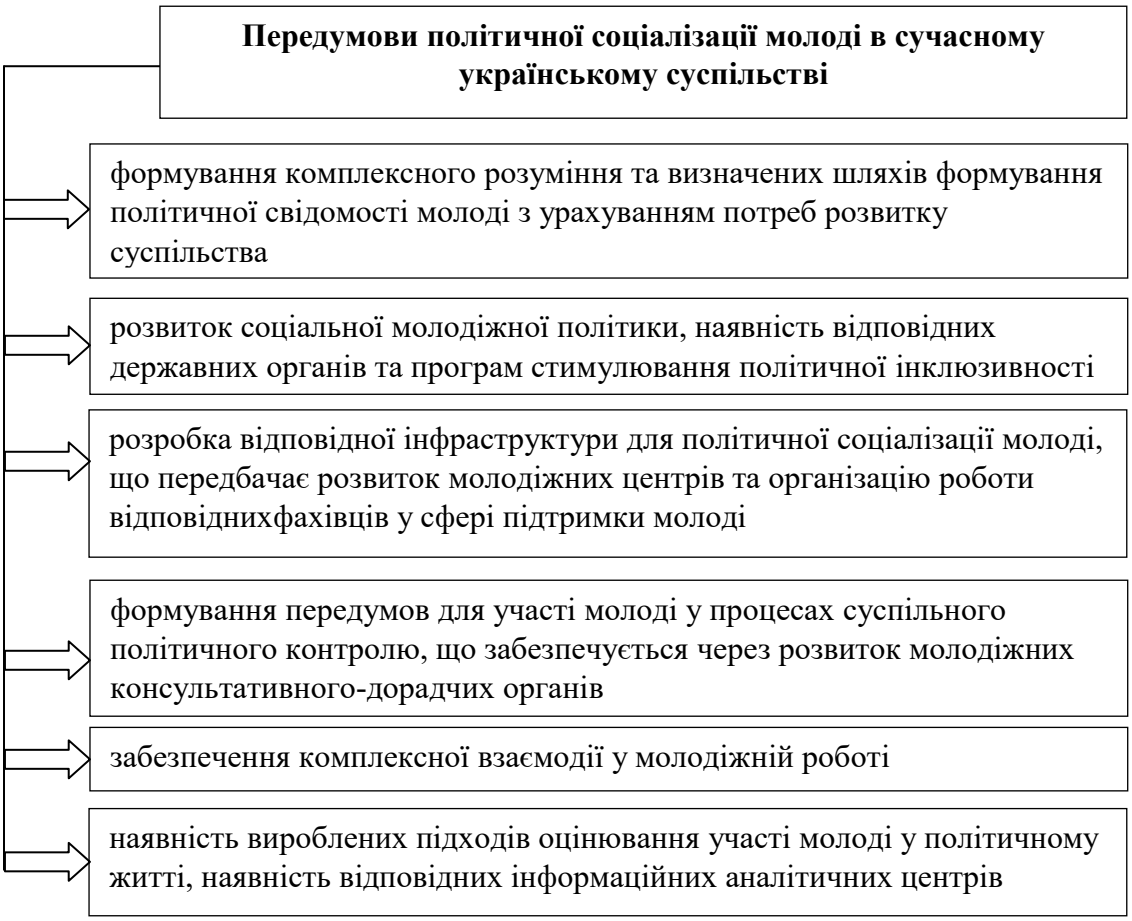

Рис. 2. Передумови політичної соціалізації молоді
в сучасному українському суспільстві

Дослідження особливостей політичної соціалізації молоді в сучасному українському суспільстві передбачає наявність двох основних протиріч, які його супроводжують: з одного боку, існує нагальна суспільна потреба в політичному розвитку особистості, а з іншого – наявною є тенденція відчуження молодих людей від політичних інститутів та агентів соціалізації; з’явились якісно нові соціально-політичні структури та відносини, що, з одного боку, створюють основу для вибору різних форм і напрямків соціальної активності молоді, а з іншого – у основної частини молодих людей

відсутній досвід засвоєння нових підходів та орієнтації в політичній діяльності, що зумовлений низьким рівнем політичної культури [1].

Основні принципи політичної соціалізації молоді в сучасному українському суспільстві узагальнено на Рис. 3. До них варто відносити обґрунтованість, відповідність та молодіжну активність. Державна молодіжна політика обов'язково має враховувати наведені принципи.

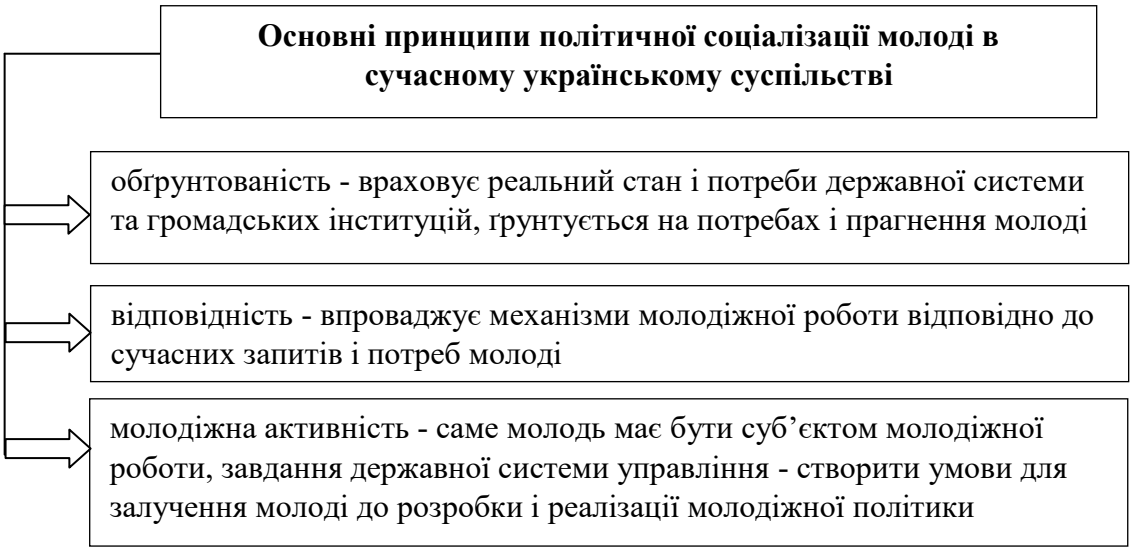

Рис. 3. Основні принципи системи молодіжної роботи [6].

Важливо також навести деякі дані проведених соціологічних досліджень, що характеризують тенденції та процеси політичної соціалізації молоді. За даними соціологічних досліджень, упродовж років незалежності України, починаючи з 1996 до 2017 року, їхнє членство є доволі низьким, на рівні 1 – 5 % [6] (див. Табл. 1).

Таблиця 1.

Частка молодих людей віком від 18 до 35 років, які заявляють, що вони є активними членами організацій громадянського суспільства, % (за даними соціологічного дослідження GFK-Ukraine [6]).

Види організацій	Роки проведення досліджень		
	2000	2006	2017
Усі організації громадянського суспільства	11,0	22,3	21,5
у тому числі:			
релігійні або церковні організації	2,1	5,8	4,6
спортивні організації або організації, пов'язані з проведенням дозвілля	3,1	8,8	8,3
організації, пов'язані з освітою, мистецтвом, музикою	2,3	4,7	8,3
профспілки	2,2	5,2	3,7
політичні партії	0,8	2,3	1,6
організації з охорони навколишнього середовища	0,6	0,9	1,4
професійні об'єднання	0,5	1,6	3,0
благодійні або гуманітарні організації	0,1	1,9	1,7

організації споживачів	-	0,6	1,0
групи самодопомоги, взаємодопомоги	-	-	1,4
Інші організації	0,5	1,0	1,8

Варто наголосити, що на сьогодні однією з цілей реформування державної молодіжної політики в Україні є розбудова громадянського суспільства за активної участі молоді, підвищення рівня залучення молоді до громадського життя до середньоєвропейського рівня (25 %). Саме в складних соціально-економічних умовах необхідним є безумовне виконання головних принципів молодіжної політики, задекларованих у законодавстві та програмних документах, основний зміст яких полягає в ставленні до молоді передусім як до суб'єкта, а не лише до об'єкта цієї політики. Однак, з іншого боку, не можна забувати й про те, що молодь вимагає пильної уваги суспільства та довгострокових інвестицій, без яких її потенційні можливості ніколи не розкриються [6].

З числа опитаних представників української молоді 54 % брали участь щонайменше в одній з громадських ініціатив (значущої різниці між чоловіками і жінками не спостерігається). Ще 88 % з числа респондентів виокремили щонайменше одну з ініціатив, в яких вони участі не брали, але були б зацікавлені взяти (Рис. 4) [6].

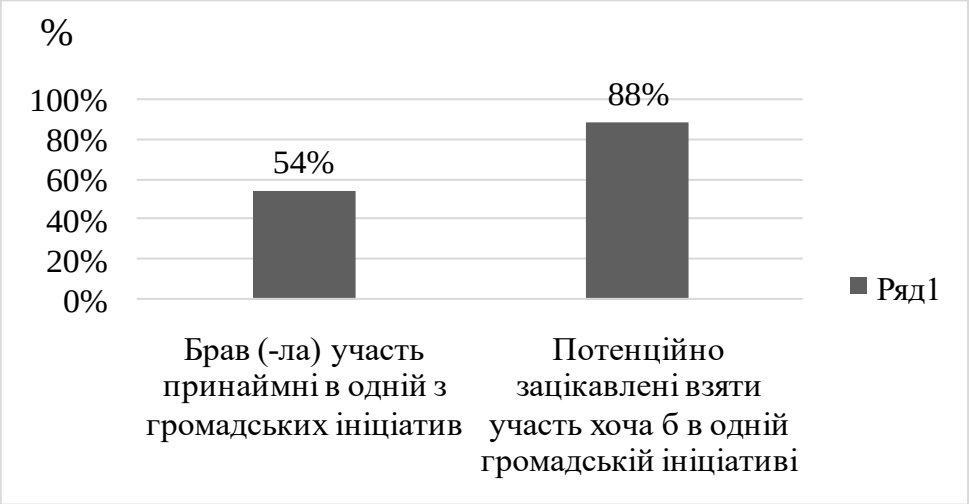

Рис. 4. Розподіл респондентів, які брали участь принаймні в одній з перелічених ініціатив або зацікавлені взяти участь принаймні в одній з наведених ініціатив (серед усіх респондентів) – за даними соціологічного дослідження GFK-Ukraine [6].

Найбільша кількість респондентів, які брали участь принаймні в одній з громадських ініціатив, живе у Черкаській (80 %), Київській (78 %) та Вінницькій (77 %) областях. Найменша кількість тих, хто брав участь принаймні у одній з громадських ініціатив, у Чернігівській області – 36 % [6].

62 % опитаних представників української молоді не брали участі в діяльності жодної організації громадянського суспільства впродовж останніх 12 місяців. 13 % брали участь у діяльності волонтерських ініціатив, 11 % – у діяльності благодійних або гуманітарних організацій, 10 % у діяльності спортивних організацій або організацій, які пов'язані з проведенням дозвілля (рис. 5) [6].

Понад третину опитаних – 35 % представників української молоді не знають про існування в Україні молодіжних громадських організацій та їх діяльність (Рис. 5).

Ще 34 % опитаних знають тільки про те, що такі організації існують. 21 % знають про діяльність молодіжних організацій із ЗМІ, але не відвідують відповідних заходів.

7 % представників української молоді іноді відвідують заходи молодіжних організацій і 2 % є членами таких організацій.

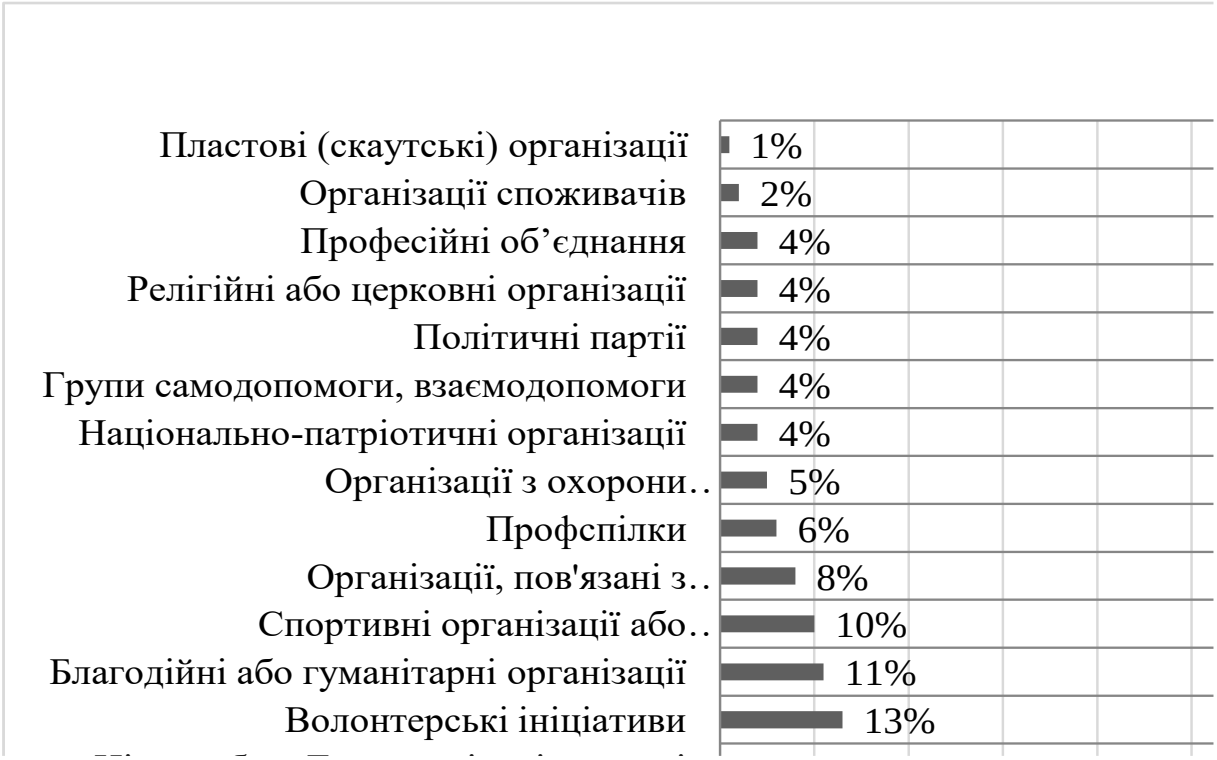

Рис. 5. Розподіл відповідей на запитання: "У діяльності яких організацій громадянського суспільства Ви брали участь за останні 12 місяців? " (серед усіх респондентів) – за даними соціологічного дослідження GFK-Ukraine [6].

Таким чином, молодіжна спільнота має змогу проводити комунікацію з іншими спільнотами, не будучи їх членами в реальному житті. Свобода зібрання стає нормою життя, важливим елементом соціуму і однією з найважливіших свобод. В даному випадку мережа виконує мобілізуючу функцію, яка сприяє об'єднанню громадян для вирішення тих чи інших проблем. Перебуваючи на етапі трансформації сучасне суспільство сьогодні процес формування політичної культури охоплює всі сфери суспільного життя, зумовлює необхідність відповідної політичної культури, від якої насамперед залежать і характер і напрями суспільного процесу.

Висновки.

1. Результати аналізу підходів та особливостей процесу політичної соціалізації молоді в Україні дозволяють виділити ряд передумов політичної соціалізації молоді в сучасному українському суспільстві, а саме: формування комплексного розуміння та визначених шляхів формування політичної свідомості молоді з урахуванням потреб розвитку інформаційного суспільства; розвиток соціальної молодіжної політики, наявність відповідних державних органів та програм стимулювання політичної інклюзивності молоді; розробка відповідної інфраструктури для політичної соціалізації молоді, що передбачає розвиток молодіжних центрів та організацію роботи відповідних фахівців у сфері підтримки молоді; формування передумов для участі молоді у процесах суспільного політичного контролю, що забезпечується через розвиток молодіжних консультативно-дорадчих органів, тощо.

2. До основних складових політичної соціалізації української молоді часто відносять засоби масової інформації. Незважаючи на те, що вони, як форма передачі інформації та забезпечення безперервних комунікацій у соціумі функціонують досить

тривалий час, у якості інструменту політичної соціалізації ЗМІ почали розглядатися відносно недавно. В інформаційному суспільстві засоби масової інформації є важливим інструментом для формування сучасної політичної системи.

3. В сучасному інформаційному суспільстві на процеси політичної соціалізації молоді, крім засобів комунікації, впливають також інші чинники: освіта, культура, система життєвих цінностей, правова система країни тощо.

Вважаємо, що результати цієї роботи можуть бути використані у подальших наукових розробках з окресленої проблематики, а також розглядатися як практичне підґрунтя для формування державної молодіжної політики в Україні.

Використана література

1. Акименко І.М. Політична соціалізація людини в сучасному середовищі. *Актуальні проблеми психології.* 2019. № 47. С. 9-18.

2. Береза В.О. Значення політичної культури суспільства у процесі політичної соціалізації індивіда. *Гуманітарний вісник ЗДІА*. 2016. № 66. С. 36-44.

3. Білецька Т. Соціально-психологічні чинники політичної соціалізації сучасної української молоді. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія "Психологічні науки"*. 2019. № 3. С. 32-47.

4. Воронкова А.І. Мода і політична соціалізація у сучасному суспільстві: основні напрями взаємодії. *Сучасне суспільство*. 2019. № 1. С. 39-50.

5. Козьма В.В. Первинні механізми політичної соціалізації особистості. *Вісник НАДУ при Президентові України. Серія "Політичні науки"*. 2016. № 2. С. 75-79.

6. Молодь України – 2017 / Результати соціологічного дослідження. Тернопіль: ТОВ "Терног раф", 2017. 72 с.

7. Ніколаєнко Н.О. Інноваційні інститути політичної соціалізації молоді в Україні. *Вісник Донецького національного університету. Серія "Політичні науки"*. 2016. № 1. С. 111-115.

8. Цивін М. Н., Матвієнко О. В. Соціалізація молоді у періоди суспільно-політичних криз. *Вісник Національної академії керівних кадрів культури і мистецтв*. 2015. № 1. С. 210-214.

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

До відома читачів

Шановні читачі !

28 серпня 2020 р. у м. Полтава відбулися засідання президії та щорічні загальні збори Національної академії правових наук України, на яких було розглянуто важливі питання її життєдіяльності – підбиття підсумків роботи в 2019 році, вирішення ряду організаційно-кадрових питань та окреслення основних завдань на 2021 рік, а також вибори дійсних членів (академіків) та членів-кореспондентів НАПрН України.

Вибори нових членів Академії проходили у повній відповідності до Закону України "Про наукову і науково-технічну діяльність" та чинного законодавства.

За результатами відкритого голосування було обрано 3 дійсних членів (академіків), а за результатами таємного голосування – 18 членів-кореспондентів, серед яких, по відділенню державно-правових наук і міжнародного права, дійсним членом (академіком) НАПрН України обрано директора Науково-дослідного інституту інформатики і права Національної академії правових наук України **Пилипчука Володимира Григоровича**, членом-кореспондентом – **Буханевича Олександра Миколайовича**.

URL: http://www.aprnu.kharkiv.org/news/news-31_08_2020.html

До відома авторів

"**ІНФОРМАЦІЯ І ПРАВО**" – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   – *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   – *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   – *відстань між рядками – 1 інтервал;*
   – *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов'язкові структурні елементи:

   • УДК.

   • Ім'я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.

   • Назва статті (укр. та англ. мовами).

   • Анотація та ключові слова (укр., англ. та рос. мовами).

   • **Розв'язання проблеми,** шляхом наукового вирішення завдання:

   ➢ **постановка проблеми** *(загальна характеристика);*

   ➢ **результати аналізу наукових публікацій** – надаються відомості про стан вирішення проблеми та ПІБ авторів, з обов'язковим посиланням на їхні роботи (в […]), повний опис бібліографії яких вказується в підрозділі "Використана література"; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;

   ➢ **формування мети** *(постановка завдання)* статті;

   ➢ **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.

   • **Висновки** за результатами розв'язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.

   • **Використана література.** Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання" або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.

   • Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- ***Актуальність теми***.
- ***Новизна та обґрунтованість одержаних результатів***.
- ***Наукова (практична) цінність результатів***.
- ***Висновок про можливість відкритої публікації***.

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України "Про затвердження порядку формування переліку наукових фахових видань України" від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов'язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту**.

Реквізити для оплати робіт:
Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада 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(34)/2020

Засновники журналу:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІІП НАПрН України); - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини "Україна".
Видавець:	© НДІІП НАПрН України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Тел.: 234-94-56; e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	URL: //www.ippi.org.ua – НДІІП НАПрН України; URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.

Founders of journal:	- Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine (SRIIL of the NALS of Ukraine); - Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine; - Open International University of Human Development "Ukraine"
Publisher:	© SRIIL of the NALS of Ukraine.
Address of release:	01032, Kyiv, Saksaganskogo str., 110-V. Scientific Rresearch Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine. Phone: 234-94-56; e-mail: bvm777@ ukr.net
Web-pages of journal in the network Internet:	URL: //www.ippi.org.ua – Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine; URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.